

# The Journal of Physical Security

## Volume 7(1), 2014

### THIS ISSUE...

Editor's Comments

SK McNeill, "Analysis of Explosive Magazine Padlock Breaching Techniques"

HA Udem, "Nuclear Containment and Surveillance Terminology"

P Kurrasch, "Money in a Glass Box"

RG Johnston and JS Warner, "Vulnerability Assessment Myths (Or What Makes Red Teamers See Red)"

RG Johnston and JS Warner, "What Vulnerability Assessors Know That You Should, Too"

B Nussbaum, "The 'Levels of Analysis' Problem with Critical Infrastructure Risk"

HS Mack, "Countering Violent Extremism in the United States: Law Enforcement's Approach to Preventing Terrorism through Community Partnerships"

JPS



## **Table of Contents**

### ***Journal of Physical Security, Volume 7(1), 2014***

Editor's Comments, pages i-viii

Paper 1 - SK McNeill, "Analysis of Explosive Magazine Padlock Breaching Techniques", pages 1-21

Paper 2 - HA Udem, "Nuclear Containment and Surveillance Terminology", pages 22-24

Paper 3 - P Kurrasch, "Money in a Glass Box", pages 25-30

Paper 4 - RG Johnston and JS Warner, "Vulnerability Assessment Myths (Or What Makes Red Teamers See Red)", pages 31-38

Paper 5 - RG Johnston and JS Warner, "What Vulnerability Assessors Know That You Should, Too", pages 39-42

Paper 6 - B Nussbaum, "The 'Levels of Analysis' Problem with Critical Infrastructure Risk", pages 43-50

Paper 7 - HS Mack, "Countering Violent Extremism in the United States: Law Enforcement's Approach to Preventing Terrorism through Community Partnerships", pages 51-56

## Editor's Comments

Welcome to volume 7, issue 1 of the Journal of Physical Security. This issue has 7 papers on the following topics: testing locks, seals and nuclear safeguards, a security thought experiment, vulnerability assessment issues, the levels of critical infrastructure risk, and community partnerships for counteracting radicalization. Volume 7, issue 2 should also be out shortly.

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.

\*\*\*\*\*

## Two Person Rule

With a two-person rule, there must be (at least) 2 persons involved in critical functions, from nuclear safeguards to check writing. Presumably this is good for security, though we don't really know; there has been remarkably little research on the topic. Moreover, in many organizations (including inside nuclear facilities), the instructions and protocols regarding two-person rules are vague, non-existent, or less than carefully thought through.

Maybe the two-person rule is not automatically a good countermeasure. Scott S. Wiltermuth, Ph.D. from USC has conducted research suggesting that a person is more likely to cheat when the benefits are split with another person. This makes the cheating seem less unethical to the perpetrator. The research wasn't specifically about two-person rules, but the possible implications are clear.

For details, see SS Wiltermuth, "Cheating More When the Spoils are Split", *Organizational Behavior and Human Decision Processes*, 115(2), 157-168 (2011).

\*\*\*\*\*

## Arresting Developments

A new study reported in the peer-reviewed journal *Crime & Delinquency* finds that by age 23, 49% of black males, 44% of Hispanic males, and 38% of white males have been arrested at least once. The corresponding figures for females at age 23 are 20%, 18%, and 16%, respectively. For more information, see [http://www.eurekalert.org/pub\\_releases/2014-01/uosc-sho010314.php](http://www.eurekalert.org/pub_releases/2014-01/uosc-sho010314.php)

\*\*\*\*\*

## **Kenneth, What is the Frequency?**

On October 4, 1986, CBS News Anchorman Dan Rather was walking along Park Avenue in Manhattan when he was physically assaulted by two men, one of whom repeatedly yelled at Rather, “Kenneth, What is the Frequency?”

Rather was relatively unharmed, though shaken. The case was unsolved for a number of years, and the incident became popular folklore. The phrase “What’s the frequency, Kenneth?” became slang for a disturbed or clueless person. It was used as the title of two songs by Game Theory in 1987 and R.E.M. in 1994. Rather was a good sport about the incident, and even sang the song with R.E.M. during a sound check prior to a concert at Madison Square Garden. A tape of Rather’s singing was shown on the *Late Show with David Letterman*.

One of the likely assailants was identified in 1997, but his motivations were still a mystery. In 2001, *Harper’s Magazine* speculated that there was some connection to postmodern fiction writer Donald Barthelme who used the phrase, “What is the frequency?” in his writing, had a recurring character named Kenneth, and once wrote a short story about a pompous editor named Lather. Barthelme (who died in 1989) and Rather may have know each other early in their careers.

The moral of the story for security: always know the frequency! (Especially with the NSA listening.)

\*\*\*\*\*

## **Keeping Your Eye on the Ball (or T-Shirt)**

It’s reassuring to know that the National Security Agency (NSA) and the Department of Homeland Security (DHS) are staying focused on America’s true enemies.

The *Washington Times* reports that NSA and DHS have issued “cease and desist” letters to a novelty store owner in Minnesota who sells products that make fun of NSA and DHS. (See <http://www.washingtontimes.com/news/2013/nov/3/nsa-dhs-issue-cease-and-desist-letters-novelty-sto/>) He sells, among other things, a T-shirt with the official NSA seal that reads, “The NSA: The only part of the government that actually listens.”

Federal officials claim the parody use of NSA and DHS official seals, “violate laws against misuse, mutilation, alternation, or impersonation of government seals.” The store owner has taken legal action against the federal government, claiming violations of his First Amendment Rights.

\*\*\*\*\*



## Homeland Security?

Average number of American deaths annually by various causes (approximate).

<b>Cause of Death</b>	<b>Deaths/Year</b>
smoking, including 2 <sup>nd</sup> hand smoke	440,000
drug overdose (accidental & deliberate)	38,000
car accidents & drunk driving	32,000
guns (intentional homicides & suicides)	32,000
alcohol abuse, excluding accidents & homicides	26,000
texting while driving	6,000
food poisoning	5,200
war (since 1775)	4,900
guns (accidental shootings)	650
falling out of bed	450
space heaters	300
heat stroke	175
(mostly accidental) overdosing on acetaminophen, the active ingredient in Tylenol	150
deer (including car accidents)	130
bee stings (including allergic reactions)	100
tornados	60
lightning	50
<b>terrorism 1900 to present, including 9/11</b>	<b>(arguably*) 33</b>
<b>terrorism, 1900 to just before 9/11</b>	<b>(arguably*) 6</b>
<b>terrorism, post 9/11 to present</b>	<b>(arguably*) 5</b>
malaria (from foreign travel)	6
trying to deep fat fry a turkey	5
roller coasters	4
shaking a vending machine until it falls	3
bear attack	1
shark attack	1

\* It's not always clear when an attack is terrorism, but most people would agree with these figures to within a factor of 2.

Average annual U.S. expenditure on homeland security since 9/11: \$58 billion to \$250 billion depending on what war/drone spending you choose to include, if any. Annual anti-smoking expenditures: ~\$100 million.

Thus, about 120 *million* times more money per death is spent on homeland security than for anti-smoking campaigns! Anti-smoking efforts are generally believed to regularly save tens of thousands of lives each year.

\*\*\*\*\*

## NSA Phone Data and Security by Obscurity

An independent review board has concluded that the National Security Agency's collection of phone metadata on Americans is illegal and needs to stop. The Privacy and Civil Liberties Oversight Board (PCLOB) found that the program raises serious threats to civil liberties, has been of little use in fighting terrorism, and lacks a solid basis in law or policy. Conclusions were not unanimous. For more information, see [http://www.washingtonpost.com/world/national-security/independent-review-board-says-nsa-phone-data-program-is-illegal-and-should-end/2014/01/22/4cebd470-83dd-11e3-bbe5-6a2a3141e3a9\\_story.html](http://www.washingtonpost.com/world/national-security/independent-review-board-says-nsa-phone-data-program-is-illegal-and-should-end/2014/01/22/4cebd470-83dd-11e3-bbe5-6a2a3141e3a9_story.html)

Reasonable people can disagree, but I find 2 things particularly disturbing about this issue. The first is that apparently no serious review of liberty/privacy/4<sup>th</sup> Amendment issues occurred until after information about the program was publicly leaked by Edward Snowden. How can this be? Capturing phone metadata is clearly a kind of "search and seizure" that the 4<sup>th</sup> Amendment addresses. Whether the program has merit or not, it clearly deserved greater scrutiny. For reference, here is the text of the 4<sup>th</sup> Amendment to the United States Constitution:

*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

Telling, the amendment does not have a clause saying, "...unless there is some perceived security benefit".

The second disturbing aspect is that federal government claims that collecting metadata had to be kept secret. But "Security by Obscurity" doesn't really work, at least long term. Individuals and organizations can't keep secrets, as Snowden (and Bradley Manning) have demonstrated. Moreover, while it is somewhat counter-intuitive, security actually works best when it is transparent. This allows for review, criticism, improvements, and accountability—things that seem to have gone lacking prior to Snowden's actions.

Now it may be that the brain-dead losers that the government likes to entrap with phony terrorist "plots" can't figure it out. But surely any terrorist that is a legitimate threat just assumes that the U.S. government is eavesdropping on his phone calls and email, not just gathering metadata. Bin Laden, for example, stayed off phones and the Internet entirely, and he was in Afghanistan and Pakistan where the U.S. has challenges in setting up communication infrastructure.

Note that it is quite illegal to classify something simply because it is embarrassing, politically controversial, or because you want to avoid scrutiny. As far as I know, however, nobody has ever been prosecuted for doing this.

\*\*\*\*\*

## **Due Diligence Overdue?**

In an eye-opening precedent, the U.S. Federal Trade Commission (FTC) filed a complaint against security camera manufacturer TrendNet. Hackers accessed TrendNet's web site in 2012 and gained access to hundreds of live wireless video feeds (including scenes in private homes), which they posted on the Internet. The FTC accused the company of failing to take reasonable security measures. TrendNet reportedly stored and transmitted user login credentials in open plaintext, even though free software was available to secure the information.

Under terms of a settlement announced in September, TrendNet agrees not to claim its products are "secure". Moreover, TrendNet will get an independent assessment of its security once a year for 20 years. (It's pretty bad when the government has to force you to do what should be obvious.)

The question now is, will the FTC start coming after numerous other companies that promise but don't delivery real security? If so, they are going to need to hire a lot more staff!

\*\*\*\*\*

## **Is Your Security in the Toilet?**

The luxury Satis toilet (\$5,686) is meant to be controlled by a smartphone. Functions such as lid opening/closing, automatic flushing, bidet spray, air spray, music playing, and fragrance release can all be instigated via an Android app called "My Satis".

The app talks to the toilet over Bluetooth. Unfortunately, the PIN for every toilet is hardwired to 0000 and cannot be reset. As a result, anybody with an Android phone and the app can take control of the toilet, hassling the current user or even causing repeatedly flushing to waste water. See <http://www.bbc.co.uk/news/technology-23575249>

While this vulnerability falls short of one that Al-Qaeda might want to exploit, it does highlight the fact that manufacturers are going to need to think more carefully about security for their wireless devices. This has already become a much more serious matter for wireless medical devices.

\*\*\*\*\*

## **Music Piracy, or Cruel and Unusual Punishment**

I guess you could call it fighting off pirates with Spears. A new weapon has emerged in the fight against Somali pirates: Britney Spears. It seems ships at risk from Somali pirates



have been blasting the singer's pop songs at very high volumes towards approaching pirates. The pirates hate Western music and culture, and tend to veer off. According to one ship's officer, "It's so effective the ship's security rarely needs to resort to firing guns." Britney's song, "Oops! I Did it Again" seems to be particularly effective.

Music has, in fact, often been used as a weapon. See, for example, <http://www.nbcnews.com/entertainment/britney-spears-music-used-drive-away-somali-pirates-8C11488068>

\*\*\*\*\*

### **New Security Threat**

The *Oregonian* reports that Sirgiorgiro Clardy, an inmate at the Eastern Oregon Correctional Institution has filed a \$100 million lawsuit against Nike (the sporting goods and shoe manufacturer), alleging that Nike failed to provide a warning label on his Air Jordan shoes that they could be a dangerous weapon.

Mr. Clardy, a professional pimp, is serving a 100-year sentence for (among other things) severely stomping on the face of one of his customers while wearing Air Jordans. Clardy is asking the court to require Nike to affix warning labels on all of its "potentially dangerous Nike and Jordan merchandise".

\*\*\*\*\*

### **A Burglar with Brains?**

An Indiana man has been charged with stealing more than 60 jars of human brains in October from the [Indiana Medical History Museum](http://www.indianamuseum.org/) and trying to sell them on eBay. (<http://www.cnn.com/2014/01/03/us/indianapolis-stolen-brains-ebay/>) Buying or selling human organs is a felony under federal law, but what is even more serious is that it is against eBay rules.

\*\*\*\*\*

### **Not on Target?**

Target Corporation has received mixed (but many negative) reviews for its post data breach handling of the credit card data theft. For good advice on how to prepare for, and how to handle, a crisis, scandal, or public relations disaster, read the excellent 2012 book, *Masters of Disaster: The Ten Commandments of Damage Control* by Christopher Lehane, Mark Fabiani, and Bill Guttentag. Much of what is in the book is little more than common sense. The problem with common sense, however, is that it is not all that common—especially in times of crisis when ego, denial, wishful thinking, organizational inertia, cover ups, and shock come into play.

\*\*\*\*\*

## More Problems at the FBI

In July, the National Employment Law Project (NELP) released a report on FBI criminal background checks for employment. (For more information, see [www.nelp.org/accurateFBIrecords](http://www.nelp.org/accurateFBIrecords)) The authors found that about 50% of the 17 million FBI background checks for employment and licensing purposes in 2012 were incomplete and/or inaccurate. NELP estimates that 600,000 workers (disproportionally minorities) may be prejudiced in their job searching because of faulty records. Often, the records fail to show that an arrest did not lead to a conviction. (Federal law mandates that the reports be complete and accurate.)

NELP blames both the states providing the raw data and the FBI—which is ultimately responsible—for problems with the background checks.

The FBI has quite a history of alleged screw ups, incompetence, scandals, and misconduct: the FBI Lab is known to have repeatedly falsified, altered, or suppressed evidence; FBI employees on the witness stand made false scientific claims that may have lead to the wrongful convictions of hundreds; there were multiple cases of forensics incompetence (including false terrorist accusations against Oregon lawyer Brandon Mayfield); Whitey Bulger allegedly successfully bribed local FBI agents; and FBI agents and former agents have been arrested in recent years for various types of misconduct including leaking classified information and federal child pornography violations. Then there is sexting by FBI employees on the job; hundreds of FBI employees allegedly cheating on exams; the botched Lee Harvey Oswald interrogation; the Wen Ho Lee debacle; the decades of inept efforts to find an alleged Soviet FBI mole named “Dick”; and the FBI ignoring warnings from its own agents that might have prevented 9/11.

And there’s more: According to a recent FBI internal report, from 2010 to 2012, the FBI disciplined over 1,000 employees for (often lurid) misdeeds. After 9/11, the FBI collected intelligence on Americans without the required court orders, and from 1950-1970+, the agency engaged in surveillance and harassment of civil rights groups, women’s organizations, and war protestors.

On the other hand, if you want to see one of the many things that the FBI does right, check out <http://www.fbi.gov/scams-safety/> for useful security and safety advice to the public.

\*\*\*\*\*

## Winning Hearts and Minds (and Eyes)

Speaking of lurid, it was pointed out to me (by someone who no doubt subscribes only for the scholarly articles) that a recent issue of *Playboy* had an interesting article by John Meroney entitled, “The Battle for Picasso’s Mind”. (For more information, see

<http://playboysfw.kinja.com/cia-operative-tom-braden-s-plot-to-topple-the-ussr-with-1457132402>)

The article describes the covert efforts of CIA agent Tom Braden to fight the Cold War by (imaginatively) winning hearts and minds in Europe—which was leaning towards communism and sympathy for the Soviet Union in the late 1940's. He did this by organizing modern art exhibits throughout Europe that convinced European intellectuals that the U.S. and the West were far more open to individual and artistic expression/freedom than the Soviets with their sterile, government approved "art".

As discussed in my previous 2010 Editor's Comments (<http://jps.anl.gov/v4iss1.shtml>), I find it unfortunate that the United States doesn't make a more concerted and competent effort to win the hearts and minds of people internationally, especially young people who are at risk for being seduced by terrorists and violent fundamentalists. Emphasizing what losers and sociopaths most terrorists are, and highlighting the benefits of tolerance and pluralism, might help to undercut the glamour and recruitment of terrorists. Braden's specific approach might not be relevant today, but his thinking-outside-the-box and the big-bang-he-got-for-the-buck are well worth emulating.

\*\*\*\*\*

## **Fire HR?**

Bernard Marr offers a provocative essay on LinkedIn entitled, "Why We No Longer Need HR Departments": <http://www.linkedin.com/today/post/article/20131118060732-64875646-why-we-no-longer-need-hr-departments>

It is well worth reading. In theory, the HR department can be a powerful tool to mitigate employee disgruntlement that can lead to insider attacks. In practice, however, many HR Departments simply make employee disgruntlement worse. HR's ability to contribute to organizational productivity and employee professional development is also often quite poor.

-- Roger Johnston  
Argonne National Laboratory  
January 2014



## **Analysis of Explosive Magazine Padlock Breaching Techniques**

S. Kevin McNeill

National Center for Explosives Training and Research

shonn.mcneill@atf.gov

### **Abstract**

A series of lock breaching tests are described in which five sets of standard shackle locks and 4 sets of puck style locks were tested for vulnerability to a Dremel rotary tool, an oxyacetylene torch, a drill press, a low temperature impact, and compressive cutting jaws. In the Dremel rotary tool test, the lock shackles were exposed to a Dremel abrasive cutting wheel for a fixed time and the depth of penetration was measured. In the oxyacetylene test, the lock shackle was moved under an oxyacetylene flame at a constant velocity and the depth of cut was measured. In the drill press test, the lock was confined in a vice and two drill attempts were made using two different diameter drill bits and the percent of lock failures was recorded. In the low temperature impact test, a pendulum was dropped while the lock temperature was lowered using difluoroethane (canned air) and the percent of lock failures was recorded. Finally, in the compressive cutting test, the lock shackle was pressed by carbide tipped cutting jaws and the maximum force at failure was measured. Results were compared to a previous study and were in general agreement, except the low temperature impact test.

### **1 Introduction**

Explosive magazine security is a key component of the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) mission to prevent the criminal misuse of explosives. These magazines contain numerous security features to prevent the theft of the explosives. The security features include hinges designed so that they cannot be removed from the outside, two padlocks at each door fastened in separate hasps and staples, locks with case hardened shackles with a minimum 3/8 inch diameter, and quarter-inch steel hoods covering the padlocks.[1, 2] While such measures make breaking into these magazines difficult, these systems are not infallible, and break-ins do occur.

From 2006 to 2010, the number of explosives thefts have dropped by approximately one-third.[3] However, given the potential threat of criminal or terrorist misuse of these explosives, ATF and the explosive industry are continuously evaluating potential improvements to magazine security. As recent as 2011, ATF approved a request by the industry to allow the use of hidden-shackle or puck locks, and approved the use of boron alloy steels in the shackle.[2] Additionally, ATF has recommended the use of locks that have an American Society of Testing and Materials (ASTM) grade of at least 5 for "forcing" and "surreptitious entry".[1,4] The explosive industry has also made strides to improve security. Austin Powder Company (APC) recently examined several types of padlocks and exposed them to various attack methods. Their objective was to determine what tool was used to defeat 8 MasterLock Series 6230 padlocks in 4 of APCs explosive magazines in Gainesville, GA. Their study focused on 4 puck-style locks and the MasterLock 6230, see figures 1.1a and 1.1b. Their results shown in Table 1 below indicate that the best

of the puck-style locks increase break-in time by almost 13 times as compared to the MasterLock 6230.[5]



Figure 1 - Photographs of typical puck and shackle-style locks. The American 2500 with shroud is on the left (puck style), and the Master Lock 6230 (shackle style) is on the right.

Table 1 - Austin Powder Company padlock test results.[5]

Lock	Dremel	Bolt Cutter	Drill Body	Drill Keyway	Low Temperature Impact
Master Lock 6230	2 min 45 sec	60 sec	NT <sup>1</sup>	NT	15 sec
Abloy PL975	NT	NT	5 min	NT	NT
American 2000	NT	NT	NT	14 min	NT
Master Lock 6270	NT	NT	NT	22 min	NT
American 2500	NT	NT	NT	35 min	Pass <sup>2</sup>

<sup>1</sup>NT: Not Tested

<sup>2</sup>"Pass" was defined as the lock not opening and the shackle not breaking.

With these results ATF turned to the National Center for Explosives Training and Research (NCETR,) to both verify and expand on APCs testing. NCETR expanded both the types of locks tested and the quantity of each type. The expansion in the types of locks tested was based on recommendations by the APC team. The expansion to 5 tests for each type of lock was done to better describe the spread in test data due to random uncertainties.[6] NCETR limited testing to physical attacks on the locks and chose not to address skilled attack methods such as bumping and shimmying as these are difficult to measure. NCETR also chose to develop test systems that more closely resemble vulnerability attacks rather than pure laboratory testing. This type of testing can produce more realistic evaluation results but makes the evaluation more dependent on the physical attributes of the test.[7]

## 2 Experimental Section

### 2.1 Dremel Test

#### 2.1.1 Dremel Cutting System

The Dremel test system is designed around a polyvinyl chloride (PVC) arm that rotates about a central axis. The arm holds a Dremel Model 4000 (110V) high-speed rotary tool on one end and a counter-balance on the other end, see figure 2.1. The counter-balance is weighted to maintain 0.18 kg (0.4 lb) at the abrasive cutting wheel

(Dremel Model 1.5-inch Metal EZ Lock). The arm measures 125.8 cm (49.5 in) in length and is made with two schedule 40 PVC sections, 5.08 cm (2 in) diameter section and a 2.54 cm (1 in) diameter section. Both sections measure 59.1 cm (23.25 in) in length. The two sections are joined with a 2 x 1 PVC reducing couple that measures 7.6 cm (3 in) in length. The 2.54 cm (1 in) diameter section is attached to a steel vertical stand by a stainless-steel sleeve that limits the arm rotation to a single axis. The abrasive cutting wheel on the rotary cutting tool is positioned on the apex of the lock shackle, 1.5 cm from the lock body, with the axes of rotation parallel with the shackle center-line. The lock is held in position by a Central Forge Model 94276 drill press milling vice that was attached to a Windsor Design hardwood work bench. Two steel "L" brackets are attached to the workbench on either side of the 5.08 cm (2 in) diameter, schedule 40, arm section for added stability during testing.

### 2.1.2 Dremel Test Procedure

The lock to be tested was placed in the vice with the abrasive cutting wheel positioned 1.5 cm from the lock body using a wooden spacer. The center-line axis of the abrasive cutting wheel was visually aligned with the center-line of the shackle. The PVC arm holding the rotary tool was leveled using a Husky 9-inch Digital Level to an accuracy of 0.1 degrees. Adjustment to the arm was made either by shimming the vice holding the lock or by loosening set-screws in the sleeve, holding the arm and sliding the sleeve vertically until the arm was level. With the arm level, the weight at the edge of the abrasive cutting wheel was adjusted to 0.18 kg (0.4 lb) using an Adam Equipment Model 18a scale to an accuracy of 1 g. Adjustment to the weight was made using counter-weights at the opposite end of the arm. The Dremel Model 4000 was set to  $(35,000 \pm 2,000)$  rpm. The Dremel was started and allowed to reach full operating speed by waiting 5 sec prior to testing. The Dremel was then lowered onto the lock shackle and a digital timer (Sportline Model AW60535W) was started.

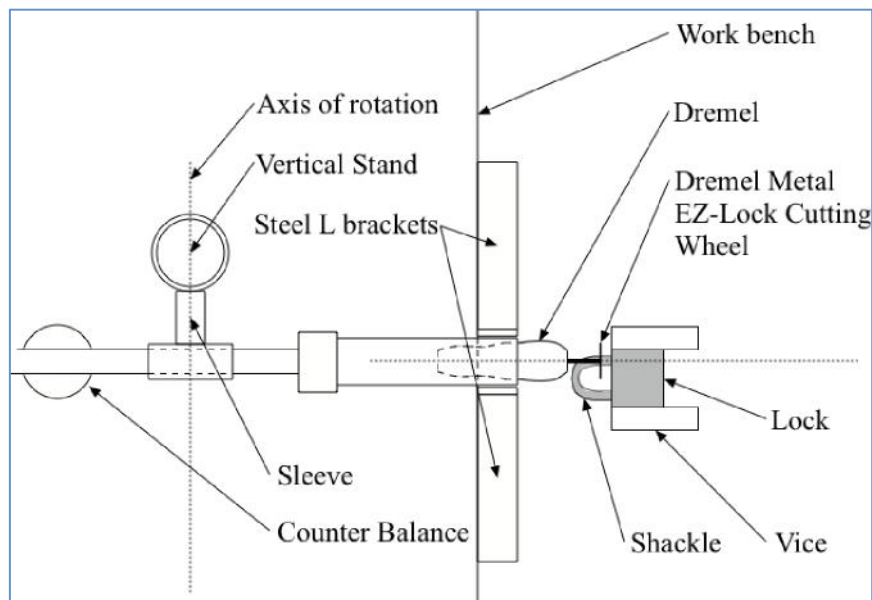


Figure 2.1 - Schematic diagram of the Dremel cutting system, viewed from above.

The Dremel abrasive cutting wheel was allowed to cut for 30 s and then the arm was raised. A new abrasive cutting wheel was used for each test. After testing, the depth of cut was measured using a General Tools Model 147 digital caliper to an



accuracy of 0.0001 in. The locks found in Table 2 were tested using this Dremel test system.

Table 2 - Shackle-style locks tested using the Dremel test system.

Make	Model	Style	Number Tested
Master Lock	6230	Shackle	5
W-LOK	SK977524-D	Shackle	5
American	A748	Shackle	5
Abloy	35050	Shackle	5
American	AH10	Shackle	5

## 2.2 Drill Press Test

### 2.2.1 Drill Press Test System

The drill test system used a free-standing JET Model J-2500 drill press to drill into the lock keyway, see figure 2.2. The lock was held in position by a Central Forge Model 94276 drill press milling vice that was attached to the drill press table assembly with 1/4 in bolts. Lock keyways were drilled with a Drill Master 4.8 mm (3/16 in) high-speed-steel, titanium-nitride coated, drill bit with 118° tips and, if required, a Milwaukee 12.7 mm (1/2 in) high-speed-steel, black-oxide coated, drill bit with 135° tips.

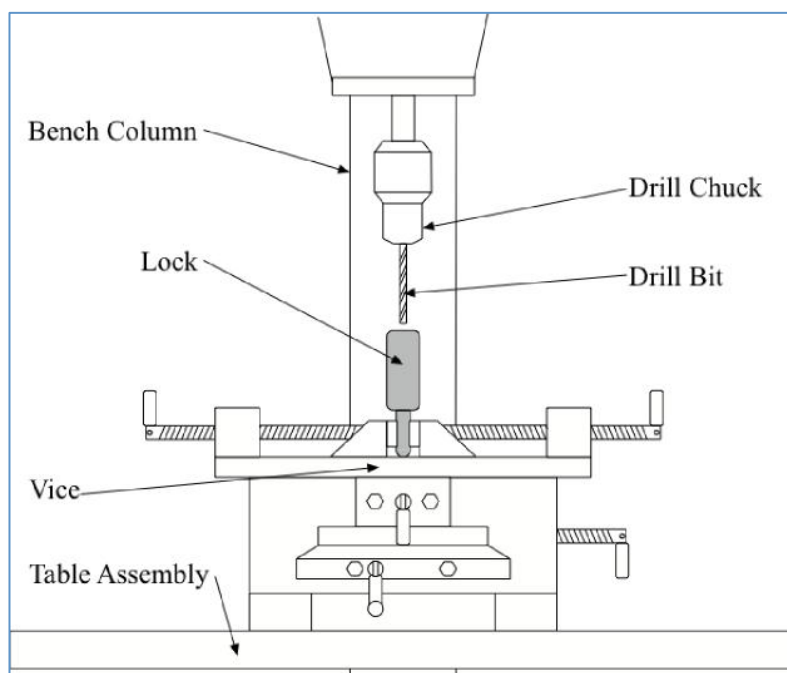










Figure 2.2 - Schematic diagram of the drill press system, viewed from the side.

### 2.2.2 Drill Test Procedure

The drill press pulley system was set to 1150 rpm. The lock under test was secured in the vice with the lock keyway facing up. A 4.8 mm (3/16 in) drill bit was placed in the drill chuck. The table assembly was then adjusted vertically so that the drill bit tip was within a few centimeters of the lock keyway. The lock position was then adjusted using the vice horizontal adjustment screws so that the drill bit was centered on the lock keyway. With the drill running, the drill bit was manually applied to the lock keyway. The drilling continued until the bit broke, the bit stopped making progress (defined as no vertical movement after 60 seconds), or the bit passed through the lock keyway and into the lock body. A second drill bit was used only if the 4.8mm (3/16 in) bit passed through the lock keyway. In that case, the table assembly was lowered and the 12.7 mm (1/2 in) bit was inserted into the drill chuck and the lock was re-centered on the lock keyway. The drill was restarted and the 12.7 mm (1/2 in) bit was applied to the lock keyway. The same drill-stop criteria were used for both drill diameters. After drilling was complete, the lock was dropped, a maximum of ten times, from a height of 1 m (39.4 in) onto a concrete floor to simulate a hammer blow. If the shackle opened, then the lock "failed" otherwise it "passed". The locks found in Table 3 were tested using this drill test system.

Table 3 - Shackle and puck-style locks tested using the drill press test system.

<b>Make</b>	<b>Model</b>	<b>Style</b>	<b>Photo</b>	<b>Number Tested</b>
Master Lock	6230	Shackle		5
W-LOK	SK977524-D	Shackle		5
American	A748	Shackle		5
Abloy	350N/50	Shackle		5
American	AH10	Shackle		5
American	2500	Puck		5
American	2010	Puck		5
Master Lock	6270	Puck		5
Abloy	PL975	Puck		5

## 2.3 Oxyacetylene Torch Test

### 2.3.1 Oxyacetylene Torch Test System

The oxyacetylene torch test used a linear actuator to control the speed of the shackle as it passed underneath an oxyacetylene torch, see figure 2.3. The actuator was a Linear Motions Inc. WP-MS33-T06LJM902 actuator with a BLH015K-A motor and motor-control unit, set to a speed of 2.5 mm/s (0.01 in/s). A spacer was attached to the linear head of the actuator to separate it from the high temperatures produced by the oxyacetylene torch. The spacer was constructed of steel box tubing measuring 101.6 mm (4 in) x 101.6 mm (4 in) x 101.6 mm (4 in) with a wall thickness of 3.05 mm (0.12 in). On top of the spacer was welded four "L" shaped brackets. Two 304.8 mm (12 in) x 304.8 mm (12 in) high temperature ceramic Silquar Soldering Blocks were bolted to the "L" shaped brackets to provide an insulated base for the lock. The lock was held in place with a 25.4 mm (1 in) x 304.8 mm (12 in) x 3.175 mm (1/8 in) aluminum bar clamped to the ceramic plates. The oxyacetylene torch head was positioned at an angle of  $\theta = 50^\circ$  relative to the ceramic plates and  $X = 1.5$  mm (0.06 in) from the lock shackle. Refer to figure 2.3.

### 2.3.2 Oxyacetylene Torch Test Procedure

Prior to each test series, a calibration test of the linear actuator was conducted. The length of travel of the linear actuator was measured using an Empire 18-inch stainless-steel ruler with an accuracy of 0.5 mm (0.02 in). The time required to move the length of travel was measured using a Suunto Model Observer stopwatch. The linear actuator motor control unit was then adjusted to achieve 2.5 mm/s (0.01 in/s). The lock under test was manually positioned on the ceramic plate to ensure a perpendicular cut was made across the shackle and clamped into position. The linear actuator was then activated, bringing the lock shackle directly below the torch cutting head where a metal spacer was used to place the head the recommended 1.5 mm (0.06 in) from the shackle.[8] The oxygen and acetylene regulator valves were then set to 289.6 kPa (42 psi) and 48.3 kPa (7 psi), respectively. The linear actuator was then activated moving the lock away from the torch. The acetylene on the torch head was turned on and ignited using a striker.

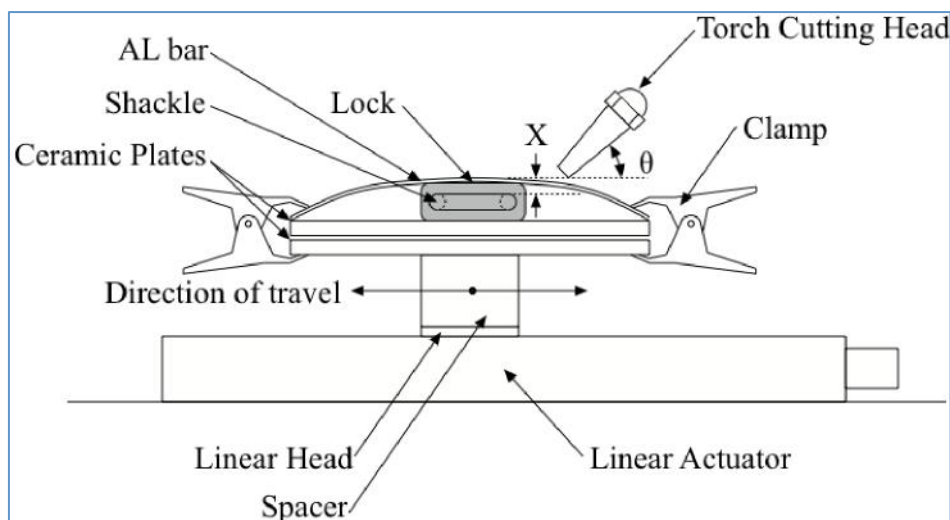


Figure 2.3 - Schematic diagram of the acetylene torch cutting system, viewed from the side.



Oxygen on the torch head was then turned on until six distinct blue points could be observed on the torch tip. The oxygen flow rate was confirmed by activating the cutting oxygen lever and confirming the length of the six blue points did not increase or decrease in length. With the torch burning correctly the linear actuator was activated moving the lock shackle toward the oxyacetylene flame. The flame was positioned at the bottom quarter of the shackle and held there until the shackle reached the oxidizing temperature of the shackle metal. This is traditionally recognized by pooling of the metal at the flame point or sparking of the metal at the flame point.[8] Once the oxidizing temperature was reached the cutting oxygen lever was depressed and the linear actuator was advanced. This process was repeated for the other side of the lock shackle. Once complete, the lock was allowed to cool, the depth of cut was measured using a General Tools Model 147 digital caliper to an accuracy of 0.0001 inch. The locks shown in Table 4 were tested using this oxyacetylene test system.

Table 4 - Shackle-style locks tested using the oxyacetylene test system.

Make	Model	Style	Number Tested
Master Lock	6230	Shackle	5
W-LOK	SK977524-D	Shackle	5
American	A748	Shackle	5
Abloy	35050	Shackle	5
American	AH10	Shackle	5

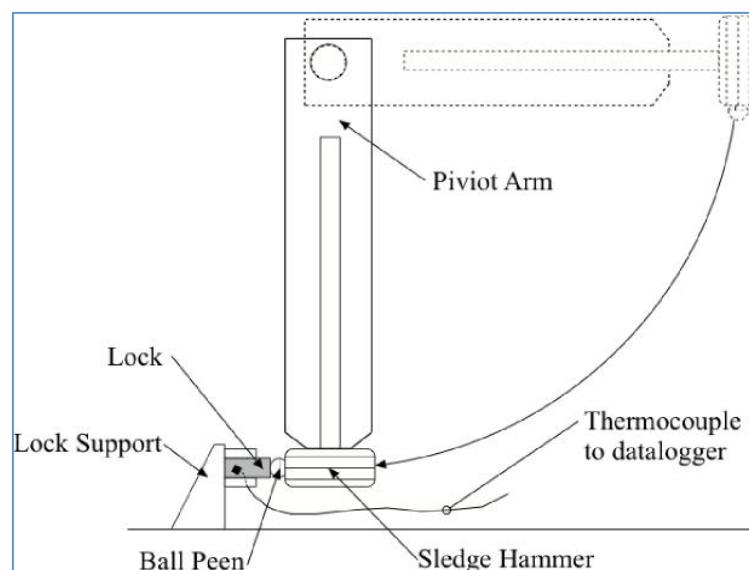


Figure 2.4 - Schematic diagram of the low temperature impact system, viewed from the side.

## 2.4 Low Temperature Impact Test

### 2.4.1 Low Temperature Impact Test System

The low temperature impact test system used a pendulum to impact a lock that was cooled using compressed difluoroethane (canned air), see figures 2.4 and 2.5. Two variations in the pendulum were constructed. The first pendulum was constructed of a 965.2 mm (38 in) x 101.6 mm (4 in) x 6.35 mm (1/4 in) steel plate and a 3.63 kg (8 lb) maul with its factory hickory handle. This pendulum had a total mass of 34.5 kg (76 lb). The second pendulum was constructed after the tenth test and the hickory handle began to fail. It was replaced with a 25.4 mm (1 in) diameter x 692.15 mm (27 – 1/4 in) schedule 40 steel pipe. A ball, from a ball-peen hammer, was also welded to the front of the maul, increasing the total mass of the pendulum to 40.4 kg (89 lb). The pendulum was designed to deliver a minimum of 300 J (221.27 ft–lbf) of energy based on an ax swing ergonomics study by Widule et al.[9] The actual energy of the pendulum prior to striking the lock was estimated using

$$E_{\text{pendulum}} = \frac{1}{2}mV^2$$

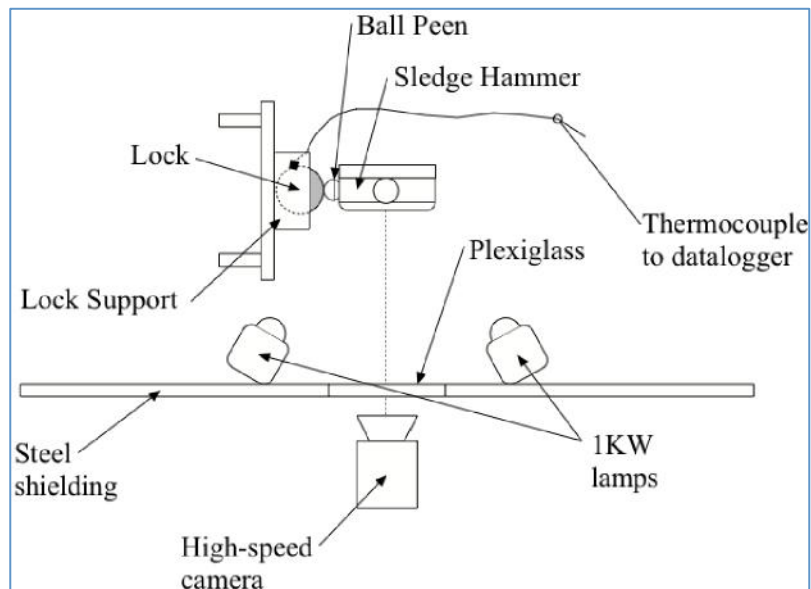


Figure 2.5 - Schematic diagram of the low temperature impact system, viewed from above.

where  $m$  is the mass of the pendulum and  $V$  is the velocity of the pendulum. The mass of the pendulum was assumed to be a point mass. The pendulum was held in its pre-release position by an electromechanical solenoid that was remotely actuated. The velocity of the pendulum prior to impact was measured using a Phantom v7.0 high-speed camera set to a resolution of 512 x 512 pixels and a frame rate of 4796 fps. The camera was triggered with a break-switch attached to the pendulum that opened when the pendulum dropped. The lock support was constructed of 6.35 mm (1/4 in) steel plate and was mounted to a 50.8 mm (2 in) thick steel table, estimated to weigh several tons. The lock support was designed to allow it to be adjusted so that the pendulum always struck the lock keyway at 90°. The lock support did not restrict the lock movement after impact. The locks were cooled using compressed

difluoroethane, commonly known as “canned air”. The cans were inverted and the extension tube was placed in the lock keyway. The temperature of the lock was measured using an Omega HH176 Datalogger Thermometer with an accuracy of  $0.3^{\circ}\text{C}$  above  $-100^{\circ}\text{C}$  and an Omega Type K thermocouple attached to the lock with Scotch Indoor/Outdoor Mounting Tape.

#### 2.4.2 Low Temperature Impact Test Procedure

Prior to testing, the Omega HH176 was calibrated using an ice-water bath and the high-speed camera was checked for alignment, lighting, and focus. The pendulum was lowered and the lock support adjusted to center the lock keyway with the ball on the pendulum. The pendulum was then moved to its pre-release position and the electromechanical solenoid locked. Next, a safety chain was positioned across the pendulum. The thermocouple was attached to the lock with tape on the side opposite the high-speed camera. The safety chain was removed from the pendulum and the Omega HH176 Thermometer Datalogger was started and a complete, inverted, can of difluoroethane was sprayed into the lock keyway. Once the can was empty, the pendulum was released striking the lock in the keyway. The release of the pendulum triggered the high-speed camera, which captured the pendulum impact. The locks found in Table 5 were tested using this low temperature impact test system.

Table 5 - Shackle and puck-style locks tested using the low temperature impact test system.

<b>Make</b>	<b>Model</b>	<b>Style</b>	<b>Number Tested</b>
Master Lock	6230	Shackle	5
W-LOK	SK977524-D	Shackle	5
American	A748	Shackle	5
Abloy	350N/50	Shackle	5
American	AH10	Shackle	5
American	2500	Puck	5
American	2000	Puck	5
Master Lock	6270	Puck	5
Abloy	PL975	Puck	5

## 2.5 Compressive Cutting Test

### 2.5.1 Compressive Cutting Test System

The compressive cutting test system used two different hydraulic presses to apply a short distance, three-point contact, shear force to the lock shackle, see figure 2.6. The hydraulic presses used were an Instron Model 8801 with a maximum compressive force of 100 kN (22,000 lbf) and a Satec Universal Test Machine with a maximum compressive force of 534kN (120,000 lbf). A displacement rate of 2.54 mm/min (0.1 in/min) was selected for a constant strain rate on all locks except the Abloy and W-Lok padlocks, which was set to 7.62 mm/min (0.3 in/min). The shear force was applied with a pair of 25.4mm (1 in) carbide-tipped chisels milled down to fit the chucks of the Instron and Satec hydraulic presses.

### 2.5.2 Compressive Cutting Test Procedure

The carbide chisels were chucked into the hydraulic press. A three-point jig, two spacer rods, and the carbide chisel, were setup around the lower-chuck. The lock

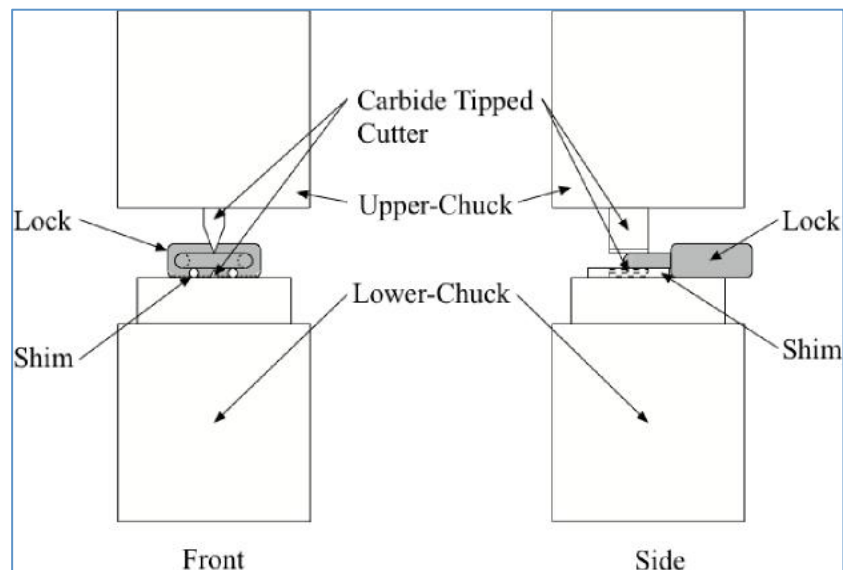


Figure 2.6 - Schematic diagram of the compressive cutting system, viewed from the sides.

was placed on the three point jig with the lock shackle centered on the lower carbide chisel. The upper-chuck of the hydraulic press was lowered until the carbide chisel just touched the lock shackle. The computer controlled hydraulic press displacement rate was set and the press was started. The Instron press was set to stop applying force once the measured force dropped below 40% of the maximum. The Satec press had no safety load shutoff. The locks found in Table 6 were tested using this compressive cutting test system.

Table 6 - Shackle-style locks tested using the compressive cutting test system.

<b>Make</b>	<b>Model</b>	<b>Style</b>	<b>Number Tested</b>
Master Lock	6230	Shackle	5
W-LOK	SK977524-D	Shackle	5
American	A748	Shackle	5
Abloy	35050	Shackle	5
American	AH10	Shackle	5

### 3 Results and Discussion

#### 3.1 Dremel Test

The Dremel test encompassed 5 shackle-type locks with 5 of each type tested for a total of 25 tests. The original test plan measured the time required to cut through the entire lock shackle, similar to what an actual attacker would attempt. However, initial tests with steel re-bar found the high rpm low torque motor of the Dremel rotary tool would stall completely or would oscillate by jumping out of the cut and back again repeatedly. It was found that this typically occurred after approximately 30 s of cutting. Based on this, a revised test method was adopted measuring the depth after 30 s. The revised test method allowed for an accurate and repeatable test without requiring the Dremel to be removed from the cut to regain speed.

Results for the 5 series of tests are summarized in figure 3.1. Plotted are the average depths of cut with error bars showing the standard deviation and the average shackle diameter of each lock type tested. Depths of cut ranged from 1.91 mm (0.075 in) for the W-LOK and 5.21 mm (0.21 in) for the American A748. The largest data scatter occurred with the Master Lock 6230 with a standard deviation of 1.16 mm (0.05 in). The W-LOK and the Abloy lock shackles were the most resistant to the rotary tool but had the largest shackle diameters, 13.9 mm (0.55 in) and 12.4 mm (0.49 in), respectively.

It is not clear from this data to what degree shackle diameter or shackle material properties influence the cutting rate observed. The W-LOK shackle diameter was approximately 26% greater in diameter than the Master Lock 6230, the lock with the smallest shackle diameter at 10.9 mm (0.43 in). All the lock shackles in the test used case-hardened, boron-alloy steels, except the W-LOK, which uses 316 stainless-steel. While boron, as an additive to steels, is used primarily to increase the hardness; its effectiveness is dependent upon: the amount of boron (5 – 30 ppm), the carbon and alloying content in the steel, and the presence of free nitrogen, and the type of de-oxidizers used during the steel making.[10]



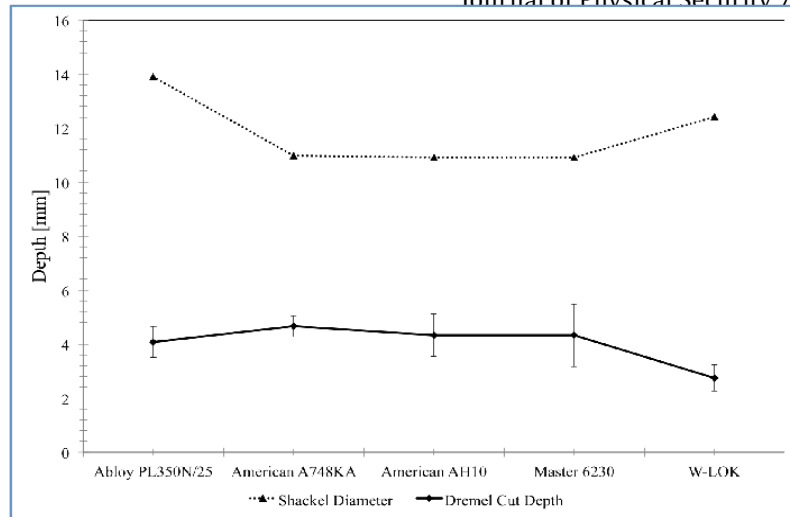


Figure 3.1 - Depth of cut in padlock shackles with a Dremel tool compared to the diameter of the lock shackle.

The same issue arises with case hardened materials, which depends on the carburization process and duration. Manufacturer data sheets do not provide information regarding the shackle material properties such as yield strength or surface hardness. Both the effect of shackle diameter and material properties require additional study to clarify the degree to which they influence the abrasion rate.

In summary, even though the W-LOK is on average 1.7 times more abrasion-resistant than the American A748, both lock shackles would on average be cut through in approximately 138 seconds and 70.5 seconds, respectively. These results are similar to the results that APC found, 165 seconds for a Master Lock 6230.[6]

Given the very short amount of time required for these rotary tools to cut through a lock, a more practical approach would be to prevent access to the shackle. More restrictive hoods can accomplish this or using puck-style locks where the shackle is not exposed. It should also be noted this process was relatively loud as opposed to the other methods tested. Also, there is currently no hardness or abrasion resistance standard in either ASTM F883-009, Standard Performance Specification for Padlocks or in ATF Publication 5400.7, ATF Federal Explosives Law and Regulations.

### 3.2 Drill Test

The drill test encompassed 5 shackle-type locks and 4 puck-style locks with 5 of each type tested for a total of 45 tests. The test was a simple pass/fail test summarized in Table 7. See section 2.2.2 Drill Test Procedure for the pass/fail criteria.

The American AH10s were the easiest locks to drill through, all failing with the 4.8 mm (3/16 in) bit. The Master Lock 6230 failed on three attempts of the 4.8mm (3/16 in). The remaining two locks passed the 4.8 mm (3/16 in) bit and also passed the 12.7 mm (1/2 in) bit. This lock has a stationary, hardened, keyway cover that made drilling with the 4.8 mm (3/16 in) bit difficult and prevented the 12.7 mm (1/2 in) bit from advancing past the keyway cover in the 60 s required by the test. The Abloy 350N/50 locks were very difficult to drill due to steel cylinder-pins. In three of the locks the tips of the 4.8 mm (3/16 in) bits melted. The other two bits

broke in the lock keyway. The W-LOKs were also difficult to drill due to steel cylinder-pins. In all five cases the drills penetrated a few centimeters before the 4.8mm (3/16 in) bits broke off inside the keyway. The American A748 locks were successfully drilled with the 4.8 mm (3/16 in) and the 12.7 mm (0.5 in) in two cases, but the locks did not open after ten drops from 1m (39.4 in). Tests in the remaining three locks resulted in the 4.8mm (3/16 in) bits breaking in the keyway. These locks use a stationary, hardened, keyway cover and steel cylinder-pins. The American 2500 lock tests resulted in the 4.8 mm (3/16 in) bits breaking in the keyway of all five locks and none opening. These locks use a rotating, hardened, keyway cover. The American A2010 tests were successfully drilled with the 4.8 mm (3/16 in) bits and all opened after several 1 m (39.4 in) drops. The Master Lock 6270 was successfully drilled with the 4.8mm (3/16 in) and the 12.7 mm (1/2 in) bits and opened after several drops from 1 m (39.4 in). The Abloy PL975 lock was difficult to drill, melting 4 out of 5 of the 4.8mm (3/16 in) bits. However, in one case the 4.8 mm (3/16 in) bit opened the lock after only a few centimeters of drilling. These locks used a rotating, hardened, keyway cover and steel cylinder pins.

Table 7 - Summary of the pass/fail results of the drill test.

<b>Make</b>	<b>Model</b>	<b>Style</b>	<b>Pass</b>	<b>Fail</b>
Master Lock	6230	Shackle	2	3
W-LOK	SK977524-D	Shackle	5	0
American	A748	Shackle	5	0
Abloy	350N/50	Shackle	5	0
American	AH10	Shackle	0	5
American	2500	Puck	5	0
American	2010	Puck	0	5
Master Lock	6270	Puck	0	5
Abloy	PL975	Puck	4	1

Several of these locks used steel cylinder pins and hardened, keyway covers (rotating and stationary). These added security features made drilling the keyways much more difficult. The Abloy, W-LOK, and the American A748 and 2500 all used one or both of these security features.

The drill press used in this test applied a great deal more downward force, drilling torque, and confinement than would be available with a hand-held drill. Therefore, locks that passed this test would be very difficult to drill with a handheld drill installed on an explosive magazine. In future tests, a center drill (bit with a wide shank and a 60 degree angle tip) is recommend prior to starting with the 4.8mm (3/16 in) bit. This would ensure that the hole is started on the centerline of the lock keyway. Finally, puck-style locks were more difficult to unlock after successful drilling than shackle-style locks. Most of the puck-style locks required all of the ten simulated hammer blows (1 m (39.4 in) drops) to get them to open. Most shackle-style locks opened when the drill bit was removed from the lock requiring no simulated hammer blows.

In summary, the addition of hardened keyway covers or the use of steel cylinder pins greatly increased the drilling difficulty. Also, puck-style locks offered some resistance to opening after successfully being drilled as opposed to standard shackle-style locks. Neither ASTM F883-009 nor ATF Publication 5400.7 address the drilling of the keyway even though this is a common locksmith practice for opening locks.[11]

### 3.3 Oxyacetylene Torch Test

The oxyacetylene torch test encompassed 5 shackle-style locks with 5 of each lock type tested for a total of 25 tests. The test was based on the maximum advance rate in mm/second required to cut the shackles off an American AH10 lock with an oxyacetylene torch. The American AH10 lock was used as a baseline because it is a standard lock issued across ATF. Results for the 5 lock types are summarized in figure 3.2. Plotted are the average depths of cut with error bars showing the standard deviation and the average shackle diameter of each lock type tested. Variability in the data was due to blow-back and slag pooling in the kerf cut by the torch. I observed during the tests that every shackle was cut through completely for all the locks except for the W-LOK.

Changing the cutting configuration to ensure there was room for cut material to move away from the shackle would significantly reduce this problem. Variability in the data was also due to variations in the flow rate of the oxygen and acetylene from test to test. Any future tests should continuously measure the flow rate of both the oxygen and acetylene and set these variables to ensure consistent cutting parameters for every test.

In summary, none of the shackle materials tested can withstand the high temperatures that an oxyacetylene torch can reach, 3,480°C (6,296°F). While the 316 stainless steel in the W-LOK does not oxidize (burn) like mild steels, at these temperatures it does melt. Portable plasma cutters, while not tested in this study, are also a serious threat to shackle-style locks. They operate at approximately 25,000°C (45,032°F), are inexpensive \$400 to \$1,200, and can cut any electrically-conductive metal (steel, aluminum, copper, stainless steel, etc.). To prevent the shackle from being cut, it must be protected. Some protection can be gained from using puck-style locks that enclose the shackle in the lock body. However, mild-steel, puck-style, lock bodies will only delay the opening with the added thickness of the lock body. Additional protection could be gained from a stainless-steel body, which

again does not oxidize when exposed to the oxyacetylene torch. Additional oxyacetylene torch testing would be required to determine if there are any significant delay advantages to puck-style locks constructed of stainless-steel versus mild-steel. Again, neither the ASTM F883-009 nor ATF Publication 5400.7 addresses the ability of the lock to withstand cutting by an oxyacetylene torch.

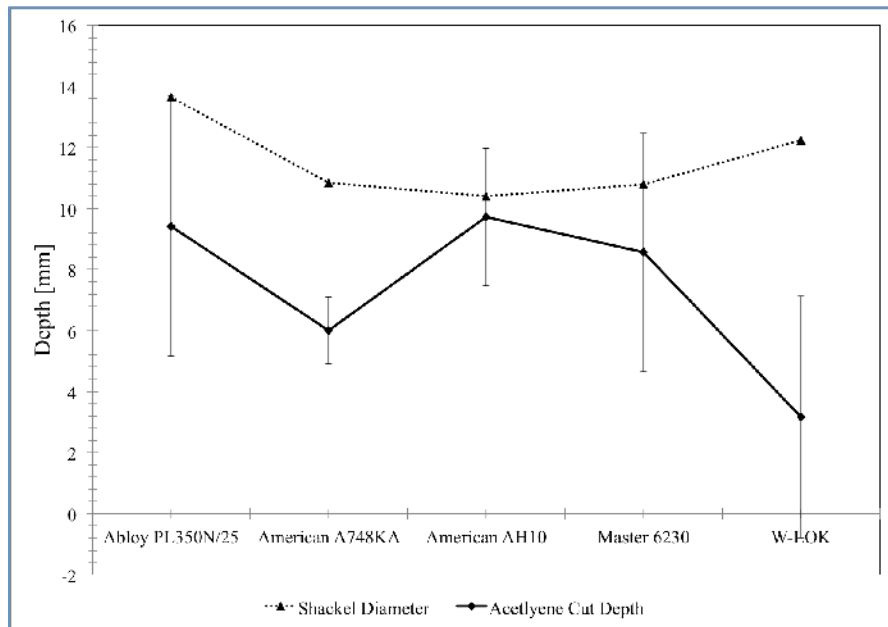


Figure 3.2 - Depth of cut in padlock shackles with an acetylene torch compared to the diameter of the lock shackle.

### 3.4 Low Temperature Impact Test

The low temperature impact test encompassed 5 shackle-style locks and 4 puck-style locks with 5 of each lock type tested for a total of 45 tests. Results for the 9 series of tests are summarized in Table 8. The average impact energy was  $(477.2 \pm 72.7)$  J ( $351.9 \pm 53.6$ ) ft-lbf at an average temperature at impact of  $(-25.2 \pm 15.1)$  °C ( $-13.36 \pm 27.18$ ) °F. Only one lock failed the test, a Master Lock 6230. It failed at an impact energy of 466.1 J (343.8 ft-lbf) at a temperature of  $-35.2$  °C ( $-31.4$  °F). The lock failed at the apex of the shackle.

Variability in the temperature data was a problem. This is probably caused by poor adhesion of the thermocouple to the lock body as the temperature dropped. I am looking at several methods to prevent this problem in the future. One is the use of Aluminum tape with a Kapton tape overlay and the other is thermally conductive epoxy.[12]

It should be noted that, while not tested in this study, both dry ice,  $-78.5$  °C ( $-109.3$  °F), and liquid nitrogen,  $-196.0$  °C ( $-321.0$  °F), are readily available and inexpensive. Additional testing is required to determine if these temperatures would result additional breakage at the impact energies tested.

In summary, locks withstood the low temperature impact tests with only one failure. Based on these results, this does not appear to be a reliable method of breaching these locks. One reason the APC results may contradict these results is the difference in test method used. In my tests, the locks were allowed to move after impact, similar to how a real lock would move if struck with a hammer. In the test conducted by APC, the lock was fixed in a vice. This difference is significant since all of the energy of the hammer blow was absorbed in the APC test as mechanical bending of the lock shackle. In my test, the impact energy was distributed in both mechanical bending and translational and rotational kinetic energy of the lock. Again, neither the ASTM F883-009 nor ATF Publication 5400.7 addresses the ability a lock to withstand low temperature impacts.

Table 8 - Test results of low temperature impact test for both the 40.4 kg and 34.5 kg pendulums.

<b>Lock</b>	<b>Energy [J]</b>	<b>Temperature [°C]</b>	<b>Pass</b>	<b>Fail</b>
Abloy 350N/50	484.6	-16.1	5	0
Abloy PL975	484.6	-12.2	5	0
American AH10	414.8	-53.7	5	0
American 2010	545.8	-15.9	5	0
American 2500	484.6	-16.7	5	0
American A748	484.6	-9.6	5	0
MasterLock 6230	466.1	-32.6	4	1
MasterLock 6270	480.9	-13.7	5	0
W-LOK	484.6	-6.8	5	0

### 3.5 Compressive Cutting Test

The compressive cutting test encompassed 5 shackle-style locks with 5 of each lock type tested for a total of 25 tests. Results for the 5 series of tests are summarized in figure 3.4. Plotted are the average maximum loads at failure with error bars showing the standard deviation of each lock type tested. Maximum loads ranged from 170.3 kN (38,277.2 lbf) for a W-LOK to 54.3 kN (12,204.0 lbf) for an American AH10. The largest data scatter occurred with the American AH10 with a standard deviation of 9.4 kN (2,111.8 lbf). All of the shackles in these tests were advertised by the manufacturer to be case-hardened, boron-alloy, steels except for the W-LOK, which uses 316 stainless-steel. It is again not clear to what degree material properties or



shackle diameter contribute to the differences in material strength. However, referring to figure 3.4, it can be observed that it takes almost twice the force to cut through the Abloy and W-LOK shackles while their diameters were only about 25% larger.

In the APC study, the lock shackles were cut with a Chinese manufactured hydraulic rebar cutter, Model CPC-22A.[6] For a comparative analysis, the force required at the handles of a set of 36in mechanical bolt cutters, Pittsburgh Model 41150, was examined, see figure 3.3. Based on this schematic, we have the following equation representing the required force at the handles and the resulting force at the jaws:

$$F_{Handle} = \frac{zx}{yw} F_{Jaws}$$

where  $w = 685.8$  mm (27 in),  $x = 15$  mm (0.6 in),  $y = 111$  mm (4.4 in),  $z = 50$  mm (2 in) and  $F_{Jaws}$  is the average maximum force measured at failure for each lock type.

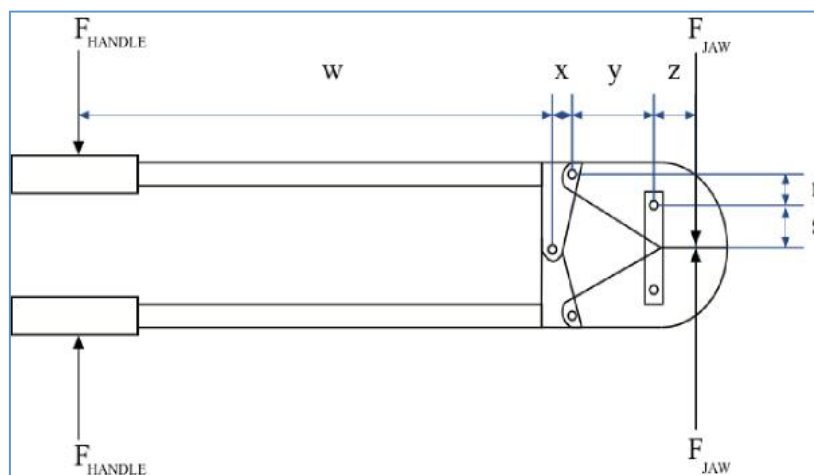


Figure 3.3 - Schematic diagram of a set of bolt cutters.

The calculated results in Table 9 show that over 609.4 N (137 lbf) would be required at the handles for the weaker shackles and over 1,556.9 N (350 lbf) for the Abloy lock. Even the lesser of these forces are considerable and would be difficult for an individual to accomplish. However, the hydraulic rebar cutter tested by APC easily broke the shackle of the Master Lock 6230. Additional, unpublished results by APC found that the hydraulic rebar cutter jaws broke when attempting to cut an Abloy 350N/50 lock.

In summary, it required twice the force to cut through the W-LOK and the Abloy lock shackles as compared to the Master 6230, American A748, and American AH10. Again, neither the ASTM F883-009 nor ATF Publication 5400.7 addresses the ability of the lock to withstand compressive cutting at the shackle.

Table 9 - Force required at the handles of 36 in bolt cutters to achieve the maximum force at failure.

Lock	Jaws [lbf]	Handle [lbf]
Master 6230	13,973.9	137.7
W-LOK	35,529.5	350.0
American A748	14,839.6	146.2
American AH10	14,639.0	144.2
Abloy 350N/50	31,635.3	311.7

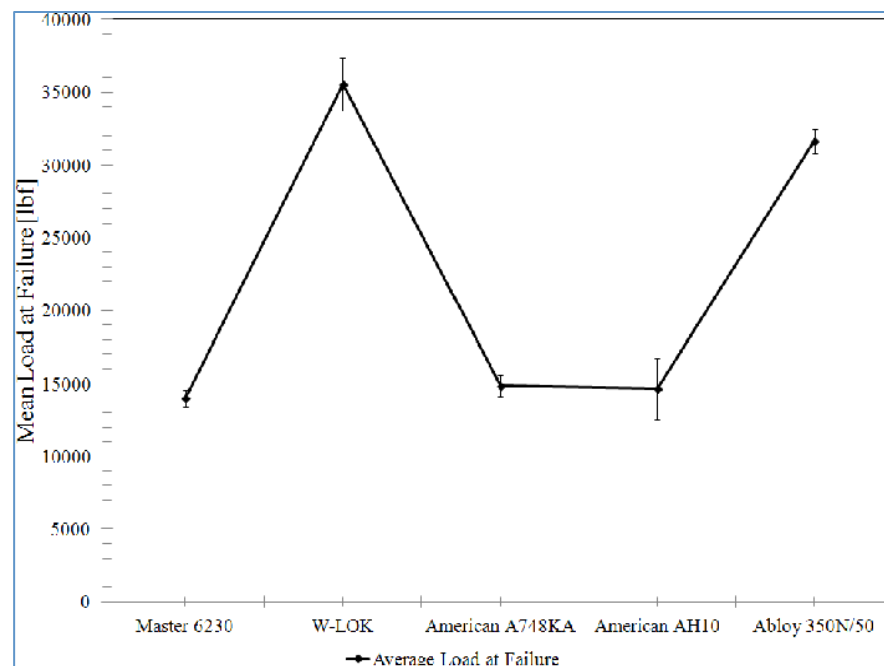


Figure 3.4 - Maximum compressive cutting-force loading on shackle-style locks.

#### 4 Conclusions

The effects of padlock breaching methods were studied using 9 different lock types. Based on these test results, I found that shackle diameter and/or shackle material can significantly increase the shear strength of the shackle. While these same comparative benefits were found with abrasion resistance, the actual time required to breach was so short that any abrasion resistance advantage was negated. I also

found that the shackle is vulnerable to the oxyacetylene torch regardless of shackle diameter or material. Drilling of the keyway was thwarted with relatively simple security measures such as stainless steel cylinder pins and hardened cylinder covers. None of the locks appear to be particularly susceptible to low temperature impacts although retesting with an improved method to adhere the thermocouple to the lock body would improve confidence in this conclusion.

In general, locks with an exposed shackle are more vulnerable than hidden or puck-style locks. All locks can be vulnerable to drilling, but with relatively simple security measures, the vulnerability to drilling can be greatly reduced. Table 10 below is a summary of lock performance in all five tests. Each lock was ranked 1-5, 1 being the worst performer in a particular test and 5 being the best performer. Puck-style locks scored 5s on the Dremel, oxyacetylene, and compressive cutting tests. This was done because the shackle of puck-style locks is hidden and not vulnerable to these tests. The highest scoring shackle lock was the W-LOK while the highest scoring puck-style lock was the American 2500.

Table 10: Summary of the five lock tests.

<b>Lock*</b>	<b>Dremel</b>	<b>Acetylene</b>	<b>Drill</b>	<b>Impact</b>	<b>Compressive</b>	<b>Total Score</b>	<b>Cost per Lock</b>
W-LOK (S)	5	5	5	5	5	25	\$82.50
American 2500 (P)	5	5	5	5	5	25	\$55.82
Abloy PL975 (P)	5	5	4	5	5	24	\$110.00
Abloy 350N/50 (S)	4	2	5	5	5	21	\$135.00
American A2010 (P)	5	5	0	5	5	20	\$25.00
MasterLock 6270 (P)	5	5	0	5	5	20	\$27.95
American A748 (S)	1	4	5	5	2	17	\$96.00
MasterLock 6230 (S)	3	3	2	5	2	15	\$25.23
American AH10 (S)	2	1	0	5	2	10	\$23.00

\*(P)=puck type and (S) = shackle type.

Figure 4.1 shows the total lock score plotted vs. unit cost. The most expensive locks do not appear to automatically be the best.

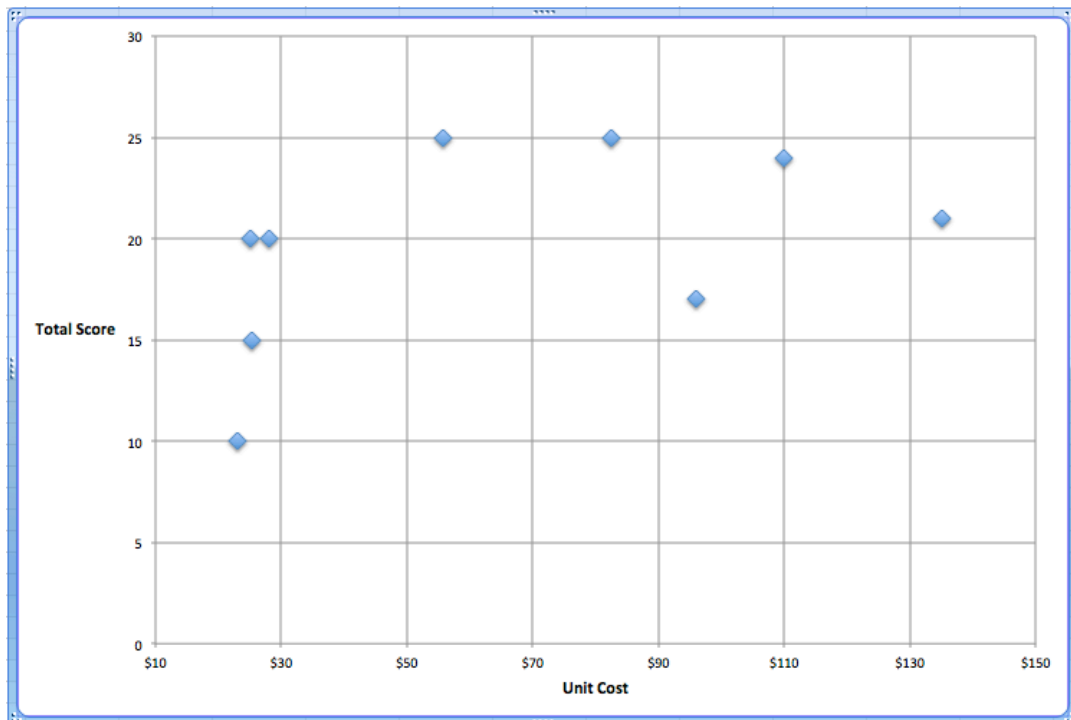


Figure 4.1 - The total score for each lock versus the lock cost in dollars.

Standards to address the vulnerabilities tested in this study do not currently exist in either ASTM or ATF. The U.S. Department of Defense, Military Standard, MIL-DTL-43607J, Padlock, Key Operated, High Security, Shrouded Shackle, dated 29 July 2010, was the most robust standard found. This standard addresses shackle resistance at low temperatures and forced entry resistance with both battery and non-battery tools. The low temperature standard requires the padlock to be cooled to  $-73^{\circ}\text{C}$  ( $-100^{\circ}\text{F}$ ) and struck a minimum of six times or for a maximum time period of 5 min with a 1.36 kg (3 lb) hammer. The forced entry test requires the lock to withstand 1 minute of forced entry with battery tools and 5 min of forced entry with non-battery tools. The total weight of tools cannot exceed 9.07 kg (20 lb). Heating equipment temperatures cannot exceed  $649^{\circ}\text{C}$  ( $1200^{\circ}\text{F}$ ). While this standard addresses many of the tools and methods used in this study, the "pass" times for powered tools are only 1 minute and the maximum temperatures are low compared to oxyacetylene. Additionally, locks that meet these standards, such as the Sargent and Greenleaf 951 cost on average over \$1,680 each.

## 5 Acknowledgments

The author gratefully acknowledges technical support from the University of Alabama Huntsville, Aerophysics Facility and Reliability and Failure Analysis Laboratory. The author also gratefully acknowledges the support from the NCETR, Explosive Enforcement and Training Division. The Editor of this journal created figure 4.1.

## 6 References

- [1] ATF. Explosives Storage Requirements, May 2013.
- [2] ATF. *ATF Federal Explosives Laws and Regulations*. Bureau of Alcohol, Tobacco, Firearms and Explosives, 99 New York Ave NE, Washington, DC, 5400.7 edition, June 2012.
- [3] ATF. Explosive Thefts from 2006 through 2010. *ATF Explosives Industry Newsletter*, page 8, June 2011.
- [4] American Society of Testing and Materials. *Standard Performance Specification for Padlocks*. American Society for Testing and Materials, 100 Barr Harbor Drive, West Conshohocken, PA, f883-09 edition, 2009.
- [5] Austin Powder Company. Breach Testing Magazine Padlocks. November 2012.
- [6] Les Kirkup. *Experimental Methods*. John Wiley & Sons Australia, Ltd., 42 McDougall Street, Milton, Qld 4064, 1994.
- [7] David J. Brooks and Benjamine Beard. A Comparison of Laboratory and Vulnerability Evaluation Methods for the Testing Security Equipment. In *Proceedings of the 3rd Australian Security and Intelligence Conference*, page 13, Perth Western Australia, 2010. Security Research Institute, Edith Cowan University.
- [8] R. Finch. *Welder's Handbook: A Guide to Plasma Cutting, Oxyacetylene, Arc, Mig and Tig Welding*. HPBooks, 2007.
- [9] Carol J. Widule, Vernard Foley, and Gail Demo. Dynamics of the Axe Swing. *Ergonomics*, 21(11): 925-930, 1978.
- [10] R. C. Sharma. *Principles of Heat Treatment of Steels*. New Age International (P) Limited, 2007.
- [11] Douglas Chick. *Steel Bolt Hacking: A Computerman's Guide to Lock Picking*. Thenetworkadministrator.Com, 2004.
- [12] Cameron Sinohui. A Comparison of Methods for Attaching Thermocouples to Printed Circuit Boards for Thermal Profiling. In *NEPCOM*, 1999.



## Viewpoint Paper

### Nuclear Containment and Surveillance Terminology

Halvor A. Undem, Ph.D., Lt Col USAF (Ret)  
Affiliate Professor, Jackson School of International Studies  
University of Washington, Seattle

I came across a term that I seriously objected to over a year ago in a private conversation, and I expressed my objections to the individual when I heard it. Now that I am beginning to see the term come into printed use, I am going to object even more in print. Call it, if you will, a wee bit of whining.

The term is “NDA Seal”.

Now, some of you might think I am being curmudgeonly or pedantic or both, but I assure you I am not. It is a particularly bad term for two reasons. Firstly, it confuses two techniques from Safeguards (and Arms Control, too) that are normally independent but vitally complementary to one another. Secondly, we have, thanks to the Human Capital Development thrust area of the Department of Energy’s Next Generation Safeguards Initiative, a lot of new Safeguards practitioners whose confusion we should work to eliminate rather than encourage.

To be specific, NDA, or more correctly *Non Destructive Assay Measurements* provide an **authentication metric**. Tamper Indicating Seals (referred to as just “Seals” from this point on), on the other hand, are simply **temporary use devices** that, given the acceptance of a lot of assumptions, buy the monitoring party a bit of time between necessary authentication measurements. In the logical scheme of things, the correct authentication metric is always necessary and sufficient. Seals may be necessary. They are never sufficient.

How shall I illustrate this? One way is to look at the history of how seals came into use, and then imagine two extreme verification worlds, one where seals are utterly and completely un-necessary, and another where, at least for a time (and maybe a very long time), that’s all you can have. Sometimes examining asymptotic cases provides interesting insights on individual variable behavior. The second illustration, which I think I like a little better, is a military one, where the **authentication metric** constitutes the offensive operation, and the **seal** the defensive maneuver.

#### Illustration 1 – History and Asymptotic Limits

##### History.

During my last year (2008) at the International Atomic Energy Agency (Agency),

I spent a good deal of time in the Agency archives, because I was working on a history of seal development and vulnerability assessments for the various Category A<sup>1</sup> seals that were already in full deployment or about to be deployed. The metal (CAPS) seal<sup>2</sup>, for example, has at least a 40-plus-year history while the EOSS<sup>3</sup> (Electro-Optical Sealing System) just started going into full scale deployment in 2008. The record indicates, fully consistent with the Seals Unit's ICAS (Introductory Course on Agency Safeguards) Module, that Seals are *ancillary/complementary* to *nuclear material accountancy* activities. This ancillary/complementary nature is important, and needs to be emphasized.

The model problem is this. Assume I have a room with  $n$  containers of SNM (Special Nuclear Material), say LEU (Low Enriched Uranium) in a fuel fabrication facility. Every 30 days (or pick the interval required), I go in with NDA instrumentation and do a full PIV (Physical Inventory Verification) of every container in the room. So, because of my *authentication metric*—my measurement campaign(s)—I know for a fact on a reasonably periodic basis that in that room there are  $n$  containers with  $x$  grams of LEU at an enrichment of such and such  $\pm y$  grams per container. That's one element of the Safeguards approach for that room which is part of a larger set of Safeguards activities to deal with the Safeguards approach for the entire facility.

But if this activity is too expensive and/or consumes too many inspector staff days, or both, what can I reasonably do? I *seal* those containers so that I do not have to do the PIV every 30 days. I extend the interval between PIVs in order to save time and money, but I do not eliminate PIVs. As long as (1) I ascertain that the seal is mine (unique), and (2) I am confident that for reasonably short (subjective) intervals the seal will tamper-indicate under most feasible attacks, then I accept the risk of stretching out the time between PIVs. *The seal introduces risk for the benefit of cost reduction. It's a trade I had to make. I am buying time.*

### **Limit 1 – A World Without Seals**

We can imagine a world without seals without too much trouble. Let's say the brilliant IAEA UMS (Unattended Monitoring Systems) Section has invented a foolproof machine, very small, that is securely affixed to every canister at a facility under Safeguards, and at the flick of a few key strokes on a computer in Vienna, a full PIV on every canister in that facility can be had in real time, and as often as desired. This is not only unattended, but real-time NDA monitoring, and in this situation, seals are utterly unnecessary. You have full and complete nuclear material accountancy, independently, as often as you like. Punch Line: NDA

<sup>1</sup> A "Category A" seal, indeed any Category A Safeguards Instrument, is one that has gone through the Agency's entire gauntlet of development, test, and evaluation before being declared fit for worldwide use.

<sup>2</sup> *Safeguards Techniques and Equipment: 2011 Edition*, International Nuclear Verification Series No. 1 (Rev. 2), International Atomic Energy Agency, Vienna, 2011, pp. 70 - 71

<sup>3</sup> Ibid, pp. 74-75.

measurements, the *offensive operation*, provides everything needed, particularly if you locate the materials with high precision in time and space.

### **Limit 2 – A World With Seals Only (And Maybe Portal Monitoring)**

This world is a bit harder to imagine, especially in Safeguards, but an Arms Control scenario comes to mind. Let's suppose that after New START, American/Russian relations are just so bad that almost everything is off the table. No direct warhead dismantlement monitoring is allowed, no agreement on what constitutes unclassified information has been reached, and no agreement on materials disposition has been reached, so we're stuck. EXCEPT both parties agree there is no utility to tactical weapons at all, and a joint facility is built with all portals and exits monitored, so that confidence is VERY high that an item that goes in, whether Russian or American, stays in, until it comes out. (This is a bit like the Mayak Fissile Material Storage Facility<sup>4</sup>, only jointly constructed and monitored.) A good jointly designed sealing system applied to jointly designed containers built for such a sealing system might provide high confidence that you have an effective item monitoring regime. This is clearly an interim solution (but it could be a long interim), because no-one really knows, without some kind of NDA measurement (currently not allowed), what is REALLY in the containers. Both parties, if they watched shrouded pointy objects being removed from missiles and placed in sealed containers, might reasonably assume the items are nuclear warheads with nuclear materials, but only an ***authentication measurement***, somehow, some day, on converted materials or otherwise, really lets you know if you have what you think you have. Punch Line: Seals, the *defensive maneuver*, buy time until you can bring offensive operations to bear.

### **Illustration 2 – Concluding the Military Analogue**

So to conclude this *wee* bit of whining, I object to the phrase “NDA Seal” in just the same way that I object, as a retired Military Officer, to the phrase “Offensive Defense” (the parallel to “NDA Seal”), or “Defensive Offense” (the opposite concept). In the military analogue, both events can and do happen, but they are anomalies. We might consider Chamberlain's bayonet charge at the Battle of Little Round Top an example of “Offensive Defense”, and the engagement in Vietnam's Ia Drang Valley<sup>5</sup> an example of “Defensive Offense”. Anomalies can happen, but they are not a good basis for either the execution or teaching of common doctrine, whether military, Arms Control, or Safeguards.

---

<sup>4</sup> Podvig, Pavel, *Consolidating Fissile Materials in Russia's Nuclear Complex*, Research Report No. 7, International Panel on Fissile Materials, May 2009, [www.fissilematerials.org](http://www.fissilematerials.org), accessed 5 November 2013.

<sup>5</sup> Galloway, Joseph and General Hal Moore, *We Were Soldiers Once and Young: IA Drang-the Battle that Changed the War in Vietnam*, Random House Publishing Group, October 1992.

## **Money in a Glass Box**

Peter Kurrasch  
Internet Security Consultant  
gtink78@hotmail.com

### **Introduction**

Let's face it: security is hard. Establishing security, maintaining security, feeling secure...each depends on a variety of factors that change over time. One minute you feel confident and secure, the next minute you learn something new that makes you think twice.

A steady stream of questions doesn't help either: How much money do I spend before I feel secure? Where will my limited resources have maximum impact? How can I make good decisions on security when I don't yet have all the facts? How will I know if a security solution actually works?

And there's another problem: talking about security is hard. It can be difficult to walk through scenarios with colleagues who might not have the same knowledge and perspectives. It can be difficult to compare notes and experiences with those in other industries who face different problems and situations. And, perhaps worst of all, it can be difficult to explain why a particular security decision was made or speak convincingly of its merits.

Though security may be hard, it is obviously important for the safety and protection it affords that makes daily living possible. Further, it is important to talk about security and to have good tools to encourage those discussions. It is in this context, then, that this article seeks to provide such a tool by way of a thought experiment. This paper will challenge some existing ideas of security and will present unconventional ideas for the purposes of provoking thought—and with it, discussion.

### **Being Obvious**

One way people talk about security is something that could be called “obvious security”: security measures that are recognizable, are easy to understand how they work, and are effective. Think of a castle with high stone walls and a moat with crocodiles. It's pretty obvious how they work, and anyone can tell you how effective they are.

The trouble with “obvious security” is that it can be expensive or inconvenient or ineffective—or all of the above. For example, a high stone wall costs a lot of money and it’s ugly and blocks the sun. Plus, someone could always build a higher ladder, so how effective would it really be? If you have a moat with crocodiles you have to keep the crocodiles happy so they don’t escape and eat the neighbor’s dog. Plus, someone could try to distract the crocodiles while someone else crosses the moat, so how effective would that really be?

And yet there is a seductive quality to “obvious security” for one simple reason: people get it. When there is so much about security that is difficult it is nice to have something easy.

### **Being Simple**

Instead of being obvious, some might try to talk about security in “simple” terms. Certainly, Hollywood has been doing that for decades: “Prevent [super villain] from taking [object of supreme importance]” or “Guard this [cultural icon] during its journey to [some region controlled by an enemy].”

“Simple security” also includes mundane examples like: “Keep those kids off my lawn!” In this case the problem at hand is fairly straight-forward, is limited in scope, and has any number of ways to keep the lawn secure: maybe I’ll put up a fence or install cameras or sit in a chair and yell at people. And the measure of success is pretty clear: grass is not trampled.

The trouble with “simple security”, however, is that it usually isn’t very interesting. In the case of Hollywood, flourishes are usually added to engage the viewer, but frequently they also require the viewer to suspend disbelief. And most people can’t be bothered to worry about grass.

### **Being Compelling**

Instead of being obvious or simple, let's try to be compelling and start with something that everyone understands: money. If you see money, you take it. If you have money, you keep people from taking it. If you are walking down the street and see a pile of cash, you grab some of it and keep on walking. If that happens to be your own pile of cash, you hire a security guard to keep people from touching it.



Easy enough, but one element is missing: the effort-risk-reward calculus. How much effort am I willing to put in? How much risk am I willing to accept? What is my reward at the end of it all—and is it worth the effort and the risk?

This element is important, for it not only informs basic human behavior but also guides the security professional when making security decisions. Consider what happens when you see a penny on the ground. As a passer-by, you have to decide if it is worth the effort to bend over to pick it up. To many people, a single penny is just not worth it. Suppose instead of a penny you find a \$100 bill. Is that a sufficient reward?

Now suppose that the \$100 is a pile of pennies. The reward is the same as a \$100 bill but the effort is much higher since you have to carry away a lot of pennies. The security professional knows this. In fact, the decision to use pennies could be a deliberate strategy to keep the money secure: By requiring more effort of the would-be money grabber, some people might decide to ignore the money and move on; so long as enough people do that, the money remains secure.

Consider another way to secure \$100: a glass box. In particular, let's take a \$100 bill, put it in a glass box, set the box in the middle of a street, and post a security guard next to the box. Here, the reward is modest (\$100), the effort is fairly modest (grab a rock, break the glass, grab the money), and if the security guard is incompetent, the risk is minimal (walk up to the box when the guard isn't looking). Is the reward sufficient for the effort and risk involved? Would enough people be dissuaded from trying to get the money? How secure would the money really be? If you hire a better security guard does that improve your security?

## Going Big

From the standpoint of "obvious security", we know that putting money in a glass box in the middle of a street is a lousy idea. Everyone knows that money belongs in sturdy containers (hard to break) with opaque walls (hide whatever is there) in a guarded place that's hard to reach (keep people away). It's obvious.

However, suppose an argument is made that the only problem with the glass box example is that everything is too small. If you want to use a glass box you should actually make everything bigger. That is, you should take a lot of money, put it in a giant glass box, and then place it in the middle of a busy street in the middle of a major American city! Would this approach keep the money secure?

Imagine the following news article:

CHICAGO, Illinois — The Federal Reserve Bank of Chicago, citing the rise in electronic banking combined with an economy still in recovery, reported today that circulation of paper currency is at an all-time low. Local banks are distributing fewer bills to customers. The banks are making fewer requests of the Fed to replenish their cash. The Fed, ultimately, must store more bills for longer periods of time.

In the Fed's Chicago office, located at 230 S. La Salle St. in the heart of Chicago's financial district, are three vaults built underground. In normal economic times, these vaults are well equipped to handle the regular ebb and flow of cash between the Fed and the region's banks. With those vaults reaching capacity, however, the Fed must expand and yet—given the tangled web of cables, tubes, and tunnels that lie beneath the city—it has run out of space.

Quite literally, the Fed has too much money and no place to keep it! But, the Fed has a plan that is as innovative as it is shocking: build a giant vault made of glass right in the middle of La Salle St.

Plans released today by the Fed call for the 200 block of La Salle St. to be closed to all vehicular traffic. The area will remain open to pedestrians, however, and a new plaza will be built so that people may gather and view the vault. In fact people will be able to walk right up to the vault and look at all the money in it—an amount that could exceed \$10,000,000. This feature has raised concerns among security experts.

A Fed spokesperson explains it this way: “The plaza and the transparent nature of the vault's walls mean that anyone at any time can walk up and see the money is there and that it is safe. Encouraging people to walk around, look inside, take pictures, eat lunch, and otherwise meet up in the plaza further improves security since would-be criminals are less inclined to act when other people are around. It may seem counter-intuitive but making the money fully visible actually makes it more secure.”

The spokesperson added: “The design of the vault will be aesthetically pleasing and referential to the architecture of the many historic buildings located in Chicago's Loop. People will want to come see the vault. It will be mesmerizing!”

The Chicago mayor's office offered its support in a press release: “The mayor enthusiastically supports the Fed's decision to build their new vault in the heart of our city. This vault will be a unique symbol of our city's dynamism and is a wonderful way to showcase to the world that Chicago is a vibrant, innovative, and secure place to do business. We believe the pedestrian plaza will be a true destination landmark and a beautiful place for office workers and tourists alike to gather.”

Critics of the plan contend that few, if any, people are seen walking around the downtown area at night. The Fed spokesperson offers a solution that can only be described as bizarrely ironic: “We plan to invite the city’s homeless population to sleep in the plaza. Bringing people in helps keep the money secure and the plaza will be a safe and welcoming alternative to parks, alleys, and doorways. It’s a win-win.”

Construction plans for the vault itself have not been disclosed for obvious security reasons, however a source close to the project has revealed the following details:

The vault will be elevated off the ground and placed atop several columns about 10 feet high. People will be able to view the vault from all four sides and from below but the Fed wants to discourage people from touching—and possibly damaging—the walls.

The walls of the vault will be made of bullet- and bomb-proof glass. The glass will be approximately 14 inches thick and composed of multiple layers of glass, laminates, and polycarbonate materials.

The vault will be fully climate controlled and will be slightly de-pressurized. Should the walls of the vault be breached the interior pressure will spike and sensors within the vault can report the security break accordingly.

The vault will be inaccessible to humans. Money is transferred in and out using a fully automated, robotic system.

Specific to that last point, the source explains that bundles of money must be moved through the support columns, beneath the street level, and into the Fed’s building. The whole system must be extremely reliable since there is no direct means of getting into the vault to make repairs. The Fed spokesperson declined to comment on this point.

We have also learned that individual bundles of money will be outfitted with an exploding dye pack. The expectation is that in the event of a containment breach, the increased atmospheric pressure will cause the dye packs to immediately explode. The dye will permanently stain the bills making them recognizable as being stolen, thereby rendering them unusable.

Undoubtedly, the Fed has other security measures in mind for their new vault, many of which may never be made public. Still, many security professionals remain skeptical. Said one, who spoke on the condition of anonymity, “Who does this? I mean, a vault like this is an open invitation to criminals and terrorists to descend on Chicago and wreak havoc. The whole project has ‘public safety risk’ written all over it. Surely it’s just a matter of time until something bad happens.”

## Start Thinking

In this glass vault scenario, four different parties are involved: (1) the Fed who has the money and needs a place to keep it; (2) the security consultants who must hatch a plan to keep the money secure; (3) a would-be thief who is keen on taking the money; and (4) the citizens who are impacted not only by the vault's construction but also its presence as a target within their city.

The thought experiment is thus: place yourself in each of those four roles and argue convincingly that the glass vault will provide secure storage for the Fed's money and will not jeopardize the safety of the general public.

For the role of the Fed, what security measures do you need and how much money are you willing or able to risk? For the role of the consultant, does the ability to destroy the money make security planning easier? How much of the security plan should be shared with the public?

For the role of the thief, in what ways could you realistically succeed in taking the money? How many people would you need to help you with your plan? How much effort are you willing to put in, how much risk are you willing to assume, and how much money would you need to get to make it all worthwhile? Would \$200,000 be enough?

For the role of the citizen, what knowledge of the security plans makes you comfortable with the vault? Would you prefer that the vault area be cordoned off to pedestrian traffic? If you saw people trying to break in to the vault, would you stop them?

After arguing that the vault is a good idea, are you yourself convinced that it is? Why not?

Obviously there is no right answer in this scenario, and probably such a plan would never be a good idea. Nonetheless, if the idea of it spurs conversations on what it means to have good security...well, that can only be a good thing.

## **Vulnerability Assessment Myths\* (Or What Makes Red Teamers See Red)**

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

The man on the other end of the phone was nothing if not enthusiastic. “So,” he said, “You folks do vulnerability assessments?” “Yes,” was the response. “That’s great,” he said, “We have an outstanding new security product we would like you to test and certify!” “Well, I’m afraid we don’t do that,” he was told. “I guess I’m confused,” said the man.

As vulnerability assessors (VAers), we encounter this kind of confusion dozens of times a year. The problem isn’t solely that security managers are confusing testing/certification (and other things) with vulnerability assessments, it’s that, by not understanding vulnerability assessments in the first place, they are probably not having them done, or at least not done well. This isn’t conducive to good security.

This article is meant to address some of the myths and misunderstandings about vulnerability assessments, including what they are, how they are done, who should do them, and what they are for (and not for).

First off, we need to appreciate that the purpose of a vulnerability assessment is to improve security. This is done in 2 ways: (1) by finding and perhaps demonstrating vulnerabilities (weaknesses) in a security device, system, or program that could be exploited by an adversary for nefarious purpose. It might also include suggesting countermeasures. And (2) by providing one of the 10 or so major inputs to an overall modern Risk Management approach to security. (See figure 1.)

**Myth: A vulnerability assessment (VA) is a test you pass.** In fact, you no more pass a vulnerability assessment (VA) than you “pass” marriage counseling. “Passing” a VA can certainly not mean there are no vulnerabilities, or even that all vulnerabilities have been mitigated. Any given security device, system, or program has a very large number of vulnerabilities, most of which you will never know about. (Hopefully the same is true for the adversaries.) We believe this because every time we look at a new security device, system, or program a 2<sup>nd</sup> or 3<sup>rd</sup> time, we find new vulnerabilities that we missed the first time, and vulnerabilities that others missed, and vice versa. (Even if all vulnerabilities were to be found, how could you ever prove there are no more?) A VA is never going to find all the vulnerabilities, but hopefully VAers can—by thinking like the bad guys—find the most obvious, the most serious, and the most likely to be exploited.

What people sometimes mean when they say that they “passed a vulnerability assessment” is that they took the results of the VA as one of the inputs, then made a subjective, context-dependent value judgment about whether their security is “adequate” for the specific security application of interest. While it may be completely necessary and

---

\*This paper was not peer reviewed. A version of this paper first appeared in *SecurityInfoWatch.com*, August 6 & 13, 2013.

reasonable to make such a judgment, that decision belongs in the domain of the security manager, not the vulnerability assessor.

**Myth: The purpose of a VA is to accomplish one or more of these things: test performance; do quality control; justify the *status quo*; apply a mindless stamp of approval; engender warm and happy feelings; praise or accuse somebody; check against some standard; generate metrics; help out the guys in the marketing department; impress auditors or higher ups; claim there are no vulnerabilities; endorse a product or security program; rationalize the expenditures on research and development; certify a security product as “good” or “ready for use”; or characterize the ergonomics, ease of use, field readiness, or environmental durability.** Certainly, some of these issues are very important and may have a bearing on security vulnerabilities, but they are not the focus or the purpose of a VA.

**Myth: A vulnerability assessment (VA) is the same thing as a threat assessment (TA).** Threats are who might attack, why, when, how, and with what resources. A Threat Assessment (TA) is an attempt to identify threats. Vulnerabilities are what these threats might exploit for nefarious purposes.

**Myth: A TA is more important than a VA.** Effective VAs and TAs are both essential for good security and for modern Risk Management. A TA, however, entails speculations about groups and people who may or may not exist, their goals, motivations, and resources. TAs are often *reactive* in nature, i.e., focused on past incidents and existing intelligence data. Vulnerabilities, on the other hand, are right in front of you (if you will open your eyes and mind), and can often be demonstrated. VAs are thus typically more *proactive* in nature.

If anything, an effective VA may be more important than a TA. If you get the threats exactly right, but have no clue as to your vulnerabilities, you are probably at significant risk. If, on the other hand, you get the threats at least partially wrong (which is likely), but you have a good understanding of your vulnerabilities and have mitigated those you can, you may well have good security independent of the threats.

**Myth: These techniques are effective for finding vulnerabilities: security survey (walking around with a checklist), security audit (are the security rules being followed?), feature analysis, TA, design basis threat (DBT), fault or event tree analysis (from safety engineering), Delphi Method (getting a consensus decision from a panel of experts), and the CARVER method (DoD targeting algorithm).** The truth is that many of these techniques—while very much worth doing—are not particularly effective at discovering new vulnerabilities. The last 4 aren’t even about discovering vulnerabilities at all, but rather are tools to help decide how to field and deploy your security resources. None of these make much sense for “testing” security (e.g., DBT) because the logic in using them that way is circular.

**Myth: Safety or safety-like analyses are good ways to find vulnerabilities.** In fact, safety is a very different kind of problem because there is no malicious adversary attacking deliberately and intelligently at the weakest points. Safety issues aren’t completely



irrelevant for infrastructure security, for example, but they are limited in their ability to predict many malicious attacks.

**Myth: These things *are* the vulnerabilities: the assets to be protected, possible attack scenarios, security delay paths, or security/facility features.** These things are important in analyzing vulnerabilities and understanding your security, but they are not vulnerabilities in and of themselves.

**Myth: One-size-fits-all.** The man on the telephone wanted his product to be given a single test and certification that would apply to nuclear safeguards applications though security for the local parish's bingo supplies; for use by highly trained security professionals and by amateurs; in conjunction with many layers of effective security or no additional security; and against adversaries that ranged from technically sophisticated nation-states through disruptive elementary school kids. Obviously, no single test or certification could have much meaning across such a wide range of security applications. The same thing is true for VAs; whenever possible, they should be done in the context of the actual security application and adversaries of interest.

**Myth: Past security incidents will tell you all you need to know about vulnerabilities.** Looking only at the past is a good way to overlook the risk from rare but catastrophic attacks. (Think 9/11.) Moreover, the world is now rapidly changing, and what was once true may no longer be true. Good security requires imagination, peering into the future, and seeing things from the adversary's perspective.

**Myth: A software program or package will find your vulnerabilities.** There is nothing wrong with using a software program as a VA starting point, as a checklist, and as a way to stimulate your thinking. But with security, the devil is in the details. No security program or package is going to understand your particular security application, facility, personnel, and adversaries in sufficient detail to adequately identify on-the-ground vulnerabilities. A software app is unlikely, for example, to recognize that frontline security officer Bob falls asleep every day at 3 pm.

**Myth: Vulnerabilities are Bad News.** In fact, vulnerabilities are always present in large numbers; finding one means you can do something about it. This concept is a tough sell to security managers ("Oh boy we found another hole in the fence, isn't that great!") but it is, we firmly believe, the correct way to look at vulnerabilities and VAs.

**Myth: You can eliminate all your vulnerabilities.** The unfortunate fact is that some vulnerabilities can't be fully eliminated, you just have to live with them (and that's ok as long as you are aware they exist).

**Myth: The ideal scenario is when a VA finds zero or just a few vulnerabilities.** The reality is that any such VA should be redone by VAers who are competent and/or willing to be honest with you.

**Myth: A VA should be done at the end, when the product is finished or the security program is ready to be fielded.** In fact, VAs should be done early and iteratively. If you wait until the end, it can be very difficult, expensive, and psychologically/organizationally challenging to make necessary changes. In our experience, having intermittent VAs (even from the very earliest design stages) while a security product or program is being developed is a useful and cost-effective way to improve security.

**Myth: It's usually hard to fix vulnerabilities.** This is not true. In our experience, simple changes to the design of a security device, system, or program (or even easier changes to how it is used) frequently improve security dramatically. Vulnerabilities can often be mitigated—or sometimes even eliminated—without spending a lot of extra money.

### Who Should Do VAs?

The old adage that “it takes a thief to catch a thief” has some merit for VAs. This isn't to say you should necessarily hire a bunch of felons to look at your security. What it does mean is that the VAers need the right mindset. Design engineers and people with lots of brains and security experience aren't automatically good at doing VAs. After all, if you are thinking like all other security professionals instead of thinking like the bad guys, you're unlikely to be able to predict what they might do. Indeed, it can be surprisingly hard for engineers and security professionals to think like the bad guys when they have spent their lives and careers desperately wanting security to work.

So what kind of mindset should VAers have? They should be psychologically predisposed to finding problems and suggesting solutions, and ideally have a history of doing so. In our experience, the best VAers have a hacker mentality and tend to be highly creative, narcissistic, skeptical/cynical, questioners of authority, loophole finders, hands-on types, and smart alecks/wise guys, as well as people skilled with their hands (e.g., artists, artisans, craftspeople) who are interested in how things work.

Another old adage also applies well to VAs: “A prophet is never honored in his own land.” As we can personally attest to, there is a lot of “shoot the messenger” syndrome (retaliation) associated with identifying security problems. Indeed, while vulnerability assessors are sometimes called “red teamers” (from the Cold War era), or “black hatters” (from cowboy westerns), they are also often called worse things that can't be repeated in polite company.

Doing a VA for your own organization can be a threat to your career, or at least place real or perceived pressure on the VAers not to find vulnerabilities. This is one of the reasons that VAers should ideally be chosen from outside the organization. Wherever they come from, however, VAers must be able to be independent and allowed to report whatever they discover. There can be no conflicts of interest. The VAers cannot be advocates for the security product or program under study, nor benefit from its implementation. (See the sidebar on the VA Report.)

## **Other Misunderstandings About VAs**

There are other common VA problems and mistakes that should be avoided. Sham rigor—thinking that the VA process can be done in a rigorous, formalistic, linear, reproducible, and/or quantitative manner—is a common problem. In fact, effective VAs are creative, right-brain exercises in thinking like somebody you're not (the bad guys); the VA process is difficult to formalistically characterize, reproduce, or automate. (See figure 2.)

Another common VA mistake is to focus on high-tech attacks. In our experience, relatively low-tech attacks work just fine, even against high-tech devices, systems, and programs. It is also a big mistake to let the good guys and the existing security infrastructure and strategies define the problem—the bad guys get to do that. We must also be careful not to let envisioned attack methods solely define the vulnerabilities—it ultimately has to work the other way around.

Yet another common mistake is placing arbitrary constraints on the VA in terms of scope, time, effort, modules, or components. Often, software experts are brought in to look at the software, mechanical engineers to look at the physical design, electronics experts to examine the electronics, etc. While there is nothing wrong with using experts, the fact is that many attacks occur at the interface between modules or between disciplines. An effective VA needs to employ a holistic approach and people who can think holistically.

## **In Conclusion**

There is nothing wrong with testing and certifying security devices, systems, and programs—assuming the tests and certifications are relevant, meaningful, and well thought through. (Many are not, in our view; sometimes being pointless or even making security worse! ISO 17712 for cargo seals is, we believe, a classic example of a harmful security standard with its misleading terminology, flawed assumptions, sloppy reasoning, and overly-simplified concepts about tamper detection.) But testing and certifying is something quite apart from undertaking a vulnerability assessment. Be sure you understand what a vulnerability assessment is (and is not), how it should be done and by whom, and why it is important to do it.

## **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.

## Sidebar: The VA Report

The difficult part of any VA isn't finding vulnerabilities and suggesting countermeasures, it's getting security managers and organization to do something about them. In physical security, unlike cyber security, making changes is sometimes viewed—unhelpfully—as admitting to past negligence.

The good things need to be praised in the VAT report at the start, because we want them to continue (they might be an accident), and we want to prepare the reader to be psychologically ready to hear about problems. It is important to at least suggest possible countermeasures in the report. Security managers and organizations will be reluctant to deal with the security problems if there aren't at least some preliminary fixes available. (Often, however, security managers can devise more practical countermeasures than the VAers starting from their suggestions.) Findings should be reported to the highest appropriate level without editing, interpretation, or censorship by middle managers or others fearful of what the report may say.

The written VA report should also include all the following:

- identity & experience of the VAers
- any conflicts of interest
- any *a priori* constraints on the VA
- time & resources used
- details, samples, demonstrations, and videos of attacks
- time, expertise, & resources required by an adversary to execute the attacks
- possible countermeasures
- a sanitized, non-sensitive summary of the findings if the sponsor wishes to take public credit for the VA; statistics are helpful.

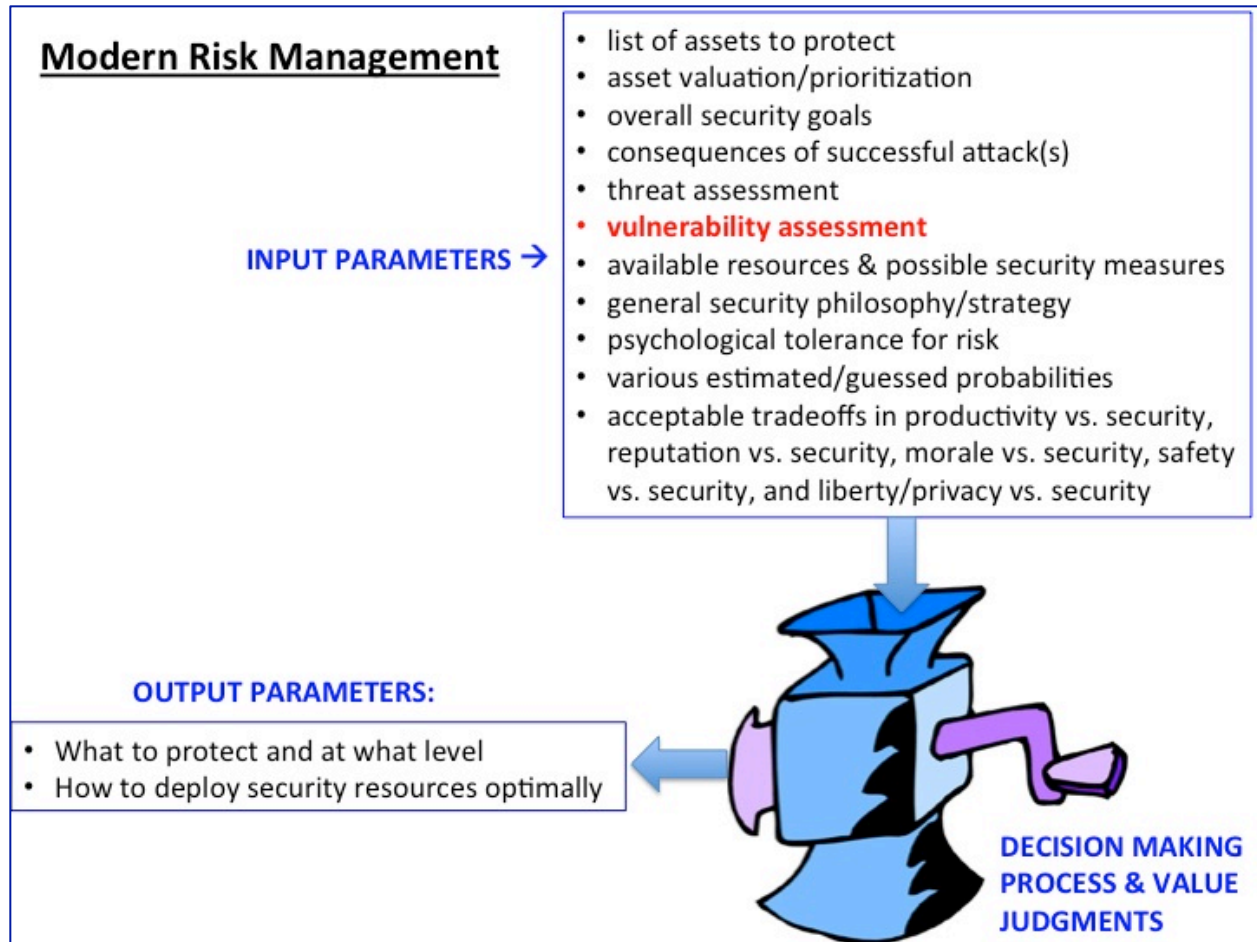
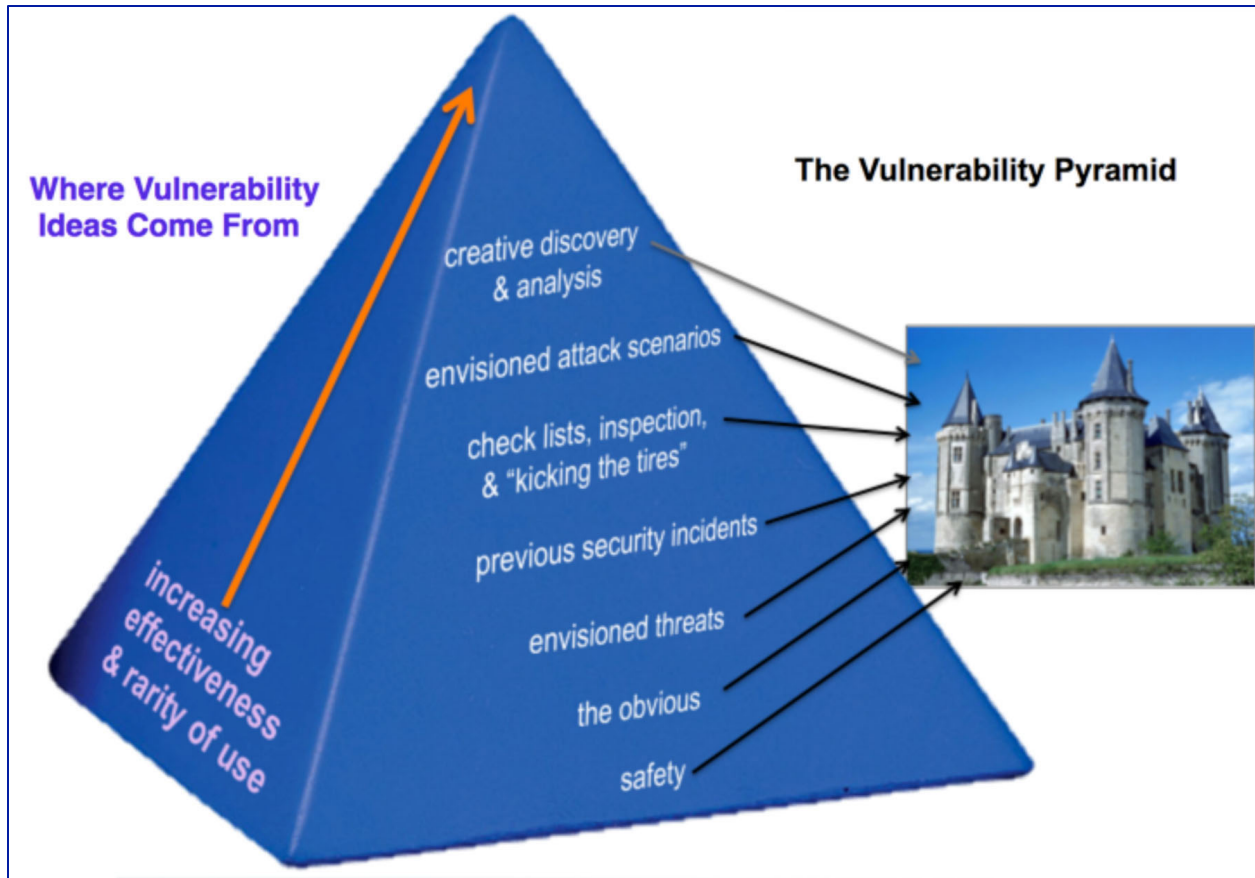


Figure 1 - Modern Risk Management.



**Figure 2** - The Vulnerability Pyramid. Where vulnerability ideas come from. The higher up you go, the more effective (but also the less common and formalistic) the technique.

## **What Vulnerability Assessors Know That You Should, Too\***

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

### **Vulnerability Lessons**

We've done vulnerability assessments on over 1000 physical security and nuclear safeguards devices, systems, and programs. This includes high-tech and low-tech, government and commercial. This work was done for more than 50 government and international agencies, private companies, and NGOs. This article explains some of the things we've learned.

First off, security managers and others often don't seem to understand what a vulnerability assessment (VA) is, or what it is for. The purpose of a VA is to improve security by finding and demonstrating security weaknesses, and perhaps suggesting possible countermeasures. A VA also often serves as one of the inputs to modern Risk Management.

A VA is not a test you "pass" or some kind of "certification". (You no more pass a VA than you pass marriage counseling.) A VA is not performance, compliance, readiness, ergonomics, or quality testing (though these things may have a bearing on vulnerabilities). It's not a threat assessment. Don't do a VA to justify the status quo, praise or criticize anybody, rationalize the R&D expenditures, endorse a product or security strategy, or apply a mindless stamp of approval. The ideal outcome of a VA is not to find zero or just a few vulnerabilities. If this happens, the VA should be redone by personnel who are competent, diligent, and honest.

The common idea that vulnerabilities are bad news is, we firmly believe, quite incorrect. Vulnerabilities are always present in large numbers; when you find one, that means you can do something about it. Admittedly, however, it is difficult to convince security managers that, "Hey, we found another hole in the fence, isn't that great news!"

Indeed, it's a mistake to think that there are just a small number of vulnerabilities. There are usually a very large number, even for a simple security device, much less a complex security program. You will never know about many (perhaps most) of your vulnerabilities but hopefully a good VA can find the most obvious and serious vulnerabilities, and the ones most likely to be exploited by adversaries.

---

\*This paper was not peer reviewed. A version of this paper first appeared in *Asia Pacific Security Magazine* 50, 40-42, Aug/Sept 2013.



Another serious security problem has to do with undue faith in security devices and high tech. For example, contrary to popular opinion, biometric signatures can usually be cloned fairly easily, but an adversary rarely needs to bother because biometric devices are usually so poorly designed that they can be easily compromised. And the civilian Global Positioning System (GPS) can be easily spoofed remotely (as we were the first to demonstrate in 2002), not just jammed. Spoofing—sending the wrong time and location information—can be done even by adversaries with little understanding of GPS, computers, electronics, or radio frequency transmission. GPS was never intended as a security technology.

RFIDs (radio frequency identification tags) are another inventory technology that does not typically provide serious security because RFIDs are usually easy to counterfeit (even for hobbyists) and are almost always easy to lift—even those with supposed tamper detection capabilities. “Lifting” means moving the RFID to another object or container without this being detected. (Prox cards are often just RFIDs, and they and their access control readers are usually easy to tamper with.) Moreover, it is typically easy to tamper with the RFID reader or spoof it from a distance. Encrypting the RFID signal is not a silver bullet.

Unfortunately, data encryption or authentication are often the focus of much wishful thinking. These techniques are useful for securing public communication between two points in space and time, but provide meaningful security if and only if all the following conditions are met: the sender and receiver are physically secure, physical or electronic tampering can be reliably detected, the insider threat has been mitigated, the secret keys(s) are secure and well chosen, and there’s a secure cradle-to-grave chain of custody on the hardware and software. Usually none of these things are true, much less all of them! The reality is that if you don’t have good security before you deploy encryption or authentication, you won’t have it after.

Speaking of chain of custody, this is not, as many organizations seem to believe, a piece of paper on which arbitrary individuals scribble their names or initials for the purpose of looking like there is some kind of security in place. Instead, a real chain of custody is a detailed, well thought-through *process*. A secure chain of custody is particularly important for security devices because typically all it takes is 15 seconds of access (with a lot of practice) to compromise them permanently. This can be done by an adversary at the factory, vendor, loading dock, while in transit, prior to installation, or after installation. Testing an access control device to see if it behaves normally is of little use in detecting when it has been compromised.

When it comes to wishful thinking, tamper-indicating seals exist inside their own giant universe of wishful thinking. Current seals are, in our view, poorly designed and almost universally poorly used. If seal installers and inspectors have detailed knowledge of the most likely attack scenarios, and plenty of hands-on training, they stand a much better chance of detecting tampering, but such knowledge and training is rare, even for nuclear safeguards applications!

The existence of the ISO 17712 standard for cargo seals is particularly unhelpful. It contains misleading terminology, sloppy reasoning, over simplification of complex issues, and confusion about VAs, or even what a seal is. Certainly an ISO 17712 “certified” seal should not be deemed superior to an uncertified one.

Regarding tamper detection, mechanical tamper switches and light sensors do not provide serious security.

We believe that tamper-evident packaging on food, drugs, and other consumer products is mostly about reducing jury awards, not serious tamper detection. Even the relatively unimaginative designs currently in use would be better if the customer were to be given more useful information.

Product counterfeiting is an especially serious worldwide problem. In our experience, most (all?) product anti-counterfeiting tags can be easily and cheaply counterfeited sufficiently to fool a consumer, pharmacy technician, shop clerk, or customs official. (Incidentally, encryption or data authentication have no significant role to play for product anti-counterfeiting. They are red herrings, as is often the case for data encryption/authentication.)

We’re partial to the use of virtual numeric tokens for dealing with product counterfeiting. This is not the same thing as serialization or track & trace. Companies who have used virtual numeric tokens could do a number of things much better, in our view.

## **Other Lessons Learned**

Other things we’ve learned over the years include:

- (1) Vulnerabilities are often blatantly obvious to outsiders.
- (2) Engineers don’t understand security; they tend to have a mindset and culture that prevents them from thinking like the bad guys.
- (3) Few organizations deal effectively with the insider threat. Mitigating employee and contractor disgruntlement is a particularly effective tool (and also has important benefits for productivity, morale, and retention/recruitment) but few organizations do it well, if at all. The Human Resources (Personnel) Department in most large organizations could theoretically be a very powerful tool for mitigating disgruntlement, but most HR Departments just make things worse.
- (4) The security protocols for employee (or athlete) drug testing are often quite poor. Given the implications for national security and public safety, not to mention people’s careers, livelihood, and reputations being on the line, this should be one area where we get security right!

(5) Organizations and security managers who cannot tolerate questions, concerns, and criticisms about their security almost always have bad security. If they cannot envision security failures, they usually won't be able to prevent them.

(6) Firing people after security incidents does not lead to accountability or better security. It just leads to cover-ups, finger pointing, scapegoating, denial, passing the buck, and Compliance-Based security—a particularly pernicious form of Security Theater.

Finally, it is clear to us that “Security by Obscurity” does not work, at least in the long run. People and organizations cannot keep secrets (see for example, Manning and Snowden), and the bad guys usually know what you are doing anyway. Somewhat counter-intuitively, security is usually better when it is transparent, allowing review, criticism, buy-in, accountability, and improvement.

## **Conclusion**

If all this sounds pretty depressing, welcome to the world of the vulnerability assessor! Thomas Carlyle (1795-1881) famously called economics the dismal science. We think he was wrong. Security is. At the very least, security is very difficult, maybe ultimately not fully possible. It's hard to counter determined adversaries.

Given this situation, we think it is worth keeping in mind the old adage that “if you are happy with your security, then so are the bad guys.” Forewarned is forearmed.

## **Disclaimer**

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

## **The “Levels of Analysis” Problem with Critical Infrastructure Risk**

Brian Nussbaum, Ph.D.  
Project on Violent Conflict  
Rockefeller College of Public Affairs  
University at Albany, State University of New York  
[Bnussbaum@albany.edu](mailto:Bnussbaum@albany.edu)

We in the world of risk assessment, particularly those of us focused on assessing risk to critical infrastructure, face a series of tough challenges. The threats are myriad, the vulnerabilities hard to mitigate, and the potential consequences are huge. Critical infrastructure varies hugely across sectors, depending on definitions of “criticality” and among publicly-owned, privately-owned, and a series of hybrid or in-between models of ownership. It is an almost intractably large problem. Therefore we make incremental progress in adapting varying risk assessment methodologies from one field to another, from one infrastructure sector to another, from private to public organizations and vice-versa, in a kind of consistent tinkering and trial-and-error. This is, in fact, a reasonable and valuable approach that enables us to see what elements of others work apply to our own, and which ones are not well suited. Ultimately this has greatly improved our ability to assess risks to infrastructure. That said, we still have large lacunae, and a need for some important innovations. One of the most serious problems we face in assessing critical infrastructure risk is a “levels of analysis” problem.

In recent years, as infrastructure protection has become a bigger part of the Homeland Security enterprise—both with 2009 release of the National Infrastructure Protection Plan (NIPP)<sup>1</sup> and the growth of concerns about cyber security—there seems to largely be a consensus that improved risk assessment and risk management tools are likely to be important to address this insurmountably large problem. With that idea in mind, many very smart people have been very focused on applying risk analysis (and component analyses of threats, vulnerabilities, and consequences) to issues of infrastructure protection and resilience. However, certain levels of analysis have received most—if not quite all—of the attention of these resources. The asset and system level are naturally where most physical risk assessments take place; and rightly so, because most owners and operators own and operate assets and systems. To a somewhat lesser extent, there has been some analysis of infrastructure protection at the national level; which again makes much sense since the Federal Government has funded much of the research on infrastructure risk assessment (through the Department of Homeland Security, the Department of Energy, etc.)

The levels that have been largely left behind in this expansion of analysis are the infrastructure sector (though some industry organizations have done yeoman’s work on that front<sup>2</sup>) and particularly the sub-national jurisdictional level: municipalities and states. Cities and states have overwhelmingly been left to themselves to conceptualize and measure infrastructure risk. With a few publicized exceptions (the Los Angeles and New York City Police Departments spring to mind) jurisdictional level infrastructure risk

assessment has been largely haphazard, ad hoc, not subject to any sort of peer review, and sometimes based on the problematic adaptation of inappropriate (or at least incomplete) asset and system level analytic tools.

In their recent survey of critical infrastructure risk assessment methodologies, the European Union mentioned, but did not sufficiently expand upon this same issue, which it termed the “domain of applicability” problem.

*Methodologies developed for certain assets are well defined, tested and validated and the vast majority follows the linear approach already mentioned. However, methodologies that aim at assessing risks at a higher level, e.g., networked systems, require further refinement. Detailed risk assessment is not applicable any more and a certain level of abstraction is necessary...*

*...The vast majority of the existing work has been sectoral and mostly at asset level. These methodologies have been then extended to cope with networked systems. This reflects the natural evolution of risk assessment methodologies existing already at organizational level to address issues at sectoral level. These methodologies reveal their limitations when cross-sectoral issues have to be addressed.<sup>3</sup>*

This constellation of problems with State and Local infrastructure risk assessment exists for a number of reasons. It's certainly easier to spend homeland security grant funds on radios and chemical suits than it is on developing risk assessment methodologies—and often more appropriate to do so depending on the jurisdiction. In many cases, jurisdictions look into competing assessment models, and find them ill-suited for their needs. (Arguably they are quite right in that assessment, but more on that later) In some cases, these sorts of analyses have been outsourced to contractors (with wildly varying levels of sophistication and value), which is not a bad thing *per se*. Though this outsourcing does often leave the jurisdiction with a product, typically an assessment and/or a slide deck, rather than with a replicable process or an internal capability to assess risk.

Why is it that so many state and local officials have had trouble choosing from the existing risk assessment models? Why is it that so many of the models used by contractors have been incomplete or poorly suited to the problems they claimed to address? This is, at least in part, a result of a broad failure in the risk assessment community to treat these jurisdictions as serious levels of analysis in terms of infrastructure risk. Additionally, it is also a result of two structural problems. The first problem is the increasing complexity of infrastructure at the jurisdictional level; while assets are reasonably simple and systems can be simple or complex, at the municipal or state level the risk analyst is looking at a geo-political area that is a collection of many unrelated assets and systems (as well as pieces of systems) that overlap in physical space and have numerous types of ownership (public v. private) and owners (Company A vs. Company B). The second major problem is that these kinds of risk assessments would require fundamentally different kind of inputs (and produce fundamentally different kind of outputs) than risk assessments at the asset or system level. The further down the narrowing “level of analysis” cone we go (see figure 1), the better understanding we have of the risk components we need to make an assessment.

Assessing the threats associated with, and the vulnerabilities and potential consequences of, an attack on a bus (asset level) is relatively straight forward when compared with assessing the risk of a particular bus system (system level). Moving up the next tier of complexity to the transportation sector (sector level) more generally is even less clear. Finally, assessing the threats, vulnerabilities, and potential consequences of a city or state is orders of magnitude harder. (See figure 2.) In each case, more and more sources of expertise are required. An asset level assessment on a bus would require someone with physical security knowledge and perhaps a bus mechanic or engineer. A system level assessment would also require managers and logistics personnel who understand the interplay of the system components. A sector level assessment would require the same as a system level assessment, but from each system associated with the sector (busing, rail, maritime, etc). Finally, a jurisdictional level analysis would require the same across many sectors, including an understanding of how first responders, business, and the citizenry would react and interact.

We actually have a series of good assessment methodologies designed to help us understand vulnerabilities and risks faced by assets and systems. Variations on the Risk Analysis and Management for Critical Asset Protection (RAMCAP),<sup>4</sup> Criticality Accessibility Recuperability Vulnerability Effect and Recognizability (CARVER)<sup>5</sup> and Probabilistic Risk Assessment (PRA)<sup>6</sup> methodologies are widely used for asset and system level analysis, and appropriately so. There are other methods that have been used as well, though less widely and arguably in a less mature and developed way, including approaches like Design Basis Threat (DBT)<sup>7</sup> and the Delphi Method.<sup>8</sup>

While the risk assessment community has been involved in the trial and error application of various risk models to various problems, there have been some difficulties with attempting to use models like these to look at sector and jurisdiction level risks. (See figure 3.) In many cases, these existing approaches are not appropriate for the kinds of assessments necessary at these “higher” levels of abstraction like the sector or city/state. Because these methods are designed for more discrete tasks (assets and systems) they require specific inputs; when applied to less narrow tasks using more complex or vague inputs they often provide an illusion of precision in their outputs that misrepresents the higher levels of uncertainty that are inevitable in a municipal or state level risk assessment. The differing level of granularity required for inputs, the differing level of uncertainty inherent in the outputs, and insufficient or inappropriate operating assumptions make the application of many common infrastructure risk assessment tools problematic when used above the asset or system level.

There have been a number of relatively recent examples of attempts to use complex systems modeling approaches to infrastructure modeling—through Hierarchical Multilevel Modeling (HMM)<sup>9</sup> and multiformalism<sup>10</sup>. Too often, however, these more complex approaches have run into the problem that the European Union saw in its assessment of many systems approaches, namely that, “...representing all assets of a networked system at the highest level of detail (mostly an operator’s approach) leads to unprecedented complexity that is out of the scope for policy and decision makers.”<sup>11</sup> Namely, when the

inputs are granular (the “*operator’s approach*”) and the assessment system complex and often opaque, the higher level of analysis decision makers—typically jurisdictional governmental officials—are given assessment outputs that are incomprehensible or, even worse, misleading. These approaches have run into the problem of not accepting that there is sometimes a need for abstraction as aggregation occurs, and that refusal to lose granularity can result in “unprecedented complexity” that is very much “outside the scope for policy and decision makers.”

A simple answer to this problem would be to suggest that risk assessments simply not be done above the asset and system level; the logic being that if we don’t have the appropriate tools to do the job, it is not a job we should be doing. This is not a tenable approach for one key reason: these assessments are being done regardless. They are either being done explicitly (with bad or inappropriate tools) or implicitly (with intuition rather than a transparent and replicable process) by officials at cities and states across the country. Rather than throwing our hands up in the air and ignoring municipal and state level infrastructure assessments, we in the risk assessment community should be taking the many valuable insights that the existing frameworks have and seeing how we can—through further trial and error—apply them appropriately to assist the many public servants across the country working on this intractable problem.

The misapplication of analytic tools is not a problem unique to critical infrastructure risk assessment, nor even just to the field of risk assessment. The Federal Emergency Management Administration (FEMA) faced similar troubles in its attempts to measure preparedness capabilities nationally. FEMA, through its Cost-To-Capability (or C2C) program attempted to measure the effectiveness of homeland security grant dollars. The C2C process was widely panned by state and local stakeholders, and it faced such strong opposition in Congress that it had to be scrapped. One critic, a former DHS official, argued on the website of Emergency Management magazine that it appeared to be largely a problem of misapplying a tool in an attempt to do too many things at once: “The bottom line is assessing capabilities and measuring the impact of homeland security investments, whether they be federal grant funds or state or local general funds, is a very complex endeavor that requires a “system of systems” approach. A single, one size fits all tool cannot manage such a huge task in a country as large and diverse as the United States.”<sup>12</sup>

So, too, is it with risk assessment. The tools we have are often very powerful, but if we misapply them to levels of analysis for which they were not designed, we will often face serious stumbling blocks. That said, since we are not alone in the problems we face, we have many other communities of smart and hardworking professionals from whom we can learn important lessons about how to most effectively use our analytic tools.



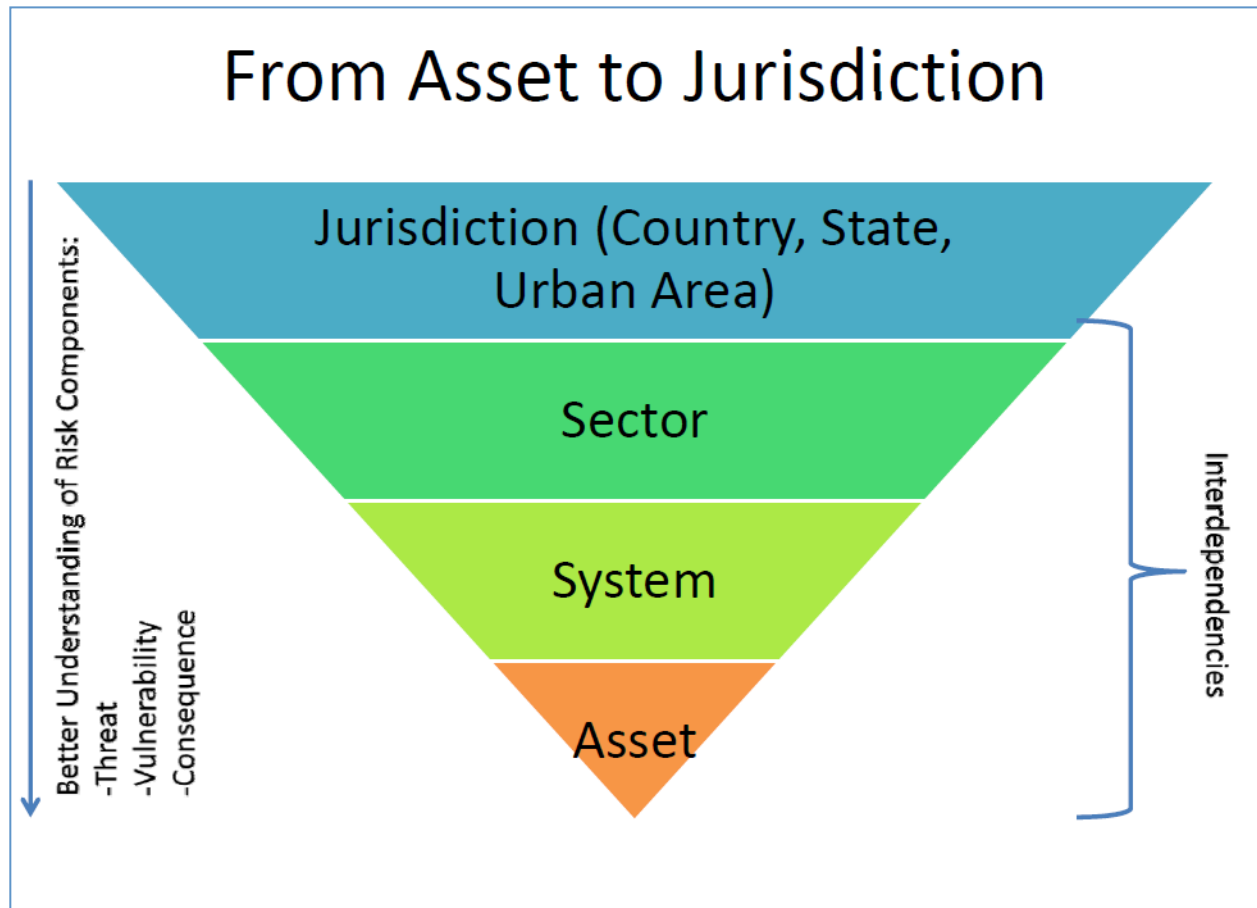


Figure 1 - The Inverted Pyramid of CI Risk Assessment. Risk analysts have fairly strong understandings of the risk components (Threat, Vulnerability, and Consequence) at the lower levels of the pyramid—the Asset and System levels—because that is where most owners and operators have historically done their analysis. Higher levels of analysis, those of industrial (“sector”) and political (“jurisdiction”) groupings, have less clear risk components because the people tasked with assessment at those levels do not typically own or operate much of the infrastructure. Interdependencies between assets, systems, sectors, and jurisdictions further complicate matters.

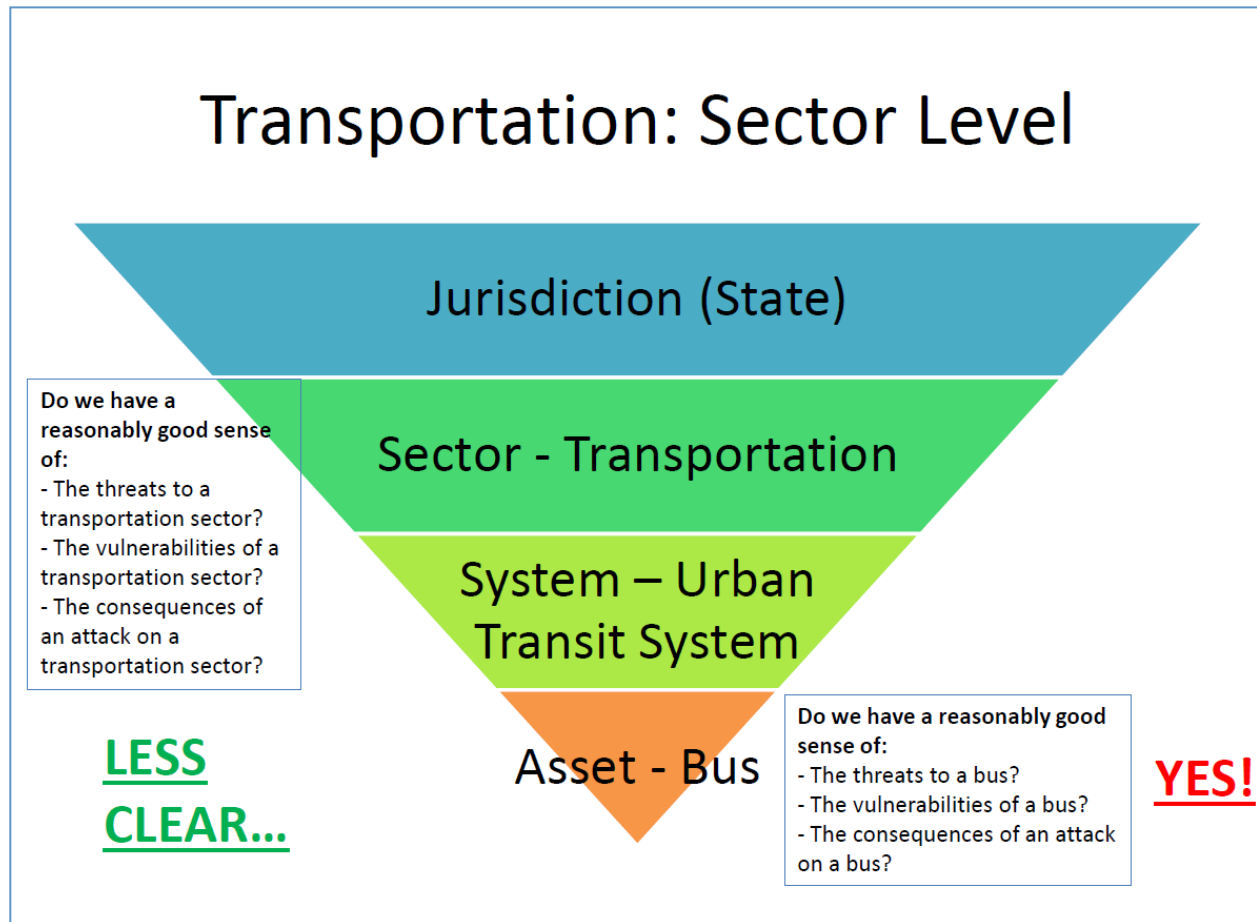


Figure 2 - The Inverted Pyramid of CI Risk Assessment—Example of Transportation. Assessing the risk to an asset (in this case a bus) is not a terribly complicated proposition. Assessing the risk to the system the bus is part of, an urban transit system, is more complicated—but probably a reasonable task. The threats, vulnerabilities, and consequences of an attack or mishap are reasonably concrete and tractable. However as the level of analysis rises to the broader sector (“transportation”) or jurisdictional level (“state”), the kinds of inputs that are reasonable for risk components change and become more problematic, as to the outputs that would be expected from such an assessment.

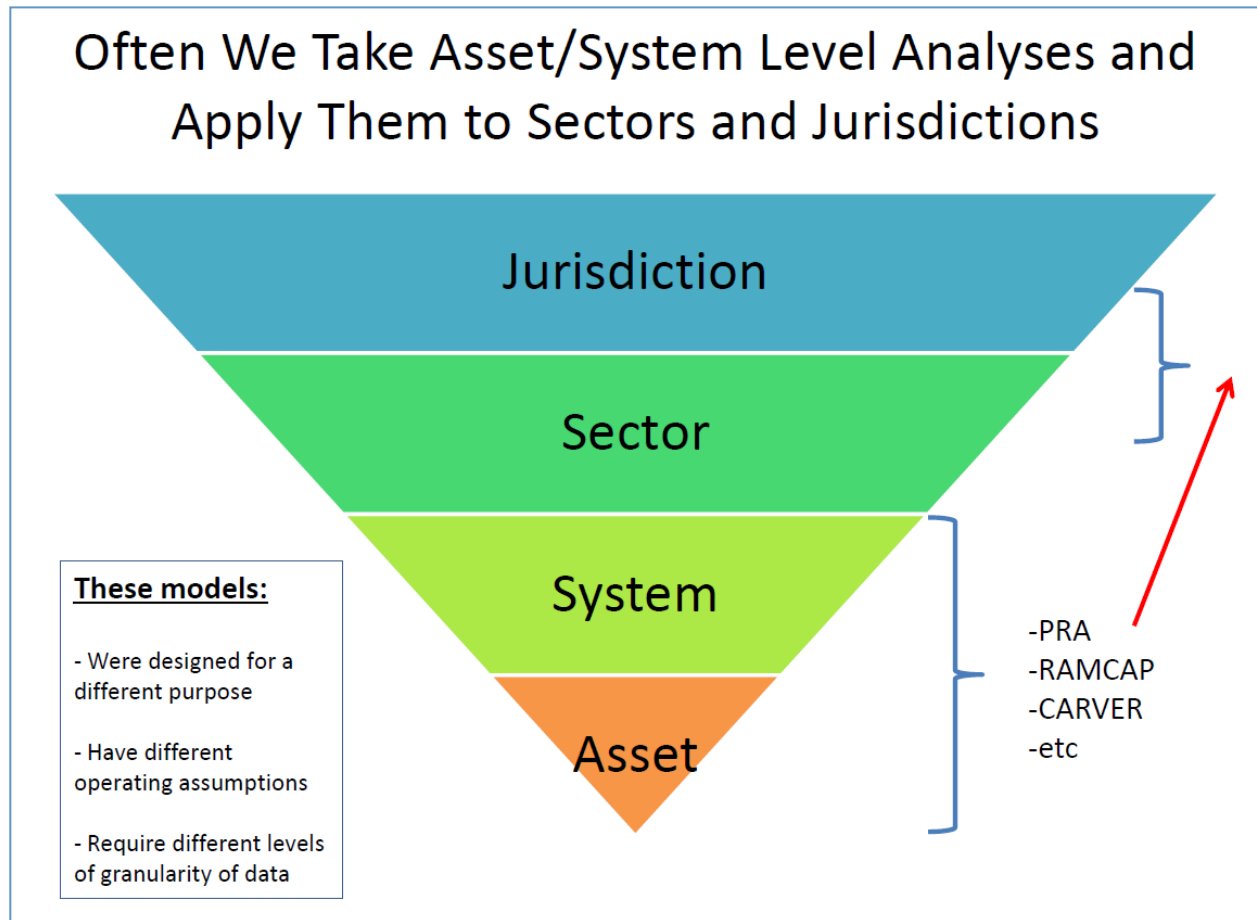


Figure 3 - The Problem of Moving Risk Assessment Methodologies “Up” the Pyramid. Many risk assessment methodologies that function quite well at the asset or system level (examples include PRA, RAMCAP, CARVER, etc.) do not translate to “higher” levels of analysis on the pyramid. This is because these well-established but narrower models require levels of granularity of data as inputs that are not reasonable to provide at the aggregate level, or that they have vastly different operating assumptions than would be appropriate to a diffuse industrial sector or jurisdiction.

- 
- <sup>1</sup> Department of Homeland Security. (2009) National Infrastructure Protection Plan. Available at: [http://www.dhs.gov/xlibrary/assets/NIPP\\_Plan.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf)
- <sup>2</sup> One example of this industrial sector work is the electrical power generation and distribution industry. Work by the North American Reliability Corporation (NERC) and other industry groups – in conjunction with government partners like the Federal Energy Regulatory Commission (FERC) – has gone a long way toward improving risk assessment and risk mitigation processes and ultimately electrical reliability. While there are critics of NERCs work, particularly in fields like cyber security, it is an example of how an industry group (in this case a not-for-profit) can play a role in improving such assessments.
- <sup>3</sup> Joint Research Center. European Union. (2012) Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. Available at: [http://ec.europa.eu/home-affairs/doc\\_centre/terrorism/docs/RA-ver2.pdf](http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf)
- <sup>4</sup> ASME Innovative Technologies. (2006) RAMCAP: The Framework. Available at: [http://www.personal.psu.edu/jsd222/SRA311/RAMCAPframework\\_Risk\\_Analysis\\_and\\_Manage.pdf](http://www.personal.psu.edu/jsd222/SRA311/RAMCAPframework_Risk_Analysis_and_Manage.pdf)
- <sup>5</sup> Food and Drug Administration. (2007) An Overview of the CARVER Plus Shock Method for Food Sector Vulnerability Assessments. Available at: <http://www.fsis.usda.gov/wps/wcm/connect/483f86d5-a566-44f8-90d5-05a16dbe3f78/CARVER.pdf?MOD=AJPERES>
- <sup>6</sup> Sandia National Laboratory. (Undated) Probabilistic Risk Assessments. Available at: <http://energy.sandia.gov/wp/wp-content/gallery/uploads/PRA.pdf>
- <sup>7</sup> International Atomic Energy Agency (IAEA) (2009) Development, Use and Maintenance of the Design Basis Threat. Available at: [http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386\\_web.pdf](http://www-pub.iaea.org/MTCD/publications/PDF/Pub1386_web.pdf)
- <sup>8</sup> Zaloom, V. Subhedar, V. (undated) Use of the Delphi Method to Prioritize Events Impacting Operations in the Maritime Domain. Available at: [http://dept.lamar.edu/industrial/ports/subhedar\\_041609\\_mdp\\_041709-r4\\_mdp\\_060609-r1.pdf](http://dept.lamar.edu/industrial/ports/subhedar_041609_mdp_041709-r4_mdp_060609-r1.pdf)
- <sup>9</sup> Haimes, Y. (2008) Identifying Risk Through Hierarchical Holographic Modeling. In Risk Modeling, Assessment and Management. Available at: <http://onlinelibrary.wiley.com/doi/10.1002/9780470422489.ch3/summary>
- <sup>10</sup> Flammini, F. Vittorini, V. Mazzocca, N. Pragliola, C. (2009) A Study on Multiformalism Modeling of Critical Infrastructures. Lecture Notes in Computer Science. Volume 5508. P336-343. Available at: [http://link.springer.com/chapter/10.1007%2F978-3-642-03552-4\\_32#](http://link.springer.com/chapter/10.1007%2F978-3-642-03552-4_32#)
- <sup>11</sup> Joint Research Center. European Union. (2012) Risk Assessment Methodologies for Critical Infrastructure Protection. Part I: A State of the Art. Available at: [http://ec.europa.eu/home-affairs/doc\\_centre/terrorism/docs/RA-ver2.pdf](http://ec.europa.eu/home-affairs/doc_centre/terrorism/docs/RA-ver2.pdf)
- <sup>12</sup> Filler, J. (2009) Congress and FEMA Examine the Cost-to-Capability (C2C) Program and the Challenges of Measuring Homeland Security Investments and Preparedness. Emergency Management. Available at: <http://www.emergencymgmt.com/emergency-blogs/homeland/Congress-and-FEMA-Examine.html>

## **Countering Violent Extremism in the United States: Law Enforcement's Approach to Preventing Terrorism through Community Partnerships**

Herbert S. Mack II

### **ABSTRACT**

The assertions of dissent in American Muslims, particularly with those who have migrated to a foreign land are often shaped by the bicultural values of assimilation. Instead of embracing the secular values of the country in which Muslim immigrants live, often times American Muslim families will identify themselves with the religious values of the country in which they originally migrated. These values are often subjective and fueled by the growing sense of socioeconomic alienation felt by second and third-generation immigrant children. This paper will explore law enforcement's strategic approach to countering domestic radicalization through community partnerships and community oriented policing.

### **INTRODUCTION**

American Jihadists influenced by al Qaeda represent a significant threat to Americans on U.S. soil. Al-Qaida and its affiliates continue to remain committed to attacking American citizens in the name of Jihad. Rather than being directed from a centralized al-Qaeda group abroad, the ever-growing trend of Islamic radicalization revolves around the social movement of al-Qaeda being an ideological reference point to extremist thought. Although adhering to extremist views does not necessarily mean a call to violent action, the ideology of al Qaeda is a precursor to action for those who commit violence in the name of jihad.<sup>1</sup> One of the biggest challenges for law enforcement is detecting homegrown radicalization that lead to acts of terrorism. The ability to prevent future terrorists from acting upon subscribed extremist thought requires effective domestic intelligence by local authorities and active community partnerships within the American Muslim community at the national and local levels. Perhaps the best defenses against violent extremist ideologies are well-informed and equipped families, local communities, and local institutions.<sup>2</sup>

### **LEGISLATIVE RESPONSE: THE USA PATRIOT ACT**

One of the most significant changes that occurred as a result of 9/11 was the development of the Homeland Security Act and the expansive police powers of The USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) which was signed into law on October 26, 2001. Due to proactive legislations such the Patriot Act, law enforcement's ability to gather and share domestic information on potential acts of terrorism was significantly expanded. The Act itself grants federal officials greater powers to trace and intercept potential terrorist communications both for law enforcement and foreign intelligence purposes. The

---

<sup>1</sup> Khalil, Lydia (2012), "US counter-radicalization strategy: the ideological challenge", Australian Strategic Policy Institute, Retrieved July 23, 2014 from the ASPI website: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=161892>

<sup>2</sup> The White House (2011), "Empowering Local Partner to Prevent Violent Extremism In The United States", Retrieved from [http://www.whitehouse.gov/sites/default/files/empowering\\_local\\_partners.pdf](http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf)

expansiveness of sharing both domestic and international information essentially improved law enforcement's ability to detect, prevent, and respond to acts of terrorism. Traditionally, law enforcement intelligence sharing was conducted in a task force environment where there was an immediate and tactical need for information. The Patriot Act ultimately acknowledged the strategic need for intelligence and the ever-growing concern of interagency communication. The lack of communication and functionality of information dissemination in the domestic realm increasingly impeded law enforcement's ability to connect critical pieces of information. The implementation of The Patriot Act created the need for a mechanism, called fusion centers, that streamlined the dissemination of information on those engaged in the radicalization process.

## **FUSION CENTERS**

Fusion centers are essentially an interdisciplinary mechanism that allows law enforcement the ability to share information. They are situated in such a way that they are used to empower front-line law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel to lawfully gather and share threat-related information.<sup>3</sup> The exchange of intelligence that takes place in fusion centers aids other intelligence and law enforcement organizations in their investigations of potential threats to national security. Fusion centers contribute to the Information Sharing Environment (ISE) through their role in receiving threat information from the federal government; analyzing that information in the context of their local environment; disseminating that information to local agencies; and gathering tips, leads, and suspicious activity reporting (SAR) from local agencies and the public.

In the post-9/11 environment, the public has expected law enforcement to adopt a proactive posture in order to disrupt terrorist plots before an attack occurs.<sup>4</sup> The challenges often presented to law enforcement, particularly when attempting to detect extremist behaviors revolves around the ability to identify the violent extremist prior to the terrorist act. President Barack Obama outlined on May 23, 2013, at the National Defense University, his administration's counterterrorism strategy, which include three areas: "targeted action against terrorists; effective partnerships; and diplomatic engagement and assistance."<sup>5</sup>

## **JOINT TERRORISM TASK FORCES (JTTF)**

In the aftermath of the September 11 terrorist attacks, the Federal Bureau of Investigation (FBI) shifted from traditional law enforcement investigations to the prevention of terrorist attacks.<sup>6</sup> The Department of Justice and the Federal Bureau of

---

<sup>3</sup> U.S. Department of Homeland Security (2013), "Fusion Centers and Joint Terrorism Task Force", Retrieved from <http://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces>

<sup>4</sup> Bjelopera, Jerome P (2013), "American Jihadist Terrorism: Combating a Complex Threat", Retrieved June 2013 from Congressional Research Service website: <http://www.fas.org/sgp/crs/terror/R41416.pdf>

<sup>5</sup> The White House (2013), "Remarks by the President at the National Defense University", Retrieved from <http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university>

<sup>6</sup> The Federal Bureau of Investigation (2013), "Fusion Centers and Joint Terrorism Task Forces", Retrieved from <http://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces>

Investigation created what is known as Joint Terrorism Task Forces (JTTF). JTTF's are multi-jurisdictional task forces that conduct investigations on plots of terrorism. Investigations conducted by JTTFs are focused on known threat actors or identified individuals who meet the thresholds established in accordance with the Attorney General Guidelines for Domestic FBI Operations to initiate assessments or investigations.<sup>7</sup>

## **DIFFICULTIES OF DETECTING RADICALIZATION**

Although the expansive powers of the Patriot Act and the development of fusion centers presented law enforcement with the greater ability to detect terrorist plots, "lone wolf actors" and Internet radicalization have become a greater challenge for law enforcement officials. This type of violent extremism is a complicated challenge for the United States, because the United States Constitution recognizes freedom of expression, even for individuals who espouse unpopular or even hateful views.<sup>8</sup> Another challenge that is often presented to law enforcement when trying to detect radicalization revolves around the individuals actually subscribing to al Qaeda ideological principles. Often times, those engaged in radical beliefs come from different socioeconomic, ethnic and religious backgrounds.

## **WHAT IS RADICALIZATION**

Radicalization is a process whereby individuals identify, embrace and engage in furthering extremist ideologies.<sup>9</sup> Radicalization that leads to violent terroristic behaviors often assigns blame and ultimately legitimizes the use of violence against those deemed responsible. NYPD officials have concluded that understanding this trend and the radicalization process in the West that drives "unremarkable" people to become terrorists is vital for developing effective counterstrategies and has special importance for the NYPD and the City of New York.<sup>10</sup> As we analyze societal trends relative to the war on terror, we are able to witness the distinct characteristics of Islamic radicalization at its core. On April 15, 2013, America experienced its most recent domestic terrorist attack. Bombing suspects Dzhokhar Tsarnaev's and Tamerlan Tsarnaev used homemade explosives to kill three people and injure 264, arguably in the name of jihad. When we use the 2013 Boston Marathon Bombing as a backdrop, we are able to see that the processes of radicalization are complex and reflect a combination of individual circumstances and ideological

---

<sup>7</sup> The Federal Bureau of Investigation (2013), "Fusion Centers and Joint Terrorism Task Forces", Retrieved from <http://www.dhs.gov/fusion-centers-and-joint-terrorism-task-forces>

<sup>8</sup> The White House (2011), "Empowering Local Partner to Prevent Violent Extremism In The United States", Retrieved from [http://www.whitehouse.gov/sites/default/files/empowering\\_local\\_partners.pdf](http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf)

<sup>9</sup> Southers, Erroll G. (2013), "The Boston Bombings: A First Look", United States House of Representatives Committee on Homeland Security, Retrieved July 2013 from <http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SouthersE-20130509.pdf>

<sup>10</sup> Mitchell D. Silber and Arvin Bhatt (2007), "Radicalization in the West: The Homegrown Threat New York Police Department", Retrieved from [http://www.nyc.gov/html/nypd/downloads/pdf/public\\_information/NYPD\\_ReportRadicalization\\_in\\_the\\_We st.pdf](http://www.nyc.gov/html/nypd/downloads/pdf/public_information/NYPD_ReportRadicalization_in_the_We st.pdf)



motivations that often elude law enforcement. Personal crisis and political cause are also paired in the process.<sup>11</sup>

### GRIEVANCE VERSES IDEOLOGY

The destructive social tactics of those who subscribe to al Qaeda's extremist ideology affects American society as a whole. Although al Qaeda's exhortations to violence lack the ability to resonate among the vast majority of Muslim Americans, radicalization ultimately lies at the intersection of grievance and ideology.<sup>12</sup> Although it is true that the formations of separate communities have created a desire for Muslims to stay true to religious practices, this is no different from any other ethnic group within the United States. The problem then occurs when individuals within that community subscribe to violent extremism as a means to vocalizing their socioeconomic conditions and law enforcements ability to stop would be terrorists by detecting radicalization. While the picture of the radicalization of the Tsarnaev brothers remains incomplete, many have already pointed to what appear to be obvious warning signs of violence.<sup>13</sup> Indicators included such things as:

1. Advocating violence, the threat of violence, or use of force to achieve goals that are political, religious, or ideological in nature.
2. Advocating support for international terrorist organizations or objectives.
3. Providing financial or other material support to a terrorist organization or to someone suspected of being a terrorist.
4. Association with or connections to known or suspected terrorists.
5. Repeated expression of hatred and intolerance of American society, culture, government, or principles of the U.S. Constitution.
6. Repeated visiting or browsing of Internet websites that promote of advocate violence directed against the United States or U.S. forces, or that promote International Terrorism or terrorist themes without official sanction in the performance of duties.

In the case of the Tsarnaev brothers, it is extremely important that we review the actions law enforcement officials prior to the Boston Marathon Bombing. The causes of radicalization can be attributed to the changing nature of American society where foreign nationals are often ridiculed and not seen as being "American". Going back to the subject of Boston Marathon Bombing suspect Tamerlan Tsarnaev, in early 2011, the FBI received information about terror suspect Tamerlan subscribing to radical Islam and his travels to southern Russia to join an underground group. The FBI also interviewed Tamerlan Tsarnaev and family members. The FBI did not find any terrorism activity, domestic or foreign, and those results were provided to the foreign government in the summer of

---

<sup>11</sup> Jenkins, Michale Brian (2010), "No Path to Glory: Deterring Homegrown Terrorism", Retrieved July 2012 from the RAND Corporation website:

[http://www.rand.org/content/dam/rand/pubs/testimonies/2010/RAND\\_CT348.pdf](http://www.rand.org/content/dam/rand/pubs/testimonies/2010/RAND_CT348.pdf)

<sup>12</sup> Khalil, Lydia (2012), "US counter-radicalization strategy: the ideological challenge", Australian Strategic Policy Institute, Retrieved July 23, 2014 from the ASPI website: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&lng=en&id=161892>

<sup>13</sup> Watts, Clint (2013), "Detecting The Radicalization and Recruitment of the Boston Bomber", Retrieved June 2013 from the Foreign Policy Research Institute website:

<http://www.fpri.org/geopoliticus/2013/04/detecting-radicalization-and-recruitment-boston-bombers>

2011.<sup>14</sup> Although the FBI is often criticized for conducting a superficial inquiry regarding Tamerlan's activities, subscribing to radical beliefs does not necessitate engaging in radical actions, and civil liberties dictate that private beliefs should be free from public scrutiny.

## **PREVENTING VIOLENT EXTREMISM THROUGH PARTNERSHIPS**

The concept of trust through community partnerships can be conceptualized in the 1990 community-policing model. The community-policing model is defined as a preventive style of policing. The goals of the community policing model revolves around:

1. Promoting outreach, enhancing inclusiveness and integration, and minimizing the disaffection that can lead to radicalization particularly among Muslim youth;
2. Serving as an early warning system on the ground resources to identify incipient radicalization or terrorist activities; and
3. Opening up new channel of communications with individuals who can navigate the linguistic and cultural complexities of Islam and provide much needed context to inform intelligence analysis<sup>15</sup>.

Community participation and empowerment are critical elements of successful partnerships between the police and Muslim communities.<sup>16</sup> Community partnerships are often depicted as the cornerstone of effective counter-radicalization strategies. Countering radicalization to violence is frequently best achieved by engaging and empowering individuals and groups at the local level to build resilience against violent extremism.<sup>17</sup> In an effort to prevent the effects extremist beliefs has on impressionable American youth, local law enforcement has strategically implemented several community-policing initiatives. One initiative that law enforcement has implemented is referred to as the Safe Schools/Healthy Students Initiative (SS/HS). The SS/HS is a partnership with local mental health experts, juvenile justice officials, and law enforcement. It is often reported that the implementation of this initiative has resulted in fewer students experiencing or witnessing violence, increased school safety, and an overall decrease in violence in communities where the program is active.<sup>18</sup> Another community initiative that presents law enforcement with the ability to prevent radicalization is known as the Building Communities of Trust (BCOT) initiative. The Departments of Justice and Homeland Security established the Building Communities of Trust (BCOT) Initiative to improve trust among police, fusion centers, and

---

<sup>14</sup> The Federal Bureau of Investigations (2013), "2011 Request for Information on Tamerlan Tsarnaev from Foreign Government", Retrieved from <http://www.fbi.gov/news/pressrel/press-releases/2011-request-for-information-on-tamerlan-tsarnaev-from-foreign-government>

<sup>15</sup> Paris, Jonathan (2007), "Discussion Paper on Approaches to Anti-Radicalization and Community Policing in the Transatlantic Space", Weidenfeld Institute for Strategic Dialogue, Retrieved from <http://www.hudson.org/files/publications/JonathonParisAug232007.pdf>

<sup>16</sup> Tufyal Choudhury & Helen Fenwick (2011), "The impact of counter-terrorism measures on Muslim communities", Equality & Human Rights Commission Research", rept. 72, Durham University, Retrieved from [http://www.equalityhumanrights.com/uploaded\\_files/research/counterterrorism\\_research\\_report\\_72.pdf](http://www.equalityhumanrights.com/uploaded_files/research/counterterrorism_research_report_72.pdf)

<sup>17</sup> The White House (2011), "Empowering Local Partner to Prevent Violent Extremism In The United States", Retrieved from [http://www.whitehouse.gov/sites/default/files/empowering\\_local\\_partners.pdf](http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf)

<sup>18</sup> The White House (2011), "Empowering Local Partner to Prevent Violent Extremism In The United States", Retrieved from [http://www.whitehouse.gov/sites/default/files/empowering\\_local\\_partners.pdf](http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf)

the communities to which they serve.<sup>19</sup> The results of this program have presented certain communities with the ability to vocalize their concerns.

## **CONCLUSION**

The assertions of dissent in American Muslims, particularly with those who have migrated to a foreign land are often shaped by the bicultural values of assimilation. The ability to prevent future terrorist from acting upon subscribed extremist thought requires effective domestic intelligence by local authorities and active community partnerships within the American Muslim community at the national and local level. The expansiveness of sharing both domestic and international information essentially improves law enforcements ability to detect, prevent and respond to acts of terrorism. Although the expansive powers of the Patriot Act and the development of fusion centers presented law enforcement with the greater ability to detect terrorist plots, "lone wolf actors" and Internet radicalization have become a greater challenge for law enforcement officials. Community partnerships are perhaps the most effective counter-radicalization strategy and should be used as a strategic tool to detect domestic radicalization.

## **ABOUT THE AUTHOR**

Herbert S. Mack is currently a federal officer who has an esteemed background and interest in analyzing national security threats. Mr. Mack is an Iraq war Veteran and gained extensive knowledge and training with the US Army Chemical Corp. He continues to develop his expertise in addressing strategic innovative challenges facing homeland security as he pursues a Master's of Science in Homeland Security Management at Long Island University's Homeland Security Institute.

---

<sup>19</sup> The White House (2011), "Empowering Local Partner to Prevent Violent Extremism In The United States", Retrieved from [http://www.whitehouse.gov/sites/default/files/empowering\\_local\\_partners.pdf](http://www.whitehouse.gov/sites/default/files/empowering_local_partners.pdf)