



VANGUARD

PROVIDING INFORMATION ON NATIONAL SECURITY FOR STATE & LOCAL POLICYMAKERS

12 August 2009

Volume 2 · Issue 35

The problem with defining likelihood

By Mead Treadwell and Jeremy Thompson, editors

The *CTC Sentinel*, a publication of West Point's Combating Terrorism Center, reported in July that at least three times in the last two years, nuclear sites in Pakistan have been attacked by local terrorists: A nuclear missile storage facility at Sargodha and Pakistan's nuclear airbase at Kamra were attacked in 2007; and in 2008, suicide bombers attacked one of Pakistan's primary assembly sites for nuclear weapons.

The article considers the question of how secure the nuclear arsenals of Pakistan are from terrorists.

"Pakistan has established a robust set of measures to assure the security of its nuclear weapons," the article states. "These have been based on copying U.S. practices, procedures and technologies, and comprise: a) physical security; b) personnel reliability programs; c) technical and procedural safeguards; and d) deception and secrecy."

Though these "robust" measures give a "high degree of confidence" to the Pakistan government that its nuclear arsenal is secure, the article says that "empirical evidence points to a clear set of weaknesses and vulnerabilities in Pakistan's nuclear safety and security arrangements."

The author addresses two concerns: The first is that the sites that manufacture, assemble or refurbish nuclear weapons are not as secure as the sites that store the deployed ones. The second concern the author considers is the possibility of collusion.

"It is widely accepted that there is a strong element within the Pakistan Army and within the lead intelligence agency, the ISI, that is anti-Western, particularly anti-U.S., and that there also exists an overlapping pro-Islamist strand...No screening program will ever be able to weed out all Islamist sympathizers or anti-Westerners among Pakistan's military or among civilians with nuclear weapons expertise," according to the author.

The question is an important one, as the likelihood of collusion in Pakistan would most certainly affect the likelihood of an EMP attack. Nuclear capability in some form constitutes one of three dots that need to be connected: nuclear capability, delivery technology, and the willingness to carry it out.

But the measure of likelihood, despite being a very complex and elusive question, is often used to create policy the way numbers are used to illustrate math equations, sometimes out of necessity. It is often asserted that EMP is a high risk scenario, but there is a low likelihood that it would occur; therefore, we should not devote resources to preparing for such a scenario. But measures of likelihood on this scale were not meant to enjoy this kind of certainty, nor is it wise to justify a policy on a likelihood that is based on another likelihood.

[The terrorist threat to Pakistan's nuclear weapons](#)
[Jihadis thrice attacked Pakistan nuclear sites](#)
[Report: Pakistan nuclear facilities attacked at least three times](#)

U.S. Military takes EMP seriously

In an interview on cybersecurity with National Public Radio, Gen. Kevin Chilton, who heads U.S. Strategic Command, was asked to comment on Electromagnetic Pulse and its effects on military systems, particularly the scenario missile being fired from a rogue state.

“What we found is that it has a greater effect on some of our high tech, microcircuit technology that we’ve deployed, and various things whether it be computers or electronics that support automobiles...etc.,” Chilton said. “Good news and bad news: The good news is that it is a finite area that is affected. It’s not infinite or global in nature.

“The bad news is you have to consider this, the detonation of a nuclear weapon and the consequences which would not only result from the blast, but also from EMP and what it would have would have on our electronic systems. For that reason, we take steps to protect our critical command and control elements from an EMP blast, so that we always provide the President the opportunity to command and control his nuclear forces even in that environment,” Chilton said.

Chilton did not address civil defense capability.

[Audio: U.S. Strategic Command: Cyber and Space Defense](#)
[EMP Commission report on Critical National Infrastructures](#)

Highlight

Opinion: Is Russia ready for Star Wars? (RIA Novosti, 08/12/09)

<http://en.rian.ru/analysis/20090812/155794013.html>

By 2030, the United States will be able to strike from space on a global scale, including Russia, Air Force Commander Alexander Zelin told journalists. "Development of air and space attack weapons by foreign countries shows that by 2030 air and outer space will turn into a single sphere for armed

struggle," he said. Zelin said that to counter this threat, Russia is planning to build a fundamentally new force of air and space defense (ASD) by 2020. This defense force will be equipped with anti-aircraft missile systems - upgraded S-300s, S-400s, which have recently been launched into production, and eventually with S-500s, which are currently under development. It is reported that the S-500 will not be based on its predecessor, the S-400, but will represent an entirely new system capable of effectively countering ballistic targets.

From the Wires this Week

Emergency Management/Homeland Security

Border security not an isolated issue, DHS secretary says (Los Angeles Times, 08/12/09)

<http://www.latimes.com/news/nationworld/nation/la-na-immigration12-2009aug12.0.6305451.story>

The Homeland Security chief, at an El Paso conference, says immigration enforcement, citizenship processes and counter-narcotics efforts are 'inextricably linked' to border safety. *Related article: [Napolitano says U.S. and Mexico see border violence as shared problem.](#)*

U.S. bought oil smuggled from Mexico (Associated Press, 08/10/09)

<http://www.chron.com/disp/story.mpl/ap/top/all/6567798.html>

U.S. refineries bought millions of dollars worth of oil stolen from Mexican government pipelines and smuggled across the border, the U.S. Justice Department told The Associated Press — illegal operations now led by Mexican drug cartels expanding their reach.

Federal officials release new swine flu guidelines for schools (Mercury News, 08/07/09)

http://www.mercurynews.com/breakingnews/ci_13017756?nclick_check=1

As they prepare to welcome back students for the fall semester, school staff across the country received new guidance for how to prevent the spread of swine flu and cope with any outbreaks. During a news conference, federal public health, education and homeland security officials said children with flu-like symptoms should be immediately separated from their classmates and stay home from school for 24 hours after their fevers have passed — not seven days total, as was recommended in the spring. *Related article: [Flu planners fear ERs flooded with the not-so-sick.](#)*

Preparation pays off: Fire, EMS, police response to NIU shootings praised (Homeland Security Today, 08/07/09)

<http://www.hstoday.us/content/view/9697/149/>

The U.S. Fire Administration issued a report documenting how, by assimilating lessons of earlier disasters, first responders to the tragic campus shooting at Northern Illinois University last year prevented the damage from that event from being far worse. The shootings that occurred at Northern Illinois University in DeKalb, Illinois in 2008 provide, according to the report, an instructive example of the benefits of emergency preparedness.

Hawaii says airports now disaster ready (KITV 4, 08/07/09)

<http://www.kitv.com/news/20324196/detail.html>

It has been one of the weakest links in Hawaii response to disaster, but now state officials said the airport system is ready. Until recently, the policy of Hawaii airports was there was no point in investing in hurricane preparations because they are so rare. However, after learning from past mistakes, the state now proclaims the airports are ready. After a natural disaster on Oahu, with power out and roads damaged, the tourist population would need evacuation.

Information and Cybersecurity

Business groups want Congress to address E-verify concerns (Federal Computer Week, 08/11/09)

<http://fcw.com/articles/2009/08/11/web-everify-senate.aspx>

Trade associations that include TechAmerica and the U.S. Chamber of Commerce say Congress should deal with worries they have about the E-Verify employment eligibility verification system. The language of provisions in the Senate bill to fund the Homeland Security Department for fiscal 2010 doesn't address concerns that employers have about the E-Verify system, the associations said in a letter.

Are private clouds the answer to public-sector concerns? (Government Technology, 08/11/09)

http://www.govtech.com/gt/articles/709350?utm_source=rss&utm_medium=link

According to Shawn McCarthy, an IDC research analyst, many IT leaders perceive that their organizational assets are safer inside their clouds instead of drifting inside one of the giant vendor-operated clouds on the Internet. "There's a certain unknown when you go through a secure provider," he said. Missouri is working on a virtual desktop initiative that will let the IT department provide application services remotely to various departments in a pay-per-use scenario. In this case, it's an internal, virtual cloud that users access on remote desktops.

Storage reliability questioned after high profile outages (PeriscopeIT, 08/11/09)

<http://www.periscopeit.co.uk/website-monitoring-news/article/storage-reliability-questioned-after-high-profile-outages/483>

The reliability of data storage facilities and managed hosting services has been brought into question following a series of high-profile internet outages, it has been claimed. According to Computer World, downtime experienced by Equinix and Primus has raised doubts about both security and reliability of such facilities and their website monitoring services.

Outdated 911 centers can't handle texting (The Philadelphia Inquirer, 08/11/09)

http://www.philly.com/inquirer/local/20090811_9-1-1_centers_lack_funds_to_handle_texting.html

The technology to send text messages has long been available. But the money to upgrade 911 call centers to receive them has not. Several states, including New Jersey, have used millions of dollars that had been dedicated to "enhanced 911 services" to plug state budget gaps or to pay for other public safety initiatives. The lack of funds has prevented call centers in New Jersey and Pennsylvania from obtaining upgraded computer systems and communication lines and to train 911 staffs to receive text messages. *Related article:* [Iowa call center first to accept text messages.](#)

Cybersecurity official resigns (Washington Post, 08/08/09)

<http://www.washingtonpost.com/wp-dyn/content/article/2009/08/07/AR2009080702805.html?referrer=emailarticle>

A top operational official in charge of protecting civilian government computer networks has resigned, dealing another blow to the federal effort to enhance cybersecurity. Mischel Kwon, the director of the Department of Homeland Security's U.S. Computer Emergency Readiness Team, submitted her resignation letter.

Pennsylvania database to help 911 crews assist disabled (Democrat and Chronicle, 08/07/09)

<http://www.democratandchronicle.com/article/20090807/NEWS01/908070335/1002/NEWS/Database%20to%20help%20emergency%20responders%20working%20with%20people%20with%20disabilities>

The Monroe County [PA] Emergency 911 Call Center launched a new initiative designed to help police officers, firefighters, emergency medical technicians and other first responders when working with people who have disabilities. The Special People In Need of 911, or S.P.I.N., program logs people with disabilities into a private, confidential database so first responders will already have their names, addresses, nature of disabilities, any history of aggression and emotional triggers before they arrive on scene.

Cybersecurity - a must for the grid (Automation World, 08/06/09)

<http://www.automationworld.com/feature-5824>

Cybersecurity has become a major issue with electric plants. The North American Electric Reliability Corporation (NERC) has launched a number of programs designed to protect the electric grid from Internet-based attacks. Any connection that goes outside the plant - whether it's Internet connectivity or dedicated connections to corporate offices - leaves the plant vulnerable to cyber attack. Prompted by new NERC standards, plants are adding or beefing up cybersecurity. Sometimes, it is involved in the process, sometimes not.

Minnesota to go high tech with 911 system (KSTP 5, 08/05/09)

<http://kstp.com/news/stories/S1069640.shtml?cat=206>

Work will begin this fall on a major upgrade to Minnesota's 911 emergency call system. When it's done, the state will have state-of-the-art technology that will save time and save lives. One of the highlights of the new 911 system is the ability for dispatch to receive text messages for help. Officials soon hope to include things like medical information to be associated with your phone number.

Missile Defense/Satellite Technology/EMP

Air-launch interceptors back in play for U.S. missile defense (Flightglobal, 08/07/09)

<http://www.flightglobal.com/articles/2009/08/07/330664/air-launch-interceptors-back-in-play-for-us-missile.html>

The U.S. Missile Defense Agency and the U.S. Air Force are in talks about the joint development of a new interceptor that can be launched by a fighter jet or unmanned aircraft system at ballistic missiles. The talks are expected to jump-start the next phase of a two-year-old competition between Lockheed Martin and Raytheon, which are developing modified versions of the PAC-3 Patriot and AIM-120 advanced medium range air-to-air missile, respectively, for the emerging requirement. Since 2007,

the MDA has provided seed money to both companies to design the weapons and perform hardware tests. But, facing a \$1.2 billion overall budget cut, the MDA balked at funding full-scale development with both concepts costing between \$137 million and \$450 million.

Energy/Transportation/Maritime/Infrastructure

Government, industry create threat forum for power grid (Federal Computer Week, 08/11/09)

<http://fcw.com/articles/2009/08/11/energysec-data-sharing-coalition.aspx>

Operators of the nation's power grid have joined with government regulators and security vendors to create forum for sharing information about threats to the U.S. energy infrastructure. The Energy Sector Security Consortium (EnergySec) has grown from an informal regional industry group in the Pacific Northwest to include more than 200 members since its launch as a national organization in December 2008. Its goal is to provide a channel for sharing security information and concerns in a way that is faster and more flexible than existing organizations.

Electrical problem causes sewer spill at Alabama wastewater treatment plant (Mobile Press-Register, 08/11/09)

http://blog.al.com/live/2009/08/electrical_problem_causes_sewe.html

A six-hour power shutdown at the Fairhope [AL] Public Utilities wastewater treatment plant caused the release of about 300,000 gallons of tainted effluent into Mobile Bay. A motor that turns a rotating arm in one of the treatment plant's settling pools burned out and, for reasons unknown, the motor's burnout shut off the plant's main power breaker. The flow of liquid through the plant's gravity-fed system can't be stopped without causing a massive overflow at the plant itself, said Dan McCrory, the city's water and sewer superintendent.

Wind promises blackouts as Obama strains grid with renewables (Bloomberg, 08/07/09)

http://www.bloomberg.com/apps/news?pid=email_en&sid=arbHcz0ryM_E

President Barack Obama's push for wind and solar energy to wean the U.S. from foreign oil carries a hidden cost: overburdening the nation's electrical grid and increasing the threat of blackouts. The funding Obama devoted to get high-voltage lines ready for handling the additional load of alternative supplies is less than 5 percent of the \$130 billion that power users, producers and the U.S. Energy Department say is needed.

NRC proposes stronger oversight of radioactive materials (Nuclear Regulatory Commission, 08/05/09)

<http://www.nrc.gov/reading-rm/doc-collections/news/2009/09-131.html>

The Nuclear Regulatory Commission is proposing to strengthen oversight of radioactive materials by limiting the amount of radioactive material allowed in generally licensed devices. The proposed rule would require owners of approximately 1,800 devices, an estimated 1,400 general licensees nationwide, to apply for specific licenses for the devices. Requiring specific licenses for such devices would improve the safety, security and control over the gauges by bringing them under increased regulation, making it harder to accumulate a risk-significant amount of radioactive material or to procure a device through subterfuge.

Announcements

To receive an EMP briefing

The Institute of the North and the Claremont Institute in Claremont, California support state legislators and emergency management groups by providing briefings on electromagnetic pulse (EMP) attack scenarios and preparedness. If you would like your committee or organization to receive one of these briefings, please contact [Jeremy Thompson](#) by email or call 907.771.2446.

To receive a copy of *Missile Defense and the Role of the States*

In February 2007, the Institute of the North and the Claremont Institute published a report on *Missile Defense and the Role of the States*, a survey of Adjutants General on questions regarding missile defense and electromagnetic pulse. To receive a hard copy of the report, please contact [Jeremy Thompson](#). You can also view the report online at: <http://www.institutenorth.org/servlet/download?id=304>.

To view the IWG report

The Institute of the North's Defense and Security program is a member of the Independent Working Group on Missile Defense, the Space Relationship, & the Twenty-First Century, a non-partisan group of defense experts who meet regularly to discuss issues and projects related to missile defense. To view the 2009 report online, please visit: <http://www.institutenorth.org/servlet/download?id=564>

To submit material

We are always looking for well-written editorials on the impact of national security at the state and local level. If you would like to submit an editorial for publication in the Vanguard newsletter, please forward factual and relevant articles of 500-750 words in length to the [Institute](#).

The Vanguard online

To view past and current issues of the Vanguard newsletter online, please visit: http://www.institutenorth.org/servlet/content/security_and_defense_program.html.

Unsubscribe

If you wish to be removed from our mailing list, please email the [Institute](#) with the word "unsubscribe" in the message field.

About the program

The Security and Defense program at the Institute of the North conducts research and educates policymakers on strategic issues relating to the defense of the United States that particularly concern decision makers in Alaska and at the state and local level throughout the nation.

The Institute of the North, based in Anchorage, Alaska, is a non-profit educational and research organization founded in 1994 by former Secretary of the Interior and twice Governor of Alaska Walter J. Hickel, focusing on strategic and natural resource issues.

*The Institute of the North · 509 West Third Avenue, Suite 107 · Anchorage, AK 99501
Phone: 907.771.2446 · Fax: 907.771.2466*