****

## http://r54.cooltext.com/rendered/cooltext1333426312.png'Suspicious device' explodes at Nogales power plant

Source: http://www.azcentral.com/story/news/arizona/2014/06/11/nogales-explosion-power-plant-arizona-abrk/10351107/

A makeshift bomb exploded at a Nogales, Ariz., power plant Wednesday morning, damaging a large fuel tank and prompting an investigation by the FBI and federal bomb experts.

Local officials were alerted at 9:30 a.m. to "suspicious activity" at UniSource Energy Services' Valencia Plant. **The explosion damaged a diesel storage tank**, but there were no reports of injuries and authorities said they knew of no suspects or witnesses.

Officials closed off the power plant and an adjacent car dealership on North Grand Avenue. The FBI, the federal Bureau of Alcohol, Tobacco, Firearms and Explosives and the Arizona Department of Public Safety were called.

Wednesday evening, agents were still processing the scene. Arizona Corporation Commission spokeswoman Rebecca Wilder said there were no power disruptions and the plant received only minor damage.

"The reason for the high-scale response is the plant is an electrical substation and critical to the area," Nogales police Lt. Carlos Jimenez said, explaining that as many as 30,000 customers depend on the plant for power.

"The whole city of Nogales could have been compromised," he added.

Authorities described the explosive as "a suspicious device" but would not elaborate. The fuel did not ignite, Jimenez said.

Plant operator UES is a subsidiary of Tucson-based UNS Energy Corp., the parent of Tucson Electric Power. UES provides energy to 237,000 customers in Arizona, according to the company website.

# Nuclear and Radiological Medical CountermeasuresInhibiting Protein Family Helps Mice Survive Radiation Exposure

Source: http://globalbiodefense.com/2014/05/26/inhibiting-protein-family-helps-mice-survive-radiation-exposure/

Tinkering with a molecular pathway that governs how intestinal cells respond to stress can help mice survive a normally fatal dose of abdominal radiation, according to a new study by researchers at the Stanford University School of Medicine.

Because the technique is still partially effective up to 24 hours after exposure, the study suggests a possible treatment for people unintentionally exposed to large amounts of radiation, such as first responders at the Chernobyl nuclear disaster in 1986.

“We were very surprised by the amount of protection the animals received,” said Amato Giaccia, PhD, professor of radiation oncology. “The important thing to note is that we didn’t change the amount of damage the intestinal cells sustained as a result of the radiation; we simply changed the physiology of that tissue and how it responded to that damage.”

The researchers believe that a similar approach may also help those patients suffering from diarrhea and nausea caused by radiation therapy for cancer.

Giaccia, who is also a member of the Stanford Cancer Institute, is the senior author of the study, recently published in Science Translational Medicine. Postdoctoral scholar Cullen Taniguchi, MD, PhD, is the lead author of the study.

The researchers were studying a molecular pathway involved in the response of cells to conditions of low oxygen called hypoxia. Hypoxic cells produce proteins known as hypoxia-inducible factors, which help the cells survive the stressful conditions. (The HIF proteins – HIF1 and HIF2 – are normally degraded quickly when oxygen levels are normal.)

Hypoxia often occurs in fast-growing solid tumors as cells find themselves far from oxygen-delivering blood vessels, but it can also occur during times of inflammation, or in tissues like the intestine that experience natural gradations in oxygen levels. HIF proteins help the intestine absorb needed nutrients while blocking the entry of pathogens and maintaining healthy fluid exchange.

“Previous studies from our group and others have suggested that the HIF proteins are important in protecting cells from many types of stress,” said Giaccia, who is also the Jack, Lulu and Sam Willson Professor. “So we wondered whether stabilizing HIF proteins, and therefore increasing their levels within the cells, could also protect the intestine from the effects of radiation.”

Radiation kills cells by irreversibly damaging their DNA. Side effects of acute radiation exposure are seen most clearly in rapidly dividing cells, such as those found in the lining of the intestine or blood and immune cells in the bone marrow. People who have undergone exposure to high levels of radiation typically experience debilitating nausea, vomiting and diarrhea when their intestines lose the ability to properly regulate fluid exchange. They are also extremely susceptible to infection. Although radiation’s effects on the bone marrow can be mitigated by a bone marrow transplant, there’s no treatment for its effects on the gastrointestinal tract, which are a major source of mortality in unintentionally exposed humans.

The scientists blocked the degradation of the HIF proteins in two ways: First, they genetically engineered mice unable to express a group of three proteins that tags the HIF proteins for destruction. They also treated unmodified mice with a small molecule called dimethyloxyallyl glycine, or DMOG, that inhibits the activity of the same group of proteins.

In both cases, the researchers found that the levels of HIF1 and HIF2 proteins increased significantly. Furthermore, 70 percent of the genetically modified mice lived for at least 30 days after receiving a normally lethal dose of abdominal radiation, and 27 percent survived at least 30 days after a normally lethal dose of whole-body radiation (a situation which more closely mimics accidental human exposure). In contrast, none of the unmodified mice survived more than 10 days after either type of radiation exposure.

Similar results were seen when unmodified mice were treated with DMOG prior to radiation exposure. In this case, 67 percent of the treated mice survived for at least 60 days after receiving a normally lethal dose of abdominal radiation, and 40 percent lived for at least 30 days after a normally lethal dose of whole-body radiation. As with the genetically modified mice, none of the untreated mice in either group lived longer than 10 days.

Further experiments showed that HIF2, rather than HIF1, is responsible for the radioprotection observed in the study.

To investigate the cause of the treated animals’ longer survival, the researchers looked directly at the epithelial cells lining their intestines. They found that treated animals exhibited lower levels of cell death in response to abdominal radiation exposure and improved survival of a gland called a crypt, which hosts the rapidly dividing stem cells necessary to accommodate the intestines’ need for repeated cell turnover. The treated animals also experienced less diarrhea and fewer imbalances in fluid and electrolyte levels than did untreated animals exposed to the same dose of radiation, and they quickly gained back the weight they had lost as a result of the exposure.

“The animals that survived the abdominal radiation have a life span that is similar to unexposed animals, which was very exciting to us,” said Giaccia. “However, we realized it would be impossible to pretreat humans unexpectedly exposed to large amounts of radiation like at Chernobyl or Fukushima because those exposures are, by nature, unpredictable.”

So Giaccia and his colleagues experimented with treating the mice with DMOG after abdominal radiation exposure. They found that, although the protective qualities of the molecule were diminished, it did still help. When DMOG was administered four hours after radiation exposure, 45 percent of the treated animals, but no untreated animals, survived at least 10 days.

After 24 hours the effect was more subtle – DMOG treatment showed little benefit at higher doses of radiation, but at a lower dose 75 percent of the treated animals lived for at least 30 days in comparison with only 18.2 percent of the untreated animals.

“We found we were still able to rescue a significant proportion of the animals,” said Giaccia.

Finally, the researchers tested the effect of DMOG treatment 24 hours after total body irradiation. They found that 37.5 percent of the treated mice survived for at least 30 days, but only if the mice were also given a bone marrow transplant to restore blood and immune stem cells killed by the radiation. None of the untreated mice lived beyond 10 days.

Although the study suggests a possible way to mitigate the effects of therapeutic radiation exposure, much work remains to be done, the researchers caution. For one thing, mice are more resistant to the effects of radiation than humans, and the radiation doses used in the study far exceed what would be used to treat a cancer patient. But the next steps are clear.

“There are a number of drug molecules that act in a manner similar to DMOG that are already in clinical trials for unrelated conditions,” said Giaccia. “Our next step will be to test some of these molecules to see if they also offer radioprotection.”

The university has filed a patent application, titled “Use of Prolyl Hydroxylase Inhibitors as a Radioprotective Drug for the Lower Gastrointestinal Tract”, based on the results of this study.

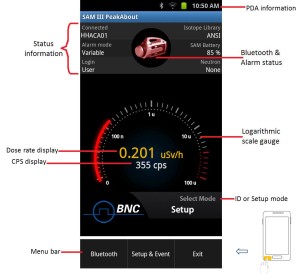
The research was supported by the National Institutes of Health, the Radiological Society of North America Resident Research Grants, the Canadian Institutes of Health and Research, the Silicon Valley Foundation and the Sydney Frank Foundation.

▶**Read more at:** http://stm.sciencemag.org/content/6/236/236ra64.abstract?sid=5b416df0-1d98-4157-b599-52ba29f988ad

# New Smartphone App Improves Nuclear Isotope ID and Training

Source: http://globalbiodefense.com/2014/05/29/new-smartphone-app-improves-nuclear-isotope-id-and-training/

Berkeley Nucleonics has launched a new Smartphone App called “PeakAbout” that allows management of their Radiation Isotope Identifier systems from a safe distance. The app controls both Backpack and Handheld radiation isotope identification devices (RIIDs) and gives users the ability to move away from the detector to perform analysis at a distance.

With PeakAbout’s Broadcast functions, users now also have the ability to stream what they are seeing on the screen back to their management or a reachback team. The Android app uses the smartphone’s data plan or WiFi connection to transmit the screen details in real time.

Streaming the screen of an Isotope Identifier has long been in demand for both operational activities and user training. The new capability allows a class full of new users to watch what is on the screen of a single detection system in real time, which improved the efficiency and quality of training.

Driverless Cargo Inspection System Launched by Rapiscan

Source: http://www.hstoday.us/single-article/driverless-cargo-inspection-system-launched-by-rapiscan/d19c95185db4c6b514b60b81db19eae3.html

Rapiscan Systems has launched the new Driverless Eagle M60 cargo inspection system. It is a fully-automated vehicle screening system which can operate without the need of a driver and has been specifically designed to assist customs and border personnel in their detection of nuclear materials, explosives, weapons and contraband such as tobacco, alcohol and currency in trucks, cargo and containers.

Rapiscan’s driverless system requires no driver to be present during scanning, which the company says eradicates driver fatigue and driver work-shift changes; improves inspection rates and vehicle throughput; and removes risks associated with lone workers, health and safety incidents and potential human error. It can be driven on the road like a standard vehicle, allowing the unit to move between locations quickly and easily as required.

Once moved into position via a remote steering system, the M60 automatically detects two positional sensors -- one placed at either end of the scan location. The positional sensors can be placed as far as 35 meters apart, allowing for oversized cargo or multiple units to be scanned in one pass.

As the scanning commences, additional sensors on the M60 make minor adjustments to the direction and position of the vehicle which ensures it consistently drives in a straight line between the two positional sensors. The system is designed not to deviate by more than 25mm from the center line.

The automated scan process is then monitored by a system operator who is housed in the M60’s onboard inspector’s office. This operator views the high resolution X-ray images produced by the system in real time.

Rapiscan was recently awarded two lucrative contracts for its vehicle and cargo inspection systems. On May 13, the company announced a $15 million order from an undisclosed Middle East customer. The order is for multiple Rapiscan Eagle M60 mobile inspection units, which the Driverless Eagle 360 is based on. This was followed by a $13 million order for an undisclosed “international customer,” again for Eagle inspection systems.

Rapiscan’s Eagle cargo and vehicle inspection systems are used by customs agencies, military organizations and homeland security operatives around the world. Eagle cargo and vehicle inspection systems use proprietary transmission X-ray technology that is able to penetrate well beyond the surface of a container or vehicle to provide comprehensive detection of threats.

# A Scenario for Jihadist Nuclear Revenge

**By Edward A. Friedman and Roger K. Lewis**

Source: http://fas.org/pir-pubs/scenario-jihadist-nuclear-revenge/

**The weapon was ready, a simple fission device similar to the bomb that destroyed Hiroshima. It had been finally assembled in a rented storage space on the outskirts of Las Vegas. Gulbuddin Hekmatyar had spent years quietly contemplating while meticulously planning this diabolical, logistically challenging mission. Among other things, the plot necessitated recruiting and directing a number of operatives, some technically skilled, located in several countries. All were individuals devoted to his cause and committed to the Jihadist goal of detonating a nuclear bomb in an American city. He chose Las Vegas because the city epitomized western decadence.

The bomb’s essential component – 140 pounds of highly enriched uranium (HEU) – had been stolen or secretly purchased, bit-by-bit, mostly from Pakistan, but also from India, North Korea, Russia, Ukraine and Kazakhstan. It took years to collect, hide and safeguard all the necessary HEU in northwest Pakistan. From there, small pieces of the fissile material and some structural bomb components, hidden and well shielded in multiple shipments, were transported to U.S. ports or border crossings, and eventually to Las Vegas and the rented storage space. With all the components covertly acquired or fabricated by dedicated Jihadists in Pakistan and the United States, the relatively simple bomb finally could be assembled. It was comprised of a long, large-bore, artillery-type barrel; a heavy-duty breech; and enough chemical explosive to propel an appropriately shaped, 70-pound HEU piece through the barrel at very high velocity into another appropriately shaped, 70-pound piece of HEU affixed to the end of the barrel. Slamming together these two sub-critical masses would create the critical mass needed for an explosive chain reaction.

It was time. The plan of attack was straightforward and foolproof. Weighing under a ton and less than a dozen feet long, the weapon in its lead-lined crate fit easily inside a small, rented truck. A lone, suicidal operative drove and parked the truck near the Strip, then activated the electronic device triggering the detonator that set off the chemical explosion. The HEU bullet accelerated through the barrel and merged almost instantaneously with the target HEU. Within microseconds, the critical mass exploded, releasing kilotons of energy, a blinding, rapidly expanding ball of light, heat and deadly radiation. A shock wave propagated through the atmosphere, flattening almost every building within a half-mile of the detonation point. Tens of thousands were dead or injured. Las Vegas was in ruins. The threat had become reality.

When President Obama declared in 2009 that “nuclear terrorism is the most immediate and extreme threat to global security,” it was scarcely noticed. Yet when questionable sources announced that the Mayan Calendar predicted the end of the world in 2012, media and public attention was astonishing. The apocalyptic prediction arising from myth took hold, while a warning of potential catastrophe based in reality, put forth by Barack Obama in Prague, passed us by. Supernatural doomsday scenarios readily gain traction in our public discourse, but threats to our civilization from proven nuclear dangers elude us.

The public and press largely ignored other sobering news in 2010 when Wikileaks revealed that a 2009 cable from the U.S. Ambassador to Pakistan, Anne W. Patterson, warned that “our major concern is not having an Islamic militant steal an entire weapon, but rather the chance someone working in government of Pakistan facilities could gradually smuggle out enough enriched uranium to eventually make a weapon.” 1)

By raising the specter of nuclear terrorism, the Wikileaks revelation gave concrete urgency to President Obama’s abstract concerns. But few paid attention, in part because few understand nuclear weapons risks and realities.

Passage of time and reluctance to think the unthinkable have generated complacency. No nuclear weapon has been used aggressively since the August 9, 1945, attack on Nagasaki. Despite the existence of vast numbers of nuclear weapons, Americans expect nuclear restraint because they believe Mutually Assured Destruction (MAD) is a reliable deterrent. MAD presumably ensures that a country first using nuclear weapons will be wiped out by a retaliatory blow. But if a non-state entity were to perpetrate a nuclear weapons attack, at whom and where would retaliation be directed? An act of nuclear terrorism would obviate 69 years of stability engendered by MAD, an appropriately chosen topic of satirical banter in the film “Dr. Strangelove,” yet a grim reality.

Obama’s words that nuclear terrorism is an “immediate and extreme threat” are not an exaggeration. Terrorists now have new opportunities to covertly fabricate nuclear weapons on their own, and the threat is compounded by the potential anonymity of the attackers.

The cable allegedly sent by Ambassador Patterson leads to several questions: what is enriched uranium and how available is it? How is it used in a bomb, and who could use it? Where and how could it be delivered? What would be its effect? And perhaps the first and biggest question – why would terrorists aspire to manufacture, deploy, and detonate a nuclear weapon?

The 9/11 attacks marked the beginning of a “Terrorist Era” with a capital T. That triple attack profoundly disturbed, shocked and injured the nation, psychologically as well as physically. It suggested that a goal of certain terrorists is the destruction of the United States and its allies, and nuclear capability would make that goal attainable.

In 1998, Osama bin Laden declared that it was his Islamic duty to acquire weapons of mass destruction. Because Islam deplores killing women and children, religious justification was sought for such weapons. In 2003, three Saudi clerics associated with Al Qaeda provided justification in a fatwa that stated:“One kills in a good manner only when one can.” 2)

Thus the “why” can be revenge for the deaths of Muslim civilians or Osama bin Laden, Jihadist punishment of a decadent, anti-Islamic civilization, or retribution for western support of Israel. Still, the easily stated words “nuclear revenge” are not readily internalized. Unlike “tsunami” or “colon cancer,” the term “nuclear terrorism” does not usually evoke a visceral reaction. Such a response is unlikely until people intellectually and emotionally comprehend the potential threat of rogue nuclear weapons. And comprehension requires some understanding of the bomb itself.

In addition to understanding the weapon, people also must grasp the feasibility and consequences of an act of nuclear terrorism. A credible scenario can provide this. In his book, The Second Nuclear Age, Yale Professor Paul Bracken argues that war games based upon scenarios involving nuclear weapons played a significant role in clarifying and shaping strategic thinking during the height of the Cold War. “Scenarios set the stage for the game’s interactions,” he wrote. “Scenarios…are hypothetical plot outlines of plausible future developments. They are not forecasts or predictions…” 3)

The Pentagon hypothesizes terrorist scenarios, but the public does not. Our opening Las Vegas scenario attempts to focus the reader’s mind on the real potential for nuclear catastrophe.

But first the Bomb.

### ****The Bomb****

Tremendous energy can be released when the nucleus or inner core of an atom undergoes a transformation. For uranium, the energy releasing transformation is the splitting apart or fission of the nucleus, producing various combinations of lighter atoms such as barium and krypton as “fission products.”

Uranium can exist in different forms or “isotopes,” but all isotopes of uranium contain 92 positively charged protons in the nucleus with 92 negatively charged electrons dancing around the nucleus. These charged particles determine uranium’s chemical properties. However, the uranium nucleus also can contain varying numbers of uncharged neutrons. Somewhat greater than ninety-nine percent of uranium found in nature – uranium isotope 238 – has 146 neutrons in the nucleus. Thus the isotope’s 92 protons and 146 neutrons account for its atomic weight of 238.

Uranium-235, with only 143 neutrons, is the dangerous isotope –because it tends to easily fission if it absorbs a neutron. The fissioning of U-235 powered the bomb that exploded over Hiroshima. Fortunately this isotope is very rare; less than one percent of all forms of uranium found in the earth consist of U-235. Uranium can create an explosive chain reaction—only if U-235 is in highly concentrated form, which is extremely difficult to obtain as described later. But first we explain the basics of nuclear bomb design.

While modern hydrogen-plutonium bombs use a fission-fusion reaction to create the most powerful explosions (which can also use highly enriched uranium instead of plutonium to start the fission reaction), the easiest first-generation atomic bomb to construct entails only fission of highly enriched uranium (HEU), with a concentration of typically 80 percent or greater in the fissile isotope U-235. The Hiroshima bomb was essentially an artillery gun in which chemical explosives fired one 70-pound piece of HEU into another 70-pound piece of HEU, with an average enrichment of 80 percent U-235. The design was so simple that J. Robert Oppenheimer, scientific director of Los Alamos, decided that the prototype did not need to be tested. (One of the reasons not to do a proof test was due to the very limited HEU available during the Second World War.) Indeed the first test of this gun-type bomb occurred when it exploded with such devastating effect at 1,900 feet above Hiroshima on August 6, 1945, killing nearly 100,000 people. Weapons developers at Los Alamos avoided using the word bomb, instead giving euphemistic names such as gadget to their creations. The Hiroshima weapon was inaptly named “Little Boy.”

During the Manhattan Project, the great challenge was collecting and concentrating fissionable U-235. Because U-238 and U-235 have identical chemical properties, separation can only be achieved by exploiting the slight difference in mass arising from one isotope having three more neutrons than the other. One method of separation for enrichment purposes was developed using electric and magnetic forces in a modified form of the cyclotron called the calutron. A second method involved creating a compound in gaseous form of uranium and fluorine, then passing the gas through successive microscopic filters making use of the principle of diffusion.

After the Second World War, improved centrifuges emerged as a more efficient method for enriching uranium. A Dutch company, which became part of the Urenco consortium that also includes Germany and the United Kingdom, was an early adopter of the improved centrifuge technology. Commercial production of enriched uranium for nuclear power plants became a worldwide activity. A. Q. Khan, a Pakistani metallurgist working at the Dutch facility, stole the centrifuge design drawings and brought the technology to Pakistan by the mid-1970s. Throughout the 1980s to the early 2000s, he then sold enrichment equipment to Iran, North Korea, and Libya, and had a vast network of suppliers in at least a dozen other countries.

Having used these centrifuge designs to enable large-scale production of enriched uranium, today Pakistan is rapidly achieving status as having one of the largest and fastest growing stockpile of nuclear weapons after the United States, Russia and China. While some nuclear-armed countries are reducing their weapons count, Pakistan has a vigorous program of nuclear weapons development. Its stockpile is thought to have 100 to 200 nuclear weapons. 4)

Production of nuclear weapons is of great concern, but production of highly enriched uranium is even more worrisome. Although a nuclear bomb might be stolen from a country’s stockpile, it would have anti-activation safeguards (such as access codes and electronic locks) that a thief would find very difficult to penetrate. However, highly enriched uranium for a terrorist is like flour for a baker. Each material is simply one ingredient from which something much more impressive can be concocted. Pakistan continues to produce weapons-grade U-235 at a more intense rate than any country in the world. It is reliably estimated that they have stockpiled thousands of pounds of enriched U-235 that could lead to the fabrication of dozens of new nuclear weapons.

Eyes continue to focus on Pakistan as a potential source of nuclear bomb material. Yet unsecured highly enriched uranium elsewhere has been a worry for many years. Of particular concern have been the vast amounts of weapons-grade uranium that were left relatively unguarded in Russia, Ukraine, Belarus and Kazakhstan after the break-up of the Soviet Union. These have been potential access points for terrorists. Hundreds of secret bombs could have been fabricated.

Prior to 9/11, we could not imagine rogue, non-state entities having the ability to construct a nuclear weapon. Yet vast numbers of reports, documents, drawings and photographs from the Manhattan Project have been declassified. The Little Boy development work at Los Alamos is available for the world to examine. Following 9/11, government agents visited war museums in the United States to remove publicly displayed, artillery-gun components replicating Little Boy. But the proverbial horse was already out of the barn.

Conceivably, determined terrorists could acquire 140 pounds of weapons-grade uranium-235, the amount used in the Hiroshima bomb. While a person weighing 140 pounds would fully occupy a seat at a dinner table, 140 pounds of uranium, the densest of all naturally occurring elements, is less than the size of a football.With the material in hand, processing and fabrication steps for constructing a weapon rely on well-established and widely known metallurgical and manufacturing techniques. Who then might do this? Where would construction take place? And under whose leadership?

### ****A Return to Our Scenario****

The villain of our hypothetical scenario is the leader of a militant group located in the tribal territory of Northwestern Pakistan.Skeptics may doubt that our protagonist, Gulbuddin Hekmatyar, could obtain the equipment and expertise needed for weaponization of highly enriched uranium. While not on Abercrombie and Kent tourist itineraries, the frontier region of Northwest Pakistan is the site of the colorful village of Darra Adam Khel. This unique tribal enclave near the Khyber Pass, just 20 miles South of Peshawar, has been manufacturing copies of small weapons since the late 19th century using basic lathes, drills and other readily available tools. 5) During the Mujahideen struggle with the Soviet Union in the 1980s, the United States was not unhappy to see their production of anti-aircraft weapons. Darra Adam Khel is a major source of weapons in the South Asia region. The potential to fabricate the components for a Little Boy clone clearly exists there.

Osama bin Laden and other Al Qaeda leaders have been eliminated, but other militant jihadists have the capacity and the will to engage in development and use of a nuclear weapon. We chose Gulbuddin for our scenario because he was involved with the 1993 bombing of the World Trade Center, he controls a formidable belligerent organization with the resources to actualize this sequence of events, and he is not part of Al Qaeda or the Taliban. An Afghan student of engineering at Kabul University in the early 1970s, he organized at that time what was probably the first militant Islamic organization in Afghanistan. His student group shot at and threw acid at women in Kabul who were wearing mini-skirts. In a confrontation in 1972 with the rival Maoist political group on campus, Gulbuddin shot and killed their leader. After being imprisoned, he escaped and was given refuge by Islamic fundamentalist elements of the Pakistani government in 1975. Some officials in Pakistan, which had border region disputes with Afghanistan since its founding in 1947, saw in Gulbuddin a potential ally in future conflicts with Afghanistan.

In the early 1980s, when the United States started channeling large amounts of funds and weapons to the Mujahideen for their struggle with the Soviet Union, the Pakistan intelligence agency, the ISI, provided Gulbuddin with a substantial portion of those resources. This enabled the charismatic fanatic to establish a formidable organization known as Hezb-e-Islami.

During the mid-1980s Gulbuddin was instrumental in organizing terrorist training camps in Afghanistan to which “Arab” fighters were invited. Gulbuddin welcomed Osama bin Laden, who first came to Afghanistan to fight the infidel Soviets. 6)

Gulbuddin and his organization did not pursue the Soviets as fully as they might have, since he was waiting to use his fighting potential in a putsch to take over Afghanistan following the departure of the Red Army. He did indeed engage in a civil war for control of Afghanistan that began in 1992. But after achieving the position of Prime Minister of Afghanistan in 1993, Gulbuddin was eventually defeated by the Northern Alliance led by Massoud. With the fall of Gulbuddin, the ISI of Pakistan threw their support in 1994 to the newly organized Taliban.

Few are aware of Gulbuddin’s contacts with the perpetrators of the 1993 bombing of the World Trade Center. Those connections and his meetings with the Blind Sheik were revealed in the trials of the World Trade Center bombers held in New York City. It is too often said that the weakening of Al Qaeda ensures the safety of the U.S. from terrorist attack. However, the 1993 bombing of the World Trade Center involved non-Al Qaeda players and leadership figures from that event are still active. This is just one example of a non-Al Qaeda terrorist group that might become a perpetrator of nuclear terrorism.

Today, Gulbuddin maintains a militant presence in the frontier region and has the organizational ability to engage in ambitious terrorist actions. Gulbuddin is neither a tribal “war lord” nor a narrowly educated religious militant. He is a sophisticated intellectual and political leader who completed two years of engineering education. There is every indication that he is as vicious a proponent of terrorism as was Osama bin Laden.

Nothing suggests that Gulbuddin is, in fact, plotting a nuclear attack on an American city. But he is the key player in our scenario because he has the knowledge, resources and frame of mind for implementing such an attack. If there is one such person and group, there are likely others.

The fissile materials available in Pakistan can be fabricated in the Khyber region to serve as components for a gun-type Hiroshima bomb. The amount of radiation released by the highly enriched uranium can be easily shielded and thus easily elude detection at border crossings or from aerial drones. Since suicidal jihadists probably would assemble it, many of the features that were built into Little Boy 69 years ago to ensure safe delivery and controlled detonation could be ignored.

While this scenario has focused on terrorism originating in the Afghanistan-Pakistan border area, other scenarios might be equally plausible. In May 2011, the Belfer Center for Science and International Affairs at Harvard University issued a report entitled, “The U.S.-Russia Joint Assessment on Nuclear Terrorism.” 7) The study group analyzed possible threats from three terrorist organizations known to have systematically sought to obtain nuclear weapons: Al Qaeda, groups in the Northern Caucasus, and the Japanese cult group, Aum Shinrikyo. Each could be a suitable scenario protagonist. If Iran began producing tens of pounds of HEU, then the possibility of Hezbollah obtaining that material would also merit consideration.

Additional scenarios can be hypothesized with sociopaths who are American citizens. Two figures stand out as prototypes with the organizational and technical capacity needed for implementation. One is Timothy McVeigh, whose homemade bomb destroyed the Alfred P. Murrah Federal Building in Oklahoma City on April 19, 1995. The other is Ted Kaczynski, the mathematics genius known as the Unabomber. He perpetrated seventeen explosive attacks killing three people between 1978 and his arrest in 1996.

The first public alert to the possibility of a small group of individuals in the United States building a nuclear bomb to attack society came in the early 1970s from Theodore B. Taylor, a physicist who invented highly efficient, small sized nuclear weapons at Los Alamos National Laboratory. He recognized and was obsessed by the possibility that fissile material could be stolen from commercial facilities that were enriching uranium. The U.S. government had encouraged corporations to process uranium for use in nuclear reactors. In his book, The Curve of Binding Energy, award-winning writer John McPhee documented the story of this eccentric but highly creative physicist. His account was first published in the New Yorker in 1973. Both Taylor and McPhee seemed convinced that a rogue nuclear weapon would detonate somewhere in the United States prior to the beginning of the 21st Century. 8)

The vulnerabilities of enriched uranium supplies in the United States in the 1970’s were astonishing. We assume that such homeland dangers have been ameliorated. Yet we are aghast at the July 28, 2012, spectacle of an 82-year-old nun and two equally unlikely compatriots penetrating the innermost sanctum of the highly enriched uranium facility at Oak Ridge, Tennessee, and spraying the storage building with graffiti. The words they posted said, “Plowshares Please Isaiah.” 9) If such lax security is exposed in Bear Creek Valley, U.S.A., what might be the case in Pakistan, Russia, North Korea or China?

### ****Implications and Actions****

A successful act of nuclear terrorism would, in a blinding flash, change the nature of civilization, as we know it. When the consequences of an action are so enormous, perhaps one should pause to reflect upon it, even if scenarios and anecdotes may not be persuasive. But our lives are frequently influenced by low probability events. We wear seat belts. We buy lottery tickets.

Perhaps we should be more proactive in supporting our government’s actions to ameliorate potential risks.  The international community is currently discussing at least three treaties. One is to create uniform legal frameworks for prosecuting terrorists who seek to use nuclear materials, another is to develop uniformly effective security procedures for safeguarding nuclear materials, and the third is the Fissile Material Cut-off Treaty. It is likely that these issues are far more important and could have much greater consequences than some of the actions that might be taken to thwart nuclear weapons development in Iran or North Korea. Nuclear policy priorities need to emphasize non-state weapons proliferation at least at the same level as state-centered weapons proliferation.

In the non-government sector, non-state weapons proliferation also should be as central in public forums, the press, blogs, general discourse and academic discussions as the continuing crises in North Korea and in Iran.

The fact that the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security are engaging in detailed analyses of emergency responses to a Hiroshima-type bomb detonation in central Washington D.C. means that they are taking that possibility seriously. 10) While the Gulbuddin scenario chose Las Vegas as a symbolic target, another team of jihadists might choose to focus on our nation’s capital.

Today, the news media continually reports about the potential for North Korea to attack the United States with nuclear-tipped intercontinental ballistic missiles. But an attack using a crate holding a lead-shielded, twelve-foot long artillery gun, delivered by sea to one of America’s busiest container ports, such as ports in New Jersey, New York, or California, is a more likely mode of attack and would be equally effective and deadly.

**▶References are available at source’s URL**

**Edward A. Friedman** is Professor Emeritus of Technology Management at Stevens Institute of Technology in Hoboken, N.J. He holds a B.S. in Physics from MIT and a Ph.D. in Physics from Columbia University.  He was director of a USAID program to develop an indigenous college of engineering in Afghanistan (1970-73) when Gulbuddin Hekmatyar was arrested for murder of a political rival at Kabul University. Dr. Friedman was a founder and senior vice president of the Afghanistan Relief Committee (1979-1995). In 2012 he developed and taught a graduate course on Nuclear Weapons in International Relations as an Adjunct Professor at The John C. Whitehead School of Diplomacy and International Relations at Seton Hall University.

**Roger K. Lewis** is an Architect and Planner. He has been a long-term columnist for the Washington Post’s “Shaping the City.” He is Planning and Preservation Trustee for the National Children’s Museum and President and Director of the Peace Corps Commemorative Foundation. His book, “Architect? A Candid Guide to the Profession” is known as the best basic introduction to the profession. He is Professor Emeritus of Architecture at the University of Maryland School of Architecture.

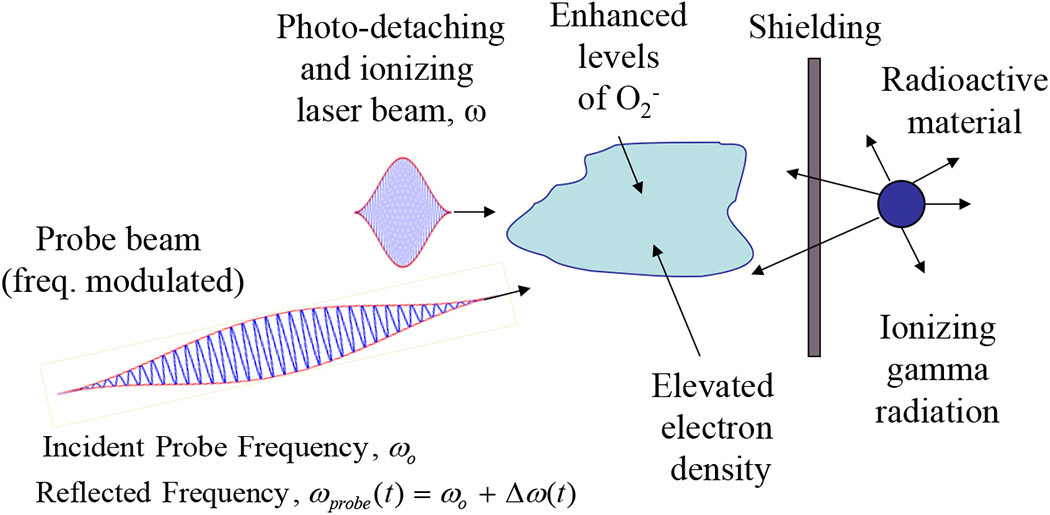
**Active remote detection of radioactivity based on electromagnetic signatures**

**By Phillip Sprangle, Bahman Hafizi, Howard Milchberg, Gregory S. Nusinovich and Arie Zigler**

Source: http://spie.org/x104009.xml

A proposed new concept uses laser radiation and a probe beam to detect electromagnetic signatures in the vicinity of radioactive material and enables standoff detection at distances greater than 100m.

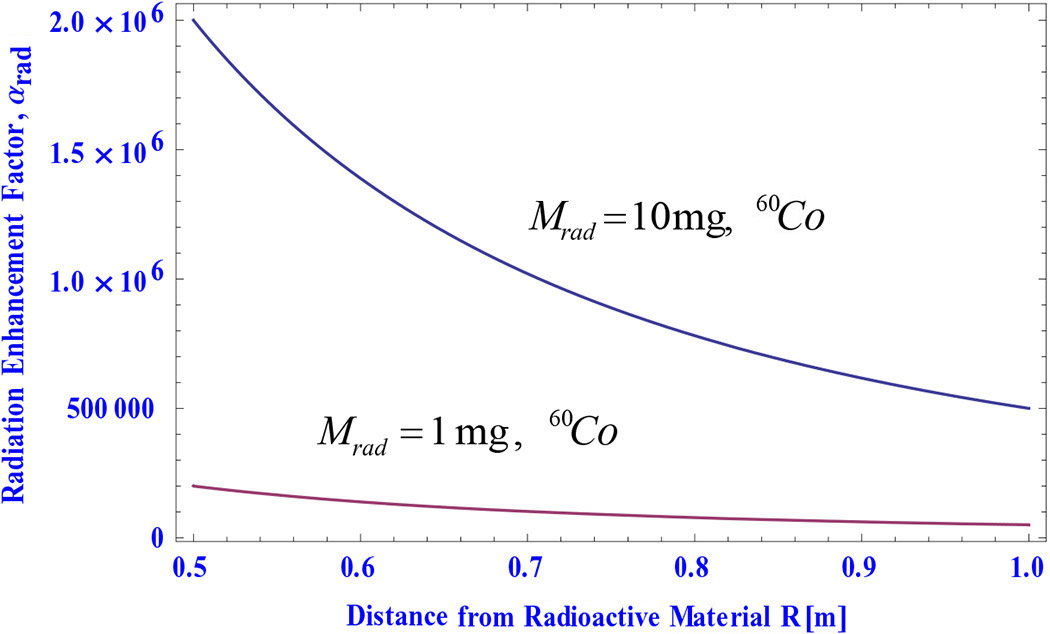
Sources of naturally occurring radioactivity range from rocks to bananas. Man-made radioactivity can be found in nuclear power plants and nuclear weapons. Moderate doses of radioactivity can be useful, for instance, in medicine and technology. At high doses, however, radioactivity is dangerous to biological entities, and it is important to have a robust means for its detection. A prominent example of this is the wrecked Fukushima Daiichi power plant in Japan. Another example is illicit transportation of radioactive materials. Other applications of methods for detecting radioactive materials include security and verification of compliance with arms control treaties. The most common type of radioactivity detector is the so-called Geiger-Müller tube: the sensing element of the familiar Geiger counter, which emits a click on detecting a particle of ionizing radiation. Useful as they are, existing techniques are passive, which results in limited sensitivity. They also have a very limited range (less than a few meters). Yet detection at extended range is critical, for example, in the case of illicit activities.

[](http://spie.org/Images/Graphics/Newsroom/Imported-2013/005044/005044_10_fig1.jpg)We previously proposed a radioactivity detection concept based on a high-power terahertz (THz) pulse that induces avalanche (collisional) breakdown and spark formation in the vicinity of the radioactive material.1,2 We have since observed that laser sources have the potential for longer standoff detection distances compared with THz sources. Here, we propose an alternative concept using laser radiation and a probe beam (e.g., millimeter beam) to detect electromagnetic signatures in the vicinity of radioactive material (see Figure 1). Studies we and others carried out between 2002 and 2008 analyzed3 and experimentally characterized4–6 propagation of short laser pulses in the atmosphere. These studies indicate the feasibility of propagating laser beams in the atmosphere as probes for the purpose of detection.

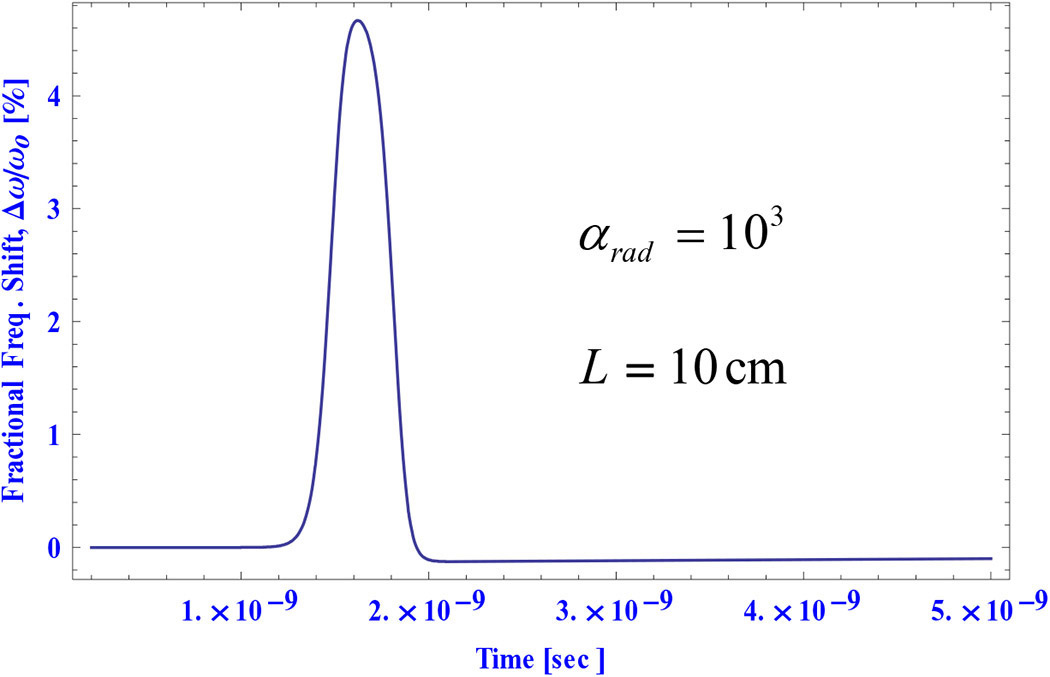
**Figure 1.** Schematic of active remote radioactivity detection concept. Laser radiation (frequency ω)photodetaches electrons from superoxide (O2−) ions, providing electrons for an avalanche (collisional) ionization process that increases the electron density, which modulates the frequency of a probe beam (e.g., millimeter beam).

The working principle is as follows. Radioactive materials emit gamma rays that ionize the surrounding air. The ionized electrons rapidly attach to oxygen molecules, forming superoxide (O2−) ions. The elevated population of O2− extends several meters around the radioactive material. Electrons are photodetached from O2− ions by laser radiation and initiate avalanche ionization, which results in a rapid increase in electron density. The rise in electron density induces a frequency modulation on a probe beam, which becomes a direct signature for the presence of radioactive material. Gamma rays emitted by radioactive material will increase the free electron density as well as the O2− density. Our proposed concept makes use of laser beams to photoionize the O2−, thus providing the seed electrons for air breakdown.

The rate of change of electron density is given by ∂Ne/∂t=(1+αrad)Qrad+Se−Le, where αrad is the radiation enhancement factor (a measure of the amount of radioactive material) and Qrad=20 disintegrations/cm3 is the ambient (background) radiation level, Se represents the various electron source terms, and Le is the electron loss terms.7–9 In the absence of radioactive material, αrad=0. Figure [2](http://spie.org/x104009.xml#fig2) shows the radiation enhancement factor αrad as a function of distance from the radioactive source, for 1 and 10mg of 60Co (cobalt-60).

[](http://spie.org/Images/Graphics/Newsroom/Imported-2013/005044/005044_10_fig2.jpg)**Figure 2.** Radiation enhancement factor (αrad) versus distance from source. Mrad: Mass of radioactive material. 60Co: Cobalt-60.

A probe beam of frequency ωo propagating in a time-varying electron density will undergo a frequency change that is given by Δω(z, t)=(2ωo)−1 [ωp2(t)−ωp2(t−z/c)], where ωp(z, t)=[4πq2Ne(z, t)/m]1/2 is the plasma frequency, q is the elementary electric charge, and m is the electron mass.

[](http://spie.org/Images/Graphics/Newsroom/Imported-2013/005044/005044_10_fig3.jpg)As an example of this method of detection, we consider the case where the ionizing laser has a peak intensity of 160GW/cm2 and pulse duration of 1ns. The probe beam is a millimeter wave source of frequency 94GHz. In the absence of radioactive material there is no frequency modulation of the probe. For αrad=103 and a probe-beam interaction distance of 10cm, the fractional frequency modulation is significant, ∼5%, which is readily detectable (see Figure [3](http://spie.org/x104009.xml#fig3)). In other words, the frequency shift is the sought-for electromagnetic signature of radioactive material and can be measured.

**Figure 3.** Fractional frequency shift Δω/ωo(%) versus time in the presence of radioactive material and a 1ns ionizing laser pulse. L: Probe-beam interaction distance.

In summary, we have proposed and analyzed a concept for active remote detection of radioactive materials. The frequency modulation on a probe beam is a signature of the radioactive material. Our analysis indicates that a measurable frequency shift can be expected for relatively small amounts of radioactive material. Proof-of-concept experiments are underway at the University of Maryland.

The authors acknowledge useful discussions with Victor Granatstein, Carlos Romero-Talamas, Richard Fernsler, and Steven Slinker. This work was supported by Naval Research Laboratory 6.1 base funds and by the Office of Naval Research.

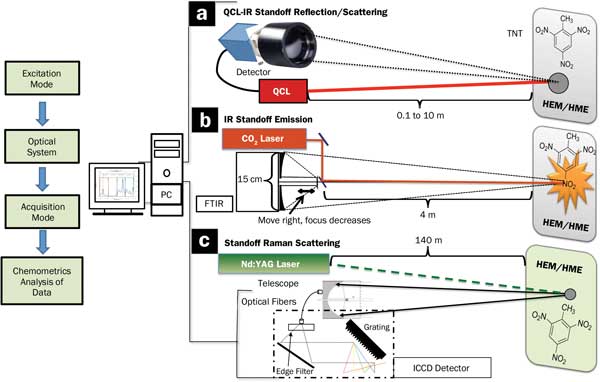
***Phillip Sprangle*** *is professor of engineering and physics at the the University of Maryland and senior scientist for directed energy physics at NRL. He is a fellow of the American Physical Society, OSA, IEEE, and the Directed Energy Professional Society.*

# Advances in Standoff Detection Make the World Safer

Source: http://photonics.com/Article.aspx?AID=53439

An abundance of new research and development in optical detection at a distance is increasing the ability of governments and military organizations to more efficiently identify and categorize explosives, biological agents and other threats.

Worldwide, government agencies and military branches are tasked with the formidable job of identifying evolving threats to national security such as concealed explosives, improvised explosive devices (IEDs), and airborne chemical and biological materials – without putting equipment or people in harm’s way. Lasers and optical techniques are of critical importance to standoff detection technology for their ability to passively and actively probe threats near and far.

Standoff detection can take place at distances from several centimeters up to a kilometer. Some standoff methods focus on chemical identification to detect explosives, breakdown products or biological signatures; they do this either up close without making contact with the target or by probing the environment from a distance. Often, standoff detection refers to the use of imaging technology such as video, x-ray and identification software to detect suspicious packages, wire, fragmentation materials, or other signs of IEDs or threats. The biggest challenges in standoff detection are extending the distance range at which effective identification can occur, improving signal detection over atmospheric and environmental noise and interference, and screening of multiple in-motion threats.

Three “active mode” standoff detection schemes for highly energetic materials (HEM) and homemade explosives (HME) in development include: (a) a quantum-cascade laser (QCL) infrared “eye safe” detection scheme for reflection and scattering, (b) a laser-induced thermal emission (LITE) detection scheme using a CO2 laser, and (c) a Raman scattering scheme using an Nd:YAG laser.

Since 2007, Erin A. Miller, senior research physicist in the Radiation Detection and Nuclear Sciences group at Pacific Northwest National Laboratory in Richland, Wash., has been part of a group developing a promising new technique for standoff explosives detection called differential phase-contrast x-ray imaging. The technology has potential for improved scanning and inspection of luggage, mail, small parts and contraband.1

The goal of phase-contrast imaging is to enhance detection and reduce the number of false alarms. It starts with a conventional x-ray source radiating through an object tens of centimeters away onto a detector 1 to 2 m from the source. The technique adds one to three silicon gratings between the source and the detector along with software processing to obtain three pieces of information: an x-ray image in absorption, a phase-contrast image and a scattering (dark field) image sensitive to nanometer- and micron-sized features such as those of powder and wood. The extra phase-contrast and scattering images are combined with the traditional x-ray image to create an image that can enhance discrimination of common explosives materials.

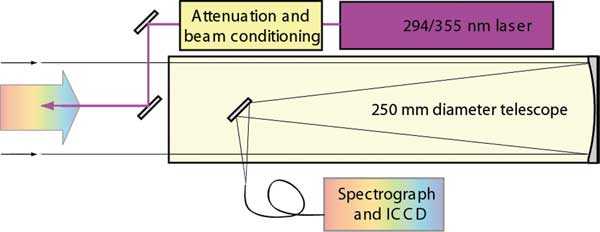
Challenges to making such a system practical include scaling up the x-ray source energy from the experimental energy of 40 kVp, Miller said. “The typical end-point energy of an airport baggage-screening system is 160 kVp. Designing a system at high enough energies requires gratings with extremely high aspect features, which are difficult to fabricate. The grating area also limits the field of view.”  
If design concerns can be overcome, such a system may appear soon at an airport near you, helping Transportation Security Administration agents discriminate threat materials such as explosives from what is in your bag.

**It’s in the air**

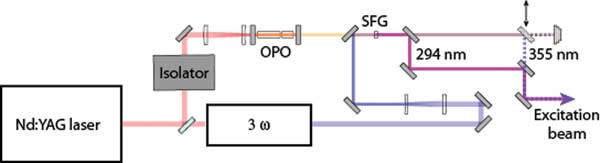
In the early 2000s, international concern about biological warfare agents increased as a result of coordinated attacks in Tokyo using sarin gas in 1995, suspicions of an Iraqi biological warfare program, and anthrax attacks on US Congress members and media outlets in 2001. Such concerns motivated NATO partners at the Norwegian Defence Research Establishment (FFI) in Kjeller to pursue better standoff detection systems for biological agents.

The lidar UV laser-induced fluorescence system demonstrated at the Norwegian Defence Research Establishment added a 294-nm laser to the more conventional 350-nm laser to improve identification of harmful bioaerosols such as anthrax.

While early instruments used ultraviolet laser-induced fluorescence (UVLIF, a lidar technique) to detect several spectral bands of excitation near 350 nm, many innocuous fluorophores, amino acids and other substances are also excited at that wavelength, making discrimination of threats challenging. Because these commonplace substances can be efficiently detected at shorter wavelengths, the FFI’s principal scientist, Øystein Farsund, and colleagues targeted the 280-nm region as an efficient wavelength for accompanying the conventional Nd:YAG 350-nm laser. Using both laser wavelengths at the same time, they theorized, would enable more effective weeding out of harmless targets and better identification of harmful bioaerosols.2   
  
The team switched between a 294-nm 10-Hz pulsed source and the 350-nm laser, both directed through a 250-mm-diameter optical telescope toward ambient bioaerosol molecules in a 5-m-long chamber. The reflectance and backscattered signal then returned through an Andor Technologies Shamrock 163i spectrograph and a range-gated intensified CCD camera with 7-nm resolution.

The laser setup for the lidar UVLIF bioaerosol detection system sent laser light from pulsed 355-nm and 294-nm lasers out via an optical telescope (spectral resolution 7 nm) that also collects the return fluorescence.

The experiments showed that UVLIF standoff detection of bioaerosols with a 294-nm laser is actually more efficient than at 355 nm with comparable pulse energies. Anthrax fluoresced at almost an order of magnitude stronger, and the toxin stimulant OA registered at twice the intensity at the shorter wavelength. With a higher intensity, standoff distance can be increased while reducing the incidence of false alarms.

“Our prime research goal is to increase the ability to discriminate one pathogen from another and from the background,” Farsund said. “In addition to the use of two excitation wavelengths, we also developed enhanced algorithms to optimize classification of bioaerosols.” With a few adaptations and optimizations, Farsund added, the lidar UVLIF technique may be applicable in surveillance of military camps and surroundings, as well as in an urban environment, such as underground stations and sports arenas.

Sum frequency mixing of a 1.7-µm optical parametric oscillator signal with the third harmonic of the 355-nm laser generated a 294-nm beam. A flip mirror and beam dump were used to switch between excitation wavelengths. Four combinations of glass filters and gratings determined the spectral responses of the system to fine-tune detection of seven different bioaserosol agents.

**Scratching the surface**

Samuel P. Hernández-Rivera, a chemistry professor at the University of Puerto Rico in Mayagüez, and colleagues are developing several advanced techniques for standoff detection of explosives, including laser-induced thermal emission, Raman and quantum cascade laser (QCL)-based detection.3 One caveat for Raman and CO2 standoff detection is that they use powerful, highly focused lasers and, as such, are not eye-safe.

“The DHS is trying to get away from lasers that damage the eye,” Hernández said. “They’re encouraging technologies like QCL, which is in the mid-IR, where the eye doesn’t focus and the power is too low to burn the retina. The QCL laser and the Fourier transform infrared (FTIR) both have a wide focus and are eye-safe.”

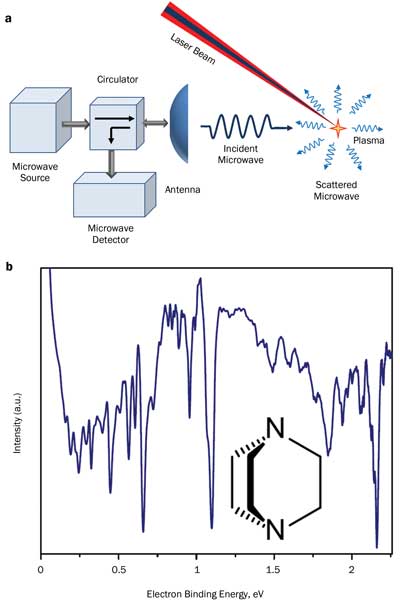
In one FTIR experiment, the team demonstrated that samples of highly energetic materials deposited on aluminum substrates could be easily discriminated if the aluminum was heated outdoors by sunlight. This passive standoff detection system coupled a reflecting telescope to an FTIR spectrometer equipped with a cryo-cooled mercury cadmium telluride detector.

The system confirmed detection of 2,4,6-Trinitrotoluene (TNT) with high confidence at distances from 4 to 55 m for several target surface temperatures. This FTIR system demonstrates effective detection of explosives traces deposited on substrates (glass, metals, painted metals, rag, travel baggage materials and others) at levels as low as nanograms per square centimeter. Thermal excitation using a tungsten-halogen lamp as a heat source to achieve a temperature difference of only 1° also proved useful for enhancing the TNT vibrational signatures.4

Baking in the sun is a useful tool for enhancing the vibrational signature of TNT in passive mode. (a) The sunlight-excited emission spectrum of 2,4-TNT deposited on an aluminum substrate (400 µg/cm2) measured 20 m from detector (Bruker Optics, EM27); (b) Reference (reflectance) spectrum of 2,4-TNT measured on a bench FTIR interferometer (Bruker Optics, IFS 66/v-S).

“The further addition of enhanced multivariate (chemometrics) regression algorithms better allows us to look for the needle in the haystack, discriminating against interferences,” Hernández said. Systems are under development in collaboration with Eos Photonics in Cambridge, Mass., and other industrial partners.  
  
**A better fingerprint**

Most well-established standoff trace-chemical sensing is based on the use of lasers to remotely acquire the vibrational spectra of target molecules. Unfortunately, vibrational spectra get more complex as molecular size increases and, thus, poorly resolved, making detection of large organic molecules such as those of explosives and chemical warfare agents challenging.

a) Trace chemical sensing using Rydberg spectroscopy/microwave scattering involves UV laser pulses at a fixed wavelength overlapped with tunable VIS/IR laser pulses and focused on a target. The UV pulse photoexcites molecules into the 3-s Rydberg state, while the VIS/IR pulse probes transitions between the 3-s Rydberg state and higher-lying Rydberg states. The ionized molecules produce a plasma probed via microwaves. (b) A Rydberg spectrum of 1,4-diazobicyclooctane is acquired via microwave scattering from a laser-induced plasma.

Scientists at Oak Ridge National Laboratory (ORNL) in Tennessee are developing an alternative approach for standoff trace chemical sensing that uses transitions between molecular Rydberg states. Molecular Rydberg states are excited electronic states with wave functions resembling those of a hydrogen atom. Peter Weber, professor of chemistry at Brown University in Providence, R.I., demonstrated that transitions between molecular Rydberg states reveal highly resolved spectra that are sensitive to the molecular structure. Complexity of Rydberg spectra does not scale with molecular size, making the technique well suited for detection of large organic molecules such as those of explosives and chemical warfare agents. But recovery of Rydberg spectra requires photoionization, which typically is detected via mass spectrometry or photoelectron spectroscopy. Both techniques require high vacuum, unsuitable for standoff detection.

As a solution, Fedor Rudakov, a research staff scientist at ORNL, in collaboration with Zhili Zhang at the University of Tennessee, Knoxville, has suggested acquiring Rydberg spectra via microwave scattering from the plasma produced by photoionization. Rydberg spectroscopy and microwave scattering are a perfect match, combining the high selectivity and applicability to large molecules with a capability for standoff detection. The technique uses radiation in the UV/VIS range, for which high-power laser sources are readily available.5 Although the method is still in early-stage R&D, Rudakov expects the technique will be scalable to chemical sensing over tens of meters.

# Why the US should keep cooperating with Russia on nuclear security

**By Siegfried S. HeckerPeter E. Davis**

Source: http://thebulletin.org/why-us-should-keep-cooperating-russia-nuclear-security7207

“You have been brainwashed,” our Russian hosts lamented during dinner at their Moscow apartment in late April. We had asked them how they reconcile biased Russian news reports with evidence of Russian Special Operations Forces in the Crimea and eastern Ukraine. “What does Washington think it is doing by sending the CIA chief to Kiev to support those fascists?” they asked in response.

We were surprised that without exception every one of our Russian colleagues, nuclear scientists who in some cases we have known for 25 years, defended Moscow’s actions and criticized Washington and the West over Ukraine. Over after-dinner vodka, we agreed that we cannot reconcile our views of what is happening in Ukraine, so we returned to problems that require our continued attention, namely how to prevent nuclear proliferation and guard against nuclear terrorism. We agreed that we have made a lot of progress working together over the past 20-plus years, but that we are not done.

The purpose of our visit was to finish work on a book we are jointly writing about how Russian and American nuclear scientists joined forces at the end of the Cold War to help deal with nuclear risks in Russia and other states of the former Soviet Union. These new risks had resulted from post-Soviet chaos and the breakdown of nuclear order. One of the main objectives of the book is to rejuvenate nuclear cooperation, which Moscow has dramatically curtailed during the past decade after having fostered it during the first decade following the end of the Cold War. During the past few years, Moscow has sent an unambiguous message to Washington—namely, that the United States can shift its efforts at nuclear security cooperation to the rest of the world, but that it is done in Russia. The shift resulted from Moscow’s increased confidence in its own nuclear security and its security services’ determination to keep Americans out of Russia’s nuclear facilities.

In contrast to Moscow’s pronouncements, Russia’s nuclear specialists recognize that continued cooperation is needed. Nuclear safety and nuclear security are never-ending jobs that require cooperation and sharing of best practices. Russia’s experts do not want to return to nuclear isolation because they believe it led to the 1986 Chernobyl disaster and to the nuclear security crisis following the breakup of the Soviet Union.

Now, the crisis in Ukraine has not only put nuclear cooperation between the United States and Russia on the back burner, but Washington appears to be erecting its own roadblocks that threaten to irreparably damage such cooperation. The House Armed Services Committee recently approved legislation that would put nuclear security cooperation with Russia on hold. While the White House has opposed the committee’s efforts to limit cooperation, the Energy Department has issued its own restrictions on scientific interchanges as part of the US sanctions regime against Russia.

It is clearly in Moscow and Washington’s common interest to prevent the proliferation of nuclear weapons and global nuclear terrorism. Keeping all nuclear materials in control of governments and erecting effective barriers to nuclear trafficking requires cooperation. It is in their common interest to make further arms reductions, rather than return to the arms race era and nuclear testing. And, if nuclear power is to provide clean electricity in more places around the world, Russia and the United States must share a common goal of making sure this spread happens safely and without exacerbating proliferation concerns.

These are precisely the objectives the Obama administration had been promoting with Russia and around the world, although Moscow has become a reluctant partner. Now, Washington appears willing to sacrifice nuclear cooperation in the short term in order to sanction Russia for its actions in Ukraine. But Washington does not have to choose between the two. It should be able to pressure Moscow on Ukraine, while still cooperating on nuclear issues.

Progress on the nuclear front requires good working relationships between Russian and American scientists. These relationships, already strongly opposed by Russia’s security services, cannot be turned off and on at will. They must be nurtured and maintained over time to foster the cooperation needed to reduce the nuclear dangers. Relationships are difficult to rebuild once they have been cut off.  In addition, curtailing cooperation now will threaten the gains that have been made over the past 20 years and jeopardize Washington’s enormous investment in cooperative threat reduction.

We realize, however, that the nature of nuclear cooperation must change to reflect Russia’s economic recovery and its political evolution over the past two decades. Future cooperative threat reduction programs must also reflect the return to adversarial governmental relations resulting from the Ukraine crisis. The programs must change from wide-ranging US-funded and -led activities to more selective, jointly sponsored collaborations in the two countries’ common interest.

A strong US role in nuclear security cooperation remains imperative. In spite of Moscow’s assertion to the contrary, its vast stockpile of nuclear materials remains vulnerable to theft or diversion. Whereas the physical security of nuclear facilities has improved greatly, both because of years of American support and the re-emergence of Russia’s overbearing security services, control and accounting of nuclear materials, which are crucial to combat insider threats, still fall far shy of international best practices. For example, Russia still has no baseline inventory of all nuclear materials the Soviet Union produced and where they are today. Moreover, it has shown no interest in trying to discover just how much material is unaccounted for. Our Russian colleagues voice concern that progress on nuclear security in their country will not be sustained once American cooperation is terminated. They believe that Russia’s nuclear security culture and the government’s commitment to fund continued security upgrades are still very fragile and require continued cooperation.

It is also in Washington’s interest for Russia to cooperate on preventing the proliferation of nuclear weapons. Iran is a good case in point. Much progress has been made toward a negotiated settlement of Iran’s nuclear program since President Hassan Rouhani was elected in June, 2013. However, little would have been possible without US-Russia cooperation. It is not in Moscow’s interest to have nuclear weapons spread to its near abroad. It needs Washington’s continued global leadership in this area. Washington, in turn, needs Moscow; especially if it is to develop more effective measures to prevent proliferation as Russia and other nuclear vendors support nuclear power expansion around the globe.

Although cooperation related to the stewardship of Washington and Moscow’s respective nuclear arsenals would be more difficult in an adversarial governmental relationship, there are numerous areas that would still benefit from collaboration. Scientific understanding of such problems as the aging of plutonium remains elusive and beyond the full reach of either country. One of the authors of this column has personally been involved in plutonium science collaboration with his Russian counterparts for the past 15 years. Continued cooperation in this area, as in some areas of nuclear weapon safety and security, remain in our common interest.

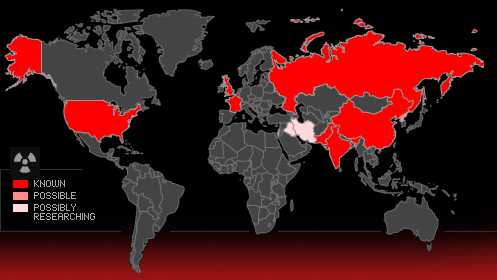
As the United States and the European Union take short-term measures to restrain Russia’s actions in Ukraine, they should not sacrifice the hard-earned gains made to stabilize the nuclear threats that arose after the dissolution of the Soviet Union. Some forms of nuclear cooperation, especially on arms control and nonproliferation, were supported even during the darkest days of the Cold War, because the alternatives proved unacceptable to both sides. With the Cold War’s end, nuclear cooperation flourished. Washington should foster continued cooperation to meet our shared challenges, rather than allowing it to be held hostage to the Ukrainian crisis. Over the past 20-plus years, when working with our Russian colleagues, we have all found that at times we must move beyond political disagreements, such as the political situation in Ukraine, to work together to advance the cause of nuclear security.

***Peter E. Davis*** *is a research assistant to Siegfried Hecker at Stanford University’s Center for International Security and Cooperation (CISAC). He received his bachelor of arts in international relations, with honors, from Stanford University in 2011.*

***Siegfried Hecker*** *is a senior fellow and affiliated faculty member at Stanford University's Center for International Security and Cooperation (CISAC) and the Freeman Spogli Institute for International Studies. He is also a research professor in the Department of Management Science and Engineering at Stanford. He is director emeritus of the Los Alamos National Laboratory, where he served as director from 1986 to 1997 and as senior fellow until July 2005.*

## Number of world’s nuclear weapons reduced, but modernization continues

Source: http://www.homelandsecuritynewswire.com/dr20140617-number-of-world-s-nuclear-weapons-reduced-but-modernization-continues

The Stockholm International Peace Research Institute (SIPRI) yesterday released its annual nuclear forces data, which assesses the current trends and developments in world nuclear arsenals. SIPRI notes that the data shows that while the overall number of nuclear weapons in the world continues to decline, none of the nuclear weapon-possessing states are prepared to give up their nuclear arsenals for the foreseeable future.

At the start of 2014 nine states — the United States, Russia, the United Kingdom, France, China, India, Pakistan, Israel, and North Korea — possessed approximately 4000 operational nuclear weapons. If all nuclear warheads are counted, these states together possessed a total of approximately 16,300 nuclear weapons compared to 17,270 in early 2013.

Over the past five years there has been a steady decline in the overall number of nuclear warheads in the world. The decrease is due mainly to Russia and the United States — which together still account for more than 93 percent of all nuclear weapons — further reducing their inventories of strategic nuclear weapons under the terms of the Treaty on Measures for the Further Reduction and Limitation of Strategic Offensive Arms (New START).

At the same time, all five legally recognized nuclear weapon states — China, France, Russia, the United Kingdom, and the United States — are either deploying new nuclear weapon delivery systems or have announced programs to do so. India and Pakistan continue to develop new systems capable of delivering nuclear weapons and are expanding their capacities to produce fissile material for military purposes.

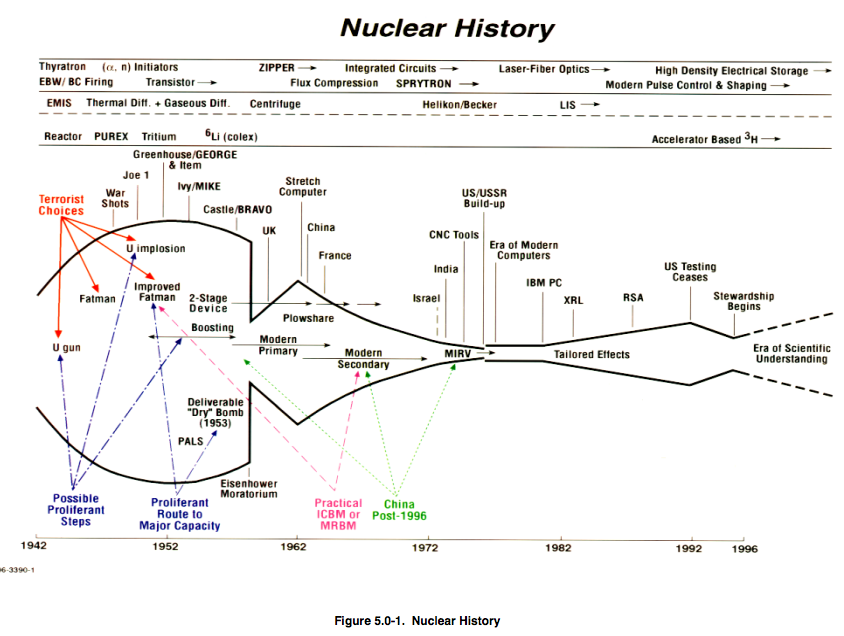
There is an emerging consensus in the expert community that North Korea has produced a small number of nuclear weapons, as distinct from rudimentary nuclear explosive devices.

**Number of nuclear weapons held by states**

* United States – 7,300
* Russia – 8,000
* United Kingdom – 225
* France – 300
* China – 250
* India – 90-110
* Pakistan – 100-120
* Israel – 80
* North Korea – 6-8

# This One Chart Shows 50 Years Of Nuclear Weapons Development

Source: http://www.businessinsider.com.au/fifty-years-of-nuclear-development-in-one-chart-2014-6



It’s easy to forget that nuclear energy is a fairly recent invention, and that the “age of discovery” of nuclear weapons was a surprisingly brief period. This chart, from a 1998 Department of Defence manual on “Weapons of Mass Destruction Technologies,” traces the worldwide spread of nuclear technology from 1942.

The top line tracks the development of triggering mechanisms for nuclear reactions. The next line does the same for uranium enrichment technology, while the third follows the progress of plutonium extraction methods.

The larger bottom timeline includes the major events in nuclear weapons development up until 1996. It marks when the declared or suspected nuclear powers other than Russia and the U.S. achieved their capability. In 1996, that meant only five other countries were included on the timeline. It would be only a relatively short time before Pakistan and North Korea tested weapons. (South Africa appears on the timeline, but the country [voluntarily destroyed its small nuclear stockpile](http://www.latimes.com/opinion/op-ed/la-oe-deklerk-south-africa-nukes-20131222-story.html) when the apartheid regime fell in the mid-90s.)

The timeline shows other big developments, like the Cold War arms race, progress in computer processing, and the notorious detonation of the high-yield [Castle Bravo](http://www.brookings.edu/blogs/up-front/posts/2014/02/27-castle-bravo-largest-us-nuclear-explosion-rowberry) thermonuclear device that resulted in massive contamination. And arrows on the far left of the chart indicate the initial steps any would-be nuclear power has to take en route to a weapons capability, like mastering uranium implosion or researching how to optimise a nuclear reaction’s yield.

Most interestingly, the chart has a novel method of visualising the rate of technological progress and conveying just how rapidly humanity entered the nuclear age.

The curve represents the frequency with which American scientists have made new nuclear discoveries. “The distance between the two curves represents the rate of progress,” the document explains, “while the area between the curves from 1942 to any arbitrary date gives an estimate of the total knowledge acquired.” A flat curve means slow progress and little new knowledge acquired. The curve is practically circular in the 1940s, when the nuclear era kicked off. And by the 1990s, the curve had flatlined — perhaps comfortingly.

But the report warns that nuclear development and broader technological progress aren’t as related as they might seem. The curve was at its fattest long before advanced computing technology was widely available. “All five acknowledged nuclear weapons states are shown to have tested their first devices before computer numerically controlled machine tools and four- or five-axis machine tools were generally available,” the report says.

If anything, the timeline shows that the barriers to nuclear development aren’t technological in nature. Instead, it’s a question of domestic political will and the vagaries of international politics. For instance, the curves abruptly narrow because of a late-1950s U.S.-Soviet agreement to halt nuclear testing.

The development of nuclear weapons is a historical watershed. It transformed international politics and gave an existential dimension to relations between the world’s great powers. Today, the maintenance and protection of the American nuclear arsenal is a trillion-dollar concern, while an incredible degree of both U.S. and global diplomacy is dedicated to preventing new countries from going nuclear. The mere fact that the human race is capable of wiping itself out within minutes is a recent development in world history, and one that politicians, artists, and thinkers have grappled with for decades.

This chart offers a mixed message for those concerned about nuclear proliferation. The world has the ability to peacefully limit the advancement of nuclear technology. But major leaps forward are possible even under circumstances that would seem primitive by today’s technological standards.

And nuclear weapons technology is already out there, with an over 70-year head start on attempts to contain it.

## Using cosmic rays to peer inside Fukushima Daiichi reactors

Source: http://www.homelandsecuritynewswire.com/dr20140620-using-cosmic-rays-to-peer-inside-fukushima-daiichi-reactors

Muon radiography (also called cosmic-ray radiography) uses secondary particles generated when cosmic rays collide with upper regions of Earth’s atmosphere to create images of the objects that the particles, called muons, penetrate. The process is analogous to an X-ray image, except muons are produced naturally and do not damage the materials they contact. Los Alamos National Laboratory the other day announced an impending partnership with Toshiba Corporation to use muon tomography safely to peer inside the cores of the Fukushima Daiichi reactors and create high-resolution images of the damaged nuclear material inside without ever breaching the cores themselves. The initiative could reduce the time required to clean up the disabled complex by at least a decade and greatly reduce radiation exposure to personnel working at the plant.

Los Alamos National Laboratory the other day announced an impending partnership with Toshiba Corporation to use a Los Alamos technique called muon tomography safely to peer inside the cores of the Fukushima Daiichi reactors and create high-resolution images of the damaged nuclear material inside without ever breaching the cores themselves. The initiative could reduce the time required to clean up the disabled complex by at least a decade and greatly reduce radiation exposure to personnel working at the plant.

“Our recent technical work has clearly shown that the muon scattering technique pioneered at Los Alamos provides a superior method for obtaining high-resolution images of nuclear materials inside structures, and this will allow plant operators to establish the condition of reactor-core material without the need to actually get inside,” said Duncan McBranch, Los Alamos’s Chief Technology Officer. “One of the most challenging, time-consuming and potentially dangerous tasks in cleaning up after a reactor accident is determining the condition and location of the core material, especially when the material itself may have melted and flowed to a different part of the building. Invasive techniques such as video endoscopy or introduction of robots run the risk of releasing radiation. Furthermore, those techniques at best offer a partial view of material location. Muon tomography will enable plant operators to see the location of the nuclear material inside, determine its condition, and provide crucial insight that can inform the design of a safer and faster cleanup. We are hopeful that our partnership with Toshiba will assist the Tokyo Electric Power Company and the Japanese government in their efforts to accelerate cleanup operations in the safest way possible.”

An LANL release reports that muon radiography (also called cosmic-ray radiography) uses secondary particles generated when cosmic rays collide with upper regions of Earth’s atmosphere to create images of the objects that the particles, called muons, penetrate. The process is analogous to an X-ray image, except muons are produced naturally and do not damage the materials they contact. Muon radiography has been used before in imaginative applications such as mapping the interior of the Great Pyramid at Giza, but Los Alamos’s muon tomography technique represents a vast improvement over earlier technology.

In developing muon tomography, Los Alamos researchers found that by placing a pair of muon detectors in front of and behind an object, and measuring the degree of scatter the muons underwent as they interacted with the materials they penetrated, they could gather detailed images. The method works particularly well with highly interfering materials (so-called “high Z” materials) such as uranium. Because the muon scattering angle increases with atomic number, core materials within a reactor show up more clearly than the surrounding containment building, plumbing and other objects. Consequently, the Los Alamos muon tomography method shows tremendous promise for pinpointing the exact location of materials within the Fukushima reactor buildings.

“Los Alamos researchers began working on an improved method for muon radiography within weeks of the 2011 earthquake and tsunami that damaged the Fukushima reactor complex,” said Christopher Morris, chief scientist and leader of the Los Alamos Muon Tomography Team. “Within 18 months we had refined our technique and published a paper showing that the Los Alamos method was superior to traditional muon radiography techniques for remotely locating and identifying nuclear materials, and that it could be employed for field use.”

As part of the partnership, Los Alamos will assist Toshiba in developing a Muon Tracker for use at the Fukushima plant.

The release notes that Los Alamos’s muon tomography technology also has the potential to be deployed in locations around the world to help detect smuggled nuclear materials. In fact, Los Alamos previously granted an exclusive license to Decision Sciences International Corporation for broad commercialization of the Los Alamos technology. The company has successfully deployed portal monitors that use muon tomography at a major seaport for cargo-container scanning as well as at other locations under their licensing agreement.

Muon tomography and development of its application at Fukushima was made possible in part through Los Alamos’ Laboratory-Directed Research and Development Program (LDRD), which uses a small percentage of the Laboratory’s overall budget to invest in new or cutting-edge research.

# Dirty bomb material secured at site in Philadelphia, thousands of sites remain in U.S.

Source: http://www.foxnews.com/tech/2013/03/15/dirty-bomb-material-secured-at-site-in-philadelphia/

Raw, radiological material that terrorists could use to build a dirty bomb was secured in a Philadelphia school this week.

On March 11, the U.S. National Nuclear Security Administration (a semiautonomous branch of the Energy Department) and Philadelphia’s Temple University announced they had secured a device containing cesium 137 -- one of more than two dozen such elements used in medicine and industry that could be turned into a dirty bomb.

“This operation is part of NNSA’s broad strategy to keep dangerous nuclear and radiological material safe and secure by enhancing our nation’s security,” NNSA deputy administrator Anne Harrington said.

A terrorist dirty bomb attack using domestic radioactive sources bomb may seem preposterous, yet the NNSA has identified more than 2,700 vulnerable buildings with high-priority radiological material in the United States alone.

**As of Feb. 28, 2011, only 251 of these buildings had completed NNSA security enhancements. The agency hopes the rest will do so by 2025 -- leaving another 12 years of vulnerability to theft and misuse.**

Dirty bombs are far easier to construct than nuclear bombs and do not use fissile material such as enriched uranium or plutonium. Extracting plutonium requires a reactor and enriching uranium is no easy task. Dirty bombs (security forces all them “radiation dispersal devices”) use conventional explosives such as car bombs to scatter radioactive materials through a densely populated area.

The physical damage is limited and the threat of dying from radiation exposure very small with such a device. But a dirty bomb would cause extensive economic damage and social upheaval while instilling panic and fear in civilians.

**Philadelphia, New York City, and around the country**

**In this case, the material came from a medical research irradiator that was removed from Temple University’s Old Medical School Building and transported to a secure location, where it will be prepared for disposal at a federal facility** (photo in p.27).

The device had been used in medical research for two decades. The cesium-137 left within it would have been an attractive target.

Prior to this decommissioning, Temple University had worked with the NNSA to install security enhancements in all their facilities with high-activity radiological materials. The city of Philadelphia has collaborated with the agency as well to secure 28 buildings with high-activity radiological materials since 2005.

**Just over two years ago, another terrorist treasure trove was recovered from a warehouse a mere 25 miles outside of Manhattan.** On January 2010, the NNSA secured of high-activity radioactive devices containing enough cesium-137 to make a bomb.

"Properly disposing of more than 3,000 curies of Cesium eliminates the threat this material poses if lost or stolen and used in a dirty bomb," NNSA administrator Thomas P. D'Agostino said at the time.

The agency has recovered and secured more than 31,000 disused and surplus radioactive sealed sources within the United States, eliminating more than a million curies of what is essentially radiological catnip for terrorists.

Each year, thousands of sources become disused and unwanted in the United States. There are regulatory requirements for in-place secure storage, and the Global Threat Reduction Initiative also helps to remove these sources for permanent and safe disposal.

Yet thousands more civilian sites use radiological materials for commercial, medical and research applications.

**Threat level**

**There are approximately twenty-five different radionuclides used in medicine and industry, from devices to measure product moisture and monitor pipe corrosion through to power sources.**

Sources, often referred to as “sealed sources,” tend to be small metal containers with radioactive material sealed inside.

The container is meant to prevent radiation from escaping, and as long as the housing remains intact and sealed (and it is properly handled), it presents no health risk.

To purchase a device with this sort of material requires a licensed and plans to safely and legally dispose of it. The International Atomic Energy Agency ranks the potential harm of such devices from 1 to 5.

Category 1 sources such as irradiators or teletherapy machines could cause death or permanent injury to those in close proximity for a short period of time, ranging from minutes to hours. Category 5 sources like X-ray fluorescence devices could cause minor temporary injury.

Upgrading physical security at civilian radiological sites is paramount, and NNSA works in cooperation with federal, state and local agencies, and private industry to install security enhancements on high priority nuclear and radiological materials.

Some facilities do not have the resources to make these security upgrades and NNSA will provide the funding if the facility agrees to take over future maintenance.

In April 2009, President Obama announced that he would secure vulnerable nuclear material around the world within four years. He described a terrorist acquiring nuclear weapons as "the most immediate and extreme threat to global security."

**The President’s FY 2012 budget request included $2.5 billion, and $14.2 billion over five years, to reduce this global nuclear threat. Yet four years have elapsed and the vulnerable material has not been completely secured.**

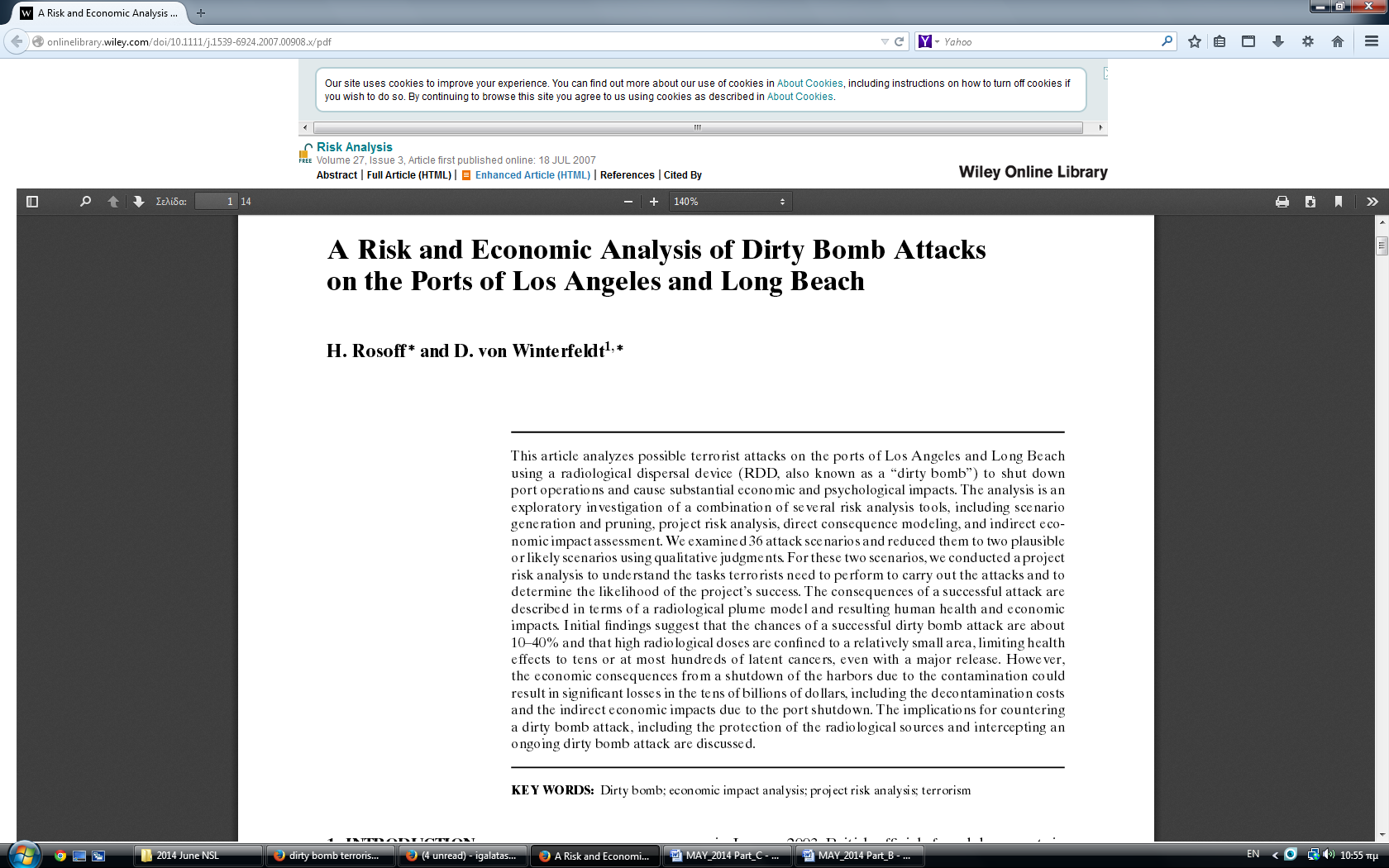
In most dirty bomb scenarios hundreds may die from the blast, but only a few, if any at all, would die from radioactivity. It is the fear of radiation or terror that a dirty bomb would unleash that makes it so attractive to terrorists.

Even if there isn’t a health threat, the public could be expected to panic about the radiation risks, possibly causing economic paralysis, mass evacuations, and displaced populations reluctant to return to their homes.

The Nuclear Regulatory Commission is developing a database to track sources. Both this National Radioactive Source Database and the Nuclear Materials Events Database to track lost sources will not be available to the public.

|  |
| --- |
| **In working to prevent the use of domestic radioactive sources in a terrorist attack, NNSA has successfully completed the following:**   * Identified more than 2,700 vulnerable buildings to date with high-priority radiological material in the United States. * As of February 28, 2011, completed NNSA security enhancements at 251 of these buildings, with the remainder aiming to be completed by 2025. * Identified more than 800 Cesium irradiators domestically, 238 received security enhancements to date using the NNSA-developed in-device delay (IDD) security technology. |

A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach

Source: <http://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00908.x/pdf>

# Nuclear Bombs vs Dirty Bombs vs Suitcase Bombs vs EMP Bombs

Source: http://www.nukepills.com/nuclear-dirty-bombs/

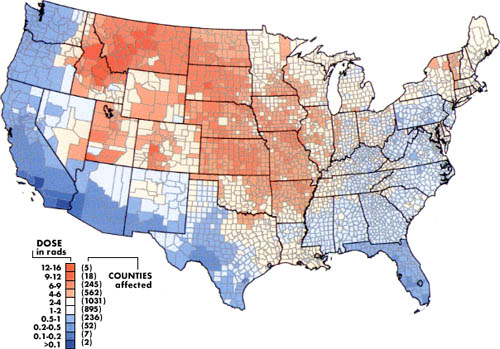
During the Cold War in the 1950s and early 1960s, the U.S. government conducted about one hundred nuclear weapons (atomic bomb) tests in the atmosphere at a test site in Nevada. The radioactive substances released by these tests are known as “fallout.” They were carried thousands of miles away from the test site by winds. As a result, people living in the United States at the time of the testing were exposed to varying levels of radiation.

Among the numerous radioactive substances released in fallout, there has been a great deal of concern about and study of one radioactive form of iodine (called iodine-131, or I-131) which collects in the thyroid gland. People exposed to I-131, especially during childhood, may have an increased risk of thyroid disease, including thyroid cancer. One particular personal radiation detector has the technology to detect both the beta and gamma radiation of I-131.

According to the National Cancer Institute’s 1999 report “Exposure of the American People to Iodine-131 from Nevada Nuclear-Bomb Tests” exposure to I-131 from the tests will produce between 11,300 and 212,000 excess lifetime cases of thyroid cancer with a point or central estimate of 49,000 cases.  
I-131 Dose/Risk Calculator

**Radioactive Iodine (I-131) exposure from nuclear bombs**

Radioactive Iodine is a byproduct of nuclear fission processes in nuclear reactors and nuclear weapons such as atomic bombs and suitcase bombs. You can protect yourself from the effects of cancer-causing radioactive iodine with FDA Approved IOSAT™ or ThyroShield™ Potassium Iodide (KI). A non-prescription drug, Potassium Iodide protects against radioactive iodine by preventing its absorption by the thyroid gland located in the neck. The U.S. government has a limited supply in case of a nuclear bomb detonation or nuclear reactor accident/attack, yet Potassium Iodide must be taken during or before exposure to radioactive iodine to be effective. You may order it from this website today. View our Potassium Iodide page for more information including F.A.Q.s.

**Exposure of American People to I-131 (Radioactive Iodine) from Nevada Nuclear Bomb Tests in the 1950s and 1960s**

## Suitcase Bombs

In 1997, the public became aware of a Russian nuclear device they had not known even existed–the “suitcase bomb”. One of these portable nuclear bombs had an explosive charge of one kiloton, equivalent to one thousand tons of TNT. If a device like this made its way to the U.S. it could destroy everything within a half-mile radius of the Capitol in Washington, D.C. Within hours, prevailing winds would carry the nuclear fallout throughout Washington. Radioactive Iodine (I-131) would be carried downwind for miles. One particular personal radiation detector has the technology to detect both the beta and gamma radiation of I-131.

Another portable weapon is a “backpack” bomb. The Soviet nuclear backpack system was made in the 1960s for use against NATO targets in time of war and consists of three “coffee can-sized” aluminum canisters in a bag. All three must be connected to make a single unit in order to explode. The detonator is about 6 inches long. It has a 3-to-5 kiloton yield, depending on the efficiency of the explosion. It’s kept powered during storage by a battery line connected to the canisters.

## Dirty Bombs

A “dirty bomb” is a conventional explosive, such as dynamite, salted with radioactive waste that scatters when the bomb goes off. It is not a nuclear bomb. The bomb can kill or injure through the initial blast of the conventional explosive and through the dispersal of the radioactive materials– hence the term “dirty.” Such bombs could be small devices or as big as a truck bomb.

There are four categories of radioactive waste ranging from very low-level waste that can be safely disposed of with ordinary refuse, to high-level waste such as spent nuclear fuel. Substantial amounts of radioactive waste are generated through civilian and military applications of radionuclides in medical facilities, food irradiation plants, chemical and manufacturing plants, etc. Some types of radioactive waste would be easier to obtain than others in order to make a “dirty bomb”.

Radiation detectors are needed to alert officials of their presence. One particular personal radiation detector has the technology to detect Gamma, X-ray and Beta radiation. This includes the ability to detect radioactive iodine, of which Potassium Iodide protects against and would most likely not be present in a dirty bomb due to the fact that it is a byproduct of nuclear fission which takes place only within nuclear reactors and during the detonation of a nuclear bomb. Obviously this type of ‘radioactive waste’ would be very difficult to obtain and incorporate in the makings of a dirty bomb.

If a dirty bomb detonates in your area, follow the instructions of local health officials concerning evacuation, decontamination and the administering of potassium iodide (though unlikely). Nukepills.com offers the Dirty Bomb Emergency Kit™ for detection and decontamination of radiation likely found in a dirty bomb.

**Federal Government statements on Dirty Bomb radiation**

* **Beta and Gamma Radiation:** “…***cesium-137*** is of particular concern because it is a potential component of a conventional explosive device (a “dirty bomb”) containing radioactive material.” - [FDA “Dirty Bomb” treatment document](http://www.fda.gov/bbs/topics/NEWS/2003/NEW00868.html)
* **Beta Radiation:** “…the Bush administration’s consensus view was that Osama bin Laden’s al Qaeda terrorist network probably had such often-stolen radioactive contaminants as ***strontium 90*** [Beta radiation] and ***cesium 137*** [Gamma radiation], which could be used to make a dirty bomb.” – [Terrorism Q&A, Council on Foreign Relations](http://72.14.203.104/search?sourceid=navclient&ie=UTF-8&rls=GGLG,GGLG:2005-50,GGLG:en&q=cache:http%3A%2F%2Fwww.terrorismanswers.org%2Fweapons%2Fdirtybomb.html)
* **Gamma Radiation:** “***Thallium-201*** has also been mentioned as a potential component of a dirty bomb.” – [*FDA Dept of Health and Human Services*](http://www.fda.gov/OHRMS/DOCKETS/98fr/03d-0023-nad00001.pdf) (PDF file)
* “A variety of radioactive materials are commonly available and could be used in an RDD [Radiological Dispersal Device, a.k.a. Dirty Bomb], including ***Cesium-137, Strontium-90, and Cobalt-60***.” – [CIA report: Terrorist CBRN: Materials and Effects](http://www.cia.gov/cia/reports/terrorist_cbrn/terrorist_CBRN.htm)
* [NRC Dirty Bomb Fact Sheet](http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs.html)

## 

## EMP (Electromagnetic Pulse) Bombs

An electromagnetic pulse EMP is a byproduct of detonating an atomic bomb above the Earth’s atmosphere. When a nuclear weapon is detonated in space, the gamma rays emitted trigger a massive electrical disturbance in the upper atmosphere. Moving at the speed of light, this overload will short out all electrical equipment, power grids and delicate electronics on the Earth’s surface. In fact, it would take only one to three weapons exploding above the continental United States to wipe out our entire grid and transportation network. It might take years to recover from, if ever.

RADTriage™ Radiation Detector is impervious to an EMP bomb. The RADTriage™ Radiation Detector will continue to work after an EMP bomb detonation because it has no electronics.

|  |
| --- |
| **SCENARIO: Radiological (Dirty Bomb)**  Source: http://www.orau.gov/cdcynergy/erc/content/activeinformation/scenario-3\_content\_print.htm |
| In this scenario, a terrorist group obtains an undetermined amount of cesium-137 unshielded and places it in a bus, packed with 2,000 pounds of explosives. Along with many other tour buses, this bus is parked 1,500 yards from the United States Capitol. At lunchtime, the explosive is detonated.  Cesium (chemical symbol Cs) is a soft, malleable, silvery white metal that may be stable (nonradioactive) or unstable (radioactive). The most common radioactive form of cesium is cesium-137.  Cesium is one of only three metals that are liquid near room temperature (83° F). The half-life of cesium-137 is 30 years. It decays by emission of a beta particle and gamma rays to barium-137m.  Since Cesium-137 is one of the most common radioisotopes used in industry, it would not be difficult for terrorists to acquire.  As with all radionuclides, exposure to radiation from cesium-137 results in increased risk of cancer. Great Britain's National Radiological Protection Board predicts that over the next 70 years, there will be up to 1,000 additional cancers among the population of Western Europe exposed to fallout from the nuclear accident at Chernobyl, in part due to cesium-137.  People may ingest cesium-137 with food and water, or they may inhale it as dust. Exposure to cesium-137 may also be external (that is, exposure to its gamma radiation from outside the body). If cesium-137 enters the body, it is distributed fairly uniformly throughout the body's soft tissues. Compared to some other radionuclides, cesium-137 remains in the body for a relatively short time. It is eliminated through the urine.  Even though there are several medical tests used to determine exposure to cesium-137, they are not routinely available because they require special laboratory equipment. This could impede accurate and rapid diagnosis, thus delaying necessary treatment.    **Ask Yourself:**   1. **Although the situation is just now unfolding and most likely you would not even be aware of it at this point, do you have a plan that addresses your organization's role, lines of responsibility, and resources needed in the event of a crisis or emergency?** 2. **How does your organization prepare (in advance) its communication team to respond quickly to crises and emergencies?** |
| **Step 1. Verify situation.** |
| Washington, D.C.-Wednesday, July 17. At 12:00 noon, a loud explosion is heard near a downtown museum. The front of the building is essentially destroyed. A minute later, 911 emergency operators receive calls from the area and are informed that a huge explosion-scattering dust and debris-has occurred over the downtown area. Federal Aviation Administration (FAA) airport tower operators witness the explosion and report the blast to 911 and to the FAA regional operations center. The 911 operator requests that further reports from the tower be made directly to the Washington, D.C., local Emergency Operations Center (EOC).  The Fire and Police Departments are notified and called to the scene. Within minutes, firefighters, police officers, and other emergency rescue teams arrive. Upon arrival, the police evacuate the survivors and close the access roads to the area. The initial Incident Commander calls a second and third alarm due to the magnitude of the damage. Teams report that glass windows and partitions in all buildings within a one-block radius are shattered, inflicting additional damage and injury from glass shards.  At 12:10 p.m., radiation detectors at the Department of Energy sound an alarm, indicating an increase in beta particles and gamma radiation over background levels.  By 12:20 p.m., emergency management team notifications are initiated and Washington, D.C.'s EOC is activated. The National Response Center is notified of the explosion and the possibility of radioactive fallout.  At 12:25 p.m., a major cable news network interrupts its broadcasts to report "a bombing that makes Washington, D.C., look like a war zone."  At 1:00 p.m., the mayor's office receives a call from the editor of a local newspaper. An unidentified individual has called the paper and claimed to be with a terrorist organization responsible for setting off a nuclear device in Washington, DC. The caller stated that additional "bombs" should be expected.  At 1:30 p.m., a local talk radio station airs a report about the explosion and announces that a terrorist group has claimed responsibility for the explosion. The announcer notes that the police and FBI do not confirm this report and that they will make further announcements as information becomes available to them. All of the major television networks follow with immediate bulletins "confirming that a terrorist organization has detonated an atomic bomb in the heart of Washington, D.C."  As news of the explosion and the possibility of fallout release become widely known, people throughout the city panic and flee.  By 2:30 p.m., the HAZMAT teams assess the extent of the radioactive contamination in the area and identify cesium-137 as the source of the radiation. An immediate evacuation of the affected area is ordered. Because the mayor will be in direct communication with the President, he wants an update on evacuation, monitoring, and containment efforts as soon as possible.  Based on the information received, the FBI believes that the device was a 1,500- to 2,500-pound conventional explosive laced with cesium-137. The FBI notifies the city EOC that they will take the lead in managing the crisis. It requests information about contamination levels around the city as soon as it is available to determine when FBI staff can access the site of the incident. The FBI indicates that it would like to meet with representatives from the Police Department immediately in order to coordinate efforts in conducting the investigation.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **What sources could be contacted to verify the situation?** 3. **What SMEs do you have on hand, or can contact, for clarification?** 4. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take.** |
| **Step 2. Conduct notifications.** |
| By 3:00 p.m., the mayor has declared a local emergency and asked the surrounding Governors for assistance. The mayor holds a news conference and indicates that he has declared a State of Emergency, and that an assessment and evacuation is in progress. Area residents who are not evacuated are asked to remain indoors. It is estimated that 150,000 people are affected by the evacuation. The mayor has requested a Presidential Stafford Act (http://www.fema.gov/library/stafact.shtm) declaration of a Federal Disaster. Community health coordinators report that approximately half of the initial emergency responders have been exposed to radiation.  At 4:00 p.m., the President issues a disaster declaration, promising Federal resources for emergency response and for bringing the responsible terrorists to justice. The FRP and FRERP are activated. FEMA and other Federal agencies are formally requested to provide assistance to the response and recovery process. FEMA activates the Emergency Response Team (ERT) and deploys the Emergency Response Team Advance Element (ERT-A) and Exposure, Fate Assessment Screening Tool (E-FAST) to the scene. Potential sites for the DFO are investigated.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **What other organizations, if any, besides those noted here should be notified of this event?** 3. **What are the internal and external communications requirements for this response?** 4. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take.** |
| **Step 3. Assess level of crisis.** |
| Area hospitals report that more than 2,500 people have requested medical treatment because they believe they have been exposed to radiation. The few hospitals that are not under evacuation notices are overwhelmed with thousands claiming to suffer from radiation sickness or requesting radiation exposure testing. Hospitals do not have the resources to conduct required tests or provide treatment, nor are they able to accurately monitor people coming to the hospital. The rush of agencies descending on the scene causes great confusion in command, control, and reporting. Confusion also exists in prioritizing response actions versus investigatory actions, leaving many responders upset.  It is 8:00 p.m. The sun is beginning to set. It is raining. The rain and darkness complicate the response efforts.  By 8:30 p.m., members of the Maryland and Virginia National Guard arrive and take up positions in and around downtown to assist the police with their duties and with the decontamination and containment efforts. The Red Cross has offered assistance in transporting food, water, medications, and other resources to shelter locations and wherever else they are needed. Officials from the EPA have contacted the District of Columbia Public Works Department and the Department of Safety in order to coordinate efforts for monitoring radiological contamination that may have migrated into public drinking water reservoirs, surrounding lakes and rivers, and soil.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **Based on the information given, what is the level of crisis for this event?** 3. **What hours of operation/schedule would you put the communication team on for this event?** 4. **What resources and other tools are needed to ensure an effective communication response?** 5. **Based on the information presented, what staffing levels do you foresee your organization contributing to the response effort? What problems do you anticipate?** 6. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take.** |
| **Step 4. Organize and give assignments.** |
| DoD, DOE, and EPA officials are concerned about the possibility that a large number of people were not monitored for contamination before leaving the area and that many contaminated vehicles have traveled to other jurisdictions. These officials are also extremely concerned about the spread of contamination throughout the area watershed.  By 10:30 p.m., the DFO is situated, staffed, and in full operation. The JIC, handling media inquiries, is inundated with questions on the adequacy of the response effort and the lack of information provided to them and the public by State and local authorities.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **What immediate public relations and media concerns must be anticipated? How will these concerns be addressed? Who will serve as your organization's spokesperson in this incident?** 3. **What portion(s) of your communications response team would you activate at this point?** 4. **Would your functional team(s) know their roles and immediate tasks? To whom would they report and take direction?** 5. **How will your organization's actions be coordinated with the actions of other agencies? What conflicts could arise from the need to simultaneously conduct extensive criminal investigation and response functions? What conflicts may be anticipated between the overlapping federal/State/local jurisdictions?** 6. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take.** |
| **Step 5. Prepare information and obtain approvals.** |
| Numerous public interest and environmental groups call the EOC and other local government officials. They also release statements to the media expressing concern about the long-term effect this event will have on the environment, the health of the community, and the drinking water supply.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **With federal, state and local agencies involved, how will media inquiries be handled?** 3. **What, if any, are the critical health communication messages that need to be released to the public?** 4. **How would you develop these messages and get them cleared efficiently?** 5. **Who in your organization is responsible for authoring media releases?** 6. **What audience(s) group(s) would you target and what concerns would you address?** 7. **How would your organization display empathy and caring to the public about this event?** 8. **What questions would you anticipate the media to ask about this event?** 9. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take.** |
| **Step 6. Release information to the public.** |
| Several hospitals request assistance with transporting patients to other hospitals due to inadequate resources. They also request immediate assistance with monitoring incoming patients and decontamination procedures or they will be forced to turn additional patients away. Proper disposal of contaminated equipment and other material accumulating at the hospitals becomes a concern. The District's Department of Health spokesperson provides information to the public via a news conference regarding the effects of radiation under the current situation and encourages people to stay indoors. This conference was not coordinated with the JIC.  By 10:00 p.m., updated reports of casualties filter in from area hospitals, shelters, and residences. It is reported that up to 12,500 people may have been exposed and still require decontamination, but these numbers are not confirmed.  Additional updates have been received from the assessment teams scattered throughout the city.  During a late-night interview, the President makes a surprise announcement that he will tour the area tomorrow to personally assess the destruction.    **Ask Yourself:**   1. **What are your priorities at this point?** 2. **What types of training does your organization need to more effectively manage the communications response to situations of this type?** 3. **List the policies and procedures included in the EOP, SOPs, and checklists that you think should be further reviewed, supplemented, or developed for your organization to handle the communication response to an event similar to this. Which are priorities?** 4. **In what ways would your organization monitor an event such as this after the initial release of information?** 5. **How would your organization determine when it would be appropriate to move into the "post-event" phase for an event similar to this?** 6. **If the event described in this scenario happened in your community, how would you verify it? List the verification steps you would take** |



# http://r70.cooltext.com/rendered/cooltext1333426779.png'White phosphorus' reports: Ukraine military 'dropped incendiary bombs' on Slavyansk

Source: http://rt.com/news/165628-ukraine-incendiary-bombs-phosphorus/

Residents of Slavyansk and its suburbs were awoken overnight on Thursday by what they say were incendiary bombs that were dropped on their city by Kiev’s military. Witnesses and local media reports suggested that **the bombs might be phosphorous.**

Much of the village of Semyonovka, located in the Slavyansk suburbs, was set ablaze. Local residents told RT that the ground didn't stop burning for some time.

“We all saw what happened here yesterday. They used rocket launchers as well as incendiary bombs against us. The ground was on fire. How can the ground burn by itself. It burned for about forty minutes,” resident Roman Litvinov told RT over the phone.

“Starting from 2 a.m. everyone I’ve met has a sore throat and is coughing all the time. I think this is because of the burning. I think we’ll feel the true consequences later. There are still a lot of people here, a lot of children we haven’t managed to get out yet,” resident Tatyana told RT.

The use of incendiary bombs – designed to start fires using materials such as napalm, white phosphorus or other dangerous chemicals – is strictly prohibited by the UN.

Kiev authorities have denied reports that such weapons were used against civilians. The National Guard also refuted reports that phosphorous ammunition was used, its press service stated.

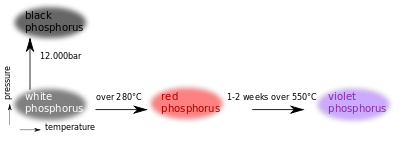
During the latest news briefing, State Department spokesperson Jen Psaki veered away from answering an AP journalist’s question about the reported use of white phosphorus bombs by Kiev’s army. But when cornered, she let it slip that she was quite clueless as to the situation on the ground – saying she thought the reference was to the Russians using the bombs.

When asked about the report for the second time, Psaki replied: "By whom? By Russians?”

The journalist replied: “No, by the Ukrainians,” specifying that there is video and photographic evidence of the attack.

Psaki replied by saying, “No, I didn’t see those reports.”

Slavyansk, an industrial city in southeastern Ukraine with a population of over 100,000 people, has been a focal point of the government’s crackdown against the region. The city’s residential area has been under regular artillery fire for weeks.

“It does appear that there is at least a case to be argued that something similar, if not itself white phosphorous, was used overnight. I’ve seen the video, I’ve looked at it closely...[there are] whole signs, whole marks of white phosphorous use. For example, a very bright light burning and multiple burns coming down **from the sky. It’s an airburst weapon that has been used, such as a mortar or a manned aircraft,” Charles Shoebridge, a former army officer, Scotland Yard detective, and counter-terrorism intelligence officer who has recently returned from Ukraine, told RT.

“White phosphorous cannot be put out with the use of water” and it will “burn through one’s body to the bone,” Shoebridge added. “If there is going to be large amounts used it can also be a poison – large amounts can be set to contaminate water supply.”

According to the video, “it’s very likely that white phosphorus" was used, Shoebridge added. “It’s very difficult to fabricate the video we saw combined with the evidence on the ground.”

Moscow demanded an immediate investigation into the reported use of incendiary bombs in Ukraine, Russian Foreign Minister Sergey Lavrov said on Thursday.

"We are concerned to hear reports that the Ukrainian military forces use incendiary bombs and some other indiscriminate weapons," he said. "These reports should be probed into immediately."

On Thursday, Russia introduced a draft resolution to the UN Security Council that condemns attacks on residential quarters and civilian facilities in southeastern Ukraine, said Vitaly Churkin, Russian envoy to the UN.

He also voiced concern over reports of the use of prohibited ammunition, including incendiary bombs, during the military crackdown.

The draft resolution calls for an immediate end to all violence and for a lasting ceasefire.

"The draft resolution will aim to stop the violence and support the political efforts the OSCE has been undertaking in vain so far. We urge the UN Secretary-General to support them," Churkin said, adding that its adoption would demonstrate the UNSC’s support for the crisis settlement efforts.

# The MIDS system (IAI)New Israeli IED Detection System

Source: http://i-hls.com/2014/06/new-israeli-ied-detection-system/

Israel Aerospace Industries’ (IAI) Ramta Division has completed the engineering testing phase and has begun building a technology demonstrator of a multi-sensor system called MIDS (Mines and IED Detection System) for detecting deep buried and surface-laid mines and Improvised Explosive Devices (IEDs). MIDS will be on display at the upcoming Eurosatory exhibition, the largest international land and air-land defense and security exhibition in Europe, held on June 16 to June 20, Paris, France.

MIDS is deployed on a ruggedized, commercial, light tracked or wheeled (manned and/or unmanned) engineering vehicle, according to customers’ needs. It carries an advanced ground-penetrating radar (GPR) and metal detector (MD) arrays into high threat environments to identify deep buried and surface laid mines/IEDs in, and next to, the advancing path of the maneuvering forces. The two main arrays (GPR and metal detector) produce data which is combined to allow real time analysis, minimizing false alarms from non-threatening materials such as rocks, wood and other debris.

An onboard IAI-manufactured electro-optic payload with day/night cameras provides remote operators with situational awareness and enables visual surveillance from a safe distance. On-board navigation systems allow the vehicle to travel along a precise series of preprogrammed or operator designated waypoints and record and transmit the exact location of discovered threats.

# New Israeli System Detects Low-flying Drones

Source: http://i-hls.com/2014/06/new-israeli-system-detects-low-flying-drones/

Israel Aerospace Industries (IAI) has unveiled the Green Rock – a mobile autonomous tactical counter Rocket, Artillery & Mortar (C-RAM) system. This system, was delivered to the Israel Defense Forces and named Wind Shield by the IDF.

The system will be on display at the Eurosatory exhibition being held between June 16-20 in Paris, France. Green Rock is designed to support a variety of ground force protection missions, including fire source location, friendly forces fire correction, and detection of low-flying airborne targets such as UAVs, gliders and hovering platforms.

The system provides a complete low/high trajectory target, real-time intelligence and rapid response solution for tactical forces. Green Rock’s mission is to locate fire squad positions, distribute selective warning alarms and enable an effective fire response.

## The FBI Is Getting Its Own, Personal 3D Printer for Studying Bombs

Source: http://www.nextgov.com/defense/2014/06/fbi-getting-its-own-personal-3d-printer-studying-bombs/86476/

At least one lucky G-Man will get to toy around with a 3D printer to study homemade explosives.

The bureau needs one order of a **Stratasys Objet24 Personal 3D Printer** "to support the advanced technical exploitation of evolving and existing high technology explosive devices," new federal contracting papers state.

Retail prices for the model start at $19,900, according to resellers and pricesheets.

“The 3D printer is cutting-edge technology that will be used by the Terrorist Explosive Device Analytical Center to enhance their capabilities in exploiting improvised explosive devices,” or IEDs, FBI spokeswoman Ann Todd said in an email on Friday.

The center, located in Quantico, inspects flammables collected from overseas battlefields and found on U.S. soil. Various Justice Department agencies, the Pentagon, other intelligence units and international partners contribute to TEDAC’s bomb library. Since opening in 2003, the center has probed more than 100,000 IEDs and receives about 800 deliveries a month.

Justice in 2013 became increasingly worried about plastic firearms faking out airport screeners and other weapon detectors.

Last fall, the Huffington Post reported that Justice's Bureau of Alcohol, Tobacco, Firearms and Explosives, during an experiment, successfully printed and fired a metal-free gun using blueprints publicly available online. "The ATF's testing showed that the weapon, while not quite as powerful as most guns, could penetrate several inches of soft flesh as well as a human skull," HuffPo wrote.

At the time, ATF declined to say whether it owned its own 3D printer.

The model the FBI plans to purchase weighs 205 pounds and measures 32.28" × 24.4" × 23.22", according to the Stratasys website. It is compatible with Windows XP and Windows 7 operating systems.

The company describes the Objet24 as "the first desktop system to print realistic models with small moving parts, thin walls and smooth, paintable surfaces."

FBI officials said they want the Stratasys machine as opposed to another vendor’s model because it "is the only instrument capable of producing the high accuracy and resolution results to meet agency testing standards."

Also, it is the sole printer that complies with the bureau’s data recovery and thermal environment requirements, officials said.

## Synthetic aperture sonar to help in hunting sea mines

Source: http://www.homelandsecuritynewswire.com/dr20140620-synthetic-aperture-sonar-to-help-in-hunting-sea-mines

Mines are plentiful and easy to make. Some mines explode on contact. Others are more sophisticated, exploding or deploying torpedoes when their sensors detect certain acoustic, magnetic or pressure triggers. Some can destroy a ship in 200 feet of water. Since the Second World War, sea mines have damaged or sunk four times more U.S. Navy ships than all other means of attack combined, according to a Navy report on mine warfare. New sonar research could improve the Navy’s ability to find sea mines deep under water. The underlying technology, known as synthetic aperture sonar (SAS), uses advanced computing and signal processing power to create fine-resolution images of the seafloor based on reflected sound waves.

Since the Second World War, sea mines have damaged or sunk four times more U.S. Navy ships than all other means of attack combined, according to a Navy report on mine warfare. New sonar research being performed by the Georgia Tech Research Institute (GTRI) could improve the Navy’s ability to find sea mines deep under water.

The underlying technology, known as synthetic aperture sonar (SAS), uses advanced computing and signal processing power to create fine-resolution images of the seafloor based on reflected sound waves. Thanks to the long-term vision and a series of focused efforts funded by the Office of Naval Research spanning back to the 1970s, SAS has become a truly robust technology. When it transitions to the fleet, the SAS will dramatically improve the Navy’s ability to carry out the mine countermeasures mission.

“The Navy wants to find sea mines,” said Daniel Cook, a GTRI senior research engineer. “There are systems that do this now, but compared to SAS, the existing technology is crude.”

A GT release reports that the SAS research is funded by a grant from the Office of Naval Research, and is conducted in collaboration with the Applied Research Laboratory at the Pennsylvania State University. In the past year, the group has made strides in improving the ability to predict and understand sonar image quality and has published and presented their work at conferences.

Sonar systems emit sound waves and collect data on the echoes to gather information on underwater objects.

The Navy uses torpedo-shaped autonomous underwater vehicles (AUVs) to map swaths of the seafloor with sonar sensors. Perhaps the most well-known example is the Bluefin 21 used to search for Malaysian Airlines Flight 370. The AUVs zigzag back and forth in a “mowing the lawn pattern,” Cook said. **These AUVs can map at a range of depths, from 100 to 6,000 meters.**

SAS is a form of side scanning sonar, which sends pings to the port and starboard sides of the AUV and records the echoes. After canvassing the entire area, data accumulated by SAS is processed into a mosaic that gives a complete picture of that area of the seafloor.

SAS has better resolution than real aperture sonar (RAS), which is currently the most widespread form of side scan sonar in use. RAS transmits pings, receives echoes and then paints a strip of pixels on a computer screen. RAS repeats this pattern until it has an image of the seafloor. This technology is readily available, and relatively cheap, but its resolution over long ranges is not good enough to suit the Navy’s mine hunting needs.

RAS sensors emit acoustic frequencies that are relatively high and are therefore quickly absorbed by the seawater. SAS uses lower frequency acoustics, which can travel farther underwater. Upgrading to SAS improves the range at which fine resolution pictures can be produced.

“RAS can give you a great looking picture but it can only see out 30 to 50 meters,” Cook said. **“For the same resolution, SAS can see out to 300 meters.”**

SAS does not paint a line-by-line picture of the sea floor like RAS. Instead, SAS pings several times and then records the echoes on a hard drive for post-processing. Once the AUV surfaces, the hard drive is removed and the data is analyzed by computers in a complex signal processing effort. The signal processing converts the pings into a large, fine-resolution image of the seafloor. The commonly accepted measure for fine resolution is a pixel size of 1 inch by 1 inch, which is what SAS can achieve.

Tests of SAS in AUVs have produced fine-resolution images of sunken ships, aircraft, and pipelines. But when looking at an image of the seafloor from above, operators might have difficulty discerning the identity of simple objects. For example, certain mines have a circular cross section. When looking at a top-down image, an operator might not be able to tell the difference between a mine and a discarded tire. To discern if that circular-shaped object is a threat, operators consider the shadow that an object casts in the sonar image. A mine will cast a shadow that is easy to distinguish from those cast by clutter objects such as tires. The shadow contrast research will be used to help ensure that this distinction is as clear as possible.

“There are other more complicated models that the Navy uses that will do this sort of calculation, but it takes too long,” Cook said. “We have developed a compact model that will allow you to predict contrast very quickly.”

The release notes that improving contrast prediction can have a ripple effect in mine hunting capability. Naval officers will be better able to plan missions by predicting how good the shadows will be in a certain environment. This can lead to improved imagery, power conservation, and better performance for automatic target recognition software.

Mines are plentiful and easy to make. Some mines explode on contact. Others are more sophisticated, exploding or deploying torpedoes when their sensors detect certain acoustic, magnetic or pressure triggers. Some can destroy a ship in 200 feet of water.

“Mines are a terrible problem. They lie in wait on the seafloor, so you want to go find them with as few people in the process as possible, which is why we’re driven towards these autonomous vehicles with synthetic aperture sonar,” Cook said.

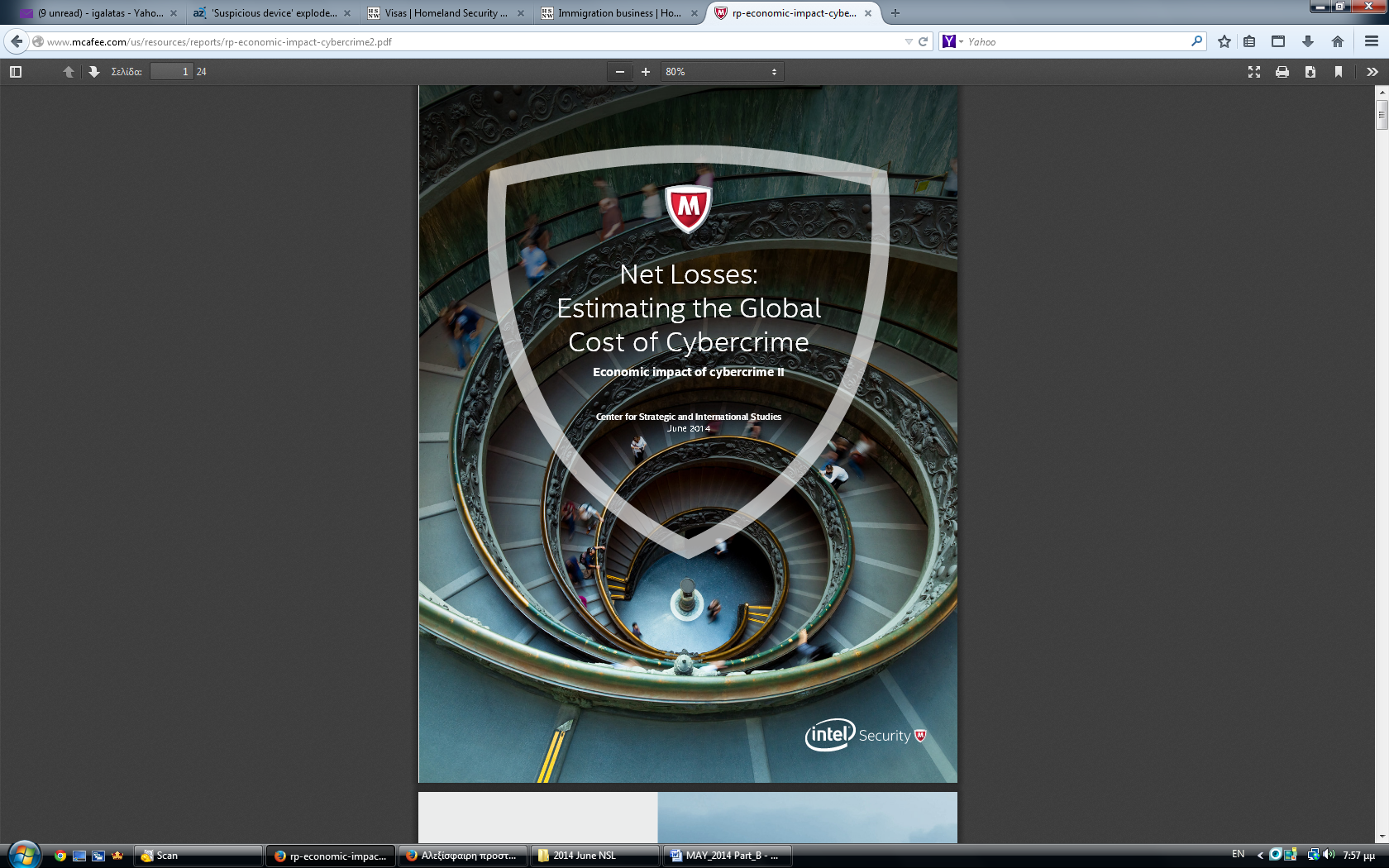
This research is supported by the Office of Naval Research, but the release notes that any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Office of Naval Research.

*— Read more in D. Cook et al. “Synthetic aperture sonar contrast,” in John S. Papodakis and Leif Bjorno, eds,* Proceedings of the First International Conference and Exhibition on Underwater Acoustics *(June 2013): 143-50; Z. G. Lowe et al., “Multipath ray tracing model for shallow water acoustics,” in* Proceedings of the 11th European Conference Underwater Acoustics, *ECUA2012 (July 2012)*

****Cybercrime Remains Growth Industry With $445 Billion Lost

Source: http://www.bloomberg.com/news/2014-06-09/cybercrime-remains-growth-industry-with-445-billion-lost.html

Cybercrime remains a growth industry.

That’s the main message from former U.S. intelligence officials, who in a report today outlined scenarios for how **$445 billion a year in trade theft due to computer hackers will worsen**. They warned that financial companies, retailers and energy companies are at risk from thieves who are becoming more sophisticated at pilfering data from their servers.

The outlook “is increased losses and slower growth,” with no “credible scenario in which cybercrime losses diminish,” according to the report published by the Washington-based Center for Strategic and International Studies. Some of the damage will be hard to trace, such as economic downturns caused by foreign competitors selling products based on stolen designs and financial markets undermined by hackers.

“Cybercrime is here to stay,” said Stewart Baker, a lead author of the study who was general counsel for the National Security Agency in the 1990s and later an assistant secretary at the Department of Homeland Security.

“The real question is do we know what cybercrime is costing us?” he asked in a telephone interview.

The **damage done already includes 40 million people in the U.S.** having their personal information stolen within the last year and an unnamed oil company losing hundreds of millions of dollars in business opportunities when hackers obtained its oilfield exploration data, according to the report. Network security company McAfee Inc. sponsored the report for CSIS, a nonprofit Washington-based policy research organization.

▶**Read the report at:**

http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

# U.S: Hackers Threaten Passenger Planes

Source: http://i-hls.com/2014/06/u-s-hackers-threaten-passenger-jets/

The interior of a Boeing 737-900. Photo: Boeing

The U.S Federal Aviation Administration is ordering Boeing to modify the technology aboard late-model 737 aircraft to prevent computer hackers from damaging the planes.

The order published Friday in the Federal Register is effective immediately, although the agency allowed a comment period until July 21. The special conditions are urgent because the FAA is trying to avoid slowing down design and delivery of new planes, according to the agency.

Doug Alder, a Boeing spokesman, said the special conditions will institutionalize actions that the manufacturer was already taken or planned, in line with similar protections for the 747-8, 777 and 787.

According to USA Today the latest FAA order applies to 737-700, -700C, -800, -900ER, -7, -8 and -9 aircraft, one of the most popular types of planes for the last 20 years. The special conditions apply to these aircraft because their technology is connected more thoroughly than other planes with computer networks outside the aircraft, making the 737 more vulnerable, according to FAA.

The plane’s technology “may allow the exploitation of network security vulnerabilities resulting in intentional or unintentional destruction, disruption, degradation, or exploitation of data, systems and networks critical to the safety and maintenance of the airplane,” the FAA said.

The order from Jeffrey Duven, manager of FAA’s certification services, calls for Boeing to “ensure that the airplanes’ electronic systems are protected from access by unauthorized sources external to the plane, including those possibly caused by maintenance activity.”

# Italy: New Cyber Defense Center

Source: http://i-hls.com/2014/06/italy-new-cyber-defense-center/



Italy’s Finmeccanica has beefed up its presence in the growing cybersecurity business by opening a cyber attack monitoring and prevention center in central Italy, using a super computer with the power of 30,000 desktop PCs.

Selex ES, a unit of Finmeccanica, unveiled the center on June 4, with managers predicting 12-13 percent annual growth in the firm’s cyber revenue, which currently stands at €100 million (US $136.1 million).

According to Defense News the move coincides with Italy’s effort to set up a government center in Rome to pull together parallel initiatives in the field to provide a unified response to cyber attacks against national targets.

While the Selex center is a commercial activity with private and government customers, it hopes to have a role in planned government cyber activities, such as establishment of a Computer Emergency Response Team.

Selex’s center at Chieti, in the mountainous Abruzzo region, will augment the cybersecurity services the firm already provides state and private customers thanks to a super computer with a capacity of 310 Teraflops, able to carry out 310,000 billion operations per second using 30,000 CPUs, making it one of the most powerful supercomputers in the world, the firm said.

# Mondial 2014: The Expected Cyber Attacks

**By Guillaume Lovet**

Source: http://i-hls.com/2014/06/mondial-2014-expected-cyber-attacks/

While thousands of Brazilian workers are trying to complete the stadium on time for the opening match, Brazilian cybercriminals are already at work. With a population of approximately 201 million in 2013, Brazil is the world’s fifth most populous country and has one of the largest cybercriminals communities. According to a survey conducted by the Brazilian Banks Federation (Febraban) in 2011, the banking sector reported losses of R$1.5 billion thanks to phishing, online theft, identity theft, online scams and credit card fraud.

A few days before the opening match kick-off of the World Cup, we can expect an onslaught of Internet scams and attacks from the global cybercriminal community in the coming days and weeks. Fortinet’s FortiGuard team is warning Internet users against online scams that they may face. It is important for football fans to remember a few tips to avoid unpleasant surprises:

-  **Unsolicited emails:** Spam email targeted at Internet users announcing that they are the lucky winners of a lottery for 2 tickets for the final of the World Cup, or they can access web sites to watch the matches live.….  While it is very tempting to a fan to click on an email link that says : “You’ve won 2 tickets for the final of the World Cup”, be careful! By clicking on that link, you could be taken to a compromised Website that downloads malware onto your computer. That malware could be used to retrieve all your personal information such as passwords or other credentials, or download additional malware, such as fake antivirus applications, or simply turn your computer into a spam generator.

-  **Online retailers offering discounted tickets**: If you discover an online store that’s offering unbelievable specials for tickets, do some digging to make sure it’s a legitimate store and not a false front that will disappear later that day along with your credit card information. Even if they are legitimate, you’ll want to make sure their site hasn’t been unknowingly compromised by SQL injection or other server attacks. Similarly, avoid believing **marketplace websites such as eBay or others** offering tickets at low prices for the event. **Good deals are often pure frauds**.

**-  Phishing and identity theft**: **Users may receive an email from their bank and / or Paypal highlighting that a payment for the purchase of 2 footballs tickets is in progress while the Internet user has in fact not made any purchase. To cancel the transaction, the Internet user must click on the link where it will be asked to complete a form with its bank login details.  Users should not reply and keep in mind that their bank would never ask for their banking ID by email.**

-  **Unsecured WiFi hotspots in Brazil**: While the Brazilian government is strengthening the safety for the World Cup, the 11,222 Israeli fans who will go to Brazil must remain vigilant. Fans who will not have the chance to watch the matches at the stadium will use the Internet to view the results in real time, by connecting to WiFi hotspots at hotels, bars… Do not connect to an unknown unsecure hotspot. An unsecure hotspot allows hackers to capture any and all data that’s flowing from the hotspot, enabling them to intercept logins and passwords, email messages, attached documents and other personal and confidential information.

All of these types of scams are flooding the Web and even well-informed Internet users could be trapped. So, here are some basic but important tips to avoid losing key personal information or money:

-          Requests for password or credit card information should set off alarm bells, double check before you comply.

-          Be very wary of links that either lead to applications or external websites.

-          Believe the popular saying: “If it’s too good to be true, then it probably is”.

-          If you haven’t entered a lottery, you can’t win it.

-          By connecting even to secure access points, check that the connections to your favorite websites are well secured HTTPS connections.

***Guillaume Lovet*** *is a senior manager of FortiGuard Labs’ Threat Response Team at Fortinet*



****Dh161m revamp of UAE’s busiest emergency unit begins

Source: http://www.thenational.ae/uae/health/dh161m-revamp-of-uaex2019s-busiest-emergency-unit-begins

June 11 – A Dh161 million expansion of the UAE’s busiest accident and emergency department is under way.

Rashid Hospital’s Trauma Centre, where about 166,000 patients were treated last year, is to be expanded to accommodate 160 more beds.

Essa Al Maidoor, director general of Dubai Health Authority (DHA), said construction has started at the centre, which is open 24 hours a day, seven days a week, and is dedicated to treating emergency patients in Dubai and the Northern Emirates.

“After detailed consultation with specialists from the trauma centre and the DHA engineering department, we finalised the design of the expansion, keeping in mind all the requirements needed for a hospital with a high volume of patients,” he said.

“The project will be completed in one year.”

He said the trauma centre will continue to function as usual while the work takes place.

The expansion is the first phase of the Dh3 billion revamp of Rashid Hospital, announced earlier this year.

It will include six new specialised health centres, a four-star and five-star hotel, villas and flats and a mosque.

The new 100,000 square metre site, to be built using green building standards, will have three towers inspired by the three-finger salute of Sheikh Mohammed bin Rashid, Vice President and Ruler of Dubai. In the salute, the fingers represent victory, triumph and love.

Each seven-storey tower will have 300 beds – bringing the total capacity to 900 beds.

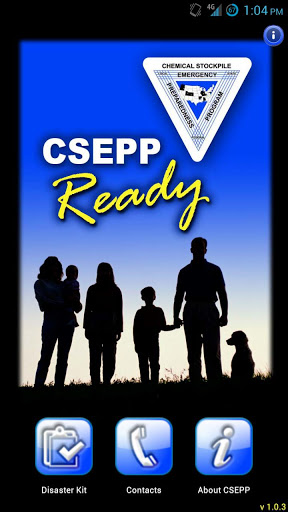
The existing hospital will eventually be demolished.

It is part of a 12-year masterplan to boost health care in Dubai and turn the emirate into a centre for medical tourism.

|  |
| --- |
| EDITOR’S COMMENT: A fascinating project but does it also include the element of management of mass CBRNE casualties? This is something that usually experts and architects forget to include! |

CSEPP Ready Mobile App Featured in Emergency Preparedness Campaign

Source: http://www.hstoday.us/single-article/csepp-ready-mobile-app-featured-in-emergency-preparedness-campaign/cc303e207d1fa92a0511f69aa24466a9.html

An ORAU-developed mobile application, Chemical Stockpile Emergency Preparedness Program (CSEPP) Ready, is intended to assist residents living in communities surrounding one of the last two active US Army chemical warfare agent stockpiles with preparing for a potential related emergency.

CSEPP is a partnership between the Department of Homeland Security’s Federal Emergency Management Agency (FEMA) and Department of the Army that provides emergency preparedness assistance and resources to communities surrounding the Army’s chemical warfare agent stockpiles.

The basic CSEPP course focuses on practical, cost-effective solutions, using the latest operational coordination technology tools—mobile applications, cloud technology and social media—for CSEPP communities to better manage, develop and deliver timely public information before, during, and after an emergency event.

“Even though an accident is unlikely,” ORAU said in an announcement, “FEMA and the Army work together to ensure the local communities are prepared through CSEPP. Through CSEPP, ORAU experts provide hands-on technology courses to train public affairs professionals and emergency managers to develop and deliver timely public information in an emergency event using the latest technology tools, including mobile apps, cloud technology and social media. Specifically, CSEPP Ready, which can be downloaded free in both Android and iPhone/iPad mobile formats, provides checklists for family disaster kits, information on how to respond to emergency sirens and directions for sheltering in place."

CSEPP Ready is a featured element in the inaugural 2013-2014 Prepare Pueblo emergency preparedness campaign in Pueblo, Colo., which is in its final phase from June to August 2014. The Prepare Pueblo campaign focuses on talking about emergency preparedness with family, friends and coworkers, knowing residents’ emergency zones and listening for alerts and notifications. The campaign was created by Pueblo-based public affairs professionals and emergency managers who had been through ORAU-led CSEPP courses.

The CSEPP Ready app, and the training that ORAU provided, made a big difference in the preparation efforts.

“When we developed the 2013-2014 Prepare Pueblo Campaign, we knew immediately we wanted to use the latest technology,” said Lisa Shorter, Pueblo County Sheriff’s Office public information officer and Prepare Pueblo campaign director. “We included QR codes on our annual Preparedness Calendar, used Google Sites to create and launch our own website, established content on Facebook, Twitter and Flickr and have encouraged the community to download the CSEPP Ready app for their phones. Having the knowledge provided to us by the ORAU team, and using the products they have developed for the program, mean that our community is better prepared.”

With the first-year Prepare Pueblo campaign coming to a conclusion this August, ORAU experts are looking ahead to identify how the training and technology can be used to help other CSEPP communities.

“The hope is that other communities will either use the hands-on technology training we provide them for building mobile apps on their own or that they will come to us to have an app built for them,” said Holly Hardin, ORAU emergency management section manager. “Either way, this kind of on-the-go technology is one of the best ways to ensure that residents have critical information close at hand when they need it.”

Another ORAU mobile app, EROs To Go, was developed to help emergency exercise evaluators have CSEPP Emergency Response Outcomes and Exercise Evaluation Guides at their fingertips during a chemical stockpile exercise. This mobile app will be put to the test at an upcoming exercise involving the other chemical stockpile in Bluegrass, Ky., later this fall.

ORAU provides innovative scientific and technical solutions to advance national priorities in science, education, security and health, and manages the Oak Ridge Institute for Science and Education (ORISE) for the Department of Energy.

# Identifying Pre-Attack Indicators for Special Events

**By Jessica A. Gladfelter & Dallas R. Mosier**

Source:http://www.domesticpreparedness.com/Infrastructure/Special\_Events/Identifying\_Pre-Attack\_Indicators\_for\_Special\_Events/

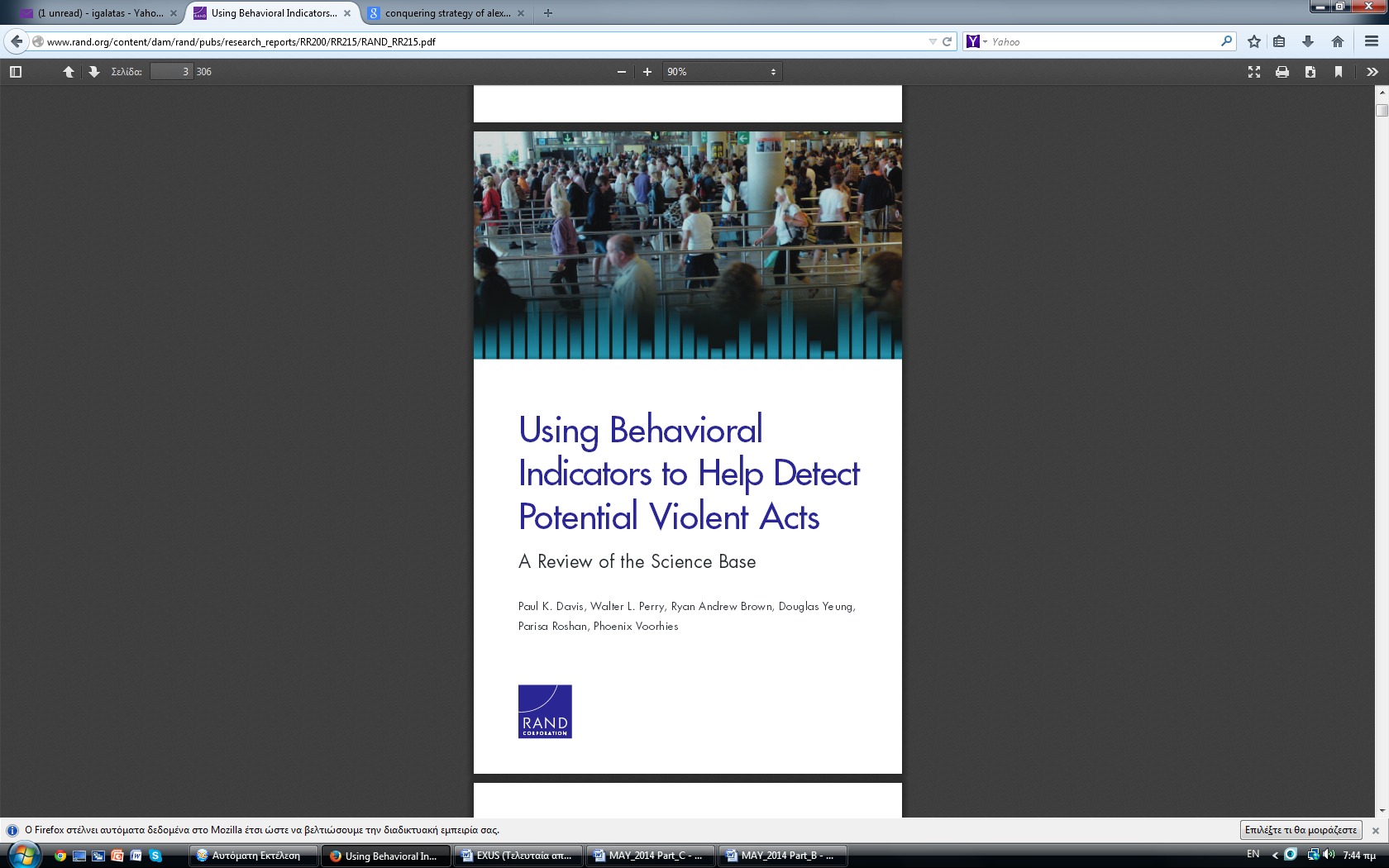
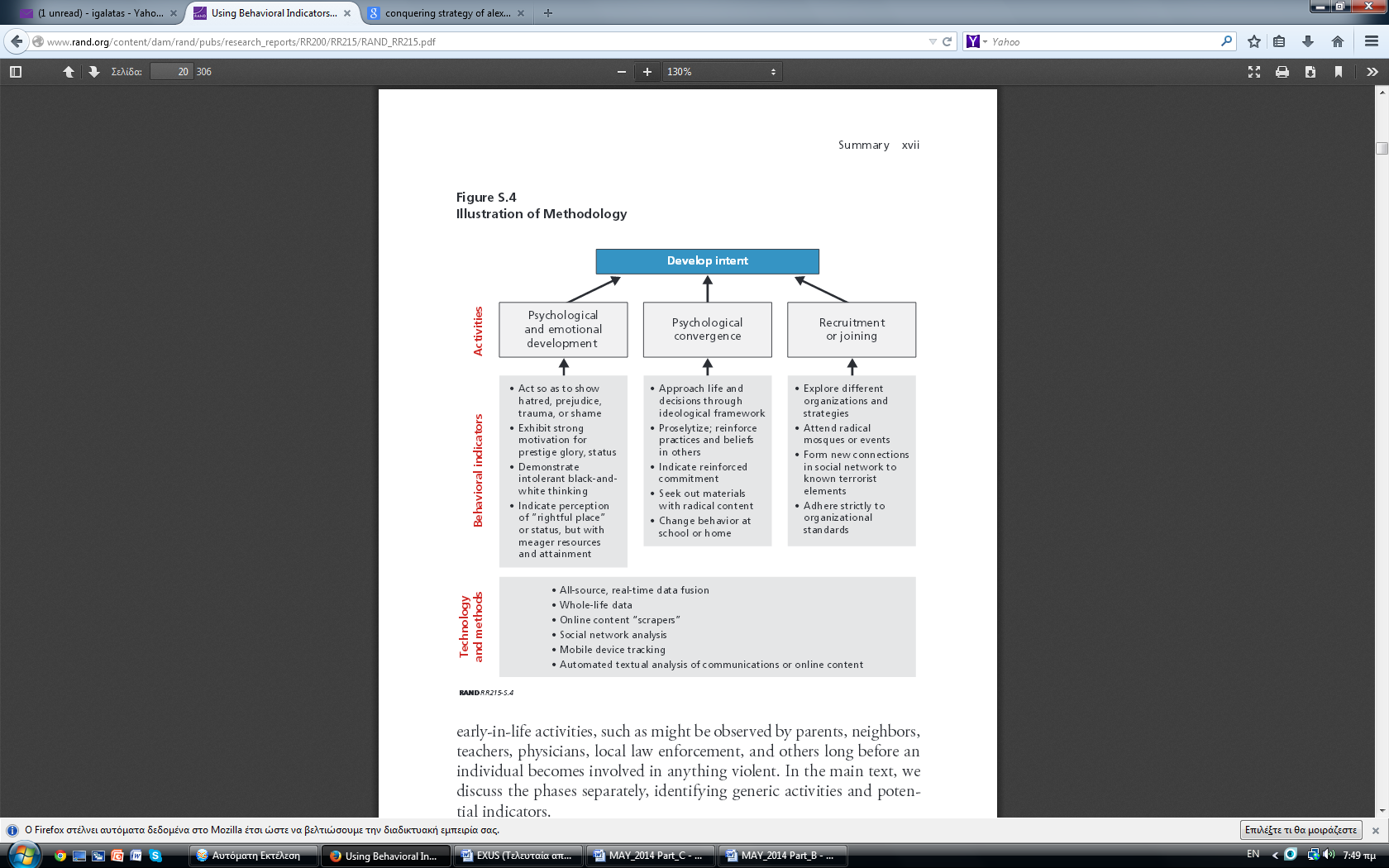
Before he went on a shooting rampage that claimed seven lives (including his own) in a California college town, Elliot Rodger had already left clues about his deadly intentions. He posted numerous threatening videos online. He e-mailed a 140-page manifesto that detailed the perceived wrongs against him and how he intended to “set them right.” He made vague verbal threats, proclaiming that he was going to kill “them.”

The video threats, the manifesto, and other verbal threats that preceded Rodger’s 23 May 2014 rampage in Isla Vista, California, were pre-attack indicators – detectable manifestations of an attacker’s intent and capability to harm. Such pre-attack indicators are important because early identification, by knowing what threatening behavior to search for, can save lives.

**Recipe for Disaster – Intent & Capability**

A person only will carry out an attack if he or she has the intent and the capability for violence. Intent is the desire to harm or attack a person, place, or thing, whereas capability refers to having the capacity to carry out the intended harm. Intent and capability have different sets of indicators.

**According to 2011 research published in *Behavioral Sciences and the Law*, indicators of intent include the following actions and behaviors: suicidal and/or homicidal thoughts; psychopathy; affiliation with terrorist or hate groups; vague or direct threats; and last-resort behaviors.** Such indicators exhibit in a variety of ways. For instance, the research found that calls to violence typically indicate a possible attack by terrorists or hate groups; issuing a call to violence for a specific venue signals a direct threat with a strong intent to harm. A 2013 report published by the RAND Corporation provided examples of capability indicators, including: gathering weapons or weapon-making materials; training for weapons or paramilitary forces; gathering security information; testing venue security; conducting dry runs; and conducting surveillance on venues.

Once a person or group has evinced the intent and capability for an attack, other kinds of pre-attack indicators may emerge. These actions, once identified, require quick response because they typically signal that the onset of an attack is imminent. **Based on security literature, such as the 2013 RAND Corporation report, actions that security personnel should look for include the following:**

* *Positioning actions* – Asking directions to ensure correct target, attempting to clear the area of “innocents,” hesitating to ensure maximum effect of attack, and communicating onsite between co-conspirators;
* *Evading detection indicators* – Avoiding checkpoints, making robotic like or unnatural movements, hiding information, and possessing suspicious containers or bags;
* *Stress indicators* – Hiding traditional stress signals, displaying subtle, less obvious signs of stress; and
* *Imminent action* – Possessing a visible weapon.

**External Factors & Internet Clues**

In addition to pre-attack indicators, there are external factors – including location, time of year, and previous attacks – that can increase the chance of an attack or violence. Location factors include vulnerable spots in specific venues or areas where known terrorist-affiliated members live. Time-of-year factors are key dates and trigger events. Large venues are often more heavily trafficked during holidays and special events; these larger crowds may attract attackers who seek to maximize harm. Trigger events – loss of a job, harassment, or the death of a colleague or loved one – may contribute to an attacker’s motive, aggression, and method. Additionally, widely reported violence triggers future attackers by giving them the idea that large-scale attacks receive media attention. Attackers may view this media coverage as a reward.

Although security personnel are familiar with the pre-attack indicators themselves, specific ways to spot them are less certain and constantly changing. The Internet, for example, is one medium through which pre-attack indicators often surface – on social media sites or through conventional search engines. Security directors for large venues that hold special events could find pre-attack indicators by searching for specific terms, including: name of the event; location of the event; names of high-profile speakers, performers, guests, and attendees; previous attacks on similar events; name of the event plus controversial topic; and trigger events. It is important that security personnel who are responsible for searching online activity download and save any evidence of threats they have discovered.

In summary, pre-attack indicators are clues that may enable security personnel to prevent an attack or mitigate the consequences of an attack. Internet searches provide means to detect pre-attack indicators. To prevent deadly incidents like the one in Isla Vista, anyone close to a potential attacker must be able to identify and promptly report pre-attack indicators to proper authorities, which in turn must be able to recognize the threat and, when necessary, take swift action.

**▶Read the RAND report at:**

*http://www.rand.org/content/dam/rand/pubs/research\_reports/RR200/RR215/RAND\_RR215.pdf*

***Jessica A. Gladfelter*** *is a rising senior at Roanoke College in Salem, Virginia. She has done research in psychology for three years and is currently pursuing a BS in psychology. Jessica has presented multiple research posters at conferences around the country. She currently serves as intern at a federal agency.*

***Dallas R. Mosier*** *is a rising junior at Saint Francis University in Loretto, Pennsylvania. She is pursuing a BS in chemistry, as well as a BS in criminal justice. She has done research in the chemistry field for the past year and has presented her research at various symposiums. She currently serves as intern at a federal agency.*

## NIST plans new Centers of Excellence for disaster resilience, forensics

Source: http://www.homelandsecuritynewswire.com/dr20140619-nist-plans-new-centers-of-excellence-for-disaster-resilience-forensics

Officials at the National Institute of Standards and Technology (NIST) have announced plans to establish two new research Centers of Excellence to work with academia and industry on issues in forensic science and disaster resilience.

NIST plans to hold merit competitions to establish the centers, tentatively planned to be funded at up to $4 million a year for five years.

A NIST release reports that NIST Centers of Excellence are meant to provide multidisciplinary research centers where experts from academia, industry, and NIST can work together on specific high-priority research topics. The agency established its first such center, dedicated to advanced materials research, in December 2013.

One of the planned new centers would focus on tools to support community disaster resilience. The center would work on developing integrated, systems-based computational models to assess community infrastructure resilience and guide community-level resilience investment decisions. The proposed center also would develop a data management infrastructure that allows for public access of disaster data, as well as tools and best practices to improve the collection of disaster and resilience data.

The second proposed center would support NIST’s efforts to strengthen forensic science through the development and delivery of improved measurement and analysis technologies and the development of best practices and standardized methodologies to improve evidence interpretation and reporting. Because forensic science covers a broad array of technical disciplines, NIST is considering one or more cross-cutting areas where research could benefit work across the field. Potential technical areas of focus include probabilistic methods (analysis techniques that produce a scientific estimate of the likelihood that a known and unknown sample match), pattern recognition and digital evidence.

Each of these centers will provide additional technical resources and expertise to support NIST’s ongoing efforts in these important areas.

# Next-Generation 911: What You Need to Know

**By David Raths**

Source: http://www.emergencymgmt.com/safety/Next-Generation-911-What-You-Need-to-Know.html? page=1

On May 1, 2010, a terrorist attack in New York City’s Times Square was thwarted when street vendors noticed smoke coming from a vehicle in which a homemade bomb had failed to explode. Imagine if those street vendors could have used their cellphones to send pictures or video of the vehicle and its license plate to a 911 call center. What if the 911 center could then push that data to first responders and police to get the location from GIS and buildings visual in the photos?

“They could really capture the dynamics of the event,” said Brian Fontes, executive director of the National Emergency Number Association (NENA). “That is what I call an information-rich 911 call, which will be supported in a next-generation 911 system.”

### What Is Next-Generation 911?

Fifty-eight percent of Americans own smartphones and people now routinely send text messages, photos and videos from their mobile devices. And although 75 percent of all calls to 911 are wireless, most 911 centers today are still tethered to the voice-centered world of communications of the last century and are unable to receive text or photos.

The existing 911 system faces difficulties in supporting text or multimedia messaging, according to NENA, and it lacks the capability to interconnect with other systems and databases such as building plans and electronic medical records.

The very structure of the current 911 system is rapidly going out of date. “It is analog network-based,” said Roger Hixson, technical issues director for NENA. “You can’t find people in the phone companies knowledgeable about the old technology anymore. We have to evolve to survive.”

There is a movement under way to move to a next-generation 911 (NG911) system based on modern Internet protocol-based networks that take advantage of capabilities such as text and video messaging. And NENA has done years of work on developing the i3 architecture standard that vendors will follow.

“The intention is to have interconnected networks,” Hixson said. “That type of interoperability requires standards. People in public safety also indicated that they wanted more flexible systems not just in terms of multimedia versus voice, but also in terms of their ability to pick different vendors and have them operate together, so they weren’t locked in with just one vendor.”

The deaf and hard-of-hearing will especially benefit from an upgrade, because it will be easier for them to reach 911 with their phones without requiring additional devices. Looking not too far into the future, it could also harness the technology of biomedical devices, such as a defibrillator that could automatically call 911 during a medical emergency. Increasingly popular automatic collision notification systems, like OnStar, could be routed to 911 and change the way a dispatcher responds to a serious accident.

Beyond receiving and sending multimedia, there are other benefits to the new types of networks. Public safety answering points (PSAPs) will be able to transfer calls and activate alternative routing to share the burden during an emergency or when PSAPs are closed by disaster. For instance, during Hurricane Katrina, 38 call centers were disabled and people in those areas were unable to reach 911. In contrast, Vermont has implemented a modern IP-based network linking its eight PSAPs. When Hurricane Irene took one of them offline in 2011, the other seven were able to seamlessly answer calls for that area. The next-generation system promises to allow seamless information sharing between 911 centers, first responders, trauma centers and other emergency response entities.

Linked PSAPs will also be able to share resources like GIS databases rather than each having to purchase its own.

“From my perspective, it will allow our 911 centers to function in the 21st-century world of telecommunications,” Fontes said. “It will allow for information — voice plus video and data — to move seamlessly from consumer to the 911 center, and then ultimately to first responders participating in FirstNet, the wireless public safety broadband network.”

### What Will Next-Generation 911 Take to Implement?

If the benefits of NG911 seem obvious, the transition itself is by no means easy. There are many issues that states and regions must work through relating to technology standards, the process of transition, governance and funding. Creating regional or state networks of previously autonomous 911 authorities raises many issues. Complicating matters is that each state handles 911 differently.

Progress is uneven across the country. Some regions, like King County, Wash., have been working on upgrading their emergency call centers with NG911 technology for almost a decade. Yet in many rural parts of the country, very little has been done.

There are more than 6,000 PSAPs in the U.S. and they all do things slightly differently, said John Chiaramonte, senior program manager with consulting firm Mission Critical Partners. “Whether these changes happen at a city, county, regional or state level depends on factors having to do with size, history and culture,” he said.

For instance, Vermont has made progress on NG911 because it has only eight PSAPs statewide. Rhode Island has just one PSAP for the whole state. It is much easier to control funding and governance in those situations compared to someplace like Texas that has hundreds of PSAPs.

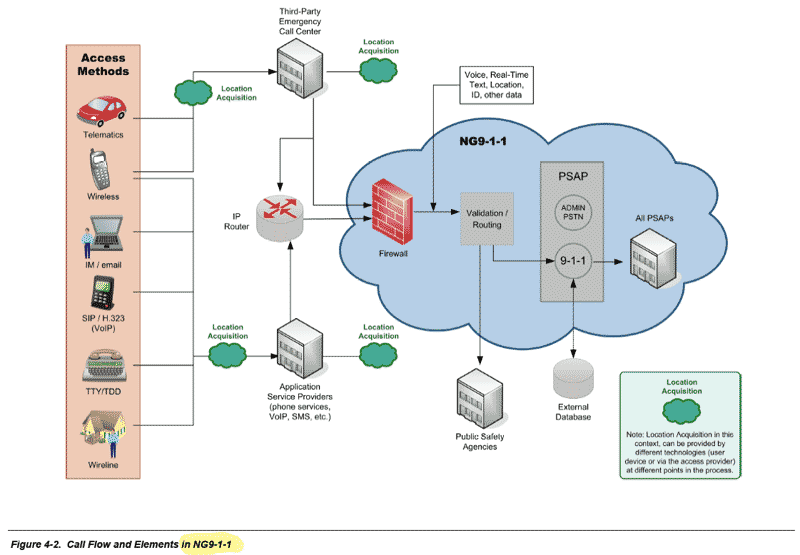
“Technology is not really the big issue,” Chiaramonte said. “It is more the funding, policies and governance that must be worked through.”

The 911 authorities also have to determine how they will maintain legacy systems while working on new ones. “There is not going to be a flash cut-over,” he said. “For a while there is going to have to be a hybrid approach.”

Regions around the country are developing Emergency Services IP networks (ESInets), which are the foundation on which 911 will be built. They are designed to expand mutual aid and allow for the sharing of applications and systems. For instance, they could provide internetwork access to databases such as hazmat information.

In one example, 17 emergency telephone system boards in southern Illinois have bound together through intergovernmental agreements to create a secure public safety broadband network. They will share voice and data associated with a next-generation capable 911 system. Instead of purchasing 17 separate sets of NG911 equipment that would each serve a limited geographic area, they are purchasing two redundant systems and connecting them through a secure IP network.

Some states, like Ohio, are planning a common statewide network structure for core functions. “That highlights an incredibly important point,” Fontes said. “Everyone wants to know what the cost is going to be, and that is a valid question to ask. But there are cost savings associated with the investment. In Washington, where they have deployed the telecom infrastructure for NG911, they have a 48 percent savings in telecommunications cost. So looking at cost is just one side of the coin.”

Colorado is a case study of the promise and challenge of NG911. Daryl Branson, executive director of the nonprofit Colorado 9-1-1 Resource Center, explained that 911 is very much a locally controlled service in his state. Many states have some level of state coordination, such as a 911 office or board. But not in Colorado where the only oversight of 911 service at the state level is the Public Utilities Commission (PUC). And the PUC is tasked only with overseeing the quality of service provided by the carriers, Branson said. “That presents some challenges for local-control states,” he added, “when they want to try to transition to a type of network that is regional or statewide in nature, which is what NG911 would be.”

Stakeholders in Colorado are trying to define a new path because there’s no desire to give up local control or create a new regulatory or oversight body at the state level, Branson said. There have been investments in preparation for NG911 in many parts of Colorado.

“In the Front Range corridor from Fort Collins to Colorado Springs, there’s an understanding that this is the direction we have to go, and a lot of authorities have put in structures already to get themselves ready for an IP-based future,” Branson said. “But in rural areas of the state, in some cases they see the potential, but in other cases it seems very far away and I don’t think it is very high on their list of priorities.”  
Speaking at a Feb. 25 PUC workshop, Matt Goetsch, 911 coordinator for the Montrose County 911 Authority, expressed concerns about going to the added expense for features that a smaller authority and PSAP may not need for some time.

Joseph Benkert, counsel for the Boulder Regional Emergency Telephone Service Authority, which has four PSAPs, said Boulder uses an IP telephone system provided by Intrado. “We could implement NG911 pretty easily at any time.” But he said there are several unanswered questions, including: When does it make sense to do so on a cost basis? And when are the features and services going to be available?

“Our concern is somewhat with the expense of those services and features that may only benefit a small number of people,” Benkert said. “And where would we take money from to pay for those services or features? Because it is a zero-sum game among the public safety agencies.”

System upgrades funded and coordinated by the Larimer Emergency Telephone Authority (LETA) have connected the five PSAPs in Larimer County with a next-generation-ready network. LETA plans to begin offering text-to-911 services in June, working with all four main mobile carriers in Colorado, said Kimberly Culp, the organization’s executive director. The five PSAPS can now communicate instantly online and reroute 911 calls to other communications centers during times of heavy call loads.

Culp agreed that funding can be a challenge, but she said that LETA had been planning for the changes for years, including setting aside funds for the upgrade. “You have to do it in steps,” she said. “You can’t do it all in one year. The biggest challenge for Colorado is how do we do it together? Here in Larimer County, we are good to go.”

The big question, Culp said, is how to connect to adjacent counties or to help them upgrade. “We don’t need state oversight. We just need to go ahead and do it on the local level.”

### How Soon Will NG911 Become Reality?

Fontes and Hixson both estimate that NG911 should be fairly ubiquitous in the U.S. within five years, although there will be outliers that take longer. So what’s the main roadblock?

In some states, 911 is woefully underfunded, and the 911 community has expressed concern that the federal government has not made enough grant funding available for the transition. The federal government has spent just $43 million on grants going back to 2008 for NG911 projects, and so far has designated $115 million (in the Middle Class Tax Relief and Job Creation Act) for it going forward.   
“If we really are going to ensure that our nation has a NG911 system, we have to make sure we are on par with other public safety services, and that we have a sufficient amount of money to enable this to occur,” Fontes said. “There are 250 million 911 calls made each year, and that is the first link to public safety. And to have that first link so critical to the whole chain of events underfunded is very unfortunate.”  
No one at the local level wants to see the federal government do anything that looks like it’s taking over local provision of 911 service, Branson said, but he noted that the federal government is spending up to $8 billion on the FirstNet network to connect first responder agencies with wireless broadband.   
“Clearly, their priority is on FirstNet and not on NG911, but the way I look at it, those are really two sides of the same service. Getting information from the public to the PSAP is the NG911 part,” Branson explained. “They are spending money on the back end, which is getting information from the PSAP to the first responders. But if you can’t get that information from the public to the PSAP first, you’re missing half the equation.”

There are great opportunities for collaboration between NG911 and FirstNet, Chiaramonte said. FirstNet is being designed as a wireless broadband network to connect all first responders. NG911 is a new network to connect all 911 systems. “These are parallel activities going on, and there needs to be more coordination and bridging between these two efforts,” he said. “There are finite resources and not enough funding for either so far, so it is imperative that the efforts be coordinated.”

Aside from funding, another hurdle is that legislative changes are needed in most states because the rules governing 911 haven’t been rewritten in 40 years, Chiaramonte said. “They often specifically reference legacy technology and might not be open to interpretation with newer technology.”

A 2011 report by the California Technology Agency noted that several state laws and regulations governing the type of devices and “calls” allowed to access the NG911 network might require modifications, including:

* reviewing laws and regulations concerning the eligible use of NG911 funds;
* ensuring that laws or regulations do not require specific technology components for 911 service delivery that are incompatible with NG911 service;
* eliminating laws and regulations that inhibit efficient sharing of NG911 data, but retain appropriate safeguards for privacy protection;
* crafting uniform requirements for all NG911 service providers that meet accepted industry standards;
* ensuring that laws and regulations are functional, standards-based and performance-based, without reference to any specific proprietary technology, manufacturer or service provider; and
* ensuring that state and local government should be prohibited from reallocating funds intended for existing 911 and new NG911 services to other purposes.

When asked what other roadblocks remain, Fontes stressed leadership. “There seems to be an understanding that 911 is important, but no one does the deep dive into how 911 really works.”

Government leaders need to treat 911 on par with police, fire and emergency medical services as a critical public safety service. Increasingly, Fontes said, consolidated emergency communications centers are operating independently and no longer tethered to police, fire or EMS. But policymakers have to understand their importance. “Of course, we would always like money,” he said. “But more importantly, we would like equal treatment for grants and funding that already exists for public safety.”

***David Raths*** *is a contributing writer for* Emergency Management *magazine.*

# Humanitarians Using UAVs for Post Disaster Recovery

Source: http://irevolution.net/2014/03/26/humanitarians-using-uavs-for-post-disaster-recovery/

I recently connected with senseFly’s Adam Klaptocz who founded the non-profit group [DroneAdventures](http://www.droneadventures.org/) to promote humanitarian uses of UAVs. I first came across Adam’s efforts last year when reading about his good work in Haiti, which demonstrated the unique role that UAV technology & imagery can play in post-disaster contexts. DroneAdventures has also been active in Japan and Peru. In the coming months, the team will also be working on “aerial archeology” projects in Turkey and Egypt. When Adam emailed me last week, he and his team had just returned from yet another flying mission, this time in the Philippines. I’ll be meeting up with Adam in a couple weeks to learn more about their recent adventures. In the meantime, here’s a quick recap of what they were up to in the Philippines this month.

Adam and team snapped hundreds of aerial images using their “eBee drones” to create a detailed set of 2D maps and 3D terrain models of the disaster-affected areas where partner Medair works. This is the first time that the Swiss humanitarian organization Medair is using UAVs to inform their recovery and rehabilitation programs. They plan to use the UAV maps & models of Tacloban and hard-hit areas in Leyte to assist in assessing “where the greatest need is” and what level of “assistance should be given to affected families as they continue to recover” ([1](http://news.pia.gov.ph/index.php?article=1141395044899)). To this end, having accurate aerial images of these affected areas will allow the Swiss organization to “address the needs of individual households and advocate on their behalf when necessary” ([2](http://news.pia.gov.ph/index.php?article=1141395044899)).

An **eBee Drone** also flew over Dulag, north of Leyte, where more than 80% of the homes and croplands were destroyed following Typhoon Yolanda. Medair is providing both materials and expertise to build new shelters in Dulag. As one Medair representative noted during the UAV flights, “Recovery from a disaster of this magnitude can be complex. The maps produced from the images taken by the drones will give everyone, including community members themselves, an opportunity to better understand not only where the greatest needs are, but also their potential solutions” ([3](http://news.pia.gov.ph/index.php?article=1141395044899)). The partners are also committed to Open Data: “The images will be made public for free online, enabling community leaders and humanitarian organizations to use the information to coordinate reconstruction efforts” ([4](http://news.pia.gov.ph/index.php?article=1141395044899)). The pictures of the Philippines mission below were very kindly shared by Adam who asked that they be credited to DroneAdventures.

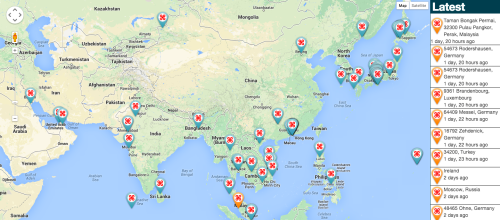
At the request of the local Mayor, DroneAdventures and MedAir also took aerial images of a relatively undamaged area some 15 kilometers north of Tacloban, which is where the city government is looking to relocate families displaced by Typhoon Yolanda. During the deployment, Adam noted that “Lightweight drones such as the eBee are safe and easy to operate and can provide crucial imagery at a precision and speed unattainable by satellite imagery. Their relatively low cost of deployment make the technology attainable even by small communities throughout the developing world. Not only can drones be deployed immediately following a disaster in order to assess damage and provide detailed information to first-responders like Medair, but they can also assist community leaders in planning recovery efforts” ([5](http://news.pia.gov.ph/index.php?article=1141395044899)). As the Medair rep added, “You can just push a button or launch them by hand to see them fly, and you don’t need a remote anymore—they are guided by GPS and are inherently safe” ([6](http://news.pia.gov.ph/index.php?article=1141395044899)).

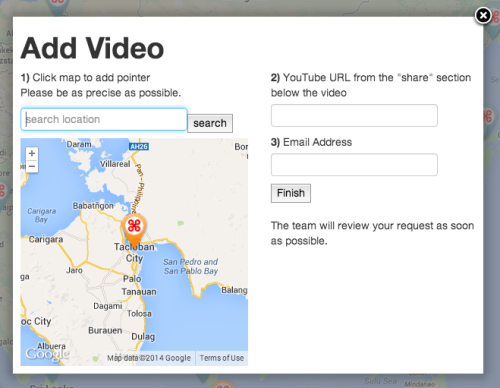


I really look forward to meeting up with Adam and the DroneAdventures team at the senseFly office in Lausanne next month to learn more about their recent work and future plans. I will also be asking the team for their feedback and guidance on the Humanitarian UAV Network ([UAViators](http://irevolution.net/2014/03/12/calling-all-uav-pilots/)) that I am launching. So stay tuned for updates!

# Crowdsourcing a Crisis Map of UAV/Aerial Videos for Disaster Response

Source: http://irevolution.net/2014/06/18/crowdsourcing-a-crisis-map-of-uavaerial-videos-for-disaster-response/

[](https://irevolution.files.wordpress.com/2014/06/travel-by-drone.png)Journalists and citizen journalists are already using small UAVs during disasters. And some are also posting their aerial videos online: Typhoon Haiyan (Yolanda), Moore Tornado, Arkansas Tornado and recent floods in Florida, for example. Like social media, this new medium—user-generated (aerial) content—can be used by humanitarian organizations to augment their damage assessments and situational awareness. I’m therefore spearheading the development of a crisis map to crowdsource the collection of aerial footage during disasters. This new “Humanitarian UAV Map” (HUM) project is linked to the Humanitarian UAV Network (UAViators).

The UAV Map, which will go live shortly, is inspired by [Travel by Drone Map](http://www.dailymail.co.uk/sciencetech/article-2659018/A-drones-eye-view-world-Map-lets-cruise-natural-wonders-remote-locations-sofa.html) displayed above. In other words, we’re aiming for simplicity. Unlike the above map, however, we’ll be using [OpenStreetMap](http://www.openstreetmap.org/) (OSM) instead of Google Maps as our base map since the former is open source. What’s more, and as noted in my [forthcoming book](http://irevolution.net/book/), the Humanitarian OSM Team (HOT) does outstanding work crowdsourcing up-to-date maps during disasters. So having OSM as a base map makes perfect sense.

Given that we’ve already developed a VideoClicker as part of our [MicroMappers](http://irevolution.net/2013/09/18/micromappers/) platform, we’ll be using said Clicker to crowdsource the analysis & quality control of videos posted to our crisis map. Stay tuned for the launch, our Crisis Aerial Map will be live shortly.

****Thinking Asymmetrically in Times of Terror

#### By Colins S. Gray

#### Source:http://strategicstudiesinstitute.army.mil/pubs/parameters/articles/02spring/gray.htm

In American common usage today, asymmetric threats are those that our political, strategic, and military cultures regard as unusual. Such threats differ significantly in character both from those that we anticipate facing from putative enemies and from the methods with which we plan to menace them. Much as international lawyers thus far have failed to define terrorism to the general satisfaction, so US national security specialists have found that the endeavor to define asymmetric threats has proved generally unproductive. Borrowing from the terrorism case, the most fruitful approach to the better understanding of asymmetric threats is not via a forlorn quest for the perfect definition, but rather by the identification of the principal characteristics of, and corollaries to, asymmetry.

**Characteristics of Asymmetry**

A problem with efforts to define an asymmetric threat is that they imply strongly that the universe of threats divides neatly into the symmetric and the asymmetric. Indeed, by definition we can make it so. Of course, this is at best misleading, if not downright nonsensical. Notwithstanding the apparent clarity of some cases, there is no more definitive a universal test for what is an asymmetric threat than there is for who is a terrorist. If one person's terrorist is another's freedom fighter, so one culture's asymmetric threat is another's standard modus operandi. Let us proceed by listing the characteristics of, and usual corollaries to, threats we generally deem to be asymmetric.

Asymmetric threats tend to be:

**. Unusual in our eyes.**

**. Irregular** in that they are posed by instruments unrecognized by the long-standing laws of war (which are keyed to control the conduct of regular military machines engaged in open combat).

**. Unmatched in our arsenal of capabilities and plans**. Such threats may or may not appear truly dangerous, but they will certainly look different from war as we have known it.

**. Highly leveraged against our particular assets**--military and, probably more often, civil.

**. Designed** not only to secure leverage against our assets, but also intended to work around, offset, and negate what in other contexts are our strengths.

**. Difficult to respond to in kind.** This is less true than we usually allow. For example, special forces can be unleashed to operate as "terrorists in uniform." Unconventional warfare of all kinds, including terrorism (and guerrilla operations), is a politically neutral technique.

**. Difficult to respond** to in a discriminate and proportionate manner. It is of the nature of asymmetric threats that they are apt to pose a level-of-response dilemma to the victim. The military response readily available tends to be unduly heavy-handed, if not plainly irrelevant, while the policy hunt for the carefully measured and precisely targeted reply all too easily can be ensnared in a lengthy political process which inhibits any real action.

**. Friendly to the frightening prospect of the "unknown unknown."** By analogy, if we do not scan the skies, including those of the southern hemisphere, comprehensively and routinely, we will probably not spot the asteroid (or other "Near Earth Object") that poses the ultimate asymmetric menace to our security. But even a superior defense community is going to miss some "unknown unknowns." We do not look for what we do not know to look for.

Undoubtedly some works of frontier social scientific scholarship one day will dissect the concept of the asymmetric threat and argue that it has N categories, Y subcategories, and who knows how many intriguing, and not wholly implausible, variations. To be useful to US policy, however, an understanding of asymmetric threats should focus only upon the core of the matter. In addition to the eight broad and overlapping characteristics itemized above, it is only a special class of asymmetric menace that need attract official US concern today. Specifically, the United States is interested not simply in threats that are unusual, different, or designed to evade American strengths. Instead, the United States has to focus on threats, which in this case happen to warrant description as asymmetrical, that if executed could wreak great damage upon American interests. In other words, it is not sufficient just for a threat to be different, also it would need to be prospectively effective. Many candidate asymmetric threats are not threats to achieve a measure of physical control, but rather work ju-jitsu fashion with the inadvertent cooperation of the victim. It follows that the effectiveness of those threats is not some absolute quality and quantity, but is very much ours to determine. This points to a general truth about the strategic utility of terrorism in particular, with the same rule applying to perpetrator and victim.

Typically, terrorists win when their outrages, though generally very minor as compared to the extraordinary events of 11 September or the kind of costs inflicted by regular warfare, induce the state-victim to overreact. The regular belligerent takes action which fatally imperils its own political legitimacy. Similarly, terrorists lose when their outrages delegitimize their political cause; this is what can be termed the mainstream strategic explanation of why terrorism succeeds or fails in particular cases. It is all but impossible for terrorist organizations themselves to inflict truly major physical damage upon the *capabilities* of states. For the parallel point, it is close to impossible for the forces of counterterrorism to root out all of the would-be warriors-by-terror. Each side usually has to be encouraged to defeat itself politically. The historical record on these points is quite clear--indeed, is overwhelming--though it is less well understood than it should be.

Lest there be any misunderstanding, I am not suggesting that the "regular" state party to an asymmetrical conflict should tolerate terrorist outrages. Underreaction, let alone no reaction, most likely would be interpreted as weakness, perhaps as evidence of successful intimidation. Nonetheless, when dealing with terrorists, a low-key response usually is preferable to heavy-handed action which both dignifies the enemy by signalling a large significance to his misdeeds and risks alienating political opinion. Though the attitudes and policies of most irregularly asymmetric foes will be accessible by carefully crafted threats and bribes, usually there is a hard core among the adversary whose mode of rationality literally will brook no compromise. In those instances, the rejectionists (of any compromise whatsoever) either have to be killed or placed in permanent detention. Ideally, the messy task of dealing with the hardest of hard-core among irregular enemies can be left to their former comrades-in-arms (as happened in Ireland, for example, in the early 1920s).

It will be abundantly clear by this juncture that for our current policy and operational purposes the asymmetrical threats of most interest are understood to be militarily, or even quite non-militarily, irregular in character. Nonetheless, we can conceive of asymmetrical threats very different indeed from menaces posed by irregular forces. Most obviously, the United States has to be ready to cope tactically, operationally, and strategically with the smart and unusual employment of regular armed forces by an enemy. Not all of America's foes, current and future, lack a regular military machine. Tactically, operationally, and strategically adroit belligerents use their regular forces in unexpected ways.

It is not obvious that smart tactics, refined operational artistry, and adroit military strategy warrant the ascription "asymmetric," even though they can manifest themselves in "different" behaviors. Indeed, careful reconsideration of the whole subject area of asymmetric threats, and responses to the same, leads the theorist and the practitioner at least to the working conclusion that good strategy on both sides is what this is all about. Because choices for asymmetric activity merge with common-sense approaches to strategy (e.g., doing what the enemy does not expect, generally practicing the precepts advanced by Sun Tzu), there is virtue in fencing off for distinctive discussion the phenomenon of hugely irregular asymmetric threats. This is not to suggest that asymmetry in conflict is synonymous with belligerency between regular and irregular foes, or between regular and irregular forces (regular security communities can license and employ irregular forces and methods), but that is the core of our current concern. How do asymmetric threats work? To repeat, although we must not equate such threats strictly with terrorism, by and large it is terroristic behavior that is the focus here.

**. *Asymmetric threats work by defeating our strategic imagination.***

Every security community is the prisoner of its own strategic expectations. Recall that efforts at strategic deception tend to work when they show enemies what they expect to see. Our historical experience, culture, and geopolitical context, as well as the practical constraints of government (limited information, time, money, flexibility), direct us to prepare for some contingencies, but not others. We prepare against threats that our community agrees consensually merit contingent responses. It may be unjust, certainly strictly inaccurate, to identify failure of imagination as the strategic culprit, when really the problem reduces to knowing how to act in face of the full array of imaginative possibilities. More often than not, the difficulty lies not so much in a failure of imagination--someone will have thought of the threat at issue--but rather in an understandable failure of confidence in imaginative threat identification.

Experience suggests powerfully that the US defense community, with its hundreds of planning staffs, study groups, and respected theorists, has little difficulty imagining dire asymmetric threats (e.g., to the twin towers in New York City, a target previously assaulted unsuccessfully). The problem lies in locating decision rules to filter threats worthy of serious attention from the rest. Even the wealthiest country on Earth cannot afford to invest in protection against all conceivable threats.

**. *Asymmetric threats work by posing possible menaces so awful and awesome that countries dare not respond, at least not until actual experience provides incontrovertible evidence of the threat.***

It is well worth remembering that the asymmetric danger leveled by terrorism can work strategically only with the unwitting cooperation of the victims. If we permit acts of terror to spread fear, despondency, and drive us into a variant of a garrison state, then at best we accept a very high price as the cost of living with this asymmetric foe. At worst, and this is the strategic logic of the terrorist, we find the responses we have initiated to counter terrorism so burdensome that we become discouraged and amenable to effecting a political deal (always assuming, of course, that our asymmetric foe is "dealable," which he may not be). Note that the (Provisional) IRA has bombed and shot its political wing, Sinn Fein, into government in Northern Ireland. While, for the least ambiguous, if in the long term historically ironic, example, Jewish terrorists bombed and shot the state of Israel into existence, as they rendered Britain's mandate over Palestine unsustainably costly.

Because most imagined threats do not occur, it follows that most of them can be safely ignored. Of course, it can be difficult to know with high assurance which threats can be ignored with impunity, and which cannot. Such "acts of God" as giant tsunamis (e.g., triggered by the collapse of a mountainside in the Canary Islands) or collision with a Near Earth Object, tend to be classified in official and popular minds along with mass bio-terrorism and even nuclear missile strikes, as events so awful as to be all but beyond prudent policy response. Apart from the obvious danger of public panic, which may be gratuitous (since nothing can be truly certain until it happens), the difficulty and cost of suitable anticipatory responses are self-deterring. Even when the asymmetric threat approaches both high plausibility and amenability to a fairly reliable solution--as, for example, with the menace of rogue missile attacks--government and public are likely to opt for the non-response of psychological denial. After all, it may never happen.

**. *Asymmetric threats work by challenging successfully our ability to respond effectively.***

By its nature the executive agency for asymmetric threats, and possibly the political force behind that instrument, will be dissimilar to us. Ideally, from his point of view, the purveyor of asymmetric threats does not leave a business card with an address at the scene of the crime. The highly irregular warriors of asymmetry can succeed tactically only in the mercifully rare cases when they are indifferent to personal survival, or when they can merge anonymously into the urban human mass or into forbidding physical terrain. Since strategy is not solitaire, even a country as powerful as the United States requires that its enemies have map coordinates as a necessary condition for chastisement. Although irregular foes generally can function only with the willing or coerced acquiescence of host polities, it is by no means an elementary matter for the United States to drain those particular swamps, as the popular pejorative expression has it.

Among other difficulties: the state-swamps at issue are inhabited by many people deemed to be innocent; they will have civilizational affiliates elsewhere, some of whose official and popular opinion we will need to take seriously; and operational problems most likely would make a mockery of robust intentions and muscular language (e.g., draining the swamp) on our part. It is not sufficient for American responses to asymmetric threats to be effective; in addition, they must be politically and morally tolerable in our culture. The Roman Republic and Empire devised and practiced exceedingly brutal standard operating procedures against irregular foes, domestic and foreign, that were extremely effective. Those procedures could not be followed today by our society in the contexts of the laws of war (as revised, to accommodate internal strife) and the CNN factor.

Americans will need to decide whether asymmetric foes are criminals or enemy soldiers. If we redefine what the concept and legal idea of "war" encompasses, then so also will we have to redefine who can wage it legitimately, which is to say who, and what kinds of behavior, enjoy some legal recognition and protection. In addition, there will have to be reconsideration of the precise meaning of a distinction that has been fundamental to the development of the laws of war, that between combatants and noncombatants ("innocents"). At present the civilized world is trapped somewhat in a timewarp of arguably obsolescent political, ethical, and strategic assumptions and practices. Had three thousand Americans been killed on 11 September 2001 in a regular attack by the conventional forces of a state-enemy, the US response would have been swift and bloody indeed. Given the terrorist nature of the attack, the US defense community had to adjust to an unfamiliar strategic context. There is a considerable danger that today's new (sometimes asymmetric) menaces will be addressed by thoughtways and operating procedures of unduly conventional character.

**. *Asymmetric threats work by acting against what appear to be our strengths.***

Bearing in mind the restricted domain allowed asymmetric threats in this discussion--confined largely to the terroristic outrages committed by the physically relatively very weak--it is the symbols, the apparent exemplars, of our strength that must attract the hostile strategist of asymmetry. In comparatively minor key, the attack on USS *Cole* in November 2000, and in truly major key, the assaults on the World Trade Center and the Pentagon, both illustrate our argument all too clearly. Notwithstanding even horrific scenarios, the Osama Bin Ladens of this era cannot wreck US global military or financial hegemony, or the political context which lends a widespread legitimacy to that preeminence--only ill-judged US policy itself can do that. But the asymmetric threat posed by expressive acts of terror can occasionally succeed in inflicting damage on a scale and of a kind that could be truly damaging to US political prestige in the world.

While US policy and operations must seek to prevent and, if need be, thwart, acts of terror, the impracticality of achieving permanent 100-percent protection (of what?) suggests the wisdom in a policy which scores well at political damage limitation. Given the very restricted physical damage that most asymmetric threats could pose (weapons of mass destruction generally are another matter), we have to think innovatively about ways to minimize loss of prestige when such outrages succeed tactically (as they will, from time to time).

Fortunately, our problem is noticeably strategic in form. The Osama Bin Ladens are not literally madmen. They are highly intelligent, resourceful, and bent upon acting in ways that, in their reasoning, will have beneficial effects. If we are to perform competently in deterrence we need to address empathetically the issue of how, by our policies, we can negate the political effects of tactically successful terrorism.

**Some Working Propositions**

Let us now turn to how we can best prepare for and shape our responses to these threats.

**. *We cannot predict specific asymmetric threats (unless we have excellent intelligence) and therefore we cannot protect everything at risk*.**

What this means is that, as in any war, the friendly side will take losses. While the United States should do all that it can, consistent with maintenance of decent standards of behavior, to make life difficult for would-be terrorists, this character of asymmetric conflict is peculiarly unrewarding to careful defense. The reason should be obvious. Simply stated, we and our friends and allies offer too many targets around the world for preclusive protection to be anything other than a worthy policy goal. Deterrence will be especially important, despite the likely fact that it will be unusually (culturally) difficult to achieve. A confident assumption that Americans are very good at deterrence--witness the course and outcome of the Cold War--needs to be jettisoned forthwith. We are urgently in need of culturally sophisticated profiles of asymmetric foes, so that we may stand some chance of understanding what might best discourage them from proceeding.

**. *We tend to lock onto yesterday's event and project it forward as the menace of the era*.**

It is of the essence of the irregular, asymmetric threat that it will not comprise a replay of yesterday's outrage (though the World Trade Center was attacked more than once). We must not give the impression that we believe that our asymmetric enemies always will be successfully cunning and proficient. From time to time they will succumb to unduly routinized, "regular," and conventional thinking, they will behave incompetently, and "friction" of several kinds can thwart them. All of which is both true and somewhat comforting to recognize, but alas it cannot serve as the basis of our policy. Bureaucracies--military and civilian--and indeed any hierarchical organization which rewards rule-following, are inherently ill-suited to think innovatively about asymmetric threats. The US armed forces have handfuls (no more) of people amongst their substantial special operations forces who truly can think "outside the box," and who can reason and, if need be, behave like "terrorists in uniform." It is not likely that even an elite group of US officials blessed with relatively unconventional mindsets would offer much of value with respect to specific asymmetric threat-spotting; there are just too many possibilities out there. But at the least such a group should be able to frame an intelligent generic strategy for response, and therefore deterrence.

**. *Although we are not likely to perform well at the identification of very specific dangers, we should be able to identify, and therefore plan how to protect against, the kind of threats that would do us major harm*.**

This thought really is complementary to the merit in the idea of trying to access the enemy's culture. Since his exact operational choices are likely to remain a mystery to us, we at least should know what we value most, and take measures to afford such protection as is feasible. The lore on sound principles for the guidance of defense planning includes the injunction not to avoid being surprised, but rather to avoid serious damage from the effects of surprise. The more one thinks about the problems of coping with asymmetric threats, the more relevant do traditional, historically founded approaches to defense planning appear to be.

**. *We need to be especially alert to the possibility that asymmetric threats can wreak their greatest damage through ill-judged measures of response that we ourselves choose to undertake*.**

While we do need to worry about, and plan to prevent, the damage that asymmetric threats might cause, we have to be particularly alert to the danger that relatively minor physical damage inflicted by terrorists may be translated--by us--into truly major societal and economic costs as we dignify the asymmetric belligerent by overreacting. If decisive action against asymmetric threats is possible, ideally after the fashion of defeating piracy by burning out the pirates' lairs, all to the good. However, the challenge to US policy lies not so much in those cases where there is a military option, but rather when there is not. The temptation to do something, for the sake of being seen to be doing something--even something strategically stupid--can be politically irresistible.

One should not forget a basic rule outlined above: the terrorist (as an asymmetric opponent) can succeed only with our assistance. He lacks the resources himself to inflict significant direct damage upon us. Even if armed with weapons of mass destruction (WMD), the scale of the terroristic asymmetric menace is but a pale shadow of the damage that the superpowers might have inflicted in a World War III. This is not to suggest that terrorists with WMD are insignificant--far from it. But it is to say that we need to keep a sense of proportion. There may be a great Sino-American struggle in our future, a possible conflict which, in its potential for harm, would demote today's roguish terroristic perils to the second-order problems that they are, historically. Less than 20 years ago we faced some danger of a war wherein casualties easily could have numbered in the many millions. Without diminishing the tragic loss of three thousand lives, it cannot be strategically sound for America to allow itself to be permanently traumatized by such an outrage, or consequently to recast its national security policy on a grand scale.

**. *We need to identify and think hard about threats to which we lack obvious responses*.**

In effect, this point advises asymmetric, even unconventionally irregular, approaches on our part. We have to learn to respond differently, but effectively, to threats which cannot be answered in kind. The United States has to ask imaginatively what it is that its asymmetric foes value highly, and devise ways and prepare means to hurt those values severely. If there are cultural barriers on our side to incorporating particularly murderous options into our policy, strategy, or operational intent, then we may need to reconsider some of our attitudes and rules of engagement. After all, war is war. Combat against terroristically asymmetric foes is likely to be about as far removed from the "clean" conditions of, say, war at sea or in the desert (where there are no civilians) as can be imagined.

**A Skeptical End-Note**

In the history of strategic ideas, the contemporary American fascination with asymmetry comprises rediscovery of the stunningly obvious. To behave in ways different from those expected by an enemy can be simply good tactics, operational art, and strategy. Since asymmetrical merely means different, it is a little hard to understand quite why the notion has been elevated as the latest fashionable Big Idea (following on from the concept of a revolution in military affairs). In this essay I have confined asymmetrical threats to those emanating from an irregular foe. However, with equal, if not greater, justification I might have set out to diminish this Big Idea by pointing out that all of America's wars have been asymmetrical contests. Even aside from the bloody, two and a half century-long experience of struggle against native American irregulars, when has the country waged a plausibly symmetrical conflict? Imperial Britain was radically different--grand strategically--from the revolting Colonies, as the Confederate States were from the Union, as Germany, Japan, and then the Soviet Union were from the United States in the 20th century.

Defense and war planning always have a significant asymmetrical dimension, which should find expression at every level--tactical, operational, and strategic. Competent tacticians, operational artists, and military strategists are obliged to be aware of salient actual and possible asymmetries. In fact, the quality of being or behaving differently--which is all that asymmetrical means--is so natural to effective defense professionals that they can be excused wondering why the US defense community today is so excited by the concept. Historically assessed, symmetrical warfare has been the rare exception, not the rule. Belligerents always differ from each other, usually in ways that are or could be strategically significant.

It is entirely admirable for the US defense community to recognize the potential importance of asymmetry. This recognition should help offset the peril of indiscriminate strategic autism to which very great powers are prone. A less happy consequence of the current fascination with asymmetry is the imputing of extraordinary efficacy and significance to it. To a greater or lesser degree, *all* tactical, operational, and strategic behavior is asymmetrical. There are no identical belligerents, with identical forces, who behave identically. But to listen in to the current American defense debate is to hear senior officials talking as if they had just discovered extraordinarily dangerous asymmetrical enemies who pose similarly awesome asymmetrical threats. To be different, or to behave differently, is not necessarily to be strategically effective. There is nothing inherently strategically magical about different--i.e., asymmetrical--behavior. There is some excuse for journalists who become overexcited when exposed for the first time to the apparently new Big Idea of asymmetry, but we defense professionals should know better. From the time of its founding, the United States repeatedly has waged war asymmetrically, as it was obliged to do against a series of "different" enemies.

A little reflection reveals that asymmetry essentially is a hollow concept. As a relational variable, that which is asymmetrical can be labeled as such only with reference to that which is symmetrical--and what is that? The concept may have some limited merit if it is corralled, as in this essay, with a carefully specified meaning (focused on an irregular foe favoring terroristic activity). As a contribution to the general lore of strategy, however, asymmetry is a complete non-starter. Given that competent American military planners have always plotted how to defeat particular enemies in the distinctive ways best suited to the individual cases at issue--albeit in ways preferred by American strategic and military culture--what exactly is novel or even especially interesting about the concept of asymmetry? Because all warfare is asymmetrical (there are no sets of identical belligerents), in effect no particular wars or warfare is distinctly so. In this respect, a course of instruction on "asymmetrical warfare" would be content-free.

***Dr. Colin S. Gray*** *is Professor of International Politics and Strategic Studies, and is Director of the Centre for Strategic Studies, at The University of Reading, England. He is also European Director of the National Institute for Public Policy. He took his B.A. in government at Manchester University and his D.Phil. at Lincoln College, Oxford University. His public service record includes five years as a member of the President's General Advisory Committee on Arms Control and Disarmament (1982-87). Of recent years his work has included studies on technology and strategy and on strategy for space. His most recent book is Modern Strategy (Oxford: Oxford University Press, 1999). In 2002 he will publish Strategy for Chaos: RMA Theory and the Evidence of History (London: Frank Cass, forthcoming).*

# These Are The 10 Most Polluted Areas Of The World

Source: http://www.businessinsider.com/these-are-the-10-most-polluted-areas-of-the-world-2013-11

This dumpsite in Accra, Ghana is full of toxic fumes from people burning electronics for copper.

Remote industrial towns, e-waste processing centers and the site of an infamous nuclear disaster top 2013's worst polluted places, according to a new list from the New York-based nonprofit Blacksmith Institute.

The toxic locations are not ranked, but they include Chernobyl, Ukraine, which is still suffering the consequences of a radioactive meltdown that occurred in 1986; the Niger River Delta in Nigeria, where each year 240,000 barrels of crude oil are spilled; and Hazaribagh, Bangladesh, where carcinogens enter the water supply from more than 200 tanneries concentrated in a small area of the city.

"In this year's report, we cite some of the most polluted places we've encountered. But it is important to point out that the problem is really much larger than these 10 sites," Richard Fuller, president of the Blacksmith Institute, dedicated to eliminating life-threatening polluting in developing countries, said in a statement. "We estimate that the health of more than 200 million people is at risk from pollution in the developing world."

According to the report, the World Health Organization (the public health arm of the United Nations) has estimated that 23 percent of deaths in the developing world can be attributed to environmental factors like pollution. Besides cancer, exposure to toxic chemicals can cause acute and chronic poisoning, cognitive impairment, organ damage and respiratory problems, the report said, adding that children are most vulnerable to these impacts.

Researchers said the 10 sites were chosen based on the severity of their health risk and prioritized by their value as examples of different kinds of pollution threats around world.

**Here are the 10 sites listed in the report, in alphabetical order:**

**Agbogbloshie, Ghana**: This dumpsite in the Ghanaian capital Accra is the second largest e-waste processing area in West Africa. When sheathed cables from electronics like microwaves and computers are burned to recover the copper material inside, metals can particulate in the smoke and get left behind in the soil. An estimated 40,000 people are affected by the pollution threat.

**Chernobyl, Ukraine**: The world's worst nuclear disaster at Chernobyl in 1986 released 100 times more radiation than the atom bombs dropped over Hiroshima and Nagasaki. Skin lesions, respiratory ailments, infertility and birth defects affected people in contaminated areas in Belarus, Russia and Ukraine for years and the accident has been linked to more than 4,000 cases of thyroid cancer. Pollution from Chernobyl is estimated to have affected some 10 million people.

**Citarum River, Indonesia**: More than 500,000 people are directly affected, and up to 5 million people are indirectly impacted, by chemical pollution in the Citarum River Basin in West Java. Lead, aluminum, manganese and iron concentrations in the river are several times higher than world averages because of pollution from industrial and domestic sources.

**Dzershinsk, Russia**: A major site of chemical manufacturing in Russia, Dzershinsk has high levels of pollutants like dioxins and phenol in the groundwater. Residents suffer from diseases and cancers of the eyes, lungs and kidneys and life expectancy in the city is just 47 for women and just 42 for men.

**Hazaribagh, Bangladesh**: Tanneries using old, outdated and inefficient processing methods to make leather dump 22,000 cubic liters of toxic waste each day into the city's main river, impacting more than 160,000 people. This waste includes the cancer-causing chemical hexavalent chromium.

**Kabwe, Zambia**: Decades of unregulated lead mining in this African city have caused serious health problems for residents of Kabwe, where more than 300,000 people are thought to be affected by pollution. In 2006, children's blood lead levels in Kabwe were found to exceed the recommended levels by five to 10 times.

**Kalimantan, Indonesia**: On the island of Borneo, Kalimantan and the surrounding areas have become contaminated with mercury because of small-scale gold mining, impacting some 225,000 people. Miners in the region use mercury in the gold extraction process, resulting in mercury emissions during the amalgamation and smelting processes.

**Matanza Riachuelo, Argentina**: More than 15,000 industries are thought to be releasing a variety of pollutants into the Matanza River, which passes through Buenos Aires and empties into the Rio de la Plata. Contaminants include zinc, lead, copper, nickel and total chromium (a term that includes two forms of chromium), making the drinking water near the Matanza-Riachuelo river basin seriously unsafe, threating more than 20,000 people who live in the area.

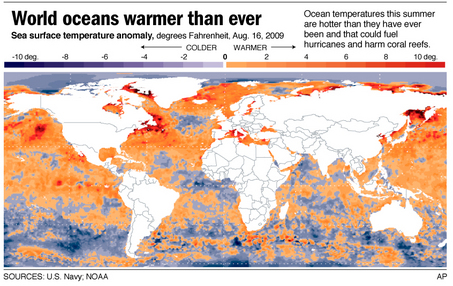
**Niger River Delta, Nigeria**: An unknown number of people are impacted by the voracious petroleum industry in this densely populated part of Africa, where there were nearly 7,000 incidents involving oil spills between 1976 and 2001. The report said that about 2 million barrels of oil were being extracted from the delta every day as of last year.

**Norilsk, Russia**: Norilsk is an industrial city in Siberian Russia, where each year, nearly 500 tons each of copper and nickel oxides and 2 million tons of sulfur dioxide are released into the air. Life expectancy for factory workers in Norilsk is 10 years below the Russian average.

# New study improves measurements of the warming oceans

**By John Abraham**

Source: http://www.theguardian.com/environment/climate-consensus-97-per-cent/2014/jun/20/new-study-improves-ocean-warming-measurements?CMP=twt\_gu

Heating of the oceans is, pardon the pun, a hot subject. There is a broad recognition that the oceans, which absorb approximately 90% of excess greenhouse gas energy, are key not only to how fast the planet will warm, but also how hot it will get in the end. Many recent studies have tried to measure deeper ocean regions or previously uncharted areas in the search for heat. A new study by Lijing Cheng and Jiang Zhu takes a different approach. They ask how large are biases in the estimates of ocean heating from the finite resolution of the devices themselves. Their findings are exciting, but first, let’s talk about the details of the study.

Measuring the oceans is difficult; they are vast and deep. In order to measure the total energy in the ocean, you have to obtain temperatures at many locations and at many depths. Not only that, you need to make measurements over many years if you want to identify long-term trends.

Oceanographers have been making such measurements for decades. But the density of measurements is not spread uniformly over the oceans. There are more in coastal regions or major shipping lanes than in other locations. To further complicate the problem, the measurement methods have changed over the years.

Decades ago, insulated buckets, then, bathythermograph devices, and now ARGO floats have been used. While these devices all go down into the ocean depths, they have different depth resolutions. Over the years, we have a large number of measurements near ocean’s surfaces but as we measure deeper and deeper, fewer and fewer data points are available. As a result, we cannot construct exact temperature-depth curves. Consequently, our discrete data points give us some error, some bias compared to real ocean temperatures.

In their paper, Lijing Cheng and Jiang Zhu quantify our ocean errors. They started with a “real” ocean temperature and then they extracted discrete data and asked themselves how their discrete data matched the original temperatures. By discrete data, I mean that they extracted temperatures every 10 meters, 20 meters, 30 meters, and so forth. Somewhat like the science of calculus where smooth curves are approximated by a series of straight-lined segments.

What they found was very interesting. **In the upper regions of the oceans, the discrete data was colder than the real ocean temperatures. However, deeper in the waters, the trend reversed and the discrete data was warmer. But to make things more complicated, the errors differed depending on location in the oceans. Near the equator (tropics), the discrete data exhibited a warm bias but further from the equator, the bias was cold. Furthermore, the extent of the error changed throughout the year.**

The authors use their findings to calculate how close together measurements would have to be to obtain accurate ocean temperature measurements. The authors also propose a method to correct past temperature data to account for these biases. It is important for readers to recognize that the biases themselves do not make us think climate change will be worse or milder. What really matter are the changes to biases over time.

Dr. Cheng, who recently graduated with his PhD, told me,

*“Ocean heat content is one of the key climate indicators. The latest IPCC report lists upper ocean heating (upper 700 meters of ocean water) that range widely among researchers. Diagnosing the sources of uncertainty in upper ocean heat content is an important task for the scientific community and the general public. I first proposed a method to examine expendable bathythermograph biases. We worked on a cooperative research effort with colleagues Tim Boyer from NOAA, and Susan Wijffels and Rebecca Crowley from CSIRO to diagnose new measurement correction schemes. This could help oceanographers obtain unbiased ocean temperatures for climate studies. We noticed that the resolution of measurements is sparse. We wanted to know whether the insufficiency in resolution could cause errors in ocean heating estimates. We assessed this problem in our paper and we are now working on improving ocean warming estimates.”*

Since this topic is one I’ve published on recently, I will be awaiting the next installment from this research team with bated breath.

***Dr. John Abraham*** *is a Professor of Thermal Sciences where he researches in climate monitoring and renewable energy generation for the developing world. His energy development work has extended to Africa, South America, and Asia.*



# http://r70.cooltext.com/rendered/cooltext1333431858.png

# The Relationship Between the Business Impact Analysis and Risk Assessment

**By Jacque Rupert**

Source: http://www.drj.com/the-relationship-between-the-business-impact-analysis-and-risk-assessment.html

The business impact analysis (BIA) and risk assessment are foundational elements of every effective business continuity program; however, in our experience, many business continuity planning participants experience a lot of confusion regarding the definitions, relationship, and expected outcomes between the two processes. This confusion often results in outcomes that fail to drive preparedness.

Avalution acknowledges that there are many different ways to design and execute BIA and risk assessment processes, depending on the objectives for each. We also know that many experienced business continuity professionals have strong opinions on this topic, which may not fully align with our view. This article simply aims to provide Avalution’s perspective on how to best design and execute the BIA and risk assessment processes to achieve results that align with how management views business continuity risk.

**Business Impact Analysis and Risk Assessment: Defined**

To understand the relationship between the BIA and risk assessment, we must first have a common understanding and definition of the two processes.

**Business Impact Analysis**

Avalution defines the BIA as an identification and analysis of business processes/activities (including required resources), with the objective of understanding the impact of downtime, which drives the assignment of recovery objectives and prioritization.

**Risk Assessment**

Avalution defines the risk assessment as an identification and analysis of business risks that may affect an organization’s ability to deliver its most important products and services, with the objective of understanding the effectiveness of existing controls, as well as additional controls to decrease the likelihood or severity of a disruption.

On its surface, this definition may not appear to be controversial or even different from other professionals’ views; however, the difference lies in the term and definition of “business risk”. A business risk is not a threat (e.g. fire, flood, or hurricane); rather, a business risk is a situation that leads to a disruption in an organization’s ability to deliver products and services. Typically, these risks take the form of a loss of required resources, including personnel, facilities, equipment, suppliers, and technology. Said another way, a threat can lead to a business risk (e.g. a hurricane can cause a loss of facility access, or a pandemic can result in high absenteeism), but the business risk is not synonymous with the threat.

Why does it matter? We’ll explain.

**Threat Assessment**

Avalution believes that there is a major difference between a risk assessment and a threat assessment. Both serve beneficial purposes, but the terms should not be used interchangeably. A threat assessment is typically an inventory of all threats that may impact the organization. The conclusions drawn from a threat assessment may be beneficial during the planning process in order to highlight where threat-specific response and recovery procedures are warranted; however, when connecting with management, executives do not necessarily need or want a list of threats that could impact them. Based on feedback, executive managers typically already feel comfortable with their understanding of the potential threats that could impact them and their organizations, or they recognize that they cannot predict all threats (e.g. no one could have predicted or imagined the events on September 11th).

**Business Impact Analysis and Risk Assessment: Outcomes**

Now that we have defined the terms BIA and risk assessment (as well as threat assessment), the next section of this perspective outlines what Avalution views are the expected outcomes from these analytic efforts.

**Business Impact Analysis**

The major outcomes associated with the BIA, include (but are not necessarily limited to):

* Understanding of business processes/activities, including the business processes’:
  + Customers (internal and external)
  + Outputs/Deliverables
  + Inputs (which enable the process to function, including resources and other internal and third-party dependencies)
* Understanding an estimation of the impact of downtime, which serves as business justification for establishing recovery objectives
* Identification of recovery objectives and a prioritized order of recovery for business processes and resources
* Collection of information that may help identify appropriate recovery strategies and document future plans (perhaps a secondary objective associated with the BIA)

Following the BIA, the organization should be positioned to identify the critical activities that contribute to the delivery of its most important **products and services**, list all resources needed for recovery, and prioritize activities and resources by recovery objective.

**Risk Assessment**

The major outcomes associated with the risk assessment include:

* Understanding of potential business risks, including their likelihood and impact
* Identification of existing controls, and potential control enhancements or new strategies to mitigate business risk by protecting resources (as to decrease the likelihood or severity associated with a disruptive incident)

Following the risk assessment, the organization should be able to list all business risks (prioritized by those that would have high impact and have a high probability of occurring), and a list of mitigating control options to address the business risks. For example, if a business activity is only performed in one location by a certain sub-set of personnel, the business risk would be an unavailability of that location or those personnel. Then, management would have the option of identifying an alternate location and/or alternate personnel to perform the business activity if the primary location and/or personnel were unavailable. Management can only protect necessary resources from disruption in order to lessen the impact of disruption; management cannot, in many circumstances, control the likelihood of a threat occurring.

**Relationship Between the BIA and Risk Assessment (Order of Execution)**

In addition to some disagreement among business continuity professionals regarding the BIA and risk assessment definitions and outcomes, disagreement also exists regarding the order of execution: whether it is best to perform the risk assessment before, during, or after the BIA. While many professionals argue that it is best to perform the risk assessment before the BIA to establish the risk landscape in which the organization operates, Avalution argues the opposite. First, we must agree on what has been stated:

* The outcomes of the BIA are:
  + The identification of resources needed to perform business activities
  + The understanding/estimation of impact of downtime
* The inputs into the risk assessment are:
  + The identification of required resources that may be impacted by a wide variety of threats (known and unknown)
  + An understanding of business impact, which contributes to the prioritization of future control enhancements and risk mitigation strategies

If those inputs and outputs are true, then performing a risk assessment before understanding impact or the identification of necessary resources would prove to be quite difficult. Thus, Avalution argues that risk assessments should be performed after the BIA (or at the very least, at the same time).

**Conclusions**

Nearly all business continuity professionals agree on the importance of the business impact analysis and risk assessment as foundational elements of all business continuity planning processes; however, this article presents Avalution’s view of the relationship between the BIA and risk assessment. Implementing an effective business continuity program enables organizations to mitigate business risk associated with disruptive incidents and thus be better prepared to respond to and recover from a loss of necessary resources. Without an understanding of potential impacts and resources established by the BIA, it would be difficult to understand the business risk of a loss of resources or identify mitigating controls to protect those resources from disruption. Avalution believes that performing a BIA and risk assessment using the approach discussed in this article enables organizations to prioritize the identification and implementation of business continuity strategies based on business strategy, obligations, and priorities.

***Jacque Rupert,*** *Avalution Consulting: Business Continuity Consulting*

