March 2015

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

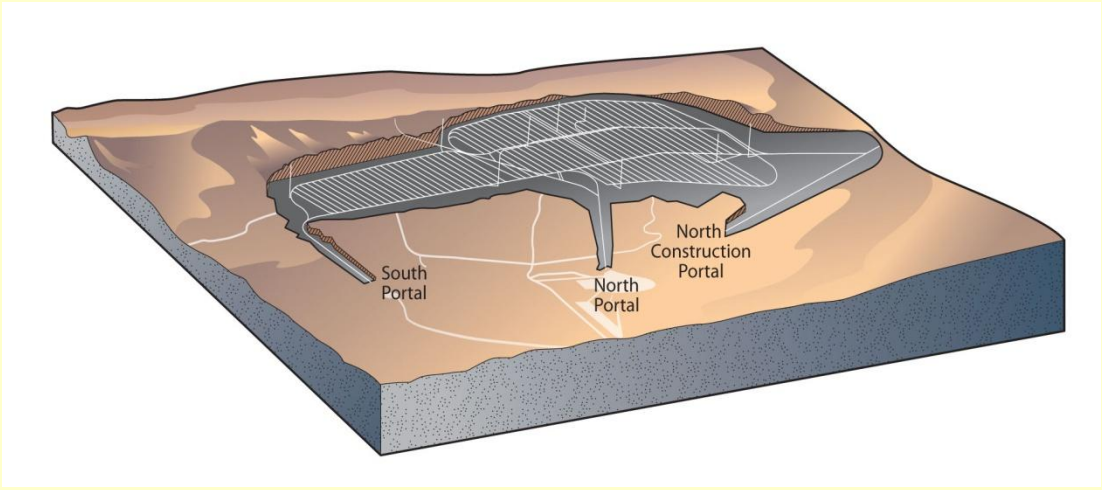
10 years

www.cbrne-terrorism-newsletter.com

Look to Texas Rather Than Nevada for a Site Selection Process on Nuclear Waste Disposal

Source: http://fas.org/pir-pubs/look-texas-rather-nevada-site-selection-process-nuclear-waste-disposal/

Republican gains in the 2014 midterm elections have refocused attention on a number of policy areas–including nuclear waste storage. Although President Obama has consistently championed nuclear power by providing federal loan guarantees for new reactors and placing nuclear power among the "clean energy" sources targeted for an 80 percent share of the nation's electricity production by 2035, he has also placed the viability of nuclear power in doubt by thwarting efforts to build a high level **radioactive waste repository at Yucca Mountain, Nevada** (photo). Several newspapers around the country have run editorials arguing that the Yucca Mountain ought to be revived or even, as the *Chicago Tribune* suggested, "fast-tracked." Arguments like these emphasize the risks associated with our current interim storage of spent fuel at more than one hundred power plants in close proximity to population centers throughout the country, commitments for disposal capacity the federal government owes utilities and contaminated legacy sites like those in South Carolina and Washington State, and the amount of research and spending that has already been devoted to investigating the suitability of the Yucca Mountain site.



However, it is unlikely that Yucca Mountain will ever receive shipments of nuclear waste. Nevada's persistent and successful efforts to thwart the Yucca Mountain project and the Nuclear Waste Policy Act of 1982 are likely to continue as they demonstrate the futility of a policy that forces disposal on an unwilling host state. Three years ago the Blue Ribbon Commission on America's Nuclear Future said as much, recommending instead a "consent-based" approach to siting nuclear waste storage and disposal facilities. How would such an approach work?

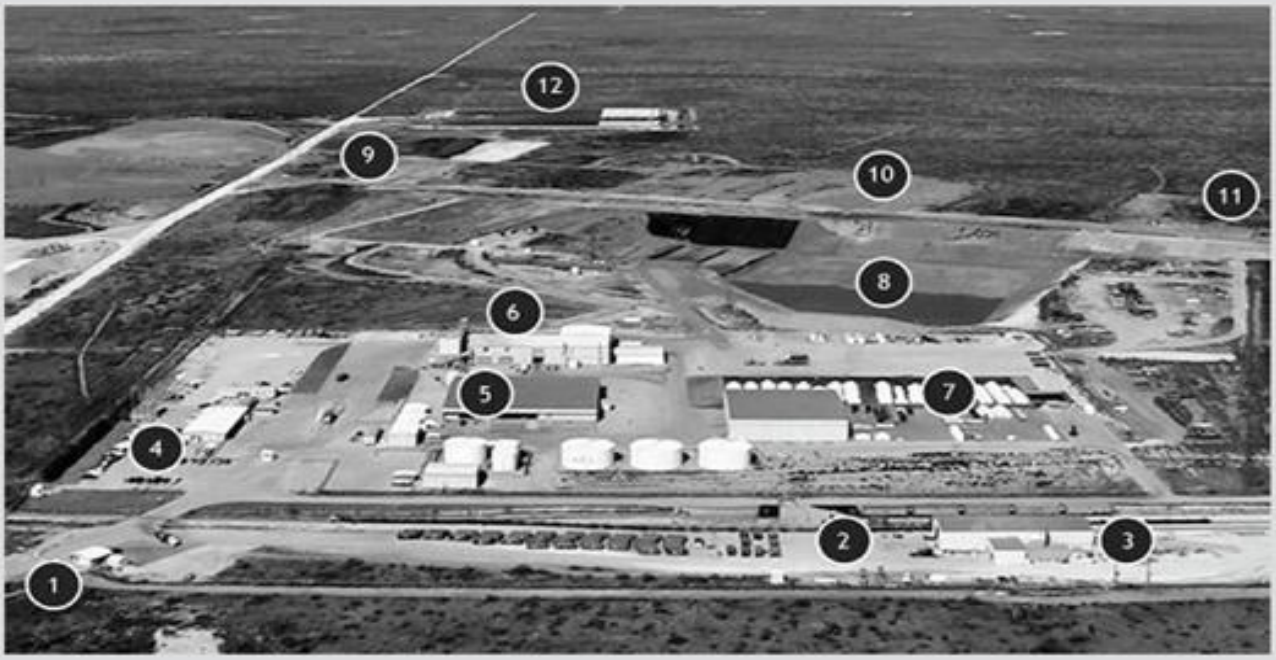
For the past three years, Texas has been accepting what so many other states and localities have rejected in past decades-radioactive waste from the nation's nuclear power plants. **A newly opened private facility operated by Waste Control Specialists in Andrews County, Texas (left) has been receiving shipments of low-level radioactive waste from multiple states.** This year, the Texas Commission on Environmental Quality has

amended the license for the Andrews County site to more than triple its capacity and it can begin accepting "Greater Than Class C Waste"- the most highly radioactive materials in the low-level radioactive waste stream, as well as depleted uranium. Residents and elected officials in Andrews County are now considering whether or not to support a proposal for a high-level radioactive waste disposal facility.

We should take a closer look at past developments in Nevada and more recent decisions in Texas to guide our future nuclear waste policy. These two states are engaging with different aspects of the nuclear waste stream, governed by very different policy approaches. Nevada's efforts to thwart the Yucca Mountain project are rooted in the coercive approach codified in the Nuclear Waste Policy Act of 1982. In contrast, the willingness of Texas to establish new disposal capacity stems from the Low-level Radioactive Waste Policy Act of 1980—a law that expanded the authority of states hosting disposal sites in an effort to overcome state opposition to waste sites in the midst of an urgent shortage of disposal capacity.

First, let's consider the troublesome politics that has infused the Nevada case. The Nuclear Waste Policy Act of 1982 established a scientific site selection process for an eastern and western waste repository. However, President Reagan abandoned this process in 1986 by halting the search for an eastern site amid fears of midterm election losses in potential host states of Wisconsin, Georgia and North Carolina. In 1987, Congress abandoned the search for a western site when House Speaker Jim Wright (D-TX), and House Majority Leader Tom Foley (D-WA), amended the law to remove

Waste Control Specialists Site in Andrews County



1. Access road to 1,338-acre fenced site *(guarded entrance)*
2. On-site rail spur and rail-unloading facility
3. Maintenance building
4. Administration building with analytical and radiological laboratories
5. Container Storage Building
6. Stabilization Building *(left portion)* and Mixed Waste Treatment Facility *(right portion)*
7. Bulk/Bin Storage Units
8. Hazardous waste landfill *(being expanded to the East)*
9. Proposed location for byproduct radioactive material landfill
10. Proposed location for Federal low-level radioactive waste landfill
11. Proposed location for Texas Compact low-level radioactive landfill
12. Ten-acre storage area for low-specific-activity

Texas and Washington from consideration. The amended law became known as the "Screw Nevada" plan because it designated Yucca Mountain as the sole site for the waste repository.

While politics effectively trumped science in the selection of Yucca Mountain, opponents- led by Senator Harry Reid of Nevada- have employed politics to effectively thwart the project. In 2005,

Reid placed 175 holds on President Bush's nominations for various executive appointments until Bush finally nominated Reid's own science advisor, Gregory Jaczko, to the Nuclear Regulatory Commission (NRC). In 2006 Reid persuaded the Democratic National Committee to move the Nevada caucuses to the front of the 2008 presidential primary calendar, prompting each candidate to oppose Yucca Mountain. President Obama fulfilled his campaign promise by tapping Jaczko to chair the NRC and dismantling Yucca Mountain. Each year the President's budget proposals zeroed out funding for the facility, the NRC defunded the license review process and the Department of Energy has continued to mothball the project. Although court decisions have forced the administration to begin reviewing the project, progress has been slow and in the meantime the Yucca facility offices have been shuttered, workforce eliminated, and computers, equipment and vehicles have been surplused. Jaczko was forced to resign amidst concern from other NRC members that his management style thwarted decision making processes. However, Jaczko's chief counsel, Stephen Burns was sworn in as the commissioner of the NRC on November 5, 2014.

We should expect, accept, and plan for such political maneuvering. Our system of locally accountable representatives empowers individual office holders with a wealth of substantive and procedural tools that make all nuclear politics local. Any decision making on this issue will be a political contest to locate or avoid the waste. Consequently, if there is to be a politically feasible nuclear waste repository, it will require a willing host. Money and the promise of jobs alone have not proven alluring enough for acceptance of such a project. We would do better to embrace our decentralized politics and offer the host significant authority over the waste stream.

This is the current situation that Texas enjoys: Congress gave states responsibility for establishing low-level radioactive waste sites and, as an incentive, enabled states to join interstate compacts. Once approved by Congress, a compact has the authority to accept or decline waste imports from other states, which is a power that is normally not extended to states because it violates the interstate commerce clause of the U.S. Constitution. Texas is in a compact with Vermont, and as host state, Texas shapes the waste market by determining disposal availability for other states. Texas also has authority to set fees, taxes, and regulations for disposal in collaboration with federal agencies. Compacts can dissolve and host states can cease accepting waste altogether at a future date. While even under these provisions most states will refuse to host radioactive waste, the extension of state authority at least courts the possibility (as in Texas) of the rare case that combines an enthusiastic local host community in a relatively suitable location, a supportive state government, and a lack of opposition from neighboring communities and states. This approach better meets our democratic expectations because it confronts the local, state and national politics openly and directly, courting agreement at each level and extending authority over the waste stream to the unit of government bearing

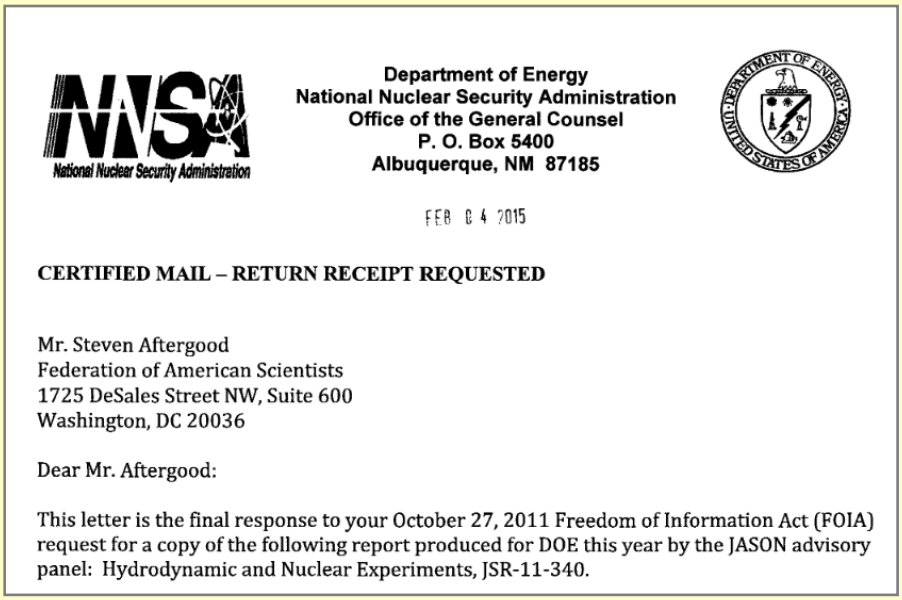
responsibility for long term disposal within its borders.
What if we adopt this approach and there is no willing host for spent fuel at a technically suitable site? What if a site is established, but at some future date the host state and compact exercise authority refuse importation or dissolve altogether? We would be left with interim onsite storage- the same result our current predictably failed policy approach has left us in. If there is no willing host, or if long term disposal is less certain due to the host's authority over the waste stream, we also gain authentic and valuable feedback on societal support for nuclear energy. That is, our willingness to provide for waste disposal in a process compatible with our democratic norms and decentralized political system should influence our decisions on nuclear energy production and waste generation.

JASON on the Physics of Nuclear Weapons

Source: http://fas.org/blogs/secrecy/2015/02/jason-hydro/

Feb 20 – **Despite the extensive data obtained through the conduct of more than 1000 nuclear explosive tests, there is still much that is unknown or imperfectly understood about the science of nuclear weapons.**

A newly disclosed report prepared in 2011 by the JASON science advisory panel assessed efforts by the National Nuclear Security Administration (NNSA) to "develop improved understanding of the underlying physics of the materials and components in nuclear weapons."



Department of Energy
National Nuclear Security Administration
Office of the General Counsel
P. O. Box 5400
Albuquerque, NM 87185

FEB 04 2015

CERTIFIED MAIL – RETURN RECEIPT REQUESTED

Mr. Steven Aftergood
Federation of American Scientists
1725 DeSales Street NW, Suite 600
Washington, DC 20036

Dear Mr. Aftergood:

This letter is the final response to your October 27, 2011 Freedom of Information Act (FOIA) request for a copy of the following report produced for DOE this year by the JASON advisory panel: Hydrodynamic and Nuclear Experiments, JSR-11-340.

The study was released in redacted form last week in response to a Freedom of Information Act request from the Federation of American Scientists. See Hydrodynamic and Nuclear Experiments, JASON report JSR-11-340, November 2011.
More recently, JASON performed "a short study of the science and technology enabling improved measurement, characterization, and understanding of the state of stress in engineered subsurface systems of the Earth's crust." See Subsurface Characterization, Jason letter report JSR-14-Task-013, September 2014.

▶ **Read the report at:** http://www.fas.org/irp/agency/dod/jason/hydro.pdf

A Syrian Nuclear Snapshot

Source: http://acdemocracy.org/a-syrian-nuclear-snapshot/?utm_source=A+Syrian+Nuclear+Snapshot*1&utm_campaign=A+Syrian+Nuclear+Snapshot*&utm_medium=email

Syria has a long history of deception and lying to the international community on matters concerning its development and use of weapons of mass destruction (WMD). Therefore, any new information concerning these matters, even if highly speculative, should set the scene for further investigations, which in the past have revealed problematic Syrian intentions and activities in the chemical and nuclear realms.
On January 9, 2015, the German weekly Der Spiegel published an article entitled "Assad's Secret: Evidence Points to Syrian Push for Nuclear Weapons," based on known facts, facts leaked to the journal,

assessments, and speculations. According to the article, Syria did not give up its nuclear weapons development ambitions following the destruction of its almost completed, North Korean-constructed nuclear reactor near the town of Deir-al-Zor, on the banks of the Euphrates River.

A Google Earth view of a Syrian scientific facility in Jamraya, near Damascus, before it was allegedly struck by Israeli warplanes in late January 2015 (photo credit: image capture from Google Earth)

Instead, according to Der Spiegel, it is in the process of erecting a new nuclear facility near the town of Qusayr, very close to Syria's border with Lebanon. The newspaper refers only to intelligence information from unnamed sources signifying that the facility is related to nuclear activities, without further assessment as to the nature of this facility, i.e., whether it is a nuclear reactor and/or a uranium enrichment facility. Both types of facilities can produce fissile materials – the materials from which nuclear weapons are produced. The article was received with much skepticism by the professional community, with some expressing their doubts as to the veracity of the information and others literally tearing the case apart, to the point of denouncing it as a hoax.

The satellite photography shown in the article does not present any indication as to the nature of the facility. It could well house a relatively small underground nuclear reactor that would be cooled by significant amounts of air that enter through a filtering system and exit through an exhaust stack (which is not visible in the photos) or concealed ventilation shafts. Were it to be cooled by water, it would need a significant water pipes system and a "heat sink" to remove the energy produced by the reactor. In the case of a reactor it would need the supplementary reprocessing and waste disposal facilities, in order to produce the plutonium needed for the production of nuclear weapons. Another option is that the facility houses a uranium enrichment facility, which does not produce energy and does not consume much energy, and thus does not need an extensive energy removal (cooling) system; alternatively, the necessary air-conditioning equipment and heat removal could be concealed from sight. It could also house auxiliary systems such as uranium conversion and storage facilities.

On a related point, the article notes that following the destruction of the Deir-al-Zor reactor, the equipment and materiel that survived the 2007 attack were removed from that site, and some of it could be used in the construction of the new facility. The Iranian Revolutionary Guards are also mentioned as involved in the Qusayr activities, as well as through the Iranian-led Hizbollah organization. But in any event, an analysis of the article confirms that the technical evidence is not sufficient to draw firm conclusions as to the nature of the activities at the Qusayr site. A review of any available past satellite photography and present-day heat photography could provide the necessary information, or at least some clues as to the nature of the site.

The article also highlights information about the continuation of Syrian-North Korean nuclear cooperation, although this comes from unnamed intelligence sources. The basis for concern regarding this bilateral relationship stems from the fact that the facility bombed in 2007 was a North Korean-style nuclear facility, and North Korean scientists were on the ground in Syria. It also raises again long-held concerns about the nature of probable trilateral cooperation in the WMD realm, among three states of concern: North Korea, Iran, and Syria. The Iranian link ties in both vis-à-vis North Korea and Syria. Bilateral cooperation between North Korea and Iran on ballistic missiles has been documented for years, and suspicions have been raised that it extends to the nuclear realm as well, with

experts noting, for example, the presence of Iranian scientists at North Korean nuclear tests. Suspicions of the trilateral link focus mainly on the facility at Deir-al-Zor and the question of funding. North Korea assists would-be proliferators but only those that can pay hard cash; Iran could likely be the source of funds, in light of the very strong strategic relationship between the two states.

While the above concerns contain an element of speculation, relations between Syria and the international nonproliferation regime are a matter of documented fact. Syria has lied outright with regard to its chemical capabilities: in a 2005 report to the UN, regarding Resolution 1540, Syria stated as a matter of fact that it has no, and never had WMD, and has no intention of developing them in the future. Yet seven years later, in 2012, Assad was already issuing chemical weapons threats, and over the course of 2013 actually used them on the Syrian population. Following its use of chemical weapons in the summer of 2013, Syria was compelled to admit its chemical weapons activities and to join the Chemical Weapons Convention; it then dismantled facilities and gave up at least some of its arsenal that was destroyed outside its territory.

Syria has also been uncooperative in the nuclear realm. Following the 2007 attack, it has stonewalled repeated requests from the IAEA to inspect the Deir-al-Zor site after the one and only inspection in June 2008. Similarly, the International Atomic Energy Agency (IAEA) is almost powerless to act in a legal way to ascertain the nature of the facility at Qusayr; its only option is to request a "special inspection" at that site. However, such a request will probably be refused by Syria, in the same manner as a North Korean refusal.

If anything is to be learned from the chemical weapons experience in Syria, it is that if enough pressure is applied, WMD-related issues can be dealt with effectively. It certainly will take tremendous political will and determination to do so, and in war-torn Syria it is not at all clear that this is an international priority, even after Assad employed chemical weapons. In the meantime, it is imperative that when information surfaces regarding possible WMD activities – even if highly speculative – the relevant intelligence organizations make a concerted effort to assess the situation, due to Syria's highly problematic WMD track record. In this case, the Der Spiegel article is cause to investigate further what is underway in Syria in the nuclear realm.

Tradition or Threat? The Diplomatic Pouch and the Potential for RN Smuggling

By Mila Ashley Johns

Source: http://www.cbrneportal.com/tradition-or-threat-the-diplomatic-pouch-and-the-potential-for-rn-smuggling/

In today's age of instant communication via secure cellphones, encrypted email, and face-to-face videoconferencing, the notion of using a physical satchel to relay confidential documents and materials between countries and their diplomatic personnel abroad may seem rather antiquated. Yet the centuries-old custom of the diplomatic pouch remains a hallmark of international relations due to its privileged, inviolable status under the Vienna Convention. This traditional practice, however, also potentially poses a thoroughly modern security threat – illicit transport of radiological and/or nuclear (RN) materials.

▶ **Read the full article at source's URL.**

__Mila Johns__ is a researcher and project manager at the Unconventional Weapons and Technology (UWT) Research Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), where she investigates and analyzes mass-casualty terrorism, transnational criminal organizations, and a variety of other open source research projects. Mila earned a B.A. in Government & Politics, with a concentration in Persian Studies, from the University of Maryland, College Park and a Masters of International Affairs, specializing in Comparative and Regional Studies of the Middle East, with a minor in Terrorism and Intelligence Studies, from American University. Her research interest includes terrorism and society; violent groups and movements; counter-terrorism; chemical and biological threats; and radiological and nuclear threats. Her career interests include research and policy relating to Iran, China, the Middle East, open source data, terrorism, intelligence, and social media.

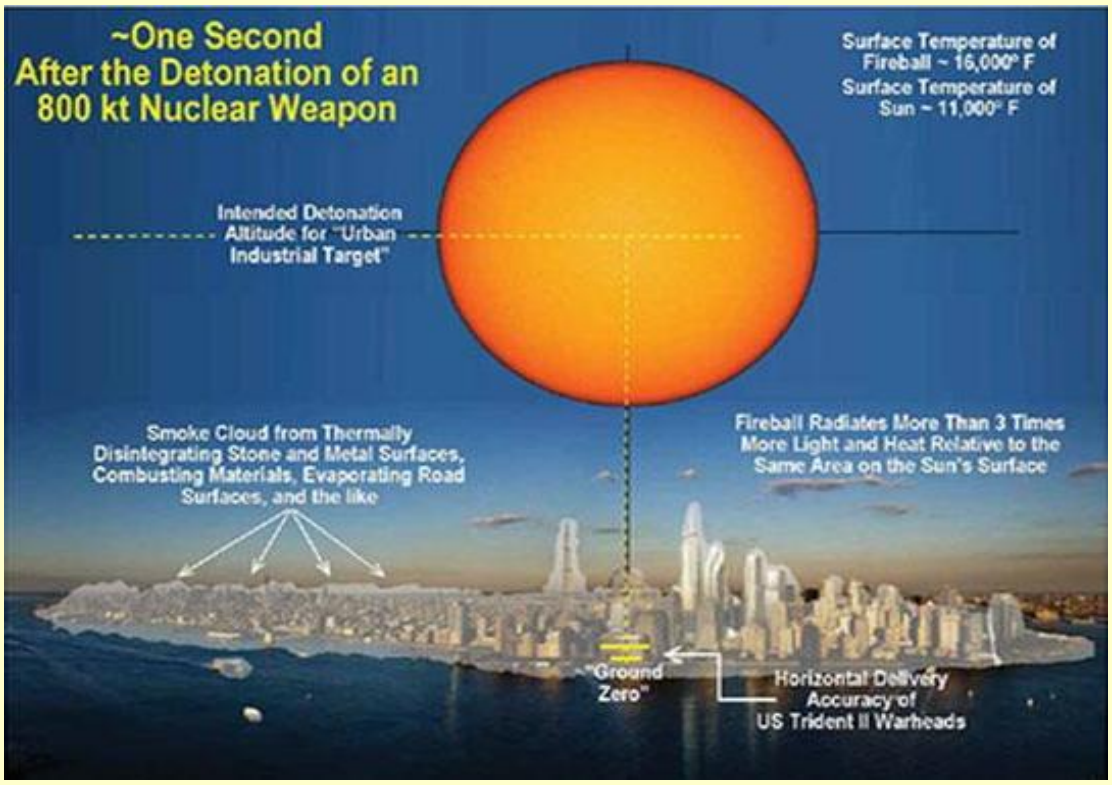
What would happen if an 800-kiloton nuclear warhead detonated above midtown Manhattan?

By Steven Starr, Lynn Eden and Theodore A. Postol

Source: http://thebulletin.org/what-would-happen-if-800-kiloton-nuclear-warhead-detonated-above-midtown-manhattan8023

Russian intercontinental ballistic missiles are believed to carry a total of approximately 1,000 strategic nuclear warheads that can hit the US less than 30 minutes after being launched. Of this total, about 700 warheads are rated at 800 kilotons; that is, each has the explosive power of 800,000 tons of TNT. **What follows is a description of the consequences of the detonation of a single such warhead over midtown Manhattan, in the heart of New York City.**

The initial fireball



The warhead would probably be detonated slightly more than a mile above the city, to maximize the damage created by its blast wave. Within a few tenths of millionths of a second after detonation, the center of the warhead would reach a temperature of roughly

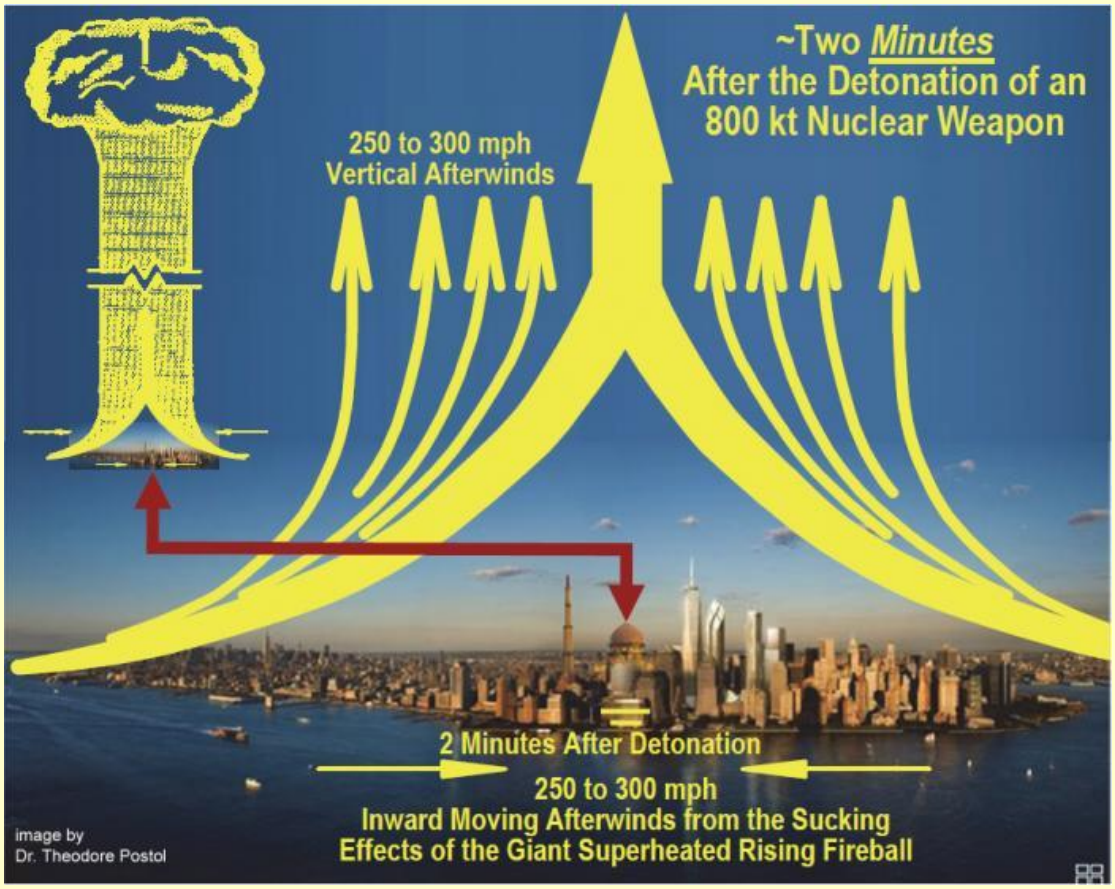
200 million degrees Fahrenheit (about 100 million degrees Celsius), or about four to five times the temperature at the center of the sun.
A ball of superheated air would form, initiallly expanding outward at millions of miles per hour. It would act like a fast-moving piston on the surrounding air, compressing it at the edge of the fireball and creating a shockwave of vast size and power.
After one second, the fireball would be roughly a mile in diameter. It would have cooled from its initial temperature of many millions of degrees to about 16,000 degrees Fahrenheit, roughly 4,000 degrees hotter than the surface of the sun.
On a clear day with average weather conditions, the enormous heat and light from the fireball would almost instantly ignite fires over a total area of about 100 square miles.

Hurricane of fire

Within seconds after the detonation, fires set within a few miles of the fireball would burn violently. These fires would force gigantic masses of heated air to rise, drawing cooler air from surrounding areas toward the center of the fire zone from all directions.
As the massive winds drove flames into areas where fires had not yet fully developed,the fires set by the detonation would begin to merge. Within tens of minutes of the detonation, fires from near and far would joinhave formed a single, gigantic fire. The energy released by this mass fire would be 15 to 50 times greater than the energy produced by the nuclear detonation.
The mass fire, or firestorm, would quickly increase in intensity, heating enormous volumes of air that would rise at speeds approaching 300 miles per hour. This chimney effect would pull cool air from outside the fire zone towards the center of the fire at speeds of hundreds of miles per hour. These superheated ground winds of more than hurricane force would further intensify the fire. At the edge of the fire zone, the winds would be powerful enough to uproot trees three feet in diameter and suck people from outside the fire into it.
The inrushing winds would drive the flames from burning buildings horizontally along the ground, filling city streets with flames and firebrands, breaking in doors and windows, and causing the fire to jump, sometimes hundreds of feet, swallowing anything not already violently combusting.

These above-hurricane-force ground winds would have average air temperatures well above the boiling point of water. The targeted area would be transformed into a huge hurricane of fire, producing a lethal environment throughout the entire fire zone.

Ground zero: Midtown Manhattan



The fireball would vaporize the structures directly below it and produce an immense blast wave and high-speed winds, crushing even heavily built concrete structures within a couple miles of ground zero. The blast would tear apart high-rise buildings and expose their contents to the solar temperatures; it would spread fires by exposing ignitable surfaces, releasing flammable materials, and dispersing burning materials.

At the Empire State Building, Grand Central Station, the Chrysler Building, and St. Patrick's Cathedral, about one half to three quarters of a mile from ground zero, light from the fireball would melt asphalt in the streets, burn paint off walls, and melt metal surfaces within a half second of the detonation. Roughly one second later, the blast wave and 750-mile-per-hour winds would arrive, flattening buildings and tossing burning cars into the air like leaves in a windstorm. Throughout Midtown, the interiors of vehicles and buildings in line of sight of the fireball would explode into flames.

Slightly more than a mile from ground zero are the neighborhoods of Chelsea, Midtown East, and Lenox Hill, as well as the United Nations; at this distance, for a split second the fireball would shine 10,000 times brighter than a desert sun at noon. All combustible materials illuminated by the fireball would spew fire and black smoke.

Grass, vegetation, and leaves on trees would explode into flames; the surface of the ground would explode into superheated dust. Any flammable material inside buildings (paper, curtains, upholstery) that was directly exposed to the fireball would burst into flame. The surfaces of the bronze statues in front of the UN would melt; marble surfaces exposed to the fireball would crack, pop, and possibly evaporate.

At this distance from the fireball, it would take about four seconds for the blast wave to arrive. As it passed over, the blast wave would engulf all structures and crush them; it

would generate ferocious winds of 400 to 500 miles per hour that would persist for a few seconds
The high winds would tear structural elements from buildings and cause them to disintegrate explosively into smaller pieces. Some of these pieces would become destructive projectiles, causing further damage. The superheated, dust-laden winds would be strong enough to overturn trucks and buses. Two miles from ground zero, the Metropolitan Museum of Art, with all its magnificent historical treasures, would be obliterated. Two and half miles from ground zero, in Lower Manhattan, the East Village, and Stuyvesant Town, the fireball would appear 2,700 times brighter than a desert sun at noon. There, thermal radiation would melt and warp aluminum surfaces, ignite the tires of autos, and turn exposed skin to charcoal, before the blast wave arrived and ripped apart the buildings.

Three to nine miles from ground zero

Midtown is bordered by the relatively wide Hudson and East rivers, and fires would start simultaneously in large areas on both sides of these waterways (that is, in Queens and Brooklyn as well as Jersey City and West New York). Although the direction of the fiery winds in regions near the river would be modified by the water, the overall wind pattern from these huge neighboring fire zones would be similar to that of a single mass fire, with its center at Midtown, Manhattan.
Three miles from ground zero, in Union City, New Jersey, and Astoria, Queens, the fireball would be as bright as 1,900 suns and deliver more than five times the thermal energy deposited at the perimeter of the mass fire at Hiroshima. In Greenpoint, Brooklyn, and in the Civic Center of Lower Manhattan, clothes worn by people in the direct line of sight of the fireball would burst into flames or melt, and uncovered skin would be charred, causing third-degree and fourth-degree burns.
It would take 12 to 14 seconds for the blast wave to travel three miles after the fireball's initial flash of light. At this distance, the blast wave would last for about three seconds and be accompanied by winds of 200 to 300 miles per hour. Residential structures would be destroyed; high-rises would be at least heavily damaged.
Fires would rage everywhere within five miles of ground zero. At a distance of 5.35 miles from the detonation, the light flash from the fireball would deliver twice the thermal energy experienced at the edge of the mass fire at Hiroshima. In Jersey City and Cliffside Park, and in Woodside in Queens, on Governors Island and in Harlem, the light and heat to surfaces would approximate that created by 600 desert suns at noon.
Wind speed at this distance would be 70 to 100 miles per hour. Buildings of heavy construction would suffer little structural damage, but all exterior windows would be shattered, and non-supporting interior walls and doors would be severely damaged or blown down. Black smoke would effuse from wood houses as paint burned off surfaces and furnishings ignited.
Six to seven miles from ground zero, from Moonachie, New Jersey, to Crown Heights, Brooklyn, from Yankee Stadium to Corona, Queens and Crown Heights, Brooklyn, the fireball would appear 300 times brighter than the desert sun at noon. Anyone in the direct light of the fireball would suffer third degree burns to their exposed skin. The firestorm could engulf neighborhoods as far as seven miles away from ground zero, since these outlying areas would receive the same amount of heat as did the areas at the edge of the mass fire at Hiroshima.
Nine miles from ground zero, in Hackensack, Bayonne, and Englewood, New Jersey, as well as in Richmond Hill, Queens, and Flatlands, Brooklyn, the fireball would be about 100 times brighter than the sun, bright enough to cause first- and second-degree burns to those in line of sight. About 36 seconds after the fireball, the shockwave would arrive and knock out all the windows, along with many interior building walls and some doors.

No survivors

Within tens of minutes, everything within approximately five to seven miles of Midtown Manhattan would be engulfed by a gigantic firestorm. The fire zone would cover a total area of 90 to 152 square miles (230 to 389 square kilometers). The firestorm would rage for three to six hours. Air temperatures in the fire zone would likely average 400 to 500 degrees Fahrenheit (200 to 260 Celsius).
After the fire burned out, the street pavement would be so hot that even tracked vehicles could not pass over it for days. Buried, unburned material from collapsed buildings throughout the fire zone could burst into flames when exposed to air—months after the firestorm had ended.

Those who tried to escape through the streets would have been incinerated by the hurricane-force winds filled with firebrands and flames. Even those able to find shelter in the lower-level sub-basements of massive buildings would likely suffocate from fire-generated gases or be cooked alive as their shelters heated to oven-like conditions.

The fire would extinguish all life and destroy almost everything else.Tens of miles downwind of the area of immediate destruction, radioactive fallout would begin to arrive within a few hours of the detonation. But that is another story.

Lynn Eden *is a member of the* Bulletin's *Science and Security Board and a senior research scholar and associate director for research at Stanford University's Center for International Security and Cooperation. Eden is also co-chair of U.S. Pugwash and a member of the International Pugwash Council. Her scholarly work focuses on the military and society, and nuclear weapons history and policy, including nuclear abolition. Eden's* Whole World on Fire: Organizations, Knowledge, and Nuclear Weapons Devastation *won the American Sociological Association's 2004 Robert K. Merton award for best book in science and technology studies.*

A physicist, ***Theodore A. Postol*** *is professor of science, technology, and national security policy at MIT. His expertise is in ballistic missile defense technologies and ballistic missiles more generally. Prior to coming to MIT, he worked as an analyst at the Office of Technology Assessment and as a science and policy adviser to the chief of naval operations. In 2001, he received the Norbert Wiener Prize from Computer Professionals for Social Responsibility for uncovering numerous false claims about missile defenses.*

Steven Starr is the director of the University of Missouri's Clinical Laboratory Science Program, as well as a senior scientist at the Physicians for Social Responsibility. He has worked with the Swiss, Chilean, and Swedish governments in support of their efforts at the United Nations to eliminate thousands of high-alert, launch-ready U.S. and Russian nuclear weapons; he maintains the website Nuclear Darkness.

Bolstering Nuclear Forensics to Prevent Nuclear Terrorism

The Fifth Anniversary of the Nuclear Forensics and Attribution Act

By Huban Gowadia

Source: http://www.dhs.gov/blog/2015/02/24/bolstering-nuclear-forensics-prevent-nuclear-terrorism

Feb 24 – Five years ago, President Obama signed into law an important piece of homeland security legislation designed to help protect our Nation against the threat of nuclear terrorism. The Nuclear Forensics and Attribution Act (NFAA) assigned to the Department of Homeland Security key nuclear forensics responsibilities and authorized the National Technical Nuclear Forensics Center within DHS's Domestic Nuclear Detection Office (DNDO).

The law states, "The threat of a nuclear terrorist attack on American interests…is one of the most serious threats to… national security." Confronted with this possibility, U. S. policy is to hold fully accountable any state, terrorist group, or other non-state actor that supports or enables terrorist efforts to obtain or use nuclear weapons.

In the face of potential nuclear threats, we need to have the capability to determine who is responsible for such acts. Nuclear forensics enables us to trace nuclear materials and devices back to their place of origin. In smuggling cases, nuclear forensics can aid in the prosecution of perpetrators, help close down smuggling networks, and identify potential nuclear security deficiencies that need to be addressed. In the case of attempted or actual acts of nuclear terrorism, scientific evidence supports the determination of those responsible which would guide U.S. actions in response.

Since the enactment of NFAA, DHS has worked with the FBI, the Departments of Defense, Energy, and State, and the Office of the Director of National Intelligence to advance the national capabilities. DNDO supports multiagency forensics exercises that include state and local partners and we also participate in exercises with the intelligence community to plan and synchronize intelligence, law enforcement, and technical forensics information into a robust attribution process.

The NFAA also highlights the importance of increased international collaboration in nuclear forensics to ensure the United States and its partners are prepared for a nuclear event overseas. Since the Nuclear Security Summit in 2010, where nuclear forensics and detection were highlighted as ongoing priorities, we have seen international collaborations expanded and enhanced.

DNDO continues to work to advance technical capabilities to perform nuclear forensics on smuggled materials as well. DNDO has led the development of technology that can replicate how foreign nations produce nuclear materials. This allows us to predict the forensic signatures without having samples of those materials and is a significant advancement in our ability to trace nuclear materials back to their origin.

Finally, DNDO is ensuring we have the scientific talent required for nuclear forensics. The NFAA-mandated National Nuclear Forensics Expertise Development Program is designed to cultivate and sustain the expertise required to execute our mission and has significantly revitalized the pipeline, through its support to students and academic institutions, which have become increasingly involved with the nuclear forensics field over the last five years.

The NFAA has been instrumental for DNDO, where we remain singularly focused on preventing nuclear terrorism. Along with our partners, we remain vigilant in our efforts to protect the Nation against this threat.

Directorates

- Architecture and Plans Directorate — Determines gaps and vulnerabilities in the existing global nuclear detection architecture, then formulates recommendations and plans to develop an enhanced architecture.
- Product Acquisition & Deployment Directorate — Carries out the engineering development, production, developmental logistics, procurement and deployment of current and next-generation nuclear detection systems.
- Transformational & Applied Research Directorate — Conducts, supports, coordinates, and encourages an aggressive, long-term research and development program to address significant architectural and technical challenges unresolved by R&D efforts on the near horizon.
- Operations Support Directorate — Develops the information sharing and analytical tools necessary to create a fully integrated operating environment. Residing in the Operations Support Directorate is the Joint Analysis Center, which is an interagency coordination and reporting mechanism and central monitoring point for the GNDA.
- Systems Engineering & Evaluation Directorate — Ensures that DNDO proposes sound technical solutions and thoroughly understands systems performance and potential vulnerabilities prior to deploying those technologies.
- **Red Team & Net Assessments** — Independently assesses the operational performance of planned and deployed capabilities, including technologies, procedures, and protocols.
- National Technical Nuclear Forensics Center — Provides national-level stewardship, centralized planning and integration for an enduring national technical nuclear forensics capability.

*On September 20th, 2013, President Obama appointed **Dr. Huban A. Gowadia** as the Director of the U.S. Department of Homeland Security's Domestic Nuclear Detection Office (DNDO). Under her leadership, DNDO develops nuclear detection capabilities, measures detector system performance, ensures effective response to detection alarms, conducts transformational research and development, and coordinates the improvement of technical nuclear forensics capabilities across the U.S. Government. Prior to this role, Dr. Gowadia served at DNDO as the Acting Director from 2012 to 2013, Deputy Director from 2010 to 2012, Assistant Director of the Mission Management Directorate from 2007 to 2010, and Assistant Director for Assessments from 2005 to 2007. Before joining DNDO, Dr. Gowadia led DHS's Science & Technology Countermeasures Test Beds as Program Executive from 2003 to 2005. Dr. Gowadia also worked as Checkpoint Program Manager in the Office of Security Technologies in the Transportation Security Administration (TSA) from 2001 to 2003. She previously served with the Federal Aviation Administration at the Aviation Security Laboratory from 2000 to 2001. Dr. Gowadia received a Bachelor of Science degree in Aerospace Engineering from the University of Alabama and a Ph.D. in Mechanical Engineering from the Pennsylvania State University.*

Nuclear forensics to the aid of nuclear detectives

Source: http://www.homelandsecuritynewswire.com/dr20150304-nuclear-forensics-to-the-aid-of-nuclear-detectives

March 04 – **Fans of the popular TV series "CSI" know that the forensics experts who investigate crime scenes are looking for answers to three key questions: "Who did it; how did they do it; and can we stop them from doing it again?"**

The field of nuclear forensics, an important element of Lawrence Livermore National Laboratory's (LLNL) national security mission, has similar goals and uses similar techniques — but with even higher stakes.

"In nuclear forensics, we want to know first, is someone able to put together the parts to make a nuclear weapon and set it off?" said LLNL nuclear chemist Dawn Shaughnessy, who leads the experimental and nuclear radiochemistry group in the

Physical and Life Sciences Directorate. **"And second, if one is set off, can we find out who did it, how they did it and are they going to do it again?**

"Like traditional forensics, we're looking for nuclear signatures, just like fingerprints; we're looking for the technological and material clues and evidence to tell us what somebody had done to make this unfortunate thing happen."

If a nuclear explosive was detonated on U.S. soil, nuclear forensics specialists would be dispatched to examine the rubble from the explosion for traces of fissile material, fission products and activation products — nearby debris or structural components of the bomb made radioactive by neutron activation. The more information the experts could glean by characterizing these materials, the better able they would be to determine the weapon's design and origin.

An LLNL release reports that the National Ignition Facility (NIF) is playing a growing role in LLNL's nuclear forensics work by providing radioactive samples from nuclear fusion experiments for analysis. "We're looking for information about the nuclear decay of certain elements - and not just the actinides," Shaughnessy said. "We also need to know about the materials used to build a device by looking for isotopes and nuclear decay signatures to piece together what was physically there when an event occurred.

"For some isotopes that would be very useful signatures for us; we don't have any data on their nuclear reaction pathways," she said. "For example, if a nuclear device was set off in a garage, the garage would have steel in it that would become radioactive, and that might help us figure out something related to the resultant neutron spectrum.

"NIF is a place where we can make these nuclear reaction measurements, and it may be the only place where some kinds of measurements are possible," she said. "The data we get at NIF — the reaction products from a NIF experiment — would be fed back to help us understand the origin of the nuclear weapon."

When the hydrogen isotopes deuterium and tritium are fused in a NIF experiment, neutrons of different energies, gamma rays and a variety of other radioactive byproducts are created, along with irradiated debris from the tiny NIF targets. Those samples can be captured and analyzed in LLNL's unique Nuclear Counting Facility in Bldg. 151, yielding high-quality data to help determine the characteristics of the fusion experiment and also providing forensics specialists with materials similar to those they would encounter in an investigation of a nuclear explosion.

In the NIF experiments, thin foils containing materials of interest are placed on the outside of the target and the foils are activated by neutrons with similar energy as in a weapon explosion. "This gives us part of the puzzle," Shaughnessy said, "because the neutrons are at higher energy than in an accelerator." By using both accelerators, such as those in LLNL's Center for Accelerator Mass Spectrometry (CAMS), and NIF, "we can get a complete reaction pathway for the whole neutron spectrum. NIF really is a very complementary facility to accelerators to cover the entire neutron spectrum."

The NIF team uses two primary diagnostics to collect reaction products of interest: the radiochemical analysis of gaseous samples (RAGS) system and the solid radiochemical collection (SRC) diagnostic. Mounted on the nose cone of a diagnostic instrument manipulator, the SRC collection plates sit fifty centimeters from the target. The plates collect the debris coming off the target that contains the reaction products.

"After the samples are collected, they're brought to the Nuclear Counting Facility where we do both chemical processing and radiation counting," Shaughnessy said. "The results are analyzed and we try to determine the cross-section for the reaction — how often that reaction will proceed in a neutron environment.

"The nuclear forensics modeling community would like to have better nuclear reaction data for various materials," she said. "For example, they would like data on how structural components, such as the iron in that garage, interact with neutrons. The NIF experiments are focusing on materials for which they have the least amount of data. We need to understand, if there were activated iron components after the event, was that from the building or from the device itself?"

The release notes that the first NIF nuclear forensics shot was conducted at the end of 2014. The second shot is scheduled for the end of this month and a third at the end of the current fiscal year. The SRC is currently being upgraded to

enhance its collection efficiency; the new diagnostic, called vast area detector for experimental radiochemistry (VADER), will be deployed for this month's shot.

Shaughnessy said NIF could play a role in enhancing the training of nuclear forensics investigators by providing realistic, real-world debris samples for readiness exercises in analyzing and interpreting post-event data. Research teams at Los Alamos, Pacific Northwest and Lawrence Livermore national laboratories regularly engage in isotope identification exercises using samples of synthetic nuclear debris to test participants' skills at isotope identification. Currently, samples are prepared by irradiating a single fuel in a reactor and collecting the fuel and its fission products.

"This process is not very realistic," Shaughnessy said. "The data is fragmented and there's no real interaction among the parts of the process." A truly realistic sample would include all the pieces of the puzzle — fuels along with reaction and activation products embedded in a matrix of dirt and debris.

"Based on the shots and data so far," Shaughnessy said, "it seems feasible to use NIF experiments as a test exercise for how we can interpret data in a post-event situation. We could use the NIF shot as a stand-in for an actual nuclear event. We could create a debris sample with a mix of nuclides and a mix of neutron fluxes, and hand it to the forensics team and ask them what the shot looked like. It would be the same forensics problem we're trying to solve for the nation.

"This would require the same integrated laboratory processing, data analysis and modeling we're trying to do in forensics on a larger scale," she said. "LLNL has a program to come up with more realistic exercises, and this would be a much better test of the whole integrated system."

By engaging in readiness exercises and sample development, Lawrence Livermore researchers are helping to establish an important national capability and fostering stronger partnerships with forensics specialists at other laboratories and with sponsors in the departments of Defense and Energy. The expertise developed by Shaughnessy's group is broadening the scope of nuclear forensics research at the national level.

Substance used to poison Litvinenko could only have come from Russia – inquiry

Source: http://www.theguardian.com/world/2015/mar/11/substance-used-to-poison-litvinenko-could-only-have-come-from-russia-inquiry

March 11 – **The rare radioactive substance used to poison Alexander Litvinenko in London could only have come from inside Russia, a world-leading expert has told the inquiry into the former spy's murder.**

Norman Dombey, emeritus professor of nuclear physics at the University of Sussex, said the polonium was produced at a closed nuclear facility in the city of Sarov, 450 miles south-east of Moscow. Its Soviet-era Avangard plant was the only place in the world with a polonium "production line", he said.

"In my opinion the Russian state or its agents was responsible for the poisoning," Dombey said.

Litvinenko died after drinking a cup of tea laced with radioactive polonium-210, during a meeting in November 2006 at a Mayfair hotel. Two Russians – Andrei Lugovoi and Dmitry Kovtun – have been charged with his murder. The Kremlin has insisted that the polonium involved did not come from Russia.

Dombey said the quantity used to kill Litvinenko – he swallowed an astonishing 26.5

micrammes – was exceptionally large. All other countries including the US and UK stopped making polonium in the 1970s. Avangard was the last remaining source of commercial polonium, with no other nuclear facility capable of making sufficient quantities.
The scientist said that different steps were involved. First, he said, the Mayak nuclear reactor in the Urals irradiated bismuth. The bismuth was then transported to Avangard and converted into polonium. Next, a "state institution" would have converted it from "metallic" to "soluble" form. Finally, Lugovoi and Kovtun smuggled it to London, he suggested.
Doctors only identified polonium as the poison hours before Litvinenko died. Unlike other radioactive substances, it emits alpha rather than gamma particles. "This poisoning was not meant to be discovered," Dombey concluded. "It was meant to be a mysterious poisoning because polonium is an alpha-emitter which a Geiger counter doesn't pick up."
He also said that the Russians involved in the murder plot would have tested the poison in advance. Too small a dose would have been ineffective; too big would have been a massive risk to public health. Citing sources in Russia, Dombey said Russian agents had previously tested polonium on a Chechen, Lecha Islamov, who was serving a nine-year sentence in jail.

Metropolitan police's 3D graphic showing polonium contamination in the teapot. From green (low) to purple (high).

Prison bosses summoned him for a chat. They offered him a snack and a cup of tea. Within five minutes of drinking the tea, Islamov fell violently ill, Dombey said. He died shortly afterwards from a mysterious illness, with symptoms similar to Litvinenko's: hair loss, a catastrophic decline in white blood cells, and multiple major organ failure.
Dombey said that given polonium's short half life – it decays after 138 days – the poison would probably have been produced a "couple of months" before Litvinenko's poisoning.
The inquiry continues.

Van transporting radioactive material crashes in Bosnia

Source: http://rt.com/news/240425-bosnia-herzegovina-nuclear-crash/

March 13 – **A van carrying radioactive isotope Iridium-192 has crashed in north Bosnia, local media reported. The vehicle ran off the road after colliding with a car.**
The police blocked the area around the crash site. Bosnia's nuclear safety agency reported that no radiation leak had been detected.
The van was transporting *"apparatus with radioactive material"* from the Vinca Institute of Nuclear Sciences,

the Banja Luka-based Nezavisne Novine newspaper reported.

After the collision, the van overturned. The

radioactiv e material, however, which is in a solid state and poses no risk of large-scale contamination, remained contained, the authorities said.

The cargo belongs to a company from the city of Prijedor licensed to work with radioactive material, said Emir Dizdarevic, director of the Bosnian nuclear regulator.

The driver of the car was killed in the crash, while the van driver and a passenger traveling with him survived.

Iridium-192 is a radioactive isotope with a half-life of 73.83 days. It is also a strong **gamma** ray emitter and is commonly used as a gamma ray source in radiography and radiotherapy as a radiation source.

According to the UN, Iridium-192 is the isotope that most frequently goes missing when radioactive materials are used to make a dirty bomb.

EDITOR'S COMMENT: The last sentence of the article is kind of srange! **Since when** we had dirty bombs manufactured and we are unaware of???

Autonomous Undersea Surveillance and Intervention

Source: http://www.cmre.nato.int/research/mine-countermeasures

NATO OTAN
SCIENCE & TECHNOLOGY ORGANIZATION
CENTRE FOR MARITIME RESEARCH & EXPERIMENTATION
S&T organization

Mine countermeasures involve finding the mine, classifying it, and destroying it so that it is no longer a threat. Currently, AUVs are being used to survey the seabed to detect mines; however, classifying the mines and destroying them still rely to a great extent on expert divers, who are placed in harm's way, and to ROVs, which are expensive if treated as an expendable device. AUVs have the potential to offer a safer, faster, and lower-cost solution for mine classification and disposal.

The Centre is working to transform the way mine countermeasures are conducted from a post-Cold War approach that focuses on post-operations clearance using surface ships to a quickly deployable, autonomous system that is scalable, cost effective, and minimizes risk to personnel. Recently, work at the Centre has focused on using AUVs for mine hunting, including developing techniques for handling the large data rates associated with modern high-resolution sonar and developing AUV systems that can make adjustments to pre-planned routes based on data that is gathered *in situ*. Now, the Centre's emphasis is expanding from using AUVs in mine hunting to using AUVs in mine identification and mine disposal.

Mine identification

Classifying mines once they are found has historically been a time-consuming, resource-intensive process. The goal of CMRE's research is to determine the feasibility of using high-resolution sonar mounted on AUVs for mine "super classification." Super classification simply means that an object is quickly classified with sufficient confidence to proceed to disposal. The task involves getting multiple images, or views, of the mine, fusing those images into a single image that can then be classified with high confidence using automated techniques.

Mine disposal

The emphasis in this area is on finding an autonomous and cost-effective solution. Currently, mine detonation weapons (MDWs) are typically guided to the mine by an ROV, which is often treated as being expendable despite its high cost. Self-guided MDWs exist, but they are even more costly. Emphasis is being placed on a stripped down, inexpensive MDW design that minimizes the number of sensors and processors on board while relying as much as possible on external support for guidance and control. A variety of options are being explored for transporting the MDW including AUVs, autonomous surface vehicles (ASVs), and airborne platforms (naval helicopters or unmanned air vehicles).

Medical aspects of terrorist bombings – a focus on DCS and DCR

Ventsislav M Mutafchiyski[1], **Georgi I Popivanov**[2] and **Kirien C Kjossev**[3]
[1] Endocrine Surgery and Coloproctology, Military Medical Academy, Sofia, Bulgaria
[2] Clinic of Abdominal Surgery, Military Medical Detachment of Emergency Response, Military Medical Academy, 3 "Georgi Sofiiski" Str., Sofia, Bulgaria
[3] Clinic of Abdominal Surgery, Military Medical Academy, Sofia, Bulgaria

MMR MILITARY MEDICAL RESEARCH

Military Medical Research 2014, **1**:13 doi:10.1186/2054-9369-1-13

Abstract
Although terrorist bombings have tormented the world for a long time, currently they have reached unprecedented levels and become a continuous threat without borders, race or age. Almost all of them are caused by improvised explosive devices. The unpredictability of the terrorist bombings, leading to simultaneous generation of a large number of casualties and severe "multidimensional" blast trauma require a constant vigilance and preparedness of every hospital worldwide. Approximately 1-2.6% of all trauma patients and 7% of the combat casualties require a massive blood transfusion. Coagulopathy is presented in 65% of them with mortality exceeding 50%. Damage control resuscitation is a novel approach, developed in the military practice for treatment of this subgroup of trauma patients. The comparison with the conventional approach revealed mortality reduction with 40-74%, lower frequency of abdominal compartment syndrome (8% vs. 16%), sepsis (9% vs. 20%), multiorgan failure (16% vs. 37%) and a significant reduction of resuscitation volumes, both crystalloids and blood products. **DCS (Damage control surgery) and DCR (damage control resuscitation)** are promising new approaches, contributing for the mortality reduction among the most severely wounded patients. Despite the lack of consensus about the optimal ratio of the blood products and the possible influence of the survival bias, we think that DCR carries survival benefit and recommend it in trauma patients with exsanguinating bleeding.

▶ **The electronic version of this article can be found online at:**
http://www.mmrjournal.org/content/1/1/13

Britain's nuclear weapons base suffers from 'serious' nuclear safety incidents and 'poor safety culture'

Source: http://www.independent.co.uk/news/uk/politics/britains-nuclear-weapons-base-suffers-from-serious-nuclear-safety-incidents-and-poor-safety-culture-10080857.html

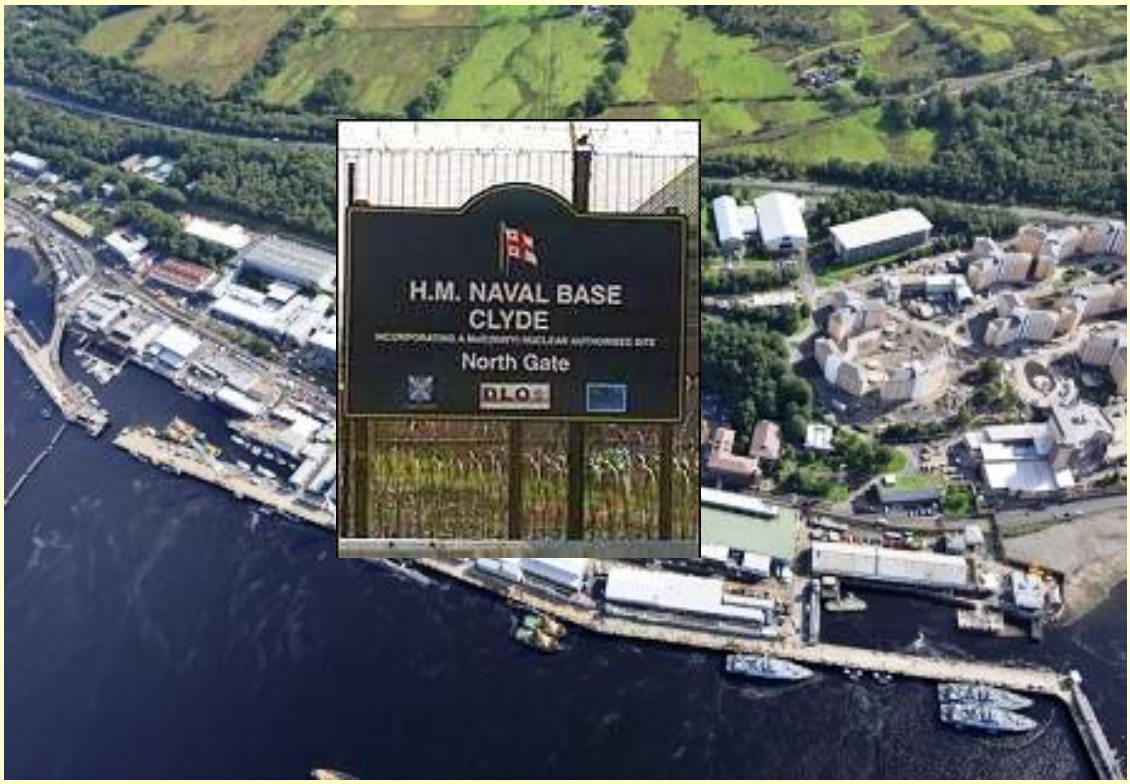
Britain's nuclear weapons base has suffered from a dozen serious nuclear safety failures in recent years, according to official records.

Over the last six years **HM Naval Base Clyde**, where Britain's Trident nuclear submarine fleet is based, suffered from nearly 400 "widespread" nuclear safety events relating to a "poor safety culture".

In 12 of these cases the problems involved an "actual or high" risk of unplanned exposure to radiation or contained release of radiation

within a building or submarine, according to information released by ministers in the last week.

Last year the number of nuclear safety events involving nuclear propulsion nearly doubled,



from **57 in 2013 to 99 in 2014.**

In one incident in 2012, contractors working on the base were exposed to radiation while repairing submarine equipment.

The 12 most serious events at the base, classified by the Ministry of Defence as "Category B", are ones in which there is an "actual or high potential for a contained release [of radiation] within building or submarine or unplanned exposure to radiation".

According to the Ministry's own criteria, this classification is used for safety events that involve a "major failure in administrative controls or regulatory compliance".

Other serious nuclear safety events included the unsafe operation of a crane on a jetty handling explosives, faulty radiation testing, and low-level radioactive contamination around a pipe that dumps supposedly decontaminated waste into the sea.

Despite the problems, the base has not recently suffered from any of the most serious category of safety failures – 'Category A' – which would have involved release into the environment in the surrounding area.

The information was disclosed by ministers after a parliamentary question by SNP MP Angus Robertson – who leads the party's parliamentary group in Westminster.

He said the base's safety record was "totally unacceptable" and that safety had to be paramount when nuclear reactors were concerned.

"It's important to note this doubling has occurred before expansion work at the base for more nuclear submarines is complete. Wherever nuclear weapons or reactors are concerned – safety must be paramount. We need to know exactly what is being done to address these breaches and tighten procedures," he said.

"These figures indicate how widespread nuclear safety breaches are. We must have an absolute assurance from the MoD that safety concerns are given then highest priority.

Mr Robertson hit out at the Government's plan to renew the Trident weapons system, describing its nuclear bombs as "obscene weapons of mass destruction".

A Ministry of Defence spokesperson told the *Independent*: "We can be clear that none of the events in the reports posed any risk to the

health of our personnel, or to any members of the public.
"Our rigorous reporting system shows how seriously Defence takes all aspects of nuclear safety and where necessary, measures are put in place to prevent a recurrence."

Protecting crops from radiation-contaminated soil

Source: http://www.homelandsecuritynewswire.com/dr20150316-protecting-crops-from-radiationcontaminated-soil

March 16 – **Almost four years after the accident at the Fukushima Daiichi Nuclear Power Plant in Japan, farmland remains contaminated with higher-than-natural levels of radiocesium in some regions of Japan, with cesium-134 and cesium-137** being the most troublesome because of the slow rate at which they decay. In a study published in *Scientific Reports*, a group at the RIKEN Center for Sustainable Resource Science in Japan led by Ryoung Shin has identified a chemical compound that prevents plants from taking up cesium, thus protecting them — and us — from its harmful effects.

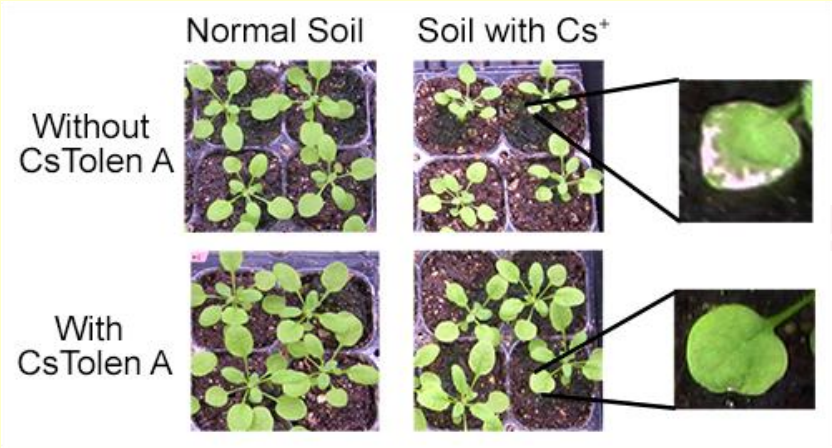
Although cesium has no beneficial function in plants, it is readily absorbed by plants in contaminated soil due to its water solubility and its similarity to potassium, a critical plant nutrient. After being absorbed, it continues to compete with potassium inside plant cells, disrupting physiological processes and causing major retardation in plant growth.

Because of this, the research team focused their efforts on finding a way to prevent cesium uptake.

Riken notes that, first, **they used seedlings from the model plant Arabidopsis thaliana and tested 10,000 synthetic compounds to determine if any could reverse the harmful effects of cesium.** The effects of each compound were quantified with a scoring scale, and after several screenings, they had **found five compounds that made plants highly tolerant to cesium**.

Next they looked at how these five compounds — termed **CsTolen A-E** — produced their effects. They found that when Arabidopsis was grown in cesium-containing liquid media with CsTolen A, more cesium remained in the liquid medium and much less was found in the plants.

Importantly, the concentration of CsTolen A needed for this effect did not prevent the plants from absorbing the potassium that they need to grow. Further tests showed that rather than helping cells to expel cesium after it has been initially absorbed, CsTolen A acted to prevent cesium from entering the roots.



Quantum mechanical modeling indicated that although CsTolen A likely binds to other alkali metal ions, such as potassium and sodium, it should preferentially bind to cesium in aqueous solutions. This was confirmed by testing in which CsTolen A did not reverse sodium-induced or potassium deficiency-induced growth retardation, indicating that its effects appear to be specific to cesium.

Most importantly, when plants were germinated and grown in cesium-contaminated soil, applying CsTolen A significantly reduced the amount of cesium absorption and resulted in greater plant growth.

As Japan prepares to mark the fourth year since the events of March 2011, lead author Eri Adams notes that, "we think our findings shed some light on the possibility of using

chemicals to prevent agricultural products from being contaminated." This technique is called phytostabilization, and Adams adds that, "unlike other methods such as genetic modification, use of chemicals is a powerful tool that can alter plant responses to the environment regardless of their species, which is especially true in the case of CsTolen A because it binds to cesium before it can enter the plants."

Riken says that Shin's research unit is devoted to finding solutions to several environmental and agricultural problems through studying the mechanisms of nutrient uptake. Not only will the current findings help plants, but by reducing the amount of radiocesium that enters them, it should also ensure the safety of agricultural products grown in contaminated soil. As decontaminating large areas of farmland is a difficult venture at best, CsTolen A could be a game saver for regions affected by radiocesium contamination.

— Read more in Eri Adams et al., "Selective chemical binding enhances cesium tolerance in plants through inhibition of cesium uptake," Scientific Reports *5, Article number: 884.*

Britain's nuclear reactors vulnerable to terrorist drone attacks

Source: http://i-hls.com/2015/03/britains-nuclear-reactors-vulnerable-to-terrorist-drone-attacks/?utm_source=Israel+Homeland+Security+%28iHLS%29&utm_campaign=d9ae3d46e8-Newsletter_English_18_3_2015&utm_medium=email&utm_term=0_8ee2e16ed1-d9ae3d46e8-87373033&mc_cid=d9ae3d46e8&mc_eid=521c0e089a

March 16 – **This danger is imminent. Britain's aging nuclear power plants are vulnerable to terrorist attacks by unmanned drones that could kill thousands of people**. This according to a warning by John Large, an engineer for Britain's Atomic Energy Authority. **He also says ministers are ignoring risks posed by nuclear terror assaults.**

Large is calling for urgent security reforms. He is also demanding the government set up a major operation to test the resilience of Britain's power plants against prospective attacks. This is in all the more relevant given the fact that nuclear power stations around the UK suffered 37 security breaches in 2014 – the highest number since 2011.

Too much energy is focused on risk assessments relating to accidents at nuclear power plants than potential terror attacks, the engineer argues. In a bid to sketch out contingency responses, Large analyzed a series of hypothetical attack scenarios. Each one's scale of devastation varied, with casualties ranging from one to tens of thousands.

According to *RT*, the engineer concluded unmanned aerial vehicle (UAV) access to nuclear plants in the UK "is relatively unimpeded." **He said drones pose a real risk to Britain's 16 nuclear reactors**.

Conservative MP Mark Pritchard, a member of Britain's Joint Committee on the National Security Strategy, said Large's policy suggestions would be considered seriously by the government. A spokeswoman for the Department for Energy and Climate Change (DECC) said security at Britain's nuclear plants is of the "highest possible standard" and is under constant review.

Large's policy recommendations follow a recent warning regarding cyber terrorism. Last month, Russian security expert Eugene Kaspersky, who advises the UK government, Europol and Interpol on cyber security issues, said most states lack adequate systems to defend themselves in the event of a severe cyber-attack. The security expert suggested if cybercriminals can carry out successful attacks on well-protected financial institutions, they have the ability to wage an attack on any enterprise.

Prime Minister David Cameron and US President Barak Obama resolved in January that British and American intelligence officials would test the defense capabilities of critical institutions during a series of cyber war games scheduled to kick off later in 2015. The joint cyber tests will be conducted against each state's banks, financial institutions, and other critical infrastructure in order to improve defenses against prospective cyber-attacks and hackers.

The first war game will test financial institutions in London

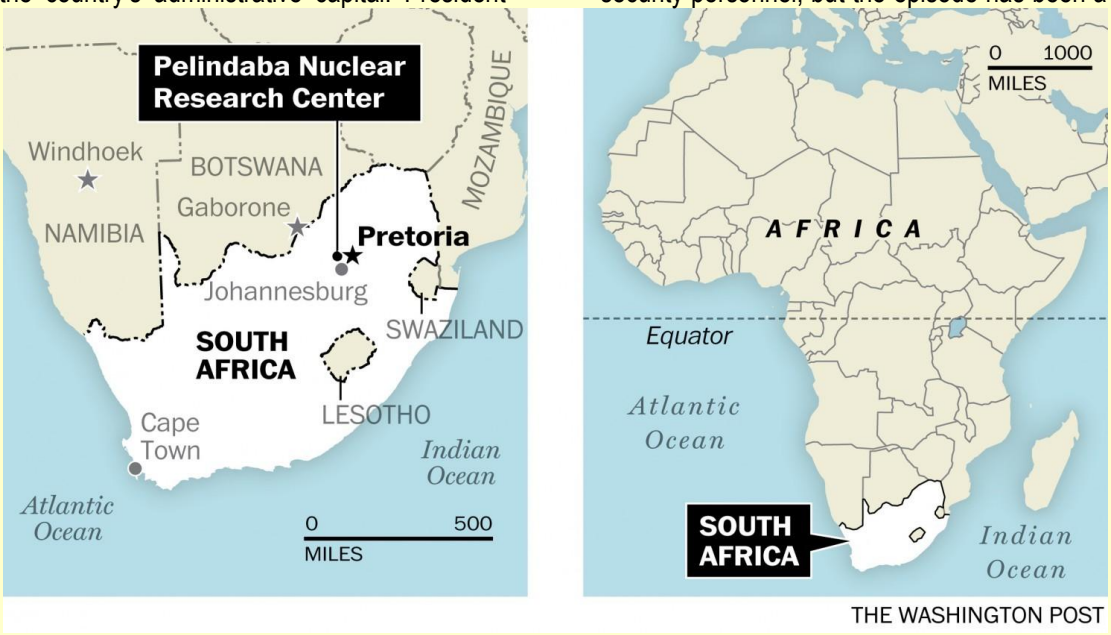
and on Wall Street. Future exercises will test other infrastructure, such as power suppliers and transportation systems.

South Africa refuses to give up cache of weapon-grade uranium

Source: http://www.homelandsecuritynewswire.com/dr20150319-south-africa-refuses-to-give-up-cache-of-weapongrade-uranium

March 19 – In 1990 the South African government extracted its inventory of highly enriched uranium from its nuclear weapons, then melted the fuel before storing it in a former silver vault at the Pelindaba nuclear research center just thirty minutes away from Pretoria, the country's administrative capital. President F. W. de Klerk was already planning the transformation of South Africa from a White minority-controlled state to a democracy – this would occur in 1994 — and he believed that South Africa no longer needed the six nuclear bombs it had built in the 1980s. The bombs, and South Africa's nuclear weapons-making infrastructure, were dismantled under IAEA monitoring.

In November 2007, the research center's security was breached when two teams of raiders entered the fenced perimeter. One group eventually broke into the center's central alarm station. Thankfully, both teams were caught when a watch officer summoned other security personnel, but the episode has been a source of contention between leaders in South Africa and U.S. officials.



THE WASHINGTON POST

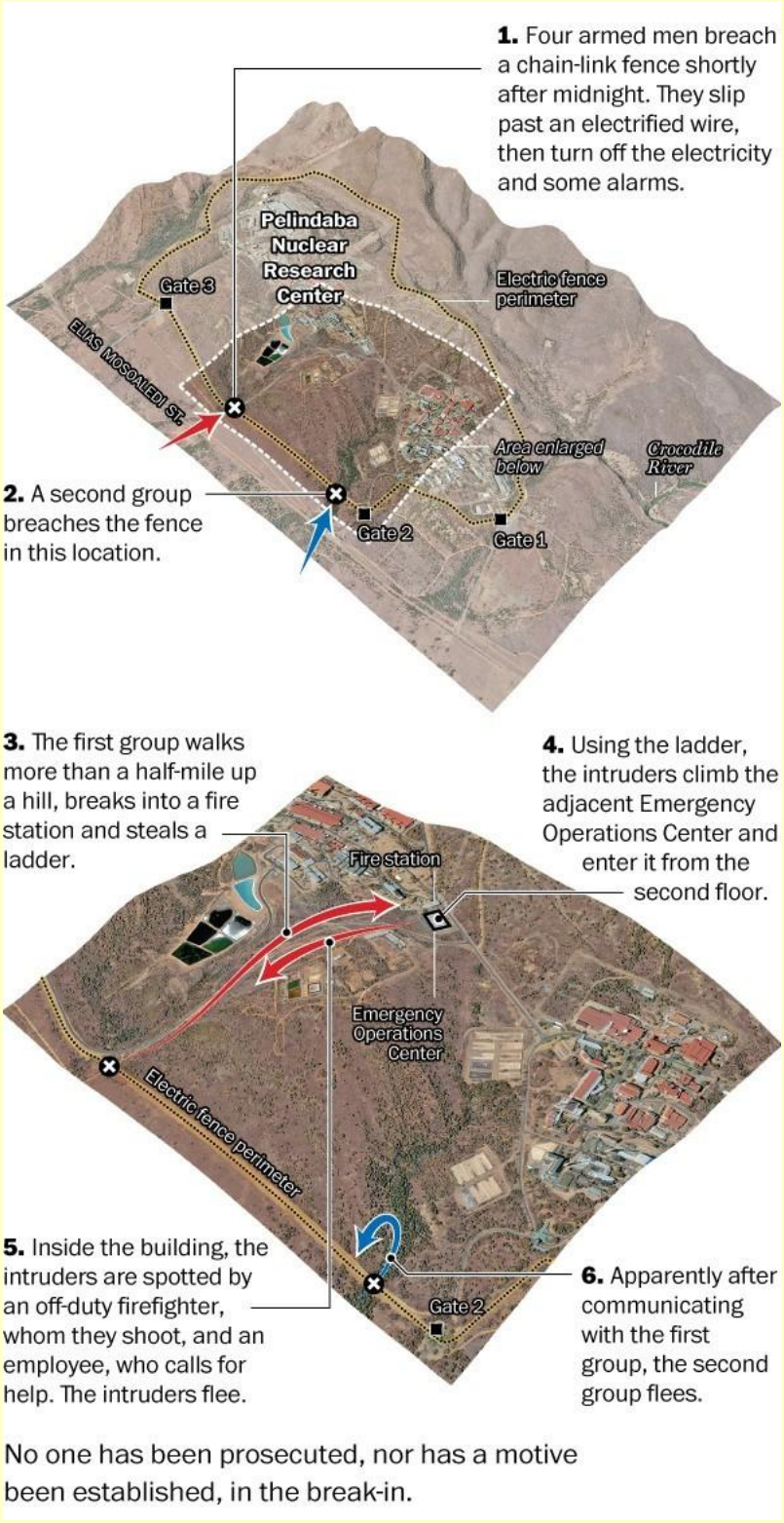
Over the years, some of the nuclear fuel has been used to make medical isotopes, but roughly 485 pounds remain.

The United States has expressed concerns over the safety of South Africa's nuclear cache.

South African president Jacob Zuma has rejected incentives from the Obama administration to get rid of his country's nuclear-weapons fuel. In an August 2011 letter, Obama warned Zuma that a terrorist nuclear attack would be a "global catastrophe," and proposed that South Africa transform its nuclear explosives into benign reactor fuel, with U.S. support. If Zuma agreed, the White House would announce the deal at a 2012 summit on nuclear security in South Korea.

Zuma rejected the proposal, along with other proposals from the Obama administration regarding nuclear fuel.

The *Washington Post* reports that the United States is partially responsible for South Africa's nuclear cache. Between 1956 and 1965 it helped the country build its first nuclear reactor under the Atoms for Peace program. The United States also trained scientists to run the South African reactor with U.S.-supplied weapons-grade uranium fuel.



In 1976, under the Ford administration, Washington cut off its fuel supply to South Africa after it concluded that the apartheid regime in South Africa had used nuclear research to create a clandestine bomb program.

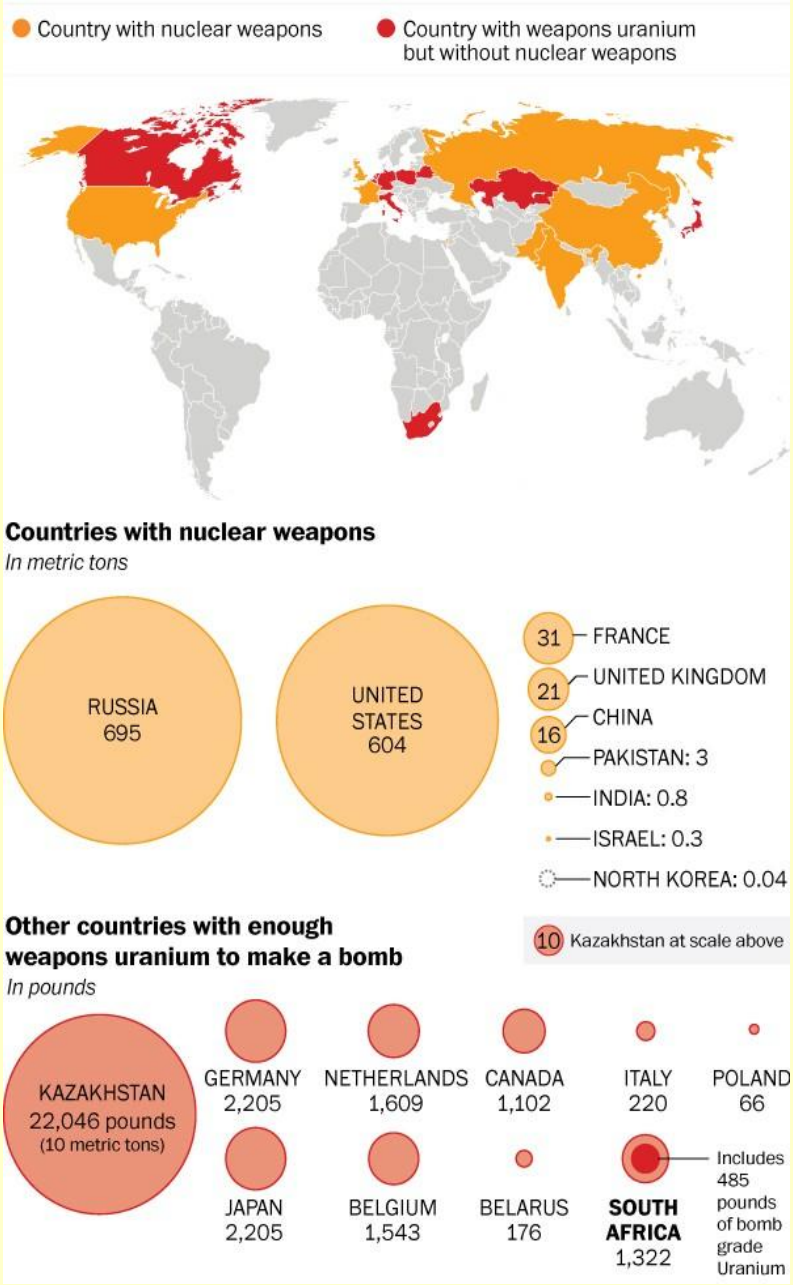
On 22 September 1979, South Africa and Israel conducted a secret nuclear test near the Prince Edward Islands off Antarctica. The telling "double flash" of a nuclear explosion was captured by a U.S. Vela Hotel satellite. The test was never acknowledged by either South Africa or Israel, and most of the information the United States gathered on the event remains classified.

The Obama administration sees South Africa's highly enriched uranium inventory as a target for terrorists and thieves. "The bottom line is that South Africa has a crime problem," said arms control expert Jon Wolfsthal, a few months before he was tasked with leading the White House's nonproliferation policy in 2014. "They have a facility that is holding onto material that they don't need and a political chip on their shoulder about giving up that material. That has rightly concerned the United States, which is trying to get rid of any cache of HEU (highly enriched uranium) that is still out there."

South African officials say America's concern with nuclear terror is an excuse to restrict the spread of peaceful and profitable nuclear technology to the developing world, adding that its nuclear fuel inventory is secure. "We are aware that there has been a concerted campaign to undermine us by turning the reported burglary into a major risk," said Clayson Monyela, spokesperson for the country's foreign ministry, the Department of International Relations and Cooperation. Monyela noted that the International Atomic Energy Agency (IAEA) had raised no concerns, and that "attempts by anyone to manufacture rumors and conspiracy theories laced with innuendo are rejected with the contempt they deserve."

South Africa has used some of its nuclear fuel to build medical and industrial isotopes which generates roughly **$85 million in**

income per year. In addition to the commercial benefit of keeping its cache of highly enriched uranium, South Africa sees its inventory as a source of pride, putting it on equal footing with other non-nuclear-weapons states which still have enough enriched uranium to build a nuclear weapon: Germany, Japan, Canada, Belgium, Kazakhstan, Poland, Italy, the Netherlands, and Belarus.



Abdul Samad Minty, who served for years as South Africa's top nuclear policy maker and now as the country's ambassador to United Nations agencies headquartered in Geneva, has dismissed the U.S. push to remove South Africa's nuclear fuel and curtail the nuclear ambitions of other developing countries. "The problem is you can't have nuclear-weapons states who feel they can have nuclear weapons and have as many as they want," he said. On efforts by the United States to reduce global nuclear arsenals: "Yes they are reducing, not disarming," Minty said.

In response, Gary Samore, the White House coordinator on weapons of mass destruction from 2009 to 2013, told Minty, "Nuclear disarmament is not going to happen," adding: "It's a fantasy. We need our weapons for our safety, and we're not going to give them up."

For Minty, that reasoning is unacceptable. "Now if you say you need nuclear weapons for your security, what stops another country from saying at another time, in another situation, I also need nuclear weapons for my security?" "People who smoke can't tell someone else not to smoke," Minty said.

Waldo Stumpf, an atomic energy official in South Africa who presided over the dismantlement of the apartheid-era bomb program, affirmed that removing of diluting the country's highly enriched uranium "was never part of the thinking here. Not within Mr. (Frederik W.) de Klerk's government. Not afterwards, when the ANC took over. Why would we give away a commercially valuable material that has earned a lot of foreign exchange? Why would we do that?"

South Africa intends not only to keep its current enriched uranium cache, but officials keep open the possibility of making or acquiring more. "Our international legally binding obligations . . . allow for the enrichment of uranium for peaceful purposes only, irrespective of the enrichment level," Zuma said at the 2012 nuclear security summit in Seoul.

▶ **Read also:** http://www.washingtonpost.com/world/africa/us-unease-about-nuclear-weapons-fuel-takes-aim-at-a-south-african-vault/2015/03/13/b17389f6-2bc1-4515-962d-03c655d0e62d_story.html

Constructing Cyberterrorism as a Security Threat: a Study of International News Media Coverage

By Lee Jarvis, Stuart Macdonald and Andrew Whiting
Source: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/402/html

This article examines the way in which the English language international news media has constructed the threat of cyberterrorism. Analysing 535 news items published by 31 different media outlets across 7 countries between 2008 and 2013, we show that this coverage is uneven in terms of its geographical and temporal distribution and that its tone is predominantly apprehensive. This article argues that, regardless of the 'reality' of the cyberterrorism threat, this coverage is important because it helps to constitute cyberterrorism as a security risk. Paying attention to this constitutive role of the news media, we suggest, opens up a fresh set of research questions in this context and a different theoretical approach to the study of cyberterrorism.

Lee Jarvis *is Senior Lecturer in International Security at the University of East Anglia (UEA) and Director of the UEA's Critical Global Politics research group. His recent books include Counter-Radicalisation: Critical Perspectives (Routledge, 2015, edited with Christopher Baker-Beall and Charlotte Heath-Kelly); Critical Perspectives on Counter-terrorism (Routledge, 2015, edited with Michael Lister) and Security: A Critical Introduction (Palgrave, 2015, with Jack Holland).*

Stuart Macdonald *is Associate Professor in Law and Deputy Director of the Centre for Criminal Justice and Criminology at Swansea University. He is co-editor of Cyberterrorism: Understanding, Assessment and Response (New York: Springer, 2014) (with Lee Jarvis and Thomas Chen). His recent project on security and liberty was funded by the British Academy. He has held visiting scholarships at Columbia University Law School, New York, and the Institute of Criminology at the University of Sydney.*

Andrew Whiting *lectures in the Department of Criminology at Swansea University. He is currently completing his PhD which investigates the construction of cyberterrorism within Internet security industry discourse. Since undertaking his doctorate has had his work published on a range of topics that reflect his research interests including terrorism, cyberterrorism and radicalisation.*

Cybercrime Affects More Than 431 Million Adult Victims Globally

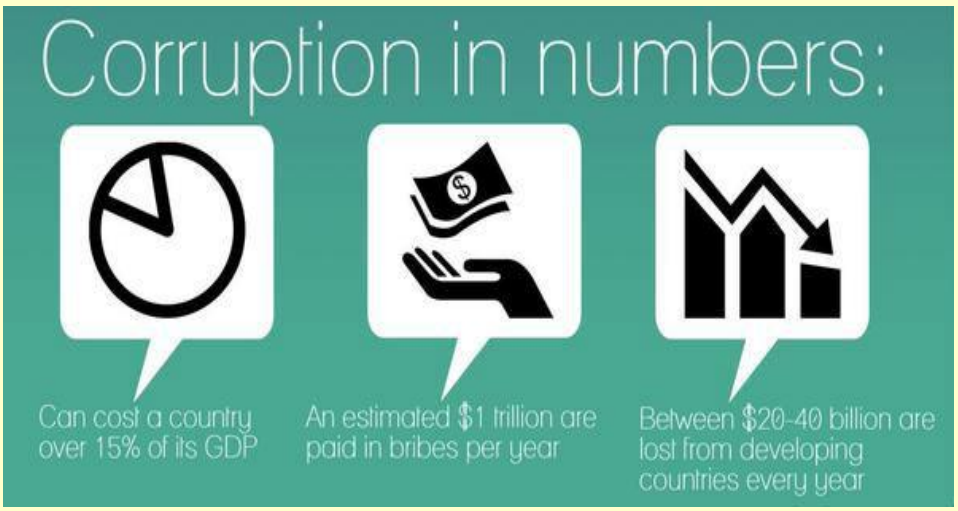
Source: http://www.inquisitr.com/1862348/cybercrime-affects-431-million-adult-victims-globally/#FEAawxLSk8YmEWYY.99

Cybercrime affects more than 431 million adult victims around the world. Since the internet has become such an integral part of governments, businesses, and the lives of millions of people, cyberspace has become an ideal place, allowing criminals to remain anonymous while they prey on victims.

The most common forms of cybercrime are offences related to identity, such as malware, hacking, and phishing. Criminals use these methods of cybercrime to steal money and credit card information. Additionally, cybercriminals use the internet for crimes related to child pornography, abuse material, and intellectual and copyright property.

As technology advances, criminals are finding it much easier to perform a cybercrime; advanced techniques and skills to perpetrate threats are no longer required. For instance, software that allows criminals to override passwords and locate access points of computers are easily purchased online. Unfortunately, the ability to find

cyber criminals is becoming more difficult. Cybercrime is a rapidly growing business, exceeding $3 trillion a year. Victims and perpetrators are located anywhere in the world. The effects of cybercrime are seen across societies, stressing the need for a pressing and strong international response.



However, many countries do not have the capacity or regulations to combat cybercrime. A global effort is required to make available firmer regulations and improved protection because cyber criminals hide within legal loopholes in countries with less stringent regulation.

Criminals perpetrate a cybercrime by taking advantage of a country's weak security measures. Additionally, the lack of cooperation between developing and developed countries can also result in safe havens for individuals and groups who carry out a cybercrime.

The United Nations is actively involved in fighting cybercrime. The organization set up the United Nations Office on Drugs and Crime (UNODC) following the 12th Crime Congress to study cybercrime. The UNODC is a global leader in the fight against illicit drugs and international crime.

Cybercrime affects one million victims every single day. More than 431 million people are affected by cybercrime, that's 14 adult victims every second.

In addition, **there are up to 80 million automated hacking attacks every day.** The most common and fastest growing forms of consumer fraud on the Internet are identity-related offences, especially through the misuse of credit card information.

Learning online protection methods is one of the simplest means of defense from becoming victim to a cybercrime. When purchasing products online, always be aware of the trustworthiness of the websites.

Avoid using public computers for anything that requires a credit card payment. By all means, be sure online purchases and banking are facilitated with a fully legitimate and safe business.

Computers should have up-to-date security software; choose strong passwords, and do not open suspicious emails or special offers that ask for personal

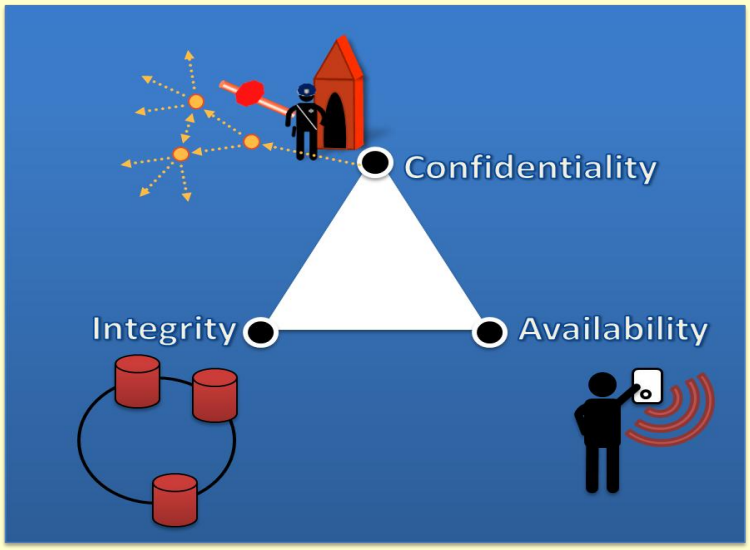
information, which are often in the form of sales, contests, or fake banks.
Internet-related crime, like any other crime, should be reported to appropriate law enforcement investigative authorities at the local, state, federal, or international levels, depending on the scope of the crime.

Citizens who are aware of federal crimes should report them to local offices of federal law enforcement. Contact the U.S. Department of Justice (USDOJ) or Internet Crime Complaint Center (IC3) for more information on reporting a cybercrime.

Information Security for Emergency Management

Source: https://www.emergency-management.expert/information-security-for-emergency-management-part-1/

We think of Information Security ("InfoSec") as a single standard set of problems, processes, and practices that apply to every organization and situation; that InfoSec means the same thing for retailers, corporations, financial institutions, government, and the military. So it seems like an obvious conclusion that InfoSec is the same for emergency management. Obvious, but wrong.



The fundamental principles of InfoSec are contained in the CIA triad, which is a nice memorable acronym for:

- Confidentiality
- Integrity
- Availability

The CIA triad are general principles for InfoSec that are, in fact, universally relevant. A "three-legged-stool" that supports InfoSec - take away any one of the legs and the stool isn't stable. But the relative importance of a leg can be very different, depending on the organization. This is critical to understanding what InfoSec means to your team.
In the spirit of *Sesame Street*, let's play a game:

One of these things is not like the others

1. Retailers [example: Target]
2. Corporate Enterprises [example: Sony]
3. Financial Institutions [example: Goldman Sachs]
4. Government Agencies [example: Health and Human Services]
5. Military [example: Army Intelligence and Security Command (INSCOM)]
6. Emergency Management

If you guessed **#6, Emergency Management** you are correct!
What all of the others have in common, other than being notorious in the popular press for high profile data breaches, is that the primary concern and focus of their InfoSec is **Confidentiality** - making sure information doesn't fall into the wrong hands. Confidentiality is paramount, but as the examples illustrate, difficult to achieve. As a result, everyone thinks InfoSec is all about confidentiality because that's what CNN says. A one-legged stool. The pervasive misconception, even in the security community, is that InfoSec and confidentiality are interchangeable concepts, and often the other legs of the stool are given short shrift.
Emergency management concerns and priorities are almost the polar opposite. **Availability** - making sure that information is accessible all the time, every time, and by

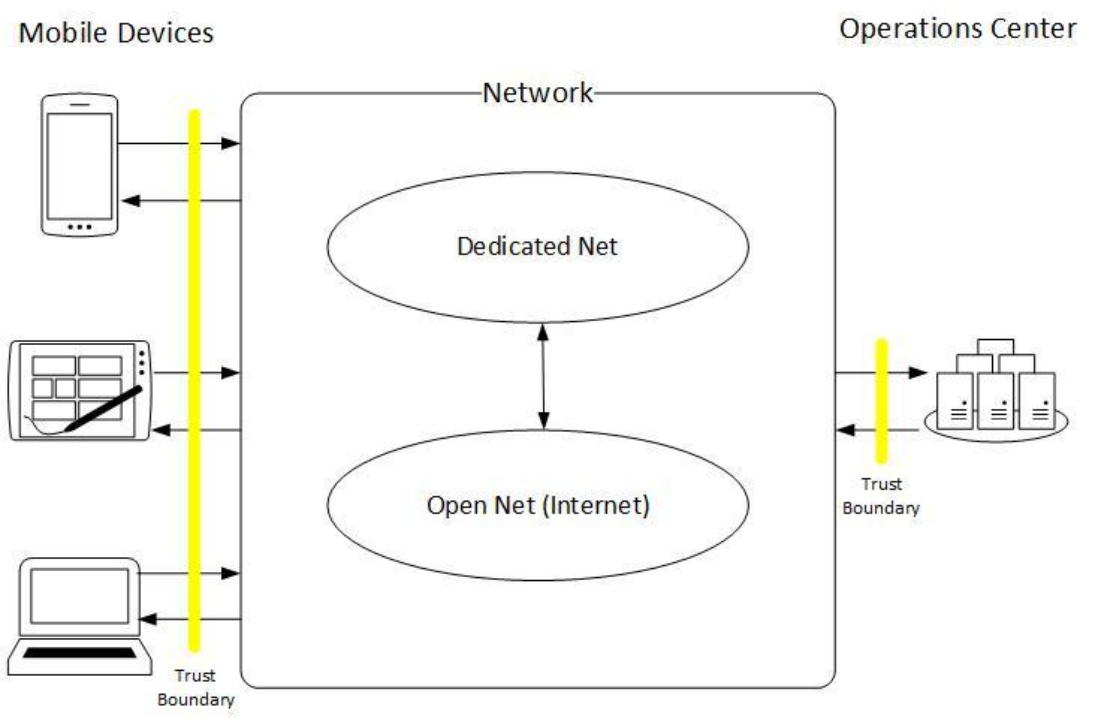
everyone who needs it - is paramount. **Integrity** - making sure that information is correct, complete, uncorrupted, and originates from where, and who, is expected - is close behind. Confidentiality, while certainly not something emergency managers can ignore, is typically related to fringe scenarios involving transfers of patient health records regulated by HIPAA or the interception of confidential communications. In other words, while everyone else is mostly worrying about how to keep information away from bad guys, emergency managers are mostly worrying about information being reliable and accessible to everyone who needs it, whenever they need it.

Given the different priority of concerns for emergency management, can InfoSec activities and processes benefit and inform emergency management practices? Is it valuable, practical, or even possible to adapt well understood, structured, and systematic InfoSec practices to emergency management? Given that emergency management is uniquely concerned with availability and integrity, and not confidentiality like the majority of actors concerned with InfoSec, are these questions even relevant?

The goal of this InfoSec-based threat assessment is to identify weak points in reliability and resiliency of information flows and to determine ways to mitigate, reduce, or accept the risk incurred by those weak points (these are the hazard-mitigation measures emergency managers engage in). What follows is a step-by-step example.

Step 1 - Information Flow Diagram

The following figure – referred to as an Information Flow Diagram – is the first step in threat modeling. This Information Flow Diagram illustrates the components, information flows, and trust boundaries that can occur in an emergency response scenario. Specifically, it depicts the flow of information between emergency responders in the field who are using mobile devices (smart phones, tablets, and computers), to the network (both the dedicated emergency network and the internet) that allows for the transfer of information, to the operations center (for example, an emergency operations center) that is supporting the coordination of information and resource sharing at the scene. Each point of separation between these components is a trust boundary.



Step 2 - Identify Trust Boundaries

To be more specific, a trust boundary is where information flows from a higher to lower level of trust (or vice versa). Trust, in this context, means confidence in the confidentiality, integrity, and availability of the information, and is defined as being high, medium, or low depending on that confidence.

Moving from left to right across our Information Flow Diagram, we start with mobile devices. For this example, we assume that mobile devices' (iPhones, iPads, laptops, etc.) hardware is sufficiently reliable, but the reliability and suitability of apps for mobile software platforms (iOS, Android, Windows) varies wildly. The reason for this is that the typical mobile app is developed quickly and released with minimal testing, and the app stores (iTunes, Google Play, Windows Store) screen out only those apps that violate store policy or are known to contain malware. Most importantly, emergency managers have **no control** over devices and apps at the site of the event because it is impossible to predict - much less specify - the mobile devices and apps used (everybody – from the public to emergency responders – can post to the internet using personal devices), so the level of trust in mobile devices is **low**.
Next up: the network. We assume that network components are highly reliable and available, so the level of trust in the network is **high** (after all, if it wasn't, the internet would be "down" all the time and Google would be out of business).
And finally, we have the Operations Center. For this example, we assume that Operations Centers have hardware and systems that are sufficiently reliable; however, and more importantly, unlike mobile devices, emergency managers are responsible to varying extents for Operations Center systems by virtue of involvement in scoping, specifying, funding, and maintaining those systems, so the level of trust in Operations Center systems is **medium**.
Identifying the level of trust between trust boundaries is important because those boundaries are where we look for threats.

Step 3 - Identify Threats at Trust Boundaries
In this context, a threat is a possible danger that, if exploited, could cause interruption or degradation of the information flow across a trust boundary (meaning emergency responders and emergency managers are not receiving the information they need). The purpose of this step is to identify specific threats to the integrity and availability of information flow, and to understand the consequences should that threat be realized. The goal is to answer these questions:

- What is the problem?
- Why is it bad? (think consequences)
- What kind/category of problem is it? (these are the InfoSec principles of Integrity (primary), Availability (primary), and Confidentiality (secondary) that were described in Part 1)
- How bad is it?

In short: trust boundaries are the best place to look for threats.
The following tables illustrate the threats that are present at trust boundaries, and consider the consequences of each threat occurring, the InfoSec principle being violated by the threat, and the priority level for mitigating against the threat.

Mobile Device/Network Trust Boundary

Threat	Consequence	Category	Priority
1. Device using inappropriate apps	Device info transfer incorrect or incomplete	Integrity: info degraded	**Low**
2. Device using inappropriate apps	Device info transfer may be intercepted without authorization	Confidentiality: info leakage	**Medium**
3. Device has insufficient access/permissions to a dedicated network	Device unable to connect to internet via dedicated network gateway	Availability: info transfer impeded	**Medium**
4. Device has insufficient access/permissions to a dedicated network	Device unable to use dedicated network as trusted gateway to internet	Confidentiality: info leakage	**Low**
5. Network gateway inaccessible by device	Information flow to device restricted or interrupted	Availability: info transfer restricted	**Medium**

Network/Operations Center Trust Boundary

Threat	Consequence	Category	Priority
6. Ops Center has insufficient network bandwidth	Time lag in Ops Center info processing	Availability: info delayed	**Medium**
7. Ops Center has insufficient network bandwidth	Info dropped or missed	Integrity: info incomplete	**High**
8. Ops Center has insufficient info for processing resources for info	Delay in Ops Center info usability	Availability: info delayed	**Medium**
9. Ops Center info saved unnecessarily	Info may be breached or stolen	Confidentiality: info leakage	**Low**
10. Ops Center info insufficient for backup/archive of info	Info and audit trail may be lost	Integrity: info and provenance incomplete	**High**

The preceding tables, as part of an example, do not attempt to outline every possible threat scenario in detail, or the many possible consequences for each identified threat. They do, however, illustrate a crucial point: Threat assessments are complex, and the quality and usefulness thereof depend on the involvement of the entire team. Emergency responders in the field, network administrators and Information Technology (IT) staff, and emergency managers in operations centers need to play a role in identifying the many threats and risk to InfoSec that occur across an emergency. No one, regardless of knowledge and expertise, can do it alone.

These are just a few examples that are intended to provide an overview of the basic form and substance of a threat assessment report.

Step 4 - Develop Mitigation Activities for Identified Threats

After identifying the threats, we need to determine how best to mitigate against them based on risk. Priority (Low, Medium, High) from the previous step, while roughly correlated to risk, is the starting point for the broader, detailed assignment of risk in the real world. Here, it is used directly to quantify risk for simplicity's sake.

The following table subs in Risk for Priority, and addresses some potential mitigation efforts that may address the identified threat.

Threat	Risk	Mitigation
1. Device using inappropriate apps	**Low**	Accept risk
2. Device using inappropriate apps	**Medium**	Identify sensitive data stored on network resources and develop plan to remove or move it to network inaccessible resources
3. Device has insufficient access/permissions to a dedicated network	**Medium**	Evaluate access controls for dedicated network, and adjust accordingly
4. Device has insufficient access/permissions to a dedicated network	**Low**	Accept risk
5. Network gateway inaccessible by device	**Medium**	Evaluate and prioritize access controls for dedicated network
6. Ops Center has insufficient network bandwidth	**Medium**	Obtain and allocate funds to upgrade network services and/or providers
7. Ops Center has insufficient network bandwidth	**High**	Obtain and allocate funds to upgrade network to necessary Quality of Service (QoS) (level of uptime, bandwidth, and fault tolerance)

8. Ops Center has insufficient info for processing resources for info	**Medium**	Obtain and allocate funds for additional or adequate computing resources
9. Ops Center info saved unnecessarily	**Low**	Evaluate stored data and implement lifecycle controls accordingly
10. Ops Center info insufficient for backup/archive of info	**High**	Obtain and allocate funds for implementation of strategic data archive and recovery processes and governance

Step 5 - Review and Certify Mitigation Efforts

This final step is crucial. This is where the threat assessment is reviewed, finalized, and accepted by those with authority to approve the allocation of resources required for mitigation efforts, and certify the acceptance or transfer of risk. This necessarily involves directors or executive management (senior leaders) who can sign off on the plan. This step requires assorted meetings, drafts, revisions, reports, and significant time, but nothing unfamiliar or outside the group's routine activities.

Adopting and incorporating InfoSec concepts into existing emergency management practices will enhance the threat assessment process by helping emergency managers to more effectively discern where to look for InfoSec-related problems, what kinds of problems to look for, and to correlate problems with solutions and plans systematically in a consistent way to effectively reduce risk.

***Joseph Webster, CISSP** is a Software and Systems Security Architect specializing in high quality secure software systems to protect privacy, valuable assets and intellectual property. Also a passionate advocate for privacy and secure development and testing methodologies to promote best security practices for all.*

Attacks against Critical Infrastructure Seek Operational

Source: http://threatpost.com/attacks-against-critical-infrastructure-seek-operational-intelligence/111244#sthash.mzhDyIE6.dpuf

In most critical industries—petroleum refineries or energy utilities, for example—there is very little in the way of proprietary information. Refining crude oil into gasoline requires science, not a secret sauce. Same goes for power generation.

So why are advanced attackers using the same data exfiltration techniques deployed in APT-style attacks against IT against critical infrastructure, too? Intelligence gathering, says one expert who spoke last week during the Kaspersky Security Analyst Summit in Mexico.

"They're not taking financial data, or [mergers and acquisitions] data. They're taking data that correlates back to the inner workings of the ICS infrastructure," said Dewan Chowdhury, principal at MalCrawler, and a longtime ICS and SCADA security consultant. "They want PLC blueprints that describe how refineries operate. They want .asr (ActionScript remote file) schemes for power distribution."

The end game, especially in the Middle East where Chowdhury has spent considerable time, is usually sabotage. The intelligence gathering assists hackers with the weaponization of malware and other attacks that will disrupt manufacturing, oil production or power distribution, and impact economies worldwide.

"Sabotage is by far the scariest thing. When we see sabotage in IT, it's more like removing files or stealing databases," Chowdhury said. "But when you can impact something tangible and cause harm from a safety standpoint, that's scary."

The intelligence being stolen from ICS enables attacks such as one Chowdhury described in which a natural gas provider in the Middle East was experiencing pressure issues in its pipelines, yet the SCADA Masters looked legitimate and reported that all was well. A physical inspection, however, determined that a control room had been broken into and the subsequent investigation of ICS gear led to the discovery of a new service in the machine's registry that was sending bogus data to the SCADA master while telling a remote terminal unit to malfunction.

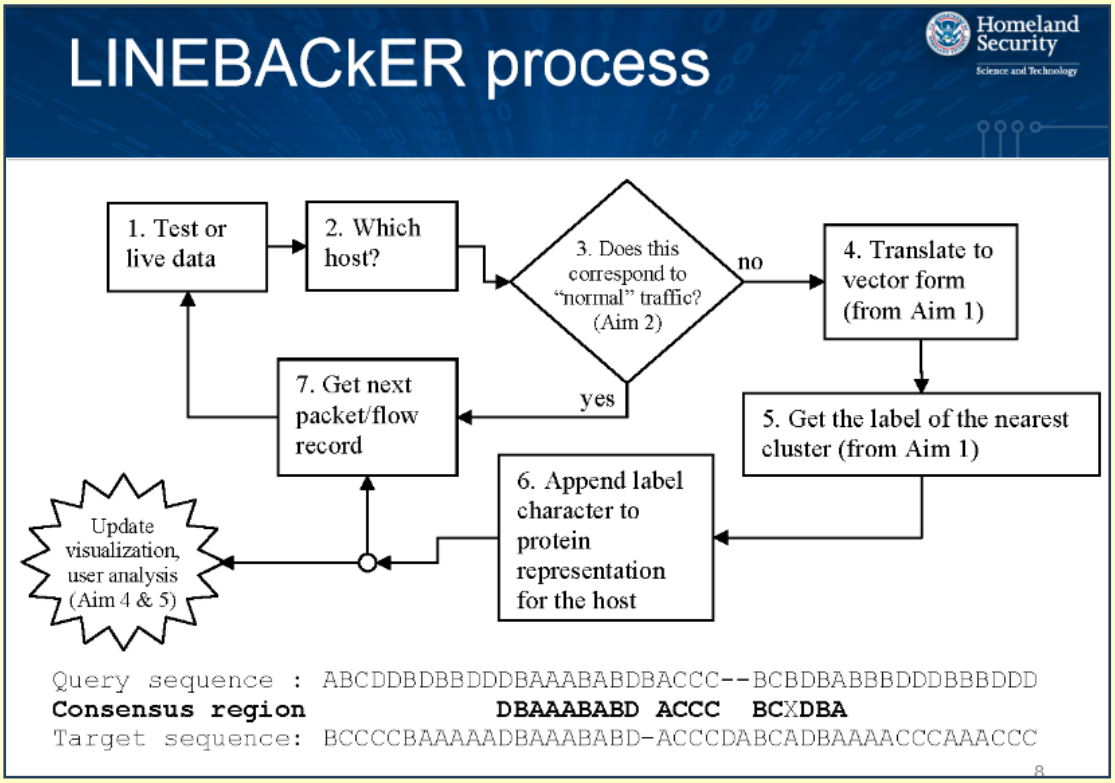
"In order to really hit something like the power grid, you need to have information about the inner workings," he said. "How is the ASR set up? And when does quality control kick in at a refinery? This is the data you need to manipulate and weaponize this stuff."
In other words, this isn't your daddy's APT.
And speaking of the power grid, the old chestnut about attackers shutting down the grid is a fallacy given the built-in redundancy. Instead, it's an effective marketing and propaganda tool for politicians wanting to create urgency for new regulations or some other part of their agenda.
Advanced attacks against ICS target data that correlates back to the inner workings of the infrastructure. via @Threatpost
"The grid is designed around self-preservation. It's designed to protect itself from hurricanes, tornadoes and it's a school of thought that's been there since day one," Chowdhury said. "And it's designed that if one part of the grid goes down, it doesn't destroy the rest."
There have, however, been attacks against industry that have been destructive, the most prominent being the use of Shamoon wiper malware against Saudi Aramco that destroyed 30,000 workstations. Last November, the Industrial control System Cyber Emergency Response Team published an advisory warning operators of ICS vulnerabilities being exploited by the BlackEnergy malware, in particular the Sandworm APT gang.
Researchers at Kaspersky Lab published a report at the time on BlackEnergy, in particular a number of plug-ins that had been discovered used in attacks used for stealing passwords, digital certificates and more. **One of the more disturbing plug-ins reported on was called dstr, a command that overwrites and destroys hard drives with random data in the event the attackers suspected they had been found out.**
Chowdhury said he'd like to see a similar evangelical effort happen with ICS that began some years ago in software development circles when a concentrated effort was made to instill security from the outset of development lifecycles.
"We're seeing the fruits of it now; a lot of layer 7 stuff is much harder to do compared to five years ago," Chowdhury said, noting that with ICS, the real challenge may be cultural since engineers, not IT, run the shop. "The cyber community needs to engage with engineers and give them the reality of it."
In some circles, for example, there still exists the mindset that it's cheaper to deal with something post-incident rather than be proactive. Chowdhury said in electric utilities, for example, regulations put forth by the North America Electric Reliability Corporation (NERC) provide utilities with not only a security checklist, but have led some to push vendors to include security controls such as IPsec or RADIUS installed on capacitor banks or electric voltage network regulators.
"That's big," Chowdhury said.

Bio-inspired analysis helps in recognizing, characterizing evolving cyberthreats

Source: http://www.homelandsecuritynewswire.com/dr20150309-bioinspired-analysis-helps-in-recognizing-characterizing-evolving-cyberthreats

March 09 – **LINEBACkER allows cyber security analysts quickly to discover and analyze behaviors of interest in network traffic to enhance situational awareness, enable timely responses, and facilitate rapid forensic and attribution analysis.** In a collaborative, operational setting, net-flow data can be converted on site in near real-time and then shared with collaborators in obfuscated form. This allows for finding attacks and anomalies faster without exposing sensitive data.
Our reliance on cyber systems permeates virtually every aspect of national infrastructure. From banking, finance and industry to education and research, from national defense to power generation and delivery, secure computer networks are the lifeblood for maintaining critical infrastructure, information, and the U.S. strategic advantage over our adversaries.
The volume of network traffic data generated has outpaced our ability effectively analyze it fast

enough to prevent many forms of network-based attacks. In most cases new forms of attacks cannot be detected with current



methods. We need a method drastically to reduce the amount of data to be analyzed, quickly to characterize an attack, and to identify previously unseen types of attacks before they're executed. Network analysts need the ability to discover malicious traffic in computer networks, and share their insight or a signature of the threat with others, without jeopardizing sensitive or institutional data.

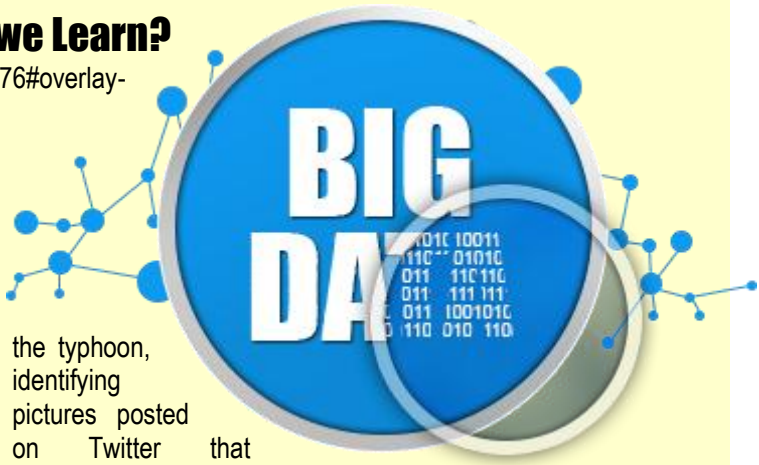
A PNNL release reports that the LINEBACkER tool allows analysts to share signatures without sharing data. This is especially beneficial when sensitive data is involved and sharing threat signatures across multiple organizations is necessary. Simply, LINEBACkER applies the MLSTONES methodology to the problem of discovering malicious sequences of traffic in computer networks. MLSTONES leverages technologies and methods from biology and DNA research, and have effectively mapped a solution to flexibly represent and identify signatures and express them in a biology-based language that cannot be "translated" back to the original data.

Researchers at the Pacific Northwest National Laboratory (PNNL) have translated several biology and bioinformatics concepts onto cyber defense data. Specifically they have created a methodology which uses the concepts of protein identification and families, inheritance, and function to apply to a number of cyber-based data types. The MLSTONES process creates cyber "proteins" and then create a single representation of an entire family of entities thus reducing the amount of data to analyze by several orders of magnitudes.

The researchers can also infer the function of a "cyber protein" by its relationship to other similar proteins. This is the same process used in biology to discover similar proteins. This helps to identify completely new (zero-day) cyber threats. The researchers apply high-performance biosequence analysis that enables inexact string matching of streaming network traffic; their approach is robust when there is more than one form of threat and supports "family resemblance" attribution. The tool characterizes baseline behavior, converts raw net-flow data to bio-representation, constructs a family tree of cyber event types, and creates visual interface to deploy in a client setting, against specific threats or suspicions. The translation of network behavior is accomplished at the site of collection and it is the translated representation that is shared among collaborating agencies.

Disasters and Big Data: What Can we Learn?

Source: http://www.homelandsecurity.org/node/3676#overlay-context=forum



From typhoons to earthquakes to influenza, "big data" is helping emergency managers and government agencies learn more about how to respond and recover from disasters. We also look into sources of big data and how data has been used in real-life disaster situations.

Making sense of big data with crowdsourcing and artificial intelligence

Patrick Meier, director of QCRI's Social Innovation Program and author of *Digital Humanitarians*, explained the challenges of big data and disasters. According to Meier, "The first 'battle' between Digital Jedis and Big Data began on January 12, 2010, following the devastating earthquake that struck Haiti. Within hours, Digital Jedis mobilized online, launching a 'Crisis Map' pinpointing the damage and resulting needs across the Haitian capital of Port-au-Prince." He looks to crowdsourcing and artificial intelligence technologies to make sense of the vast volumes of data generated during major disasters.

Using big data to ask the right questions

In the World Economic Forum Agenda, Laura Gurski explains that corporations are using big data to anticipate how much of what product is needed where. In applying big data to disaster relief, Gurski asks if we could use today's technology to deliver things differently, more efficiently or even potentially avoiding, or reducing, the effects of the disaster. She concludes that "What we have learned from big data in the corporate world is that it becomes a question of leveraging the fact base to ask different and smarter questions."

Using big data after Typhoon Ruby

Just after Typhoon Ruby hit the Philippines in December 2014, the United Nations Office for the Coordination of Humanitarian Affairs (OCHA) activated the Digital Humanitarian Network (DHN) to look for tweets related to urgent needs. The DHN used MicroMappers , which combines crowdsourcing and artificial intelligence, to analyze a variety of data from tweets, Instagram pictures, YouTube videos, satellite imagery, and aerial imagery. The UN also asked DHN to analyze images following the typhoon, identifying pictures posted on Twitter that showed disaster damage and then rating and mapping the damage.

Looking to the past to teach today's teachers

While the Spanish-influenza pandemic of 1918 is almost a hundred years past, a team of humanists and computer scientists from Virginia Tech is using 21st-century big data analysis tools to analyze early 20th-century sources to better understand how America responded to the outbreak in 1918. The Data Mining the 1918 Influenza Epidemic project explored how newspapers shaped public opinion using data mining techniques combined with historical and rhetorical analysis to understand the flow of information about the spread and impact of disease.

To help disseminate the results of their research, Virginia Tech has received a grant from the National Endowment for the Humanities to lead a summer course for teachers on the epidemic.

Opening up data sources

One source of open data has recently been launched - disasters.data.gov is designed to foster collaboration and continual improvement of disaster-related open data, tools, and ways to empower first responders, survivors, and government officials with the information needed in the wake of a disaster. This subset of Data.gov includes: data of specific types of disasters, apps and tools and disaster-related datasets from all levels of government and the private sector.

Using big data to solve real world problems

A new report, Quantifying Human Mobility Perturbation and

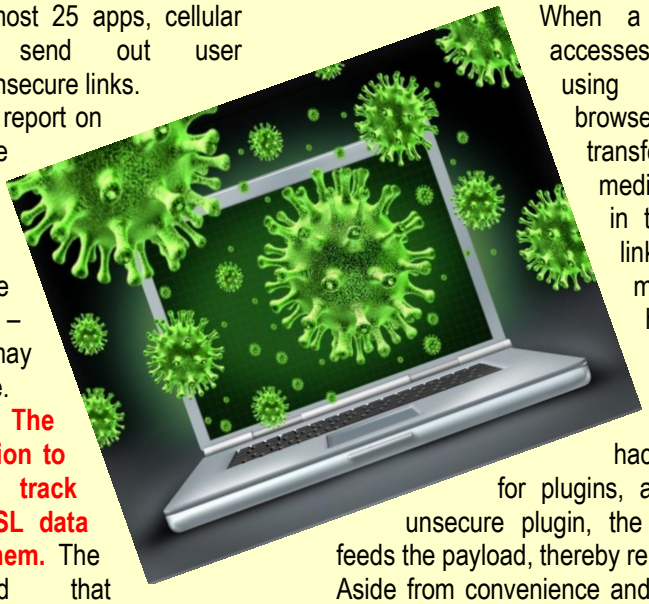
Resilience in Hurricane Sandy published in PLOS One, used big data to study how people's mobility patterns changed during and after Hurricane Sandy in 2012. The study used high-resolution data from Twitter, a total of 702,188 tweets from 53,934 individuals. The researchers located each user using geolocation information attached to each tweet. Their research suggests that human mobility data in steady states can possibly predict the mobility during and after disasters. According to the authors, "Understanding nuances of human mobility under the influence of such disasters will enable more effective evacuation, emergency response planning and development of strategies and policies to reduce fatality, injury, and economic loss."

Dangerous Apps

Source: http://i-hls.com/2015/03/dangerous-apps/?utm_source=Israel+Homeland+Security+%28iHLS%29&utm_campaign=32ff278c8b-ENGLISH_DYNAMIC&utm_medium=email&utm_term=0_8ee2e16ed1-32ff278c8b-87373033&mc_cid=32ff278c8b&mc_eid=521c0e089a

No less than six new malware are born each second. This, according to a recent report on various cyber threats.

The report focuses on the level of security of cellular applications and their ability to contribute to numerous security breaches. The editors examined the most 25 apps, cellular applications, which send out user authorizations through unsecure links.



According to Feburary's report on cyber threat by McAfee Labs, most apps continue to run, without the breaches being fixed. This, despite version updates operate – which, it turns out, may only make matters worse.

The team used Man In The Middle (MITM) simulation to successfully track supposedly secure SSL data feeds and intercept them. The simulations revealed that usernames and passwords can be mined successfully, along with entry authorizations. As these apps are downloaded by hundreds of millions of users, SSL breaches have become a source of major concern for any business. This, especially given the ongoing process of transitioning employees from desktops to smartphones.

Another major trend the report cites concerns the successor of the Blacole malware. The person behind it was jailed at the end of 2013. Now, there void has been filled by Angler, an on the shelf software available on the black internet, designed to perpetrate hacks. Using Angler does not require computer savvy. It mostly directs browsers such as Explorer, Chrome and Firefox. This malware is also capable of using security breaches in software such as Adobe and Java's flash drives, respectively.

When a potential victim accesses a high risk server using a compromised browser, the server transfers the user to a mediator server, who in turn transfers the link on to the malicious server hosting the landing page used to perpetrate the hack. The page tests for plugins, and if it finds an unsecure plugin, the malicious server feeds the payload, thereby relaying the virus.

Aside from convenience and efficiency for the average hacker, Angler also features advanced applications such as direct memory download to compromise the target, avoiding virtual achiness and security products, alongside mining means focusing on data feeds. These include Trojan horses designed for the banking industry, ransom software, Rootkits, Cryptolocker and backdoor Trojans. As Angler keeps changing its patterns to cover its tracks, it is harder to detect.

Geographically speaking, the report highlights the 14% increase in the last quarter in the number of mobile malware

in Africa and Asia. Both regions are also the ones with the highest risk of contamination. The report also warns against Potentially Unwanted Programs (PUP), citing it adversely affects 91 million systems each day. These malware mostly pose as legitimate apps, but then they run unauthorized scripts such as gathering user data and system data.

Conversely, ransom malware, which have fueled the imagination of many TV series' writers, have been recovering nicely after a long period of decline. In the last quarter of 2014, their number jumped by 150%.

After a decline in the number of malicious signed binaries, they are making a comeback, with a 17% increase.

Justice Ministers decides the creation of a special Europol unit to fight terrorism through the internet

Source: http://cyprus-mail.com/2015/03/13/justice-ministers-decides-the-creation-of-a-special-europol-unit-to-fight-terrorism-through-the-internet/

The Council of Justice and Home Affairs decided today the creation, within the framework of Europol, of a special unit that will track down sites and other locations on the internet that promote terrorism and radicalization.

According to the Cypriot Minister of Justice Ionas Nikolaou, who took part in the Council and the discussion on specific anti terrorism measures, the Ministers decided also specific measures for the control of the external borders of the EU, on the basis of common danger estimates, with the use of computerized systems for people and documents.

Nicolaou stressed that the exchange of information is of particular importance, between all EU countries and not only the ones that belong to the Shengen Treaty (Cyprus is not a member), as well as with third countries.

The Minister of Justice said that Cyprus will do everything she can for the battle against terrorism and will take all the necessary measures to prevent a terrorist action and to safeguard Cypriots and European citizens alike.

Anonymous links 9,200 Twitter accounts to terrorist organisation Islamic State

Source: http://www.itproportal.com/2015/03/16/anonymous-links-twitter-accounts-islamic-state/

A co-op effort between Anonymous, GhostSec and CntlSec has resulted in 9,200 Twitter accounts being linked to the terrorist organisation Islamic State, all blatantly promoting the material and spreading the propaganda through the micro-blogging service.

It is one of the first times the three loosely tied hacking groups have come together, under the #OpISIS to rid of the West of Islamic State propaganda.

The push by Anonymous follows a series of people from Europe and the US moving to Syria, Iraq and other Islamic State base-states, where they join the terrorist organisation.

Most accounts appear to still be active, showing a reluctance by Twitter to remove this harmful material. Twitter has removed this type of material in the past, but might be a bit slow when it comes to en-masse removal.

The Islamic State use a whole range of tools to spread propaganda, including launching its own 'Caliphate Book', which was closed down a few days later after members warned the social network was not safe from US surveillance.

Twitter does not block IP, meaning that even if it blocks all 9,200 accounts, another thousand could spring up by the time all are blocked. Islamic State has been using quite a lot of accounts simply to retweet and act as bots for the main accounts.

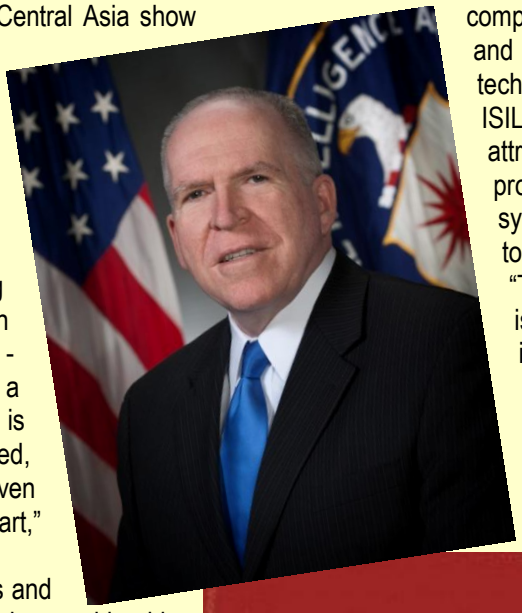
Twitter did announce it would be stamping down on hate speech and revenge porn, hopefully terrorist activity is also on the list.

CIA Chief: Terrorism Morphing Into Different Threats

Source: http://www.defense.gov/news/newsarticle.aspx?id=128373

March 16 – Terrorism is morphing into different types of threats, including cyberattacks that can impact nations across the globe, the director of central intelligence said in New York last week.

John Brennan told the Council on Foreign Relations that terror attacks in Europe, the Middle East, Africa and Central Asia show the terror threat is changing. The CIA working with foreign partners is key to defeating the terror threat, he added.



"These attacks underscore a disturbing trend that we have been monitoring for some time -- the emergence of a terrorist threat that is increasingly decentralized, difficult to track and even more difficult to thwart," Brennan said.

Though the United States and its partners have had considerable success in attacking core al-Qaida, affiliates have risen, said Brennan, pointing to al-Qaida groups in Libya, Egypt, Somalia, Nigeria "and especially Yemen where al-Qaida in the Arabian Peninsula has demonstrated a capability to plot attacks well beyond Yemen's borders, including in our homeland."

ISIL a 'Serious Danger' Beyond Region

But the heartland of terror, the director said, now operates in Syria and Iraq where the Islamic State of Iraq and the Levant is waging a campaign of unspeakable brutality against the local population and anyone who does not share its ideology.

Left unchecked, ISIL poses a serious danger not only to Syria and Iraq, but to the wider region and beyond, including the threat of attacks on the U.S. homeland and the homelands of its partners, Brennan said.

The intelligence chief echoed DoD leaders in saying the fight against ISIL will be a long one. "If there is one thing we have learned over the years, it is that success against terrorism requires patience and determination," he said. "Clearly our country will be dealing with terrorism in one form or another for many years to come."

Threats in the Cyber Realm

Modern communications technologies complicate the fight against ISIL and its ilk, Brennan said. "New technologies can help groups like ISIL coordinate operations, attract new recruits, disseminate propaganda and inspire sympathizers across the globe to act in their name," he said. "The overall threat of terrorism is greatly amplified by today's interconnected world where an incident in one corner of the globe can instantly spark a reaction thousands of miles away, and where a lone extremist can go online and learn how to carry out an attack without ever leaving home."

The cyber domain brings tremendous benefits, but also brings tremendous dangers, he said.

"Threats in the cyber realm are an urgent national security priority, as America has no equivalent to the two wide oceans that have helped safeguard our country's physical, maritime and aviation domains for centuries," Brennan added.

Nations, terrorist organizations, criminals and hackers are trying to penetrate U.S. digital networks, he said.

"Government institutions are under constant assault, and private companies are spending enormous sums of money to defend against hacking attempts, denial of service attacks and other efforts to disrupt their networks," Brennan said.

The North Korean attack on Sony last year highlighted the cyber threat, he said.

"CIA is working with our partners across the federal government to strengthen cyber defenses, to share expertise and to collaborate with the private sector to mitigate these threats," Brennan said. "Together we have advanced our understanding of the threats in the cyber realm."

Lesson to be learned from Torch blaze: Respect fire alarms

Source: http://www.thenational.ae/uae/lesson-to-be-learned-from-torch-blaze-respect-fire-alarms

Feb 25 – Strict procedures are followed by security guards when fire alarms go off in a building – but residents who are used to false alarms often pay little heed.

Alarms are often set off inadvertently by people cooking or smoking, which can lead to a lack of faith in the system.

"If the alarm rings more than three minutes then it should be taken seriously," said a receptionist at the Icon 1 building in Jumeirah Lakes Towers.

"This is when the Civil Defence is informed. But a lot of times people cook and it sets the alarm off so it has to be shut down from our side in that case."

Mohammed A, a resident in Dubai Marina's Bay Central Tower, said the alarm in his building used to go off at least twice a week for no reason.

"The worst is when it would happen at about 3am or 4am. I took my passport and went down with everyone else only to find security guards telling us they were false alarms, so no one takes it seriously anymore."

A security guard at the tower, which was developed by the Select Group, the same company that created The Torch that caught fire on Saturday, said every alarm should be treated seriously.

"We can immediately see on our monitor which unit set off the alarm," he said. "If it is more than one unit that would usually mean a fire has spread. But many times people cook so we switch off the alarm and we go up to their apartment to check if everything's OK. Usually, if residents hear a recorded voice warning asking them to evacuate then it's a fire."

Mohammed said sometimes alarms went off only on specific floors.

"I called the Civil Defence once because the alarm kept ringing for two hours on and off from 6am and I couldn't sleep," he said. "They arrived in 20 minutes and told the security guards they would be fined if they didn't sort the system out. We're getting scared as residents because this is really a safety issue."

Transguard Security Services, the security company at Bay Central, has 4,000 personnel across the country. Each building it is contracted to work for has its own site-specific

major incident plan that includes evacuation procedures.

"Regular drills are scheduled through the building's property

management or facilities management team and carried out in consultation with the Civil Defence," said company director Simon Currie.
"In all cases, residents are informed of any scheduled incident activities through notices in public areas and in the building lifts."
He said all of the company's guards were trained in basic first aid and firefighting skills.
"We also identify key individuals who will receive enhanced training to become certified in these disciplines. Every team member will have been briefed thoroughly on the building's emergency procedures and will know exactly how to react, whether it is a drill or a real incident."
Mr Currie said in the case of a fire alarm, residents should immediately vacate the building.
He said false alarms had more to do with system faults rather than a security team neglecting their duties.
A property management company, Mr Currie said, "should be applying greater pressure on the contractors that have been appointed to manage and maintain the building's fire alarm and other systems to ensure they are functioning properly at all times, because regular false alarms can lead to complacency".
"The on-site security teams are responsible for monitoring the building management systems and for reporting any error messages or faults. These are passed on to the team which then contacts the main fire detection systems contractor for immediate response to the faults."
After an alarm ends, security staff visit the affected area.
"If there is no fire, the main panel is reset. If it is a fire that requires action the alarm is immediately reactivated and the normal building evacuation procedure is carried out."

Robotics and Emergency Management

By Eric Holdeman

Source: http://www.emergencymgmt.com/emergency-blogs/disaster-zone/roboticsandemergencymanagement.html

In the current edition of *Emergency Management* there is the article How Robots Are Changing Disaster Response and Recovery, (see Jan 2015 issue of the Newsletter) which has some interesting

thoughts and comments. First and foremost is this one, "I think if you have a disaster and you're an agency and you haven't figured out a way to use a small unmanned aerial system, it's kind of surprising."
Surprising for the interviewee, but not to me. **I personally don't know of an emergency management agency here in Washington State that has a drone of any size that they are ready to employ.** The one agency that did have one was the Seattle Police Department, and the former mayor told them to get rid of the two they had. I'm not sure how that turned out.
I do like the idea of leasing equipment rather than buying it. With the rapid change in technology and capabilities you are not stuck with a less capable system after only a few years.
There is also the thought of using teams of people to utilize and look at data coming in from a remote system. As stated, "One person will catch something that the other person didn't and it just adds a vast improvement to performance."
The other concepts that struck home for me was the idea that when you capture data you have to first visualize it and then be able to share it. When thinking "share" think regionally: "Who else needs to have this information?"
Lastly, and this is coming, **"We need to act at a distance and not just see at a distance."** This one means that there will be additional capability to our remote sensors. Like a bomb robot that has a disruptor on it to set off a bomb, we will need the capability to perform tasks at a distance.
When will your program add a drone?

Oil Train Derailment in West Virginia Renews Safety Questions

Source: http://www.emergencymgmt.com/disaster/Oil-Train-Derailment-West-Virginia-Safety-Questions.html

A fire burns Monday, Feb. 16, 2015, after a train derailment near Charleston, W.Va. Nearby residents were told to evacuate as state emergency response and environmental officials headed to the scene. *(AP Photo/John Raby)*

The derailments this week of two trains carrying crude oil have raised new questions about the adequacy of federal efforts to improve the safety of moving oil on tank cars from new North American wells to distant refineries.

A 100-car, southbound CSX train derailed Monday in a West Virginia river valley, destroying a home and possibly contaminating the water supply for downriver residents. A thundering fireball rose hundreds of feet above the community amid an intense winter storm.

On Sunday, an eastbound oil train derailed in Ontario, Canada, near the city of Timmins, engulfing seven cars in an intense fire and disrupting passenger service between Toronto and Winnipeg.

The most recent accidents follow a long string of crashes that have occurred amid an exponential increase in the amount of crude being transported by rail, as energy production booms across the U.S. and Canada.

Scrutiny of the rail industry began to intensify after the July 2013 accident in Lac-Megantic, Quebec, in which a train carrying 72 tank cars of crude crashed into the small Canadian town's center and killed 47 people. It was followed by derailments and fires in North Dakota, Alabama, Virginia and elsewhere.

Data compiled by the federal government and the petroleum industry show that there have

been more than a dozen derailments of trains carrying either crude or ethanol since 2009, not including several that occurred in Canada.

The West Virginia accident occurred Monday during intense cold and heavy snow near Mount Carbon, where the CSX rail line winds through a narrow valley carved by the Kanawha River about 60 miles southeast of Charleston.

The train consisted of 109 cars carrying oil from North Dakota to Yorktown, Va., CSX said.

"At least one rail car appears to have ruptured and caught fire," a CSX spokesman said. "The derailment has resulted in the precautionary evacuation of nearby communities, and precautionary suspension of operations at the Cedar Grove and Montgomery water treatment plants."

State safety officials said some of the cars had ended up in the river and were burning.

Adena Village, a residential community along the river, was evacuated. One house was destroyed by fire.

The National Transportation Safety Board has increased its focus on oil tanker safety, and environmental groups are calling for tougher controls.

"Back-to-back fiery derailments involving crude oil trains should be an unmistakable wake-up call to our political leaders: Stop these dangerous oil trains and stop them now," said Mollie Matteson, a senior scientist with the Center for Biological Diversity.

The U.S. Department of Transportation responded last year, reducing speed limits in urban areas and calling for better brakes and stronger standards on rail tank cars so that they could withstand crashes without rupturing.

But the tank car rule is not expected to be unveiled until later this year, and it could be years before it has a measurable effect on safety, depending on how many of the existing 98,000 tank cars have to be retired or retrofitted.

Brigham McCown, former chief of the Pipeline and Hazardous Material Safety Administration, the federal agency that oversees tank car safety, said government needed to cut the number of derailments by such measures as improving brakes, including the introduction of electronically controlled brakes.

Current air brakes are applied sequentially on each rail car, meaning that it takes more than a minute for all the brakes to be applied on a 100-car oil train, he said.

"There are a lot of technical improvements we could be looking at, and I don't think we are," he said.

McCown said most of the derailments have occurred in extreme weather, when rain has washed out rail beds or when intense cold or heat distorts or weakens steel rails.

Infrastructure protectionWireless sensors keep public infrastructure safe

Source: http://www.homelandsecuritynewswire.com/dr20150225-wireless-sensors-keep-public-infrastructure-safe

Feb 25 – European researchers have developed a wireless sensor system to monitor the safety of large infrastructure such as bridges – but also historic monuments. The new system will potentially save lives as the structure ages, and it will reducing construction cost of new infrastructure.

Building structures can be affected by earthquake, landslides, or construction defects from a previous era. But collapse of infrastructures, sometimes tragically resulting in deaths, can be avoided in the future if early-warning sensors are placed on them right from the start.

The challenge of safeguarding major infrastructures — especially those used intensively by the public, such as bridges or historic monuments **— led researchers in the EU-funded GENESI**

project to design a wireless sensor network (WSN) for monitoring structural health.

"You want sensors to work for the whole lifetime of the structure, which could be tens or hundreds of years," explained coordinator Professor Chiara Petrioli, of La Sapienza University in Rome. "This was the technical challenge before us. But we also found we could deploy the sensor networks in construction works, to make design amendments if necessary and safeguard workers on the project."

A CORDIS release reports that cCompared to existing technology, GENESI's sensor networks are non-intrusive and cheap to deploy and maintain. Being battery-driven, they are also suitable for remote areas with no electricity supply and can be used when the power grid is down, such after an earthquake.

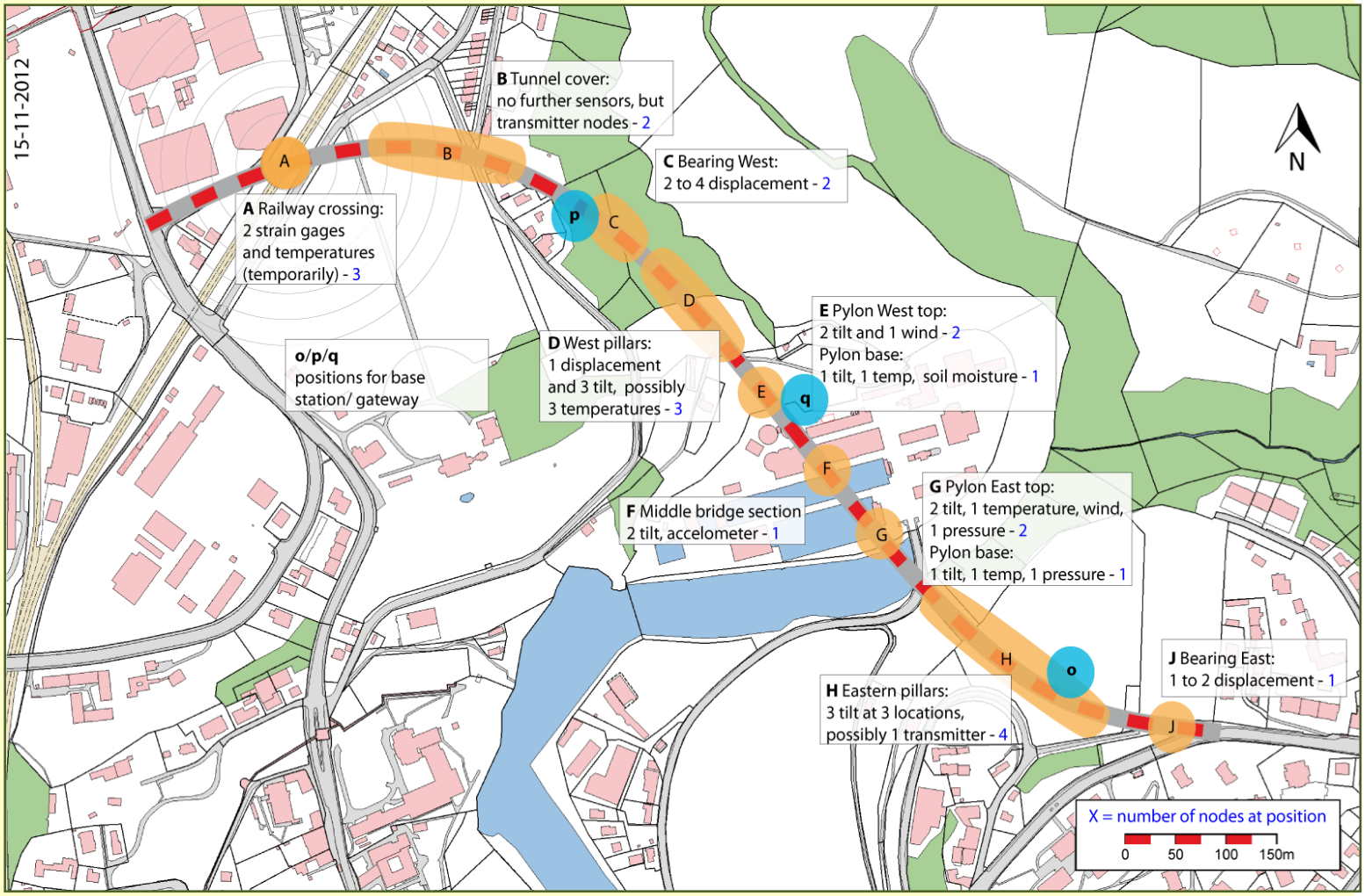
Rome's metro and a Swiss road bridge

The technology was validated at two construction sites: the new B1 metro line in Rome, and the Pont de la Poya bridge in Fribourg, Switzerland.

In the metro, concrete segments of the tunnel final lining, instrumented with GENESI sensors, were deployed directly next to the tunnel-boring machine (TBM) to measure parameters such as strain, temperature and deformation in real time.

The data was fed back via proprietary low power protocols, 3G and Internet to a control and alarm panel supervised by engineers and geologists working on the project. These professionals were able to check if the drilling was being performed with safety of workers and passengers in the metro foremost in mind.

The network is simpler, quicker, and cheaper to install and maintain than traditional cable-connected sensor systems and, in pursuit of long-lasting energy-efficient monitoring of the tunnel when in operation, it is partly powered by micro turbines spinning in the gusts of passing trains.



During the construction of the Swiss bridge, around twenty-five sensors measured parameters such as the pull on the pylons, bearing displacement, and wind, temperature and water levels.
"It proved very useful, because there always are a lot of uncertainties in design, planning and construction," said Holger Wörsching, an engineer with Solexperts AG, a Swiss measurement company and partner in GENESI. "When the bridge was shifted to connect to both sides, we got feedback on deformation and bending and could check the loads were right."

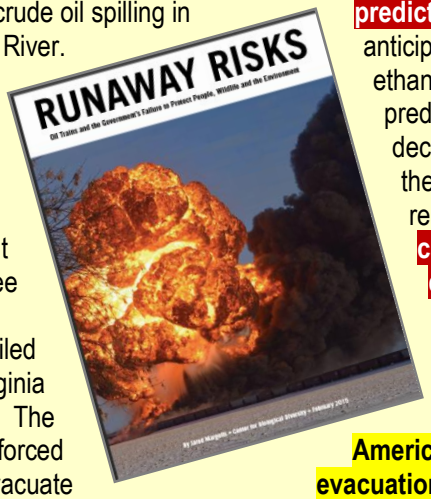
Other applications
Solexperts sees many opportunities for the technology and is now also deploying it in an access tunnel for a hydro plant in Innertkirchen and an Alpine railway line vulnerable to landslides.
CORDIS notes that a GENESI spin-off company (Wsense), employing six people, is also exploring the deployment of a miniaturized version of the GENESI system to monitor Italy's many public heritage sites. Wsense is helping the country's Ministry of Cultural Heritage with another, previously-unimagined application: the precarious task of transporting artworks between museums.
The FP7 has invested in GENESI to the tune of €2 million. The project ran from April 2010 to August 2013 and involved seven partners in four countries.

▶ **Read more on GENESI Project at:** http://genesi.di.uniroma1.it/

Cost of derailments of oil-carrying trains over the next two decades: $4.5 billion

Source: http://www.homelandsecuritynewswire.com/dr20150226-cost-of-derailments-of-oilcarrying-trains-over-the-next-two-decades-4-5-billion

Feb 26 – The Virginia Department of Environmental Quality has proposed a $361,000 civil fine against CSX Transportation Inc. for a 2014 derailment that led to roughly 30,000 gallons of Bakken crude oil spilling in and around the James River.
The agency also wants CSX to pay $18,574 for costs associated with investigating the spill, which occurred after seventeen oil tankers went off track, with three launching into the river.
Another CSX train derailed last week in the West Virginia town of Mount Carbon. The explosion that followed forced about 1,000 people to evacuate from their homes. Authorities are still investigating what cause that derailment.
The United States will likely experience more oil train derailments as long as Bakken crude oil is transported via rail from the Northern Plains' Bakken region to U.S. refineries. The*Morgan Messenger*, citing a July 2014 analysis by the U.S. Department of Transportation (DOT), reports that federal authorities expect oil train accidents to be commonplace in the United States over the next twenty-years. **Roughly ten derailments will happen each year, the department predicted.** "Based on past accident trends, anticipated shipping volumes and known ethanol and crude rail routes, the analysis predicted about 15 derailments in 2015, declining to about five a year by 2034," the AP reports, adding that DOT researchers expect **oil derailments to cause at least $4.5 billion in damages over the next two decades.**



A study by the Center for Biological Diversity (CBD) reports that an estimated **twenty-five million Americans live within the one-mile evacuation zone that DOT recommends in the event of an oil train derailment.** "The reality is that there's no way to safely transport highly volatile crude from the Bakken oil field in North Dakota or heavy crudes from the Alberta tar sands," said CBD's Jared Margolis. "Instead these fossil fuels should be left in the ground, both for our safety now and to

avoid the impending climate catastrophe."
At least twenty-one oil train and thirty-three ethanol train accidents involving a fire, derailment, or significant amount of fuel have occurred in the United States and Canada over the past nine years. Regulators are now renewing calls for stronger tank cars and effective braking systems, along with other safety improvements. "This underscores why we need to move as quickly as possible getting these regulations in place," said Tim Butters, acting administrator for DOT's Pipeline and Hazardous Materials Safety Administration (PHMSA).
Oil train accidents often lead to pipeline advocates pushing for more pipelines, but data from PHMSA shows that **while oil trains have more frequent accidents, pipelines accidents cause much larger spills. Between 2004 and 2012, pipelines in the United States spilled three times as much oil as oil trains did**, according to an International Energy Agency study based on DOT data.

▶ **Read the CBD Study at:**
http://www.biologicaldiversity.org/campaigns/oil_trains/pdfs/runaway_risks_web.pdf

Press Release: The first Innovation in the world to extinguish major fires

2/24/2015
Source: http://www.hub911.com/hub911-products-blog/press-release-the-first-innovation-in-the-world-to-extinguish-major-fires

The new invention deals with all the major fires: (Forests, Petroleum, Factories, High-rise buildings, Merchandise Store, Also for disengagement rioters) The invention has been designed on a CH47 plane.

Invention system
Achieving a visual contact with the fire target, and determinate the spot flame, and the ignition area, hen the authorized specialist will activate the system program.
The plane fly's at a high nearly equal to 40º of the air temperature surrounding the ignition area. A pumping instrument for fire extinguishing materials will be air-dropped. The width of the water fire tube is zooming, and could easily control a 40m burning area in a minute.

The pressure bar power of the water fire fighters rush is 16bar. Taking into consideration, that the invention system works independent without the need of human factors (fire fighters) as it differs from the traditional wags normally using in fire fighters. Also the new invention is able to extinguish large fire in ideal time comparing to the current fire fighting plane which actually does not work effectively to extinguish fires.

It is my pleasure to present an actual clarification for the invention system, in case of the seriousness of he contract or the implementation, and I'm ready for an immediate implementation with the for modern inventions all over the world.

The invention has been registered and authorized by the academy of scientific research in Egypt, and has been published at the official newspaper.

Mustafa Elnahrawy
Researcher and consultant
At the Civil Protection Council of scientists Egypt

Mall of America Showcases Security after Video Threat

Source: http://www.emergencymgmt.com/safety/Mall-America-Showcases-Security-after-Video-Threat.html?elqaid=25865&elqat=1&elqTrackId=C6F2161993CF4AF7546C9FA09CA0706F

The Mall of America is visited by 40 million people annually. Photo courtesy of the Mall of America.

Feb 24 – Facing a terror threat and a nervous public, the Mall of America pulled back the curtains halfway on its security operations Monday, signaling how seriously it takes safety issues.

For the first time, reporters were shown MOA's underground operations center, along with its corps of bomb-sniffing dogs, its officer-training exercises and security at its hardened loading dock where "vehicles are getting swabbed down and checked" for explosives, an official said.

"This is a safe place," Bloomington Police Chief Jeff Potts told reporters inside the megamall. "We encourage people to come on out and shop."

Mall of America officials have said for two days that they've scaled up their security operations, both those visible to the public and those that aren't.

On Monday, as the terror warning continued to be national news, mall officials decided to invite reporters to witness how extensive its security operations are.

Mall security and Bloomington police wouldn't talk about every security measure Monday. But they signaled that MOA has been dealing with terrorism concerns for years, and has responded with layers of safeguards.

"We've dealt with this thing in the past," Potts said Monday. "There was a statement in the video (Saturday) that mentioned Mall of America. It was very general; there were no specifics.

But we've built contingency plans for years."

The immense size and worldwide fame of Mall of America has made it a bit of a target at least since 2001, when the first reports surfaced that terrorist cells had scouted out iconic U.S. properties, including Disneyland and what was then called Sears Tower in Chicago.

In the years since, officials have steadily ratcheted up security at MOA and other landmark properties, even as the public has

grown accustomed to the alerts and continued to go about their business.
Shopper traffic at the megamall was heavy Saturday, then a bit lighter on Sunday as the temperature plunged and the news spread. By Monday afternoon, traffic inside MOA was very light, but officials didn't attribute that to a terrorism scare.
"Today is Monday in Minnesota when it's 10 below," said mall spokesman Dan Jasper. "So it's like any other Monday in Minnesota when it's 10 below."
Chief of MOA Security Doug Reynolds highlighted some of the multiple security layers at the mall, including a group of five dogs that have a single purpose: sniffing explosives. The dogs are chosen both for their detection abilities and for not looking scary to children and other shoppers.
Whenever the mall is open, at least two dogs are always on duty -- and sometimes, more than that, Reynolds said.
Officers on bicycles are always patrolling the perimeter, watching for anything suspicious.
A network of "hundreds" of security cameras feeds into an underground center, which also includes banks of video screens, communications equipment and computers.
And inside the mall, teams of mall security and Bloomington police officers are patrolling the corridors.
In an underground training room, security training supervisor Lt. Zach Hamann demonstrated how he put security trainees through their paces, part of a four-month-long required training regiment, Reynolds said.
MOA security has been such a fixture that in 2010, it was featured in a reality program on TLC, called "Mall Cops: Mall of America." The series ran for 12 episodes and drew solid ratings, but Reynolds said MOA rejected a proposal to extend the series for three years.

Behavior Profiling Redefines Security at the Mall of America

By Elaine Pittman | February 6, 2013
Source: http://www.emergencymgmt.com/safety/Behavior-Profiling-Security-Mall-of-America.html

After 9/11, the owners of the Mall of America handed the facility's security director a blank check. They wanted the mall to be outfitted with cameras and metal detectors, but Security Director Doug Reynolds didn't think that was the right solution. While the tech tools would aid security efforts, Reynolds didn't think they were the best fit for the unique facility that he is charged to protect.
The term "mall" doesn't provide a complete picture of the Mall of America. Located near Minneapolis in Bloomington, Minn., the facility is visited by 40 million people annually and spans 4.2 million square feet. Not only does it house the stores one would expect to find in a shopping mall, but it also features the United States' largest indoor theme park complete with roller coasters, an aquarium and a movie theater. In addition, a hotel is scheduled to open early this year. All of these attractions combine to create an extraordinary environment for a security department.
Reynolds surveyed different security methods and industry standards, but none of the conventional approaches in the United States seemed to be the best fit for the Mall of America. "We thought cameras were good but they were missing an element, which ended up being the human element," he said.
Looking to Israeli security methods, Reynolds learned about how behavioral profiling is used in the country, especially at Tel Aviv's Ben Gurion International Airport. He attended training in Israel to better understand how the technique is used and how security officials there have improved it.
"Most people think that behavioral profiling started in Israel but it did not; it actually started in the U.S. through the FBI to do different types of profiling for crimes, such as serial killers, sexual predators, that kind of thing," Reynolds said. "The Israelis — when they were looking for best practices — found the FBI doing it, and they took it on and honed the skills and perfected the science behind it."
A former Israeli Airports Authority security agent, Michael Rozin, was brought onto the Mall of America's security team to help adopt the country's behavioral profiling principles to the public environment at the U.S. facility. Rozin and Reynolds worked to

create the mall's Risk Assessment and Mitigation (RAM) program, which instead of relying on technology to help identify a potential security risk, uses trained officers who look for behavior that isn't considered normal in the mall's setting.

The Mall of America's security department consists of about 150 people with the lion's share constituting what most people consider typical security. RAM personnel make up a small percentage of the department's staff, Reynolds said, but all security personnel are exposed to the program and its concepts. "A handful are given the additional 10 to 12 weeks of training in it," he said.

The RAM officers work in what Reynolds described as "visually undercover" — they wear plain clothes and ear pieces, but visitors can spot the officers if they're looking for them.

"We want people to see them. We want them to know they're out there," Reynolds said. "If it's a person with harmful intentions then they think that this thing, I don't know what it is or how big it is, but it's there, it's a factor and this is not the place to commit the crime."

Although the behavior profiling program was adapted to fit the Mall of America's environment, it uses the same three components as Ben Gurion airport: detecting suspicious indicators, security interviewing (which Rozin said is the most important) and operational deployment.

RAM officers look for behaviors or objects that are not considered normal in the mall. And once something suspicious is observed, RAM officers look into the situation further and if it involves a person, they conduct a security interview to get more information. "Here it's very different because in an airport setting you are somewhat expected to answer some questions, especially in Israel where everyone has to go through an interview session before they board a flight," Rozin said. The interview techniques had to be adapted to fit the public environment of the mall including how RAM officers approach people and obtain cooperation as well as the way they ask questions. The principles of interviewing are maintained and what officers are looking for are the same, but the method differs.

Is observing behavior and talking to people more effective than a security measure like using metal detectors? Rozin believes so, highlighting what he said are the two main factors that create acts of violence: intent and means or weapons.

"If you look through the years both in the United States and overseas, you see that the weapon itself as a factor has constantly been evolving and changing," he said. "Bad guys have the ability to outsmart technology like metal detectors, X-ray machines, whatever is out there and come up with a weapon they can get into the secure environment and use to attack."

Ultimately the Mall of America's RAM program seeks to deter people with harmful intentions from coming to the facility. Rozin said technology, like metal detectors, doesn't necessarily deter someone; instead they just pose a challenge. "What creates true deterrence is an unpredictable system — a security system that is there and looking for intent constantly," he said.

And this highlights the importance of the security interviews. Asking the right questions at the right time is a problem for anyone with harmful intentions, according to Rozin. In one example of how the right questions can unravel a person's lies, during a security interview, RAM officers identified a man who had been going onto military bases, although he wasn't in the military.

Reynolds said that a couple of years ago, two RAM officers were nearing the end of their shift and walking down a parking ramp when they passed a man wearing a Marine Corps uniform who was waiting for the elevator. The RAM officers continued walking down the parking ramp until one said he got a weird feeling about the man in uniform and the other agreed. They found the man still waiting for the elevator, identified themselves and asked if they could talk to him. Reynolds said they asked him if he was in the military and he said he was a sniper. A RAM officer asked what his longest shot was and he didn't know. They went on to inquire about the rifle he used and he didn't know answers that they thought he should have. The officers identified the man's car and saw an Air Force uniform in the backseat as well as a U.S. Department of Defense sticker on the vehicle.

The police were called and the Defense Department sticker was identified as legitimate, but as the interview continued, the man's story fell apart. "It turned out he was a runaway and his guardians were retired members of the military,"

Reynolds said. "As a dependent of a retiree, you're given an ID card that lets you on military bases and [gives] access to a place called clothing and sales where you can buy uniforms." The man had created a false identity by going onto bases and listening to the conversations of military members.

Securing the Mall of America isn't strictly an internal function. The security department has created a "solid" relationship with the Bloomington Police Department, said Reynolds acknowledging that as a private entity, the mall has limitations and must rely on other law enforcement. Local agencies become involved when the security interview reaches a point at which additional information is needed or if someone provides a fraudulent identification card. In addition, the mall has provided awareness training to law enforcement officers on the RAM program and its security procedures, which Reynolds said makes things run more smoothly when they are called to the mall. "Certainly a big piece on that is to be able to articulate to the responding police officer why we called the police over."

Reynolds also attributes the program's success to the use of red teaming, where a scenario is created that should get the attention of a RAM officer. Indicators are set up in an area and the officer is watched to see how he or she responds and how the interview process goes. Reynolds said red teaming is critical because the program is relatively new (it's been in use in the Mall of America for about five years) and the testing process not only helps him know if something isn't being taught properly, but it also ensures that the officers are always aware of their surroundings.

Another aspect that's been key to the program's success has been enlisting the help of everyone who works for the mall — from sales clerks to janitors. Reynolds said they are the subject-matter experts of their areas and notice when something doesn't match typical behavior in that setting.

"We would not be as successful as we are without utilizing all of the different entities, whether it be other departments or, even to a degree, guests," he said. "We have guests that come to us and tell us when something doesn't look right."

Reynolds has presented the program to a diverse range of groups, and Rozin is now working as a consultant to educate others about behavior profiling and how it could fit into their security processes. "We want people to know about this program," Reynolds said. "We want this to be the new industry standard."

Expanding Practice

When the Mall of America began its behavior profiling program about five years ago, it was breaking new security ground in the U.S. "When you step outside of what society is used to, there is always risk, and we told folks ... that there are going to be people who don't know what the program is about," said Security Director Doug Reynolds.

The risk seems to have paid off. Behavioral profiling is being embraced by other U.S. security officials, and Michael Rozin is using his experiences from helping launch the mall's program and being a security agent for Ben Gurion International Airport in Tel Aviv where the method is used.

For example, the security director for the Greenway Plaza business complex in Houston adopted the program about a year and a half ago. It's also being expanded into school systems.

Timothy Kingsley, associate vice president of operations and government affairs for American Security and Investigations, said a good job has been done in academic environments to identify students who may be experiencing a crisis, but an appropriate system must be in place to identify key indicators of a possible future event.

"We have had an unprecedented amount of events in the last decade surrounding active shooters and what I call catastrophic crimes in the workplace," Kingsley said. "I think it's time that we really start not looking for the weapon — of course always look for those things — but let's look for the common denominator. Human beings have similar behaviors."

American Security and Investigations is in the early stages of rolling out the program in a Minnesota school district. He said key staff members in the company are being trained first, but eventually it could be a districtwide awareness campaign and not limited to security personnel. Kingsley said the company also is looking to use behavior profiling in other environments, including hospitals and commercial real estate.

Elaine Pittman is the associate editor of Emergency Management *magazine. She covers topics including public safety, homeland security and lessons learned. Pittman is also the associate editor for* Government Technology *magazine.*

Police Taking Page from the Military by Saving Lives with Tourniquets

By Adam Stone

Source: http://www.emergencymgmt.com/safety/Police-Page-Military-Saving-Lives-Tourniquets.html?elqaid=25865&elqat=1&elqTrackId=CB721838544D1D3EE3524DA98D2685EB

Beside the horrific nature and senselessness of the acts, the Sandy Hook shooting and the Boston Marathon bombing share a critical commonality. In both cases, many of the fatalities were caused not by the immediate blast or bullet, but by rapid and catastrophic bleeding. It's an increasing phenomenon that can be prevented.

With this in mind, many police departments and public safety advocates have turned to a simple solution in recent years, a tried-and-true method for emergency response to traumatic bleeding. It's the return of the tourniquet.

"The name of this game is to stop bleeding to death, so you need to be empowered to stop the hemorrhaging. Can you do that? Yes, you can," said Dr. Lenworth Jacobs, director of trauma and emergency medicine at Hartford Hospital in Connecticut.

In the wake of recent violent events, and with the backing of the American College of Surgeons, Jacobs founded the Hartford Consensus. This interagency task force encourages police and other first responders to train on, and be equipped with, tourniquets as part of their regular routine.

The trend toward tourniquets as a first responder tool comes in large measure from the experience of U.S. military forces in Iraq and Afghanistan over the past decade. **As far back as 2005, the military has recognized the value of the simple constrictive devices, which can cost between $15 and $30 each. At that time, some 38,000 nylon and plastic tourniquets were arriving at a staging area in Qatar, the first of 172,000 being rushed to the war zone, as reported in *The Baltimore Sun*. The Marine Corps was expecting to order more than 200,000 tourniquets.**

That evolution came in response to a military study that found battlefield deaths from blood loss had not changed much since Vietnam, when about 7.4 percent of fatalities bled to death, the Associated Press reported at the time. Early on in the Afghanistan war, bleeding still caused about 7.8 percent of deaths.

Researchers declared that applying a tourniquet could cut those numbers. **The military responded and by 2011, deaths from bleeding extremities had dropped to 2.6 percent.**

Police Sign On

Under the guidance of the Hartford Consensus, law enforcement has been applying those lessons as well. Since 2013 some 200,000 police officers have begun to carry the devices, along with all FBI officers, Jacobs said.

The new tool is needed in response to the changing nature of emergencies, especially the rise of large-scale attacks in public places. Explosives are becoming more common, and the munitions in use are evolving too.

"When you are shot with a .22 or a .32 [caliber round], that bullet is generally going fairly slowly, so if it hits something fairly important like the liver or a major blood vessel, then you face the likelihood of being seriously injured or dying," Jacobs said.

Today's shooters on the other hand are more likely to be armed with high-speed military ammunition. "That blows things off and creates massive bleeding," Jacobs said. Rather than dying immediately from the blow, "now you have a high likelihood of bleeding to death — but it is fast, within five or 10 minutes. So you need to have an immediate response."

While the Hartford Consensus has had considerable success in making its case among law enforcement professionals, there have been challenges along the way.

There's the money, of course, and the time and expense of training. And there are mindset issues as well. Police officers have been trained to control a crisis scene, to stop the bad guy, "and if you were bleeding to death they would step right over you to complete that mission," Jacobs said.

The military, on the other hand, works on a buddy system. "If your buddy gets shot, you drop off and let your comrades carry on the mission," Jacobs said. In civilian life, that means you stop the bleeding while others continue the crisis response. Police officers generally aren't conditioned to think along those lines, so tourniquet advocates have needed to drive new ways of thinking.

C-A-T tourniquet

The Hartford Consensus has been able to close the gap thanks in large measure to its broad base of membership. Representatives of major city police, fire and EMS departments all have been a part of the effort, thus helping to ensure a measure of buy-in from across the user base.

Boston police officers got 1,500 tourniquets and training within a month after the bombings in 2013. In Dallas, where police officers have been issued tourniquets, Lt. Alex Eastman said it's about time. "I've been pushing for this for years," he told New Jersey's *Courier Post*. "But I think it was the Boston experience that pushed people to act."

It has already paid off. A man was shot in the leg on Feb. 7 in an Allegheny County, Penn., mall, suffering a torn femoral artery. A police officer on the scene acted quickly with his department-issued tourniquet to staunch the heavy bleeding and save the man's life. The officer and his colleagues were issued tourniquets last September.

In the long run, Jacobs would like to see tourniquet use expand beyond first responders, to assume a place in the public understanding as common as the Heimlich maneuver or CPR. One day, security guards in public spaces should all have tourniquets in their emergency supplies, right alongside the automatic external defibrillator.

"The goal is to put them in universities, in malls, in ballparks," Jacobs said. "You want people who are close to the problem to be educated and to have access to these things."

Adam Stone is a contributing writer for Emergency Management *magazine. Stone writes on business and technology from Annapolis, Md. He also contributes to* Government Technology *magazine.*

EDITOR'S COMMENT: Ideal additions apart the C-A-T tourniquets: (1) modern haemostatics like QuikClot (and similar products); (2) chest seal Asherman; and (3) an escape hood (for CBRN and smoke). Either on the belt or at least in the police car! Extremities' bleeding and pneumothorax accounted for ~90% of KIA in modern wars! In recent times police officers confront criminals and terrorists bearing military grade weaponry!

How long should an emergency message be to prove effective?

Source: http://i-hls.com/2015/02/how-long-should-an-emergency-message-be-to-prove-effective/?utm_source=Israel+Homeland+Security+%28iHLS%29&utm_campaign=9e7112f7bb-Newsletter_English_4_3_2015&utm_medium=email&utm_term=0_8ee2e16ed1-9e7112f7bb-87373033&mc_cid=9e7112f7bb&mc_eid=521c0e089a

Short 90- and 140- character wireless emergency alert messages delivered over mobile devices are "substantially less effective" than much longer messages to spur people to take action in case of a hazard, a recent study concluded.

According to *Fierce Homeland Security*, the study from the National Consortium for the Study of Terrorism and Responses to Terrorism, or START – a research and education center based at the University of Maryland – also found that rearranging the content within the message and including a map showing an area that's been affected by a hazard could also improve public responses.

Among the findings, the study said that shorter messages were less effective "at helping people overcome their pre-conceived perceptions about different hazards and likely would be less effective at guiding people to take protective actions appropriate to the risk they face in an actual event."

While, obviously, shorter messages didn't have as much information as a message 1,380 characters in length, the study said that 90-character messages can be rapidly disseminated and reach affected populations faster.

The study also found that rearranging the content in a 90-character message could improve public response. Currently, such messages follow a certain order: hazard, location, time, guidance and source. Rearranging them by source, guidance, hazard, location and time improved outcomes, but the arrangement may be different for 140-character and 1,380-character messages.

Another finding was that including a high-information map – as opposed to a low-information one – in 90-character messages had a "statistically significant and positive effect" on outcomes. It "improved most participants' understanding, belief and risk personalization across all message lengths," the study said.

It should also be noted that length is critical to a mass communication. "Brevity is the soul of wit", but even more importantly, it is emergency related. Mass communication alerts have typically been sent for extreme weather bulletins or when there is a dangerous situation taking place at a specific location, such as a particular building on a campus or business site.

Now that alerts have become broader in scope, it is becoming more common to see alerts about event notification; to alert of upcoming, canceled, or even impromptu events attendance alerts; in an educational setting, this can alert parents and faculty when a student is tardy or absent; road closure: for maintenance reasons or some emergency. The applications are endless.

OMAN – National Multi Hazard Early Warning System to be launched on March 22

Source: http://www.muscatdaily.com/Archive/Oman/National-Multi-Hazard-Early-Warning-System-to-be-launched-on-March-22-3vv1

The National Multi Hazard Early Warning System (NMHEWS) will become operational on March 22 when a two-day conference on Reducing Tsunami Risk in the western Indian Ocean will begin in Muscat.

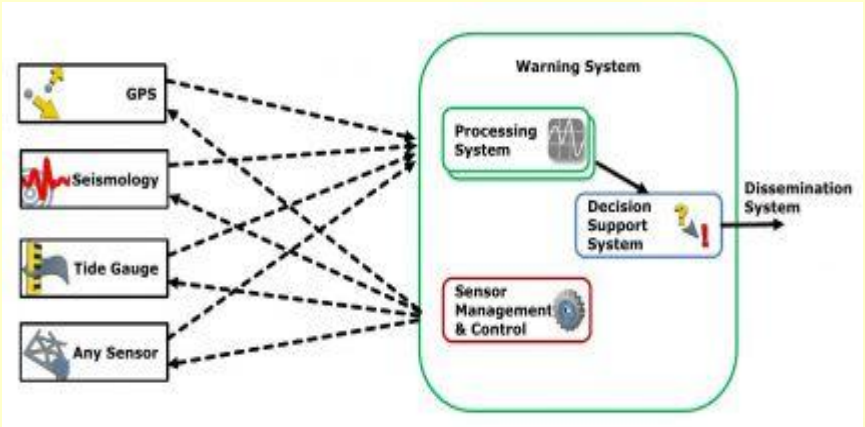
The conference is being organised by the Directorate General of Meteorology and Air Navigation (DGMAN) along with the Intergovernmental Oceanographic Commission of Unesco (IOC-Unesco).

Oman, just like many countries in the Indian Ocean, is affected by different hazards on different time scales from seasonal, to yearly, to decadal to centuries. "Since these hazards are not frequent, it is not cost effective to establish an Early Warning Centre with complete infrastructure and trained personnel dedicated for just one particular hazard," said a senior official at DGMAN.

He added that the Makran Subduction Zone is no doubt a potential threat for generating a local tsunami that may affect the Oman coastal areas within 30 minutes, but it is not certain.

One of the seven new stations along the coast of Oman

To overcome this scenario, Oman embarked on a multi hazard approach to establish a state-of-the-art NMHEWS with the assistance of IOC-Unesco in implementing the required infrastructure for tsunami and other hazards such as tropical cyclones, storm surge, severe



weather, flash flood, sand and dust storm etc.
"The most important milestone in implementing this multi hazard approach is to guarantee sustainability in the most cost effective manner as opposed to establishing infrastructures for individual dedicated centres supporting typically one hazard," said the official.
The conference will bring more than 60 participants from diverse fields together with modellers, geologists, and seismologists, infrastructure specialists, and communication experts.
The gathering will help facilitate collaboration in diverse areas.

These expected outcomes are intended to yield better understanding of tsunami generation in the western Indian Ocean and the greater efficacy of the region's early warning systems.

Some of the papers to be presented at the conference include, Comparison between the 2007 Cyclone Gonu Storm Surge and the 2004 Indian Ocean Tsunami in Oman and Iran, Probabilistic Tsunami Hazard along the Coast of Oman and Maximum Probable Earthquake from Eastern Makran Subduction Zone among others.

Tech Trends for Digital Volunteerism - An Introduction

Source: http://www.disasternet.co/blog/2015/3/9/tech-trends-for-digital-volunteerism-an-introduction

Recently, there has been a surge of groups and tools supporting digital volunteerism. Digital volunteers are "a new breed of people willing and able to respond is emergencies — ones with technical skills. These are digital volunteers who, whether they can code or simply use a computer or mobile device, are saying 'I want to help, so help me help!' They generally fall into two categories: 1) I have a technical skill [novice to advanced] that could help, or 2) I am not near the disaster and can't be there in person, but I want to help. They are not mutually exclusive."

In the spirit of pushing this concept forward, I was recently asked to present on this topic to a number of non-profits that support disaster relief efforts. Below is the presentation that outlines existing digital volunteer groups as well as some common tools. There are of course many more tools, but this should provide a brief introduction.

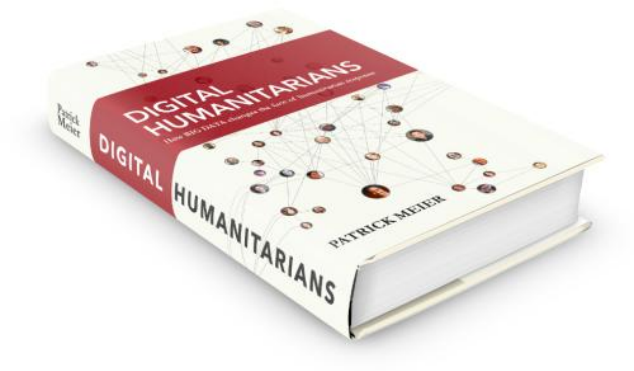
▶ **Watch the presentation mentioned above at source's URL.**

NEW BOOK – Digital Humanitarians: How Big Data is Changing the Face of Humanitarian Response

By Patrick Meier (author – Taylor and Francis Press; Spring 2015)
Source: http://irevolution.net/book/

The overflow of information generated during disasters can be as paralyzing to humanitarian response as the lack of information. Mobile phones, orbiting satellites and humanitarian UAVs each generate vast volumes of data during major disasters. This flash flood of information is often referred to as Big Data, or *Big Crisis Data.* Making sense of this overflow of information is proving to be an impossible challenge for traditional humanitarian organizations, which is precisely why they're turning to *Digital Humanitarians*.

Who exactly are these Digital Humanitarians? They're you, me, all of us. Digital Humanitarians are volunteers and professionals from the world over and from all walks of life. What do they share in common? The desire to make a difference, *and they do* by rapidly mobilizing online in collaboration with international humanitarian organizations. In virtually real-time, they make sense of vast volumes of social media, SMS and imagery captured from satellites and UAVs to support relief efforts worldwide. How? They craft and leverage ingenious crowdsourcing solutions with trail-blazing insights from artificial intelligence.



This book charts the sudden and spectacular rise of Digital Humanitarians by sharing their remarkable, real-life stories, highlighting how their humanity coupled with innovative solutions to Big Data is changing humanitarian response forever. *Digital Humanitarians* will make you think differently about what it means to be humanitarian and will invite you to join the journey online.

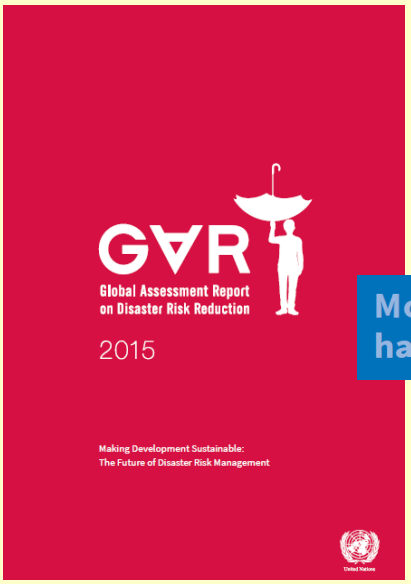
Patrick Meier, PhD, is an internationally recognized thought leader on humanitarian technology and innovation. Author (2015): "Digital Humanitarians: How Big Data is Changing Humanitarian Response." Previously: Harvard Humanitarian Initiative, United Nations, World Bank. Currently: QCRI. PhD from Fletcher School, Pre-Doctoral Fellow at Stanford and MA at Columbia. Born & raised in Africa.

▶ **Read also:** http://irevolution.net/2013/04/09/humanitarianism-network-age/

GAR 2015

Source: http://www.preventionweb.net/english/hyogo/gar/2015/en/gar-pdf/GAR2015_EN.pdf

The fourth edition of the United Nations *Global Assessment Report (GAR) on Disaster Risk Reduction* is being issued at a pivotal moment for the future of development.



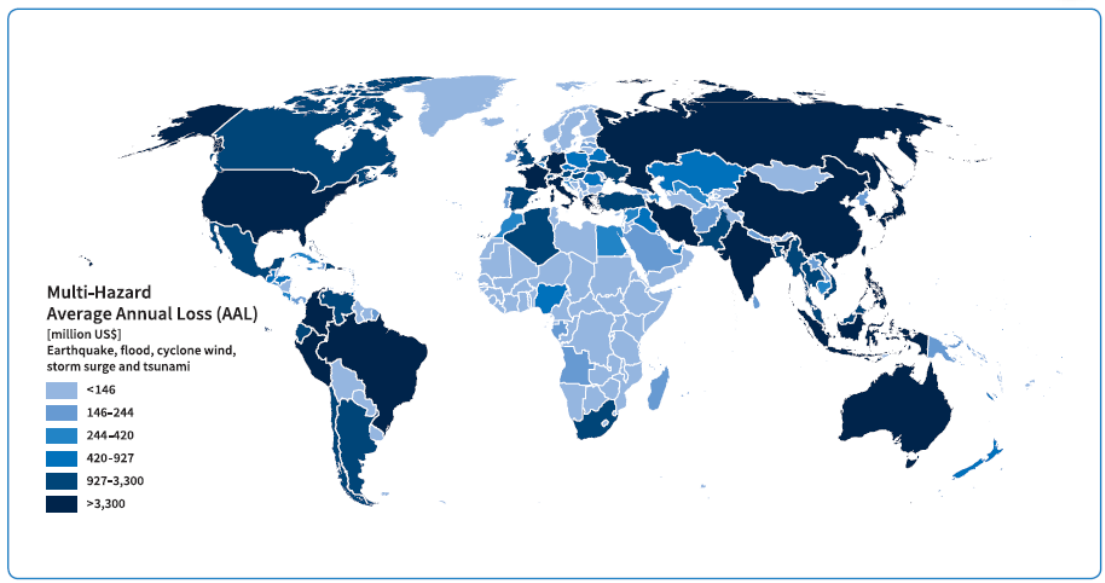
In 2015, the global community is aiming to adopt an ambitious set of sustainable development goals and a meaningful, universal agreement on climate change. Disaster risk reduction can play an important role in advancing these agendas through its close links with poverty reduction, sustainable growth and shared prosperity.

As we prepare for the third *World Conference on Disaster Risk Reduction* in Sendai, Japan, it is crucial

Most disasters that could happen have not happened yet.

to understand and act upon the messages of this report. Many countries continue to face large potential losses from disasters – especially those which can least afford to invest in future resilience. Global models suggest that the risk of economic losses is rising as a result of the rapidly increasing value of the assets that are exposed to major hazards. In addition, a large proportion of losses continue to be associated with small and recurring disaster events that severely damage critical public infrastructure, housing and production – key pillars of growth and development in low and middle-income countries.

Governments, civil society and the private sector have the opportunity and obligation to work together to



commit to a safer future. A more inclusive and ambitious framework for disaster risk reduction is crucial

Economic losses from disasters such as earthquakes, tsunamis, cyclones and flooding are now reaching an average of **US$250 billion to US$300 billion** each year. **Future losses** (expected annual losses) are now estimated at US$314 billion in the built environment alone. **This is the amount that countries should set aside each year to cover future disaster losses.** (→ Chapter 3)

The mortality and economic loss associated with **extensive risks** (minor but recurrent disaster risks) in low and middle-income countries are **trending up.** In the last decade, **losses due to extensive risk** in 85 countries and territories were equivalent to a total of **US$94 billion.** (→ Chapter 4)

Extensive risks are responsible for most **disaster morbidity** and **displacement,** and represent an ongoing **erosion of development assets,** such as houses, schools, health facilities, roads and local infrastructure. However, the cost of extensive risk is not visible and tends to be **underestimated,** as it is usually **absorbed by low-income households and communities and small businesses.**

to our efforts to build a better world for all. Together, let us ensure that development is resilient and sustainable.

PreparedEx Now Offering Fully Scalable Version of LaunchPAD

Source: http://www.preparedex.com/press-release-preparedex-announces-launch-of-crisis-simulation-application/

March 18 – PreparedEx, the leading crisis, emergency, business continuity and security management company, today announced the introduction of a fully scalable version of its crisis simulation application called LaunchPAD. The new product now enables small-to-medium-size organizations to cost-effectively

conduct realistic crisis exercises with the same sophisticated tools and expertise LaunchPAD currently provides to large multi-nationals.

Organizations of any size and geographical footprint can now use LaunchPAD to test their crisis plans and the performance of their response teams in highly realistic and rapidly changing crisis simulations. Organizations can conduct exercises using simulations tailored to their training needs, such as a natural disaster, workplace violence, pandemic, cyber-attack or fire scenario. During the exercise, the application records the response teams' actions at each step as the distressing scenario unfolds, creating a record for after-action review and assessment.

"We're excited to offer this new version of LaunchPAD for improving crisis preparedness. Its scalability and flexibility can now put this vital tool into the hands of any size organization," said Rob Burton, founder and managing director of PreparedEx. "LaunchPAD's ability to improve crisis preparedness and response not only benefits the organizations but also benefits the societies in which they operate."

LaunchPAD is accessed securely through a web browser via most web-enabled devices permitting an organization's response teams to collaborate during the exercise from wherever they might be in the world — as would invariably be the case during an actual crisis. Exercise participants coordinate their responses within the system via the response interface, or they can utilize their own existing documentation record-keeping procedures as they conduct the sessions.

LaunchPAD allows organizations to design their own crisis scenarios and gives them the option to use the PreparedEx crisis experts to supplement the scenario with multi-media "injects" that move the scenario forward to make the exercise realistic and engaging.

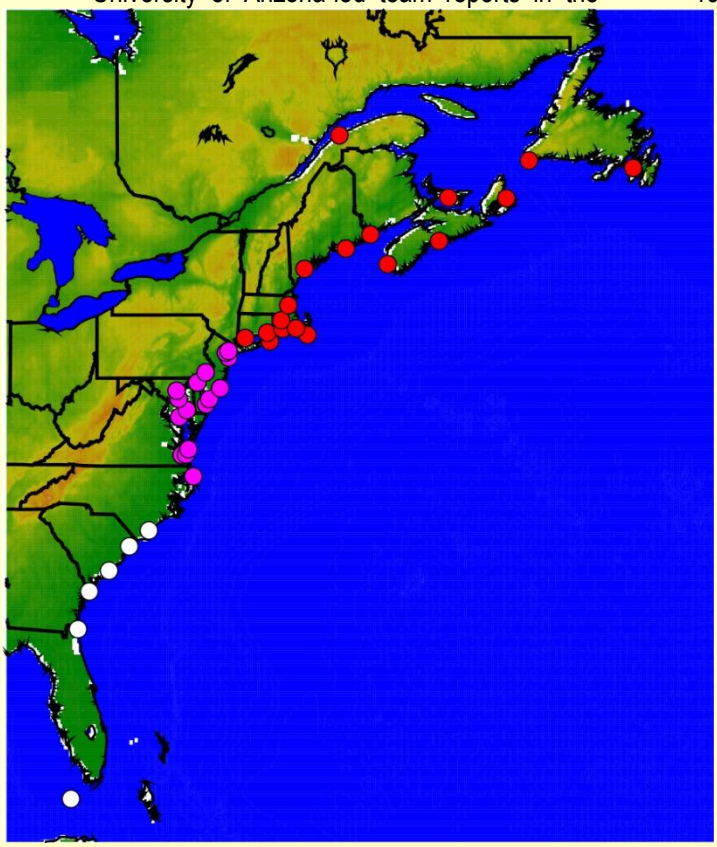
At the end of each scenario, LaunchPAD stores the session so it can be reused in the future to remind existing team members or to bring new team members up to speed. LaunchPAD also produces a PDF report at the end of each session.

LaunchPAD is ideal for any organization that is serious about contingency planning. The application is offered based on an annual subscription through Bronze, Silver, Gold and Platinum packages.

A 2-year spike in sea level along NE North America

Source: http://www.homelandsecuritynewswire.com/dr20150226-a-2year-spike-in-sea-level-along-ne-north-america

Sea levels from New York to Newfoundland jumped up about four inches in 2009 and 2010 because ocean circulation changed, a University of Arizona-led team reports in the recent issue of *Nature Communications*.



By using historical data from the 40 tide gauges shown on this map, UA geoscientist Paul Goddard and his colleagues determined that sea level rose four inches from New York to Newfoundland (red dots) in 2009 and 2010. Gauges from New York south to Cape Hatteras (pink dots) showed a smaller spike in sea level for the same time period. No sea level spike was recorded on the gauges (white dots) south of Cape Hatteras. (Image credit: Paul Goddard/UA Department of Geosciences)

The team was the first to document that the extreme increase in sea level lasted two years, not just a few months.

"The thing that stands out is the time extent of this event as well as the spatial extent of the event," said first author Paul Goddard, a UA doctoral candidate in geosciences.

A UA release reports that independent of any hurricanes or winter storms, the event caused flooding along the northeast coast of North America. Some of the sea level rise and the resulting flooding extended as far south as Cape Hatteras.

The paper is also the first to show that the unusual spike in sea level was a result of changes in ocean circulation.

Co-author Jianjun Yin, UA assistant professor of geosciences, said, "We are the first to establish the extreme sea level rise event and its connection with ocean circulation."

Goddard detected the two-year-long spike in sea level by reviewing monthly tide-gauge records, some of which went back to the early 1900s, for the entire Eastern Seaboard. No other two-year period from those records showed such a marked increase.

The team linked the spike to a change in the ocean's Atlantic Meridional Overturning Circulation and also a change in part of the climate system known as the North Atlantic Oscillation. The researchers then used computer climate models to project the probability of future spikes in sea level.

The team found that, at the current rate that atmospheric carbon dioxide is increasing, such extreme events are likely to occur more frequently, Goddard said.

Goddard's and Yin's research paper is titled "An Extreme Event of Sea Level Rise along the Northeast Coast of North America in 2009-10." Stephen Griffies and Shaoqing Zhang of the National Oceanographic and Atmospheric Administration's Geophysical Fluid Dynamics Laboratory in Princeton, New Jersey, are also co-authors. NOAA funded the research.

Yin's previous work on climate models suggests that weakening of the Atlantic Meridional Overturning Circulation could cause sea levels to rise faster along the northeast coast of North America.

Yin wondered whether such sea level rise had actually been observed, so he asked Goddard to compile the tide-gauge records for the east coast of North America. The 40 gauges, spanning the coast from Key

West, Florida, north to Newfoundland, have been recording sea levels as far back as the 1920s.

Goddard's work revealed a surprise — that during 2009 and 2010, sea level between New York and Newfoundland rose an average of four inches. Sea level from Cape Hatteras to New York also had a notable spike, though not as dramatic.

"The sea level rise of 2009-10 sticks out like a sore thumb for the Northeast," Goddard said.

His research also confirmed that, as others have reported, sea level has been gradually rising since the 1920s and that there is some year-to-year variation.

About the time Goddard finished analyzing the tide-gauge records, another group of researchers reported that the Atlantic Meridional Overturning Circulation, or AMOC, had a 30 percent decline in strength in 2009-10. Those researchers reported the decline started just two months before the tide gauges started recording the spike in sea level.

"To me, it was like putting together a puzzle," Goddard said.

The more he and his colleagues examined the timing of the AMOC downturn and the subsequent increase in sea level, the more it fit together, he said.

The AMOC brings warm water from the tropics and the southern Atlantic Ocean to the North Atlantic and the polar regions. The water then cools and sinks, eventually flowing south in the deep ocean. Yin's climate model predicted that when the AMOC weakened, sea level in northeastern North America would rise.

In addition to the weakening AMOC, during 2009-10 the region's atmosphere was in a very negative phase of the climate mode called the North Atlantic Oscillation. The NAO flip-flops between negative and positive phases.

"The negative North Atlantic Oscillation changes the wind patterns along the northeast coast, so during the negative NAO the winds push water onto the northeast coast," Goddard said.

Although the NAO has resumed flipping between positive and negative states, observations show that the AMOC, while somewhat stronger, has still not recovered its previous strength.

Even now, sea level is still higher than before 2009, Yin said. He is not surprised, because most of the climate models predict a weakening of the AMOC over the 21st century.

Yin said that at the current rate of increase in greenhouse gases, most climate models predict a weakening of the AMOC over the twenty-first century. Therefore, such extreme sea level rise events and coastal flooding are quite likely to occur along the densely populated northeast coast of North America more often.

— Read more in Paul B. Goddard et al., "An extreme event of sea-level rise along the Northeast coast of North America in 2009–2010," Nature Communications *6, Article number: 6346 (24 February 2015)*

Ocean acidification threatens U.S. coastal communities

Source: http://www.homelandsecuritynewswire.com/dr20150226-ocean-acidification-threatens-u-s-coastal-communities

Feb 26 – **Coastal communities in fifteen states that depend on the $1 billion shelled mollusk industry (primarily oysters and clams) are at long-term economic risk from the increasing threat of ocean acidification, a new report concludes.**

This first nationwide vulnerability analysis, which was funded through the National Science Foundation's National Socio-Environmental Synthesis Center, was published in the journal *Nature Climate Change*.

The Pacific Northwest has been the most frequently cited region with vulnerable shellfish populations, the authors say, but the report notes that newly identified areas of risk from acidification range from Maine to the Chesapeake Bay, to the bayous of Louisiana.

"Ocean acidification has already cost the oyster industry in the Pacific Northwest nearly $110 million and jeopardized about 3,200 jobs," said Julie Ekstrom, who was lead author on the study while with the Natural Resources Defense Council. She is now at the University of California at Davis.

George Waldbusser, an Oregon State University marine ecologist and biogeochemist, said the

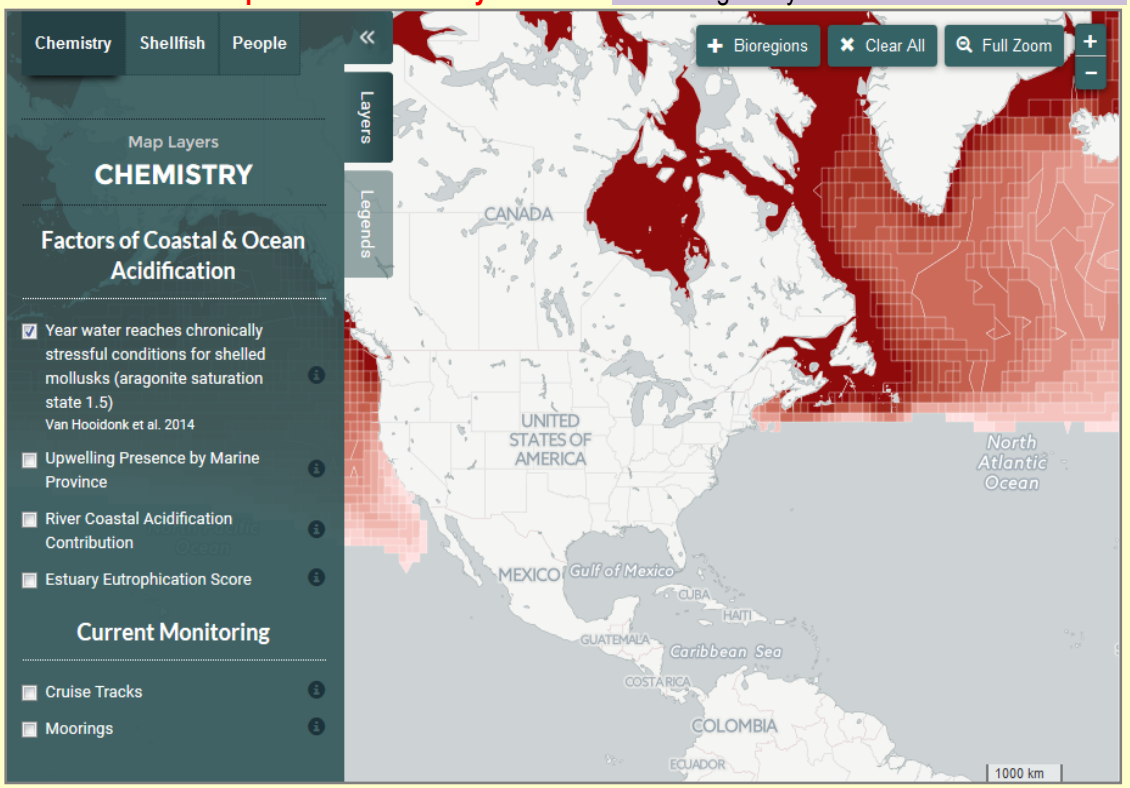
spreading impact of ocean acidification is due primarily to increases in greenhouse gases. "This clearly illustrates the vulnerability of communities dependent on shellfish to ocean acidification," said Waldbusser, a researcher in OSU's College of Earth, Ocean, and Atmospheric Sciences and co-author on the paper. "We are still finding ways to increase the adaptive capacity of these communities and industries to cope, and refining our understanding of various species' specific responses to acidification.

"Ultimately, however, without curbing carbon emissions, we will eventually run out of tools to address the short-term and we will be stuck with a much larger long-term problem," Waldbusser added.

An OSU release reports that the analysis identified several "hot zones" facing a number of risk factors. These include:

- **The Pacific Northwest:** Oregon and Washington coasts and estuaries have a "potent combination" of risk factors, including cold waters, upwelling currents that bring corrosive waters closer to the surface, corrosive rivers, and nutrient pollution from land runoff
- **New England:** The product ports of Maine and southern New Hampshire feature poorly buffered rivers running into cold New England waters, which are especially enriched with acidifying carbon dioxide
- **Mid-Atlantic:** East coast estuaries including Narragansett Bay, Chesapeake Bay, and Long Island Sound have an abundance of nitrogen pollution, which exacerbates ocean acidification in waters that are shellfish-rich
- **Gulf of Mexico:** Terrebonne and Plaquemines Parishes of Louisiana, and other communities in the region, have shellfish economies based almost solely on oysters, giving this region fewer options for alternative — and possibly more resilient — mollusk fisheries.

The project team has also developed an interactive map to explore the vulnerability factors regionally.



One concern, the authors say, is that many of the most economically dependent regions — including Massachusetts, New Jersey, Virginia and Louisiana — are least prepared to respond, with minimal research and monitoring assets for ocean acidification.

The Pacific Northwest, on the other hand, has a robust research effort led by Oregon State University researchers, who already have helped oyster hatcheries rebound from near-disastrous larval die-offs over the past decade. The release notes

that the university recently announced plans to launch a Marine Studies Initiative that would help address complex, multidisciplinary problems such as ocean acidification.
"The power of this project is the collaboration of natural and social scientists focused on a problem that has and will continue to impact industries dependent on the sea," Waldbusser said.

Waldbusser recently led a study that documented how larval oysters are sensitive to a change in the "saturation state" of ocean water — which ultimately is triggered by an increase in carbon dioxide. The inability of ecosystems to provide enough alkalinity to buffer the increase in CO_2 is what kills young oysters in the environment.

— Read more in Julia A. Ekstrom et al., "Vulnerability and adaptation of U.S. shellfisheries to ocean acidification," *Nature Climate Change* (23 February 2015)

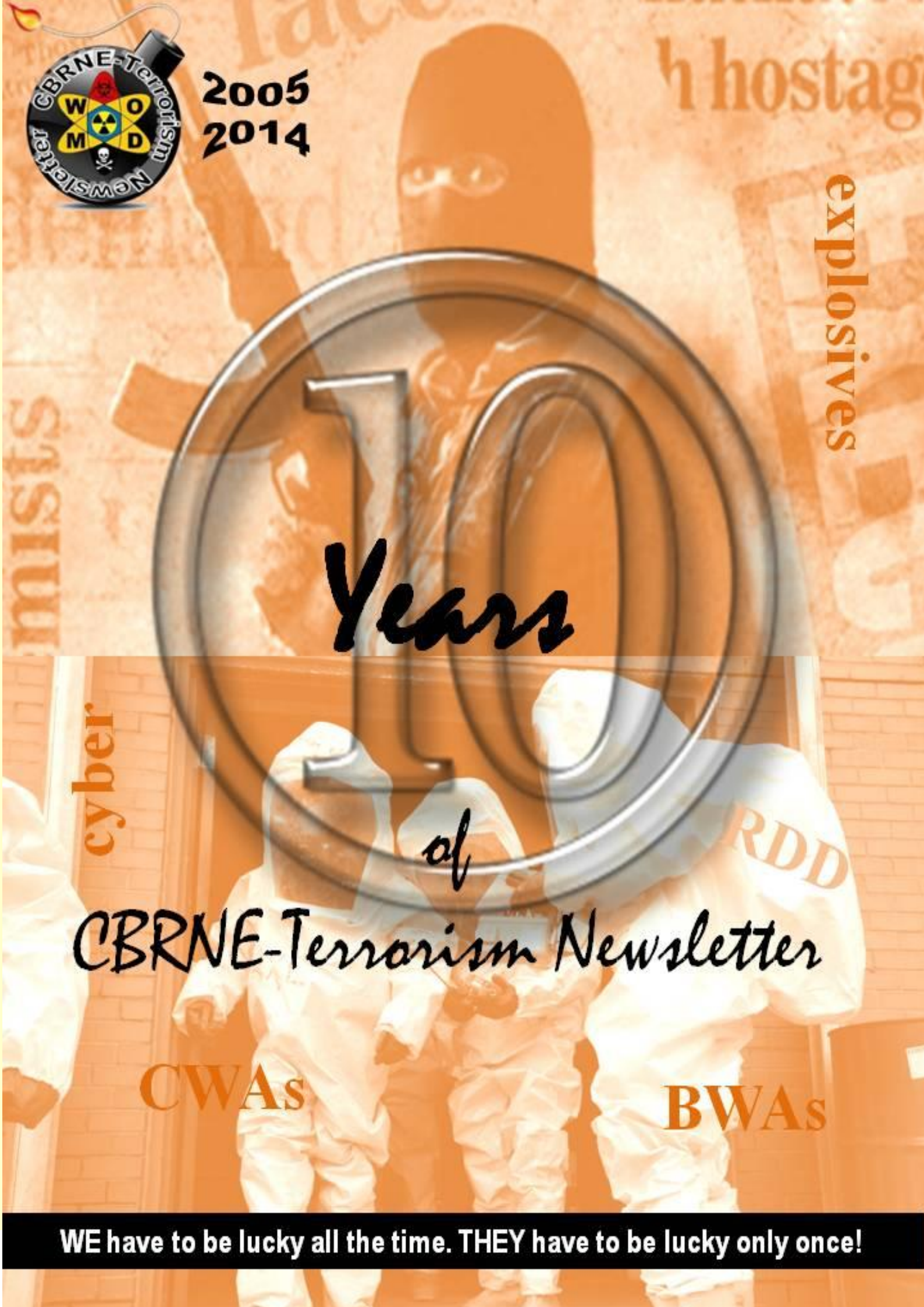
Climate change and the origins of the Syrian war

Source: http://www.homelandsecuritynewswire.com/dr20150303-climate-change-and-the-origins-of-the-syrian-war

March 03 – **A new study says a record drought that ravaged Syria in 2006-10 was likely stoked by ongoing man-made climate change, and that the drought may have helped propel the 2011 Syrian uprising.**
Researchers say the drought, the worst ever recorded in the region, destroyed agriculture in the breadbasket region of northern Syria, driving dispossessed farmers to cities, where poverty, government mismanagement, and other factors created unrest that exploded in spring 2011. The conflict has since evolved into a complex multinational war that has killed at least 200,000 people and displaced millions.
The study was published in the *Proceedings of the National Academy of Sciences*.
"We're not saying the drought caused the war," said Richard Seager, a climate scientist at Columbia University's Lamont-Doherty Earth Observatory who coauthored the study. "We're saying that added to all the other stressors, it helped kick things over the threshold into open conflict. And a drought of that severity was made much more likely by the ongoing human-driven drying of that region."
A Columbia University release notes that a growing body of research suggests that extreme weather, including high temperatures and droughts, increases the chances of violence, from individual attacks to full-scale wars. Some researchers project that manmade global warming will heighten future conflicts, or argue that it may already be doing so. Recent journalistic accounts and other reports have linked warfare in Syria, Iraq and elsewhere in part to environmental issues, especially lack of water. The new study, combining climate, social, and economic data, is perhaps the first to look closely and quantitatively at these questions in relation to a current war.
The recent drought affected the so-called Fertile Crescent, spanning parts of Turkey and much of Syria and Iraq, where agriculture and animal herding are believed to have started some 12,000 years ago. The region has always seen natural weather swings. Using existing studies and their own research, however, the authors showed that since 1900, the area has undergone warming of 1 to 1.2 degrees Centigrade (about 2 degrees Fahrenheit), and about a 10 percent reduction in wet-season precipitation. They showed that the trend matches neatly with models of human-influenced global warming, and thus cannot be attributed to natural variability.
Global warming has had two effects, they say. First, it appears to have indirectly weakened wind patterns that bring rain-laden air from the Mediterranean, reducing precipitation during the usual November-April wet season. Second, higher temperatures have increased evaporation of moisture from soils during the usually hot summers, giving any dry year a one-two punch. The region saw substantial droughts in the 1950s, 1980s and 1990s. However, 2006-10 was easily the worst and longest since reliable recordkeeping began. The researchers concluded that an episode of this severity and length would have been unlikely without the long-term changes.
The release notes that other researchers have observed the long-term drying trend across the entire Mediterranean, and

attributed at least part of it to manmade warming; this includes an earlier study from the U.S. National Oceanic and Atmospheric Administration. The Intergovernmental Panel on Climate Change has predicted that the already violent Mideast will dry more in coming decades as human-induced warming proceeds.
The study's authors say Syria was made especially vulnerable by other factors, including sheer population growth — from four million in the 1950s to twenty-two million in recent years. Also, the ruling al-Assad family encouraged water-intensive export crops like cotton. Illegal drilling of irrigation wells dramatically depleted groundwater that might have provided reserves during dry years, said coauthor Shahrzad Mohtadi, a graduate student at Columbia's School of International and Public Affairs who did the economic and social components of the research.
The drought's effects were immediate. Agricultural production, typically a quarter of the country's gross domestic product, plummeted by a third. In the hard-hit northeast, livestock herds were practically all obliterated; cereal prices doubled; and nutrition-related diseases among children saw dramatic increases. As many as 1.5 million people fled from the countryside to the peripheries of cities that were already strained by influxes of refugees from the ongoing war in next-door Iraq. In these chaotic instant suburbs, the Assad regime did little to help people with employment or services, said Mohtadi. It was largely in these areas that the uprising began.
"Rapid demographic change encourages instability," say the authors. "Whether it was a primary or substantial factor is impossible to know, but drought can lead to devastating consequences when coupled with preexisting acute vulnerability."
Solomon Hsiang, a professor of public policy at the University of California, Berkeley who studies climate and conflict, said the study is "the first scientific paper to make the case that human-caused climate change is already altering the risk of large-scale social unrest and violence." Hsiang said this is not the first time the region has faced the issue: research by other scientists has suggested that the Akkadian Empire, spanning much of the Fertile Crescent about 4,200 years ago, likely collapsed during a multi-year drought.
Marshall Burke, an environmental scientist at Stanford University who studies climate and agriculture, said, "There were many things going on in the region and world at that time, such as high global food prices and the beginning of the Arab Spring, that could have also increased the likelihood of civil conflict." But, he said, the study is "consistent with a large body of statistical evidence linking changes in climate to conflict."
The study's lead author is climatologist Colin Kelley, who did the work while working on his Ph.D. at Lamont-Doherty Earth Observatory; he is now a postdoctoral researcher at the University of California, Santa Barbara. It was also coauthored by climate scientists Mark Cane and Yochanan Kushnir, also of Lamont-Doherty.

— Read more in Colin P. Kelley et al., "Climate change in the Fertile Crescent and implications of the recent Syrian drought," Proceedings of the National Academy of Sciences *(30 January 2015); Solomon M. Hsiang et al., "Quantifying the Influence of Climate on Human Conflict,"* Science *341 no. 6151 (13 September 2013); and John Bohannon, "Study Links Climate Change and Violence, Battle Ensues,"* Science *341 no. 6145 (2 August 2013): 444-45.*


CBRNE-Terrorism Newsletter
W
O
M
D
2005
2014
10
Years
of
CBRNE-Terrorism Newsletter
explosives
cyber
RDD
CWAs
BWAs
WE have to be lucky all the time. THEY have to be lucky only once!