

July 2014



CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders



The curse of...



www.cbrne-terrorism-newsletter.com

After the Unthinkable: Medical Consequence Management of Nuclear & Radiological Terrorism

By Frank G. Rando

Source: <http://www.cbrneportal.com/after-the-unthinkable-medical-consequence-management-of-nuclear-radiological-terrorism/>



2

Since the earliest discoveries related to nuclear energy by scientists such as Pierre and Marie Curie and Wilhelm Roentgen, there have been biomedical implications associated with radiological exposure. That first detonation of a prototype nuclear device in the New Mexico desert, and the effects of the atomic bombings on Hiroshima and Nagasaki vividly demonstrated the fearsome destructive forces unleashed and subsequent health effects of a nuclear detonation. These effects are well documented, as are the ones of the unfortunate intentional human experimentation utilizing radionuclides and external sources of radiation.

During the Cold War, elaborate national plans were drafted and implemented, along with an active Civil Defense program to engage citizens in emergency preparedness and community recovery in the aftermath of a strategic nuclear strike against the U.S. Similar plans and programs were initiated in nation-states that had acquired nuclear capabilities, such as Russia, as the primary adversary during this period. The concept of "Mutually Assured Destruction" (M.A.D.) may have kept the balance of terror at an even keel; however,

during this tense period of history, there were frequent miscalculations, failures and other incidents that may have triggered nuclear confrontation and subsequent global thermonuclear warfare.

Despite the fact that there has been downsizing of nuclear arsenals, the grave possibility of strategic thermonuclear warfare still remains and the threat of nuclear – radiological terrorism utilizing an improvised nuclear device (IND) or large radiological dispersal device (RDD) looms on the horizon. The increasing likelihood of rogue nations acquiring nuclear weapons, and the use of INDs and RDDs by terrorist factions have created pressing concerns and needs for a workable medical response system to address these specific threats.

Data continues to suggest that health care systems are still woefully underprepared to handle victims of an IND or large RDD attack on a civilian population. Addressing such attacks involves unique advanced planning due to the potential magnitude of the event, lack of warning, and inherent radiological hazards. Even in a small yield IND attack, catastrophic damage to any existing local infrastructure,

including hospitals and health care could be expected, hindering meaningful response to mass casualties. At once, the challenges of responding to nuclear-radiological events are complex and daunting.

In the U.S., a conceptual and interagency approach to medical consequence management has been developed, which can be considered as a model for planning and response to other global stakeholders: **The "RTR" system (Radiation –specific TRIage, TRreatment, TRansport sites) is designed to support medical care following a nuclear or radiological event.** Its purpose is to characterize, organize and efficiently deploy appropriate materiel and personnel assets as close as physically possible to various victim categories and provide for the safety of responders. It addresses medical, public health and human service needs specific to nuclear-radiological events.

The RTR model was planned and conceived with analysis of the US Department of Homeland Security's (DHS) National Planning **Scenarios**, ie. Improvised Nuclear Device (IND, Scenario #1) which utilizes a potential 10-kiloton (kt) detonation in an urban environment, and Radiological Dispersal Device (RDD, Scenario # 11), a Cesium-137 (CS 137-cesium chloride) improvised explosive RDD detonation. Compliance and consistency with the roles and responsibilities of the US Department of Health and Human Services (HHS) by Homeland Security Presidential Directives (HSPDs) # 18 and # 21, and the National Response Framework (NRF), Emergency Support Function # 8 (ESF # 8-Public Health and Medical Services), are essential requisites for the overall RTR functional model.

The development of the RTR model engaged the evaluation of various military/civilian medical response plans and casualty loads and injury/illness matrices were provided by the Interagency Modeling and Atmospheric Assessment Center (DHS), the National Atmospheric Release Advisory Center, and the Defense Threat Reduction Agency (DTRA). While not designated as an individualized triage system, the RTR would be able to establish sites after the event characterization and perimeters are established. RTR sites need to be determined and established in real-time and must take into account event severity, damage assessments, available infrastructure,

evacuation and transportation routes, radiological hazards, and environmental factors, eg. topography, precipitation, wind speed and direction, and non-radiological hazards.

RTR sites are divided into three categories:

- **RTR1** – Designated near the epicenter with residual radiation and would provide medical response and support for major traumatic injuries, including blast injury and radiation exposure.
- **RTR2** – Established in relationship to plume modeling, varying amounts of residual radiation and serving mostly ambulatory victims.
- **RTR3** – Serve as casualty collection points (CCPs) and transport venues with minimal or absent radiological hazards or exposure risks and an assorted matrix of injuries and /or radiation exposures.

Medical Care (MC) sites are predetermined venues at which definitive medical care is administered to those that have been triaged as requiring immediate medical care. The obvious components of a health care system, such as local and regional hospitals, Veterans Administration hospitals, nursing homes, outpatient clinics, and specialty centers such as burn, shock-trauma, oncology and related facilities would all be involved in catastrophic medical care and expected to function in an austere operational environment, and must be prepared to decontaminate patient influxes. Alternative Care Sites (ACS), such as predetermined Federal Medical Stations (FMS). These could be school gymnasiums, convention centers or other venues designated to expand medical surge capacity in communities. In addition, adequate medical countermeasures, such as colony-stimulating factor cytokines for bone marrow suppression due to Acute Radiation Syndrome (ACS) and decorporation agents must be made available based upon medical triage decision-making and health physics evaluations. Proper personal protective countermeasures, ie., time, distance and shielding ,and personal protective equipment (PPE) must be applied by all health care providers and pre-hospital/emergency response personnel.

Protective Action Guidelines (PAGs) have been developed for nuclear power accidents, and have been made applicable to intentional nuclear–radiological events utilizing evidence-based development and interagency consensus. PAGs are to be utilized to provide

guidance on time limitations and “allowable exposures” during operational duties in various conditions involving radioactivity.

The spectrum of medical consequences associated with IND or RDD detonation include temporary and permanent blindness, such as flash blindness, retinal burns, (IND), blast injuries, burn trauma, crush syndrome due to structural collapse and victim entrapment, and acute and latent/chronic health effects observed with radiation exposure, including the possibility of increased cancer risk. The **behavioral health impacts** will be great and require both immediate mental health crisis interventions and long term mental health services for survivors, including responders. It is important to denote that traumatic injuries and concomitant radiation exposure contribute to higher mortality rates, than the sum of

individual injuries. In addition, blast and thermal injuries may occur without radiological exposures and radiological exposures may occur without traumatic injuries. Ethical dilemmas will be present, during the allocation of scarce resources. Assembly Centers for displaced populations and evacuees are also a component of the RTR scheme.

While realistic planning for the medical and public health consequences of an IND or RDD detonation are obvious priorities given our current threat assessments, improvements and proactive measures and methodologies to detect, deter and interdict weapons-grade nuclear material, thwart acquisition of nuclear weapons by rogue regimes, and tighter controls on other radioactive sources will do much to avert that fateful day.

Frank G. Rando possesses over 30 years of real world experience in tactical ,disaster and operational medicine ,as well as in the fields of medical intelligence analysis,emergency preparedness and response, environmental safety and health, toxicology,,risk and threat assessments ,public health and public safety. He serves as a Subject Matter Expert, instructor and consultant for several academic and DHS, .DoD and other governmental and private programs and projects.

As Baby Boomers retire, nuclear industry faces manpower shortages

Source: <http://www.homelandsecuritynewswire.com/dr20140627-as-baby-boomers-retire-nuclear-industry-faces-manpower-shortages>

Many nuclear power plants in the United States are facing an employment and training crisis as their largely Baby Boomer-generation (1946-64) workforce begins to retire.

As the *Star-Ledger* reports, the nuclear industry is making an effort to usher in new and better-trained workers — many from university programs and former military service — to fill in the gaps created by retirement-aged engineers.

Richard Coe, the assistant dean of the School of Applied Sciences and Technology at Thomas Edison State College, told the paper, **“Current nuclear plants — all 104 of them — have a Baby Boomer crisis coming in which they are going to have a huge exodus of the workforce.”**

Thomas Edison State College, located in New Jersey, is just one of many institutions that now offer courses, included distance learning curriculums that prepare students the field. Additionally, there are federal scholarships as large as \$5,000 for qualified students that aim to move more prospective employees into the realm of nuclear science.

Thomas Edison alone has roughly 1,000 undergraduates that are engaged in course work such as energy systems technology, nuclear energy engineering technology and nuclear engineering technology and radiation protection programs.

The military also is a major training ground for prospective hires due to intensive training on nuclear submarines and other similarly powered equipment. At times, it is even incentivized, as was the case for John Richardson, a manager at Hope Creek Nuclear Generating Station. He told the paper, “They offered me a bonus for going into the nuclear power program.”

In the United States, most nuclear power workers can expect to earn an average salary of at least \$50,000 a year. Upper level positions often earn closer to \$100,000 a year. Electrical Technicians earn a medium annual salary of \$58,000, while licensed operators and plant

engineers range from \$75,000-\$90,000 on average. Those figures are likely to go higher as the demand for fresh workers increases.

StemRad 360 Gamma

Source: http://stemrad.com/?page_id=29

StemRad introduces the revolutionary 360 Gamma, wearable PPE that has been developed in order to protect first-responders and affected populations from the deadly effects of exposure to high doses of gamma radiation.



Exposure poses immediate life-threatening risk from Acute Radiation Syndrome (ARS), also known as radiation sickness. ARS arises due to the destruction of an individual's hematopoietic stem cells which



reside within the bone marrow, resulting in anemia, infections, internal bleeding and death within several weeks, sometimes days. StemRad's tested and patent-pending technology protects hematopoietic stem cells from the toxic effects of gamma radiation, providing affected individuals with an increased

chance of survival in the event of inadvertent exposure to ionizing gamma radiation, from a nuclear catastrophe such as an explosion or reactor leak.

Importantly, StemRad's 360 Gamma enables first-responders to perform their life-saving role of containing the catastrophe, while also enabling those in close proximity, to safely evacuate exposed areas.

Fears of a German dirty bomb

By Alex Wellerstein

Source: <http://blog.nuclearsecrecy.com/2013/09/06/fears-of-a-german-dirty-bomb/>

For good reason, much has been made of the **initial fear of a German atomic bomb**. But there was another, **lesser-known atomic fear** as well. If the Germans could make nuclear reactors — which the Americans thought they were probably doing — could they not take the dangerously-radioactive spent-fuel out of them and use them to make **dirty bombs**?



Hanford spent fuel rods — the sort of thing that could have been weaponized during World War II as a radiological weapon.

In the summer of 1942, Arthur Compton, head of the University of Chicago's Metallurgical Laboratory, wrote a memo to Harvard President and atomic-bomb big-wig James B. Conant expressing the need for "**protection against ionizing bombs**":



We have become convinced there is **real danger of bombardment** by the Germans **within the next few months** using **bombs designed to spread radio-active materials in lethal quantities**. ... Since protection against the danger from such bombs will be primarily a matter of detection of radiation and instruction with regards to the dangers, it is essential that the matter be brought at once to the attention of the appropriate military officers.¹

Compton and his scientists were, at the time, working **under the assumption that the Germans were ahead of the Americans**, and had already gotten a nuclear reactor running. They estimated that with a 100 kilowatt reactor, 100,000 Curies of radioactivity could be produced daily for bomb usage.

A radiation survey device of the sort produced during World War II by the Victoreen Instrument Company in Cleveland, in collaboration with the University of Chicago scientists.

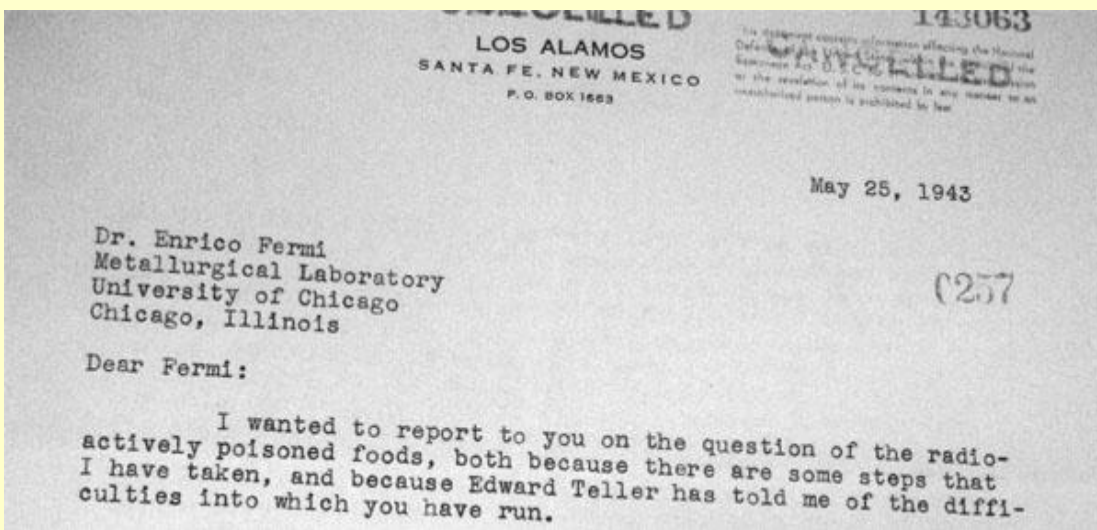
A result of this was that in the fall of 1942, the first steps were taken to, at a minimum, detect whether the Germans used any kind of radiological attack against the Allies. **Survey meters** were developed that would **trigger alarms** if they **detected high levels of radioactivity**. These were secretly dispersed to Manhattan District offices in **Boston, Chicago, New York, San Francisco, and Washington, DC**. At each location, a small number of officers were trained in their use. Further instruments were held in reserve in case they needed to be deployed further. If the alarms went off, or if there were other suspicious signs (like reports of a large-scale blackening of photographic film), scientists at the University of Chicago were kept on the ready to be brought in to assess the situation.²

This was a fairly small program, as far as they go. **Those involved were acutely aware that the secrecy of the atomic bomb made it impossible to adequately prepare for this possibility**. They were stuck in a bind that was very common during the wartime period. The atomic bomb was, at that time, what I like to call an **“absolute secret”**: the fact that there **was a “secret”** at all **was itself a secret**. They could not draw attention to matters relating to atomic energy without drawing attention to the fact that they were engaged in a secret research program with regards to atomic energy. This is a very peculiar situation, one primarily specific to the war, when the secrecy of the project could not be acknowledged (they could not simply say, “oh, the details are secret,” as they could in the Cold War).

What did they think the Germans would do with such a radiological weapon? They considered four possibilities. First, it could be used as an “area-denial” weapon, by making areas uninhabitable. Second, it could be used to contaminate critical war infrastructure (e.g. airports). Third, it could be used as a “radioactive poison gas” to attack troops. Fourth, it could be used “against large cities, to promote panic, and create casualties among civilian populations.”³ Their assessment of the effects, by 1943, was grim:

Areas so contaminated by radioactive material would be **dangerous until decay of the material took place, perhaps for weeks or months**. ... As a gas warfare instrument the material would be ground into particles of microscopic size to form dust and smoke and distributed by a ground-fired projectile, land vehicles, or aerial bombs. In this form it would be inhaled by personnel. **The amount necessary to cause death to a person inhaling the material is extremely small**. It has been estimated that one millionth of a gram accumulating in a person’s body would be fatal. **There are no known methods of treatment for such a casualty**.⁴

In the time-honored method of worrying about threats, they also then immediately realized that **maybe the United States should be weaponizing fission products**: “It is the recommendation of this Subcommittee that if military authorities feel that the United States should be **ready to use radioactive weapons in case the enemy started it first**, studies on the subject should be started immediately.” Note that this isn’t really a deterrent capability, it is a response capability. Deterrence requires your enemy *knowing* that you have the capability to respond, and secrecy precluded true deterrence.



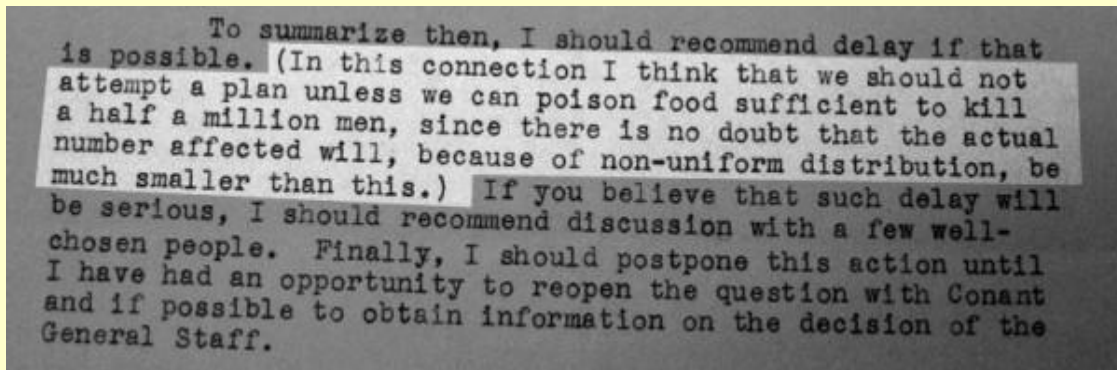
In this context, there is an interesting letter in the J. Robert Oppenheimer papers at the Library of Congress, where Oppenheimer is writing to Enrico Fermi in May 1943 on **“the question of radioactively poisoned foods.”** From the context, it is clear that both Edward Teller and Fermi had

devoted time to this project. The full document is available [here](#). Two parts stand out. One is that one of the acute problems in looking into the issue was, as Oppenheimer put it, difficult to study the subject “**without telling anyone about it.**” That is, it would be hard to investigate some of the substances in question “without letting a number of people into of the secret of why we want” the substances. The “absolute secret” bind again.

The other is Oppenheimer’s criteria for the project being worth looking into:

...I think that we should not attempt a plan **unless we can poison food sufficient to kill a half a million men**, since there is no doubt that the actual number affected will, because of non-uniform distribution, be much smaller than this.⁵

Frank Oppenheimer later called this a very “**bloodthirsty**” statement by his brother; the historian Barton Bernstein instead argued that this was just scientists trying to help the war effort.⁶ **Either way, it makes Oppenheimer look like a very cold fish indeed.** And not much of a “dove.” Even if one isn’t clear how much of a “non-uniform distribution” he was assuming.



To summarize then, I should recommend delay if that is possible. (In this connection I think that we should not attempt a plan unless we can poison food sufficient to kill a half a million men, since there is no doubt that the actual number affected will, because of non-uniform distribution, be much smaller than this.) If you believe that such delay will be serious, I should recommend discussion with a few well-chosen people. Finally, I should postpone this action until I have had an opportunity to reopen the question with Conant and if possible to obtain information on the decision of the General Staff.

The **offensive angle was basically dropped** — they didn’t think they’d need it, and they were focused intently on making the actual atomic bomb, a much more devastating weapon. **But defensive measures did proceed.** By late 1943, it was thought that the use of radioactive poisons against the UK by the Germans was of low probability, but an unpleasant possibility.⁷ To avoid being completely taken by surprise in such an event, General Groves (with the concurrence of General Marshall) had four officers from the European Theater of Operations staff briefed on the subject “under most complete secrecy,” and a *Manual on Use of Radioactive Materials in Warfare* was drawn up for these four officers. Signals officers were instructed to report any “peculiar or unexplained effects” on photographic films or personnel, and the officers in question were given radiation detection instruments to use in the case of suspected cases.

In March 1944, General Groves had the matter brought to the attention of General **Dwight D. Eisenhower**, commanding general of the Supreme Headquarters Allied Expeditionary Force, fearing that the Nazis might use such weapons to prevent an Allied invasion of Europe. Eisenhower concluded that since the Combined Chiefs of Staff had not brought up the issue, that they must consider that “**the enemy will not implement this project.**” To keep secrecy, in order to “**to avoid a possible scare,**” Eisenhower informed only a handful of people, which he acknowledged was not really enough to counter “enemy action of this nature”: “**No US or British Commander participating in OVERLORD [the landing at Normandy] has been briefed.**” However, radiation detectors were being kept in the UK for deployment on short notice, and a “cover” letter was sent out with symptoms of radiation poisoning listed as a “**mild disease of unknown etiology**” that was going around, requesting any medical officers to report further cases.⁸

The plan to deploy radiation monitoring during the D-Day invasions was dubbed “**Operation Peppermint,**” one of the more amusing code-names of the war. Dry runs of the detection apparatus were taken before D-Day, and German bomb craters were surveyed for radioactive residues, but since no evidence of German radiological weapons preparations or use were uncovered, **the “Peppermint” preparations were never put into effect.**

We now know that the Germans never got anywhere near this kind of plan. They didn’t even get a reactor running by the end of the war, the necessary prerequisite for this kind of operation. **It wasn’t a totally crazy fear, though.** There are aspects of radiological warfare which would make it preferable to, say, chemical warfare from the German point of view. Still, there’s an aspect to this of the old saying,

“when the only tool you have is a hammer, every problem looks like a nail.” **When you’re studying radioactive hazards intently, every threat looks like a radioactive hazard.**

The secrecy angle is what intrigues me the most about this story: the secrecy of the bomb made it difficult to enact serious preparation from this related, but separate threat. **The secrecy of one fear made addressing another fear difficult, because the relevant information of both fears were too deeply entangled.**

Notes

1. Arthur H. Compton to James B. Conant (15 July 1942), Bush-Conant file, Roll 7, Target 10, Folder 75, “Espionage.”
2. Manhattan District History, Book 1, Volume 14, Foreign Intelligence Supplement No. 2 (Peppermint), 31 July 1952.
3. “Use of Radioactive Material as a Military Weapon” (n.d., c.a. early 1943).
4. Ibid.
5. J. Robert Oppenheimer to Enrico Fermi (25 May 1943), J. Robert Oppenheimer Papers, Library of Congress.
6. Barton J. Bernstein, “Oppenheimer and the Radioactive Poison Plan,” *Technology Review*, 88 (May-June 1985), 14-17. There is also some follow-up in Barton J. Bernstein, “Four physicists and the bomb: The early years, 1945-1950,” *Historical Studies in the Physical and Biological Sciences*, 18, No. 2 (1988), pp. 231-263, on 252-253.
7. Leslie Groves to George C. Marshall (30 November 1944), Manhattan Engineer District (MED) records, Records of the Army Corps of Engineers, RG 77, National Archives and Records Administration, Box 64, “Security.”
8. Dwight D. Eisenhower to George Marshall (11 May 1944), *Correspondence (“Top Secret”) of the Manhattan Engineer District, 1942-1946*, microfilm publication M1109 (Washington, D.C.: National Archives and Records Administration, 1980), Roll 5, Target 8, Folder 18, “Radiological Defense.”

Alex Wellerstein is an historian of science at the American Institute of Physics.

Ultimate Explosive & Dirty Bomb Detector

Source: <http://www.global-security-solutions.com/UltimateExplosive&DirtyBombDetector.html>

The Ultimate Explosive & Dirty Bomb Detector (UEDD) is a highly sensitive, portable, multi- functional explosives detector and analytical system offering optimal power & flexibility for fast, reliable detection and positive identification of all types of explosive substances.



Some exclusive features:

- Touch screen programming & commands
- Option of setting product sensitivity
- Unique infrared sampling mode (**not available on any other Explosive Detector**), enables the detection of non-volatile explosives in vapor mode
- New Gun Shot Residue Mode
- Full remote control via USB, RS 232, Ethernet, Internet, GPRS, GSM, WiFi
- EZ-VIEW PC suit for drag&drop data transfer, full remote control and Internet communication
- Radio active material (Dirty Bomb) Detection (Optional)
- Optional Bar code reader to identify scanned objects
- Easy integration with other security technologies (X- Ray scanners, bomb-squad robots)
- Remote factory diagnostic & repair services via Internet from any global location
- Car charger
- Docking station for 24 hour operation & charge



- Optional Flammable liquid detection available for additional cost

Additional features:

- Choice of: Two ultra-fast 1-second response
- Continuous Vapor Mode with instant reading
- Analytical Vapor Mode* with instant reading and identification or
- Analytical Particulate Mode* with detailed identification all operating to highest level of sensitivity

* Analytical Particulate Mode and Analytical Vapor Modes offer explosive identification with ultra-low false alarm rate, extreme overload resistance and fast self- cleaning

- Highly resistant to potential overload from a wide range of interfering agents and/or various sampled compounds
- Extremely low running cost

Mass panic was aim of £70,000 dirty bomb

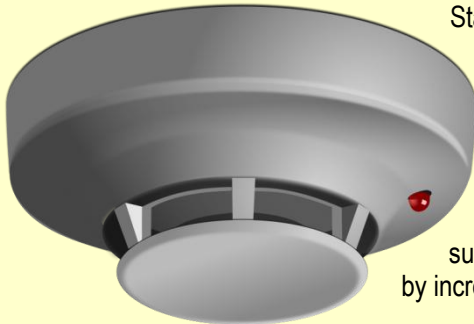
Source: <http://www.independent.co.uk/news/uk/crime/mass-panic-was-aim-of-16370000-dirty-bomb-423425.html>

Nov 2006 – The full details of Dhiren Barot's plot to set off a radioactive "dirty bomb" containing smoke detectors was revealed yesterday. **At a cost of £70,000, Barot, 34, proposed building a bomb that would cause radiation sickness in about 500 people and produce mass panic.**

The Muslim extremist suggested setting off the bomb in central London, or a city in Spain or the United States, Woolwich Crown Court in London was told yesterday.

Edmund Lawson QC, for the prosecution, said that the plan appeared to have been based on an incident in France when a lorry carrying 900 smoke detectors crashed, provoking concern about possible exposure to radiation - the detectors contained small amounts of radioactive material.

In a terrorist document Barot wrote: "If something so small and simple such as 900 burning smoke detectors could cause so much havoc, then by increasing the amount used, the possibilities are good."



He suggested in his presentation document to al-Qa'ida leaders that **the radiation project should use around 10,000 smoke detectors and either "set them alight" or "place them on top of an explosive device"**.

His proposal also contained research into the possible effects of the radioactivity released if such an attack was carried out, including the long-term risks of cancer and infertility.

Barot speculated that such a dispersal of radiation could cover a large area. He wrote: "The burning has the potential to affect around 500 people... as soon as we realised this... we concluded that it deserved to be an independent project in its own right."

He said the bomb would cost £50,000, with each smoke detector costing £5. He thought £20,000 might be needed for storage, bringing the total cost to £70,000.

In other suggestions, Barot discussed the consequences of train crashes and referred to the carnage caused following the Ladbroke Grove accident, the court heard. Barot wrote: "For some time now we



have had thoughts on executing a project on a busy train network. Moreover, I have a personal friend who is a train driver. Every so often he takes a friend on to his train in the driver carriage with him just for the sake of company."

The document also contained Barot's comments on the Heathrow Express, where he speculates that gas could be leaked into the train during the day because it was relatively quiet.

Securo-prof claims to invent new, much deadlier dirty bomb

Source: http://www.theregister.co.uk/2007/08/10/another_day_another_kind_a_bomb/

Aug 2007 – Researchers from King's College London have raised the spectre of a new terrorist technique which would "kill an order of magnitude more people than a dirty bomb" and is "likely to incite considerably more fear".

Writing in securo-thinktank journal *Survival*, James Acton, M Brooke Rogers and Peter Zimmerman lay out their thoughts. The article is called *Beyond the Dirty Bomb: Rethinking Radiological Terror*.

Essentially, the three academics have been inspired by the recent murder of Russian emigre Alexander Litvinenko, internally poisoned with radioactive Polonium-210. They have thought of a new abbreviation to describe mass radiological poisoning without the use of



explosives - I3, for ingestion, inhalation and immersion. The idea is that terrorists might get large numbers of people to swallow, breathe, or be drenched with fluids containing deadly amounts of radioactive isotopes.

The *Guardian* reports on the research this morning, and *Guardian* scribe Julian Borger spoke to Mr Zimmerman, who is professor and chair of science and security at King's College London.

"The article does not provide details of the most devastating method of attack the authors have conceived, for security reasons, but Professor Zimmerman described one scenario using a water-soluble radioactive isotope widely used in hospitals and industry: 'I can then tap into the anti-fire spray in a theatre, and if I can trigger the spray, I can soak everyone in the room'," Borger wrote.

Prof Zimmerman is talking about powdered caesium-137, widely used in radiotherapy machinery and such like.

According to the UN nuclear watchdog, just such a nightmare scenario already occurred in Brazil in 1987.

In that case, scavengers broke open a canister of caesium-137 from an old radiotherapy machine. Brazilian locals, thinking the glowing blue powder was pretty, circulated the stuff widely over the next week. Many rubbed it on themselves. Others ate food adulterated with the powder. In all, 237 people were reckoned to have been contaminated by the Brazilian authorities. Four of them died, and a major cleanup operation was required in the various affected homes and businesses.

So, terrorists might get hold of some caesium-137 and put it into a sprinkler system, say in a theatre. Hundreds of people would then be drenched with a solution of the isotope. Probably they wouldn't start drinking it, though, and it's reasonable to hope that they might shower quite soon rather than rubbing the solution into their skins and waiting a week or so.

Indeed, if it was known what had occurred, the best defence would be to leave the sprayers on until all the contaminated water had been washed off with fresh - such is a standard defence against fallout in military organisations. Royal Navy warships are fitted with deck water-spray points for precisely this reason.

All in all, then, such an attack could be expected to be significantly less deadly than the Brazilian mishap. So it might kill one or two

people tops. Why not just block the fire exits and do a bit of arson? You'd kill a lot more people that way, and you'd need even less knowhow. Why not sabotage some railway tracks, or do your arson in the Tube - Potters' Bar, King's Cross, here we come again. Why not sneak about taking raw chicken out of restaurant fridges at night, then putting it back in without the chef knowing. Why not drive an 18-wheeler into a school playground at 50mph? Why not pour oil out of a car window along the fast lane of the M25 just before rush hour?

No need to bust into any hospitals or hang around the radioisotope bazaars of Central Asia for any of that, is there? And you'd kill a lot of people.

Prof Zimmerman's proposal is a tough new control and licencing regime for all radioactive materials (bound to have a great effect on the NHS budget). Maybe his special undisclosed attack method really is so deadly as to justify this. He told the *Graun* that his secret plan "would be capable of killing several hundred, maybe upwards of a thousand, and paralyzing

a city without any question at all", so maybe it is.

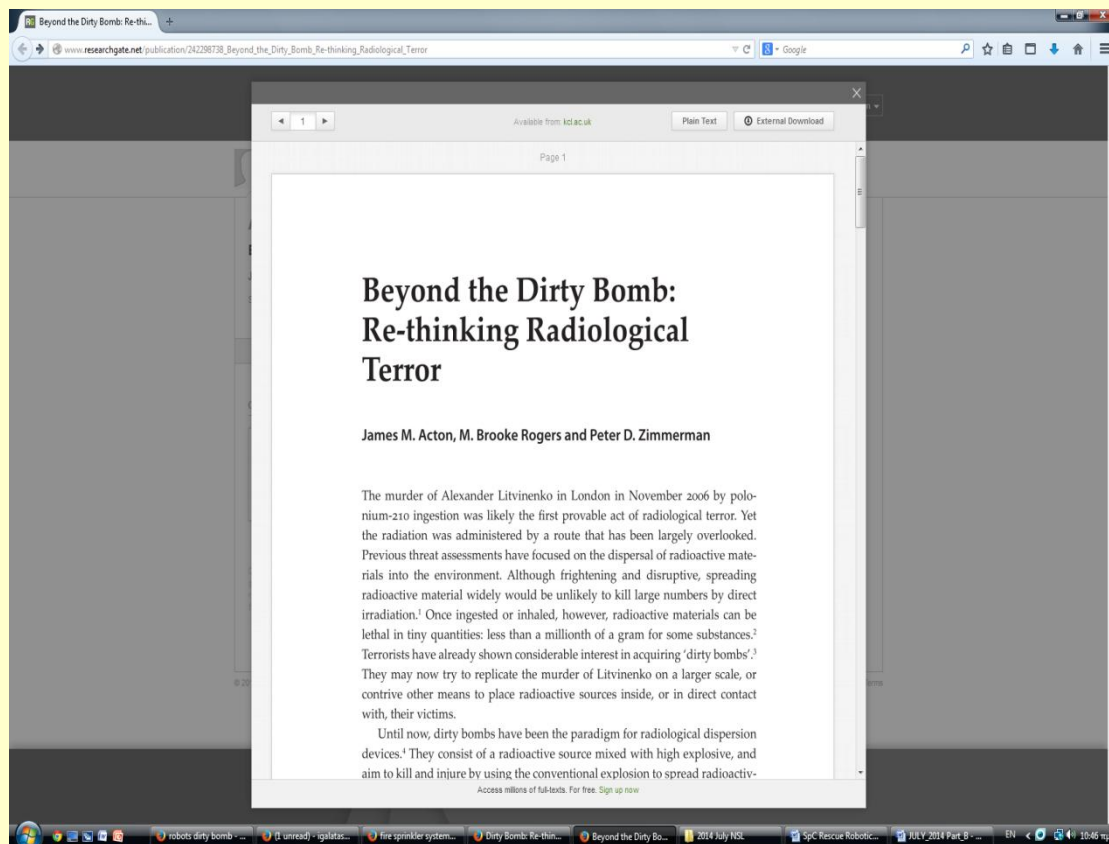
Still, what's next? Control and licencing of petrol, matches and prybars? Security cameras and alarms in every fridge?

No, obviously not. Terrorist incidents with one or two figure death tolls are only different from the ordinary run of accidents and crime and deadly mayhem if we make them so.

Perhaps Prof Zimmerman has thought of something new - 1,000 dead in one hit would be serious (your chance of survival as a Londoner, though? 99.99 per cent or better). But his caesium-137 sprinkler attack notion doesn't lend much credence to his arguments. Nor does his decision to publish now, before the suggested countermeasures are in place - which they surely will be presently, if his special-sauce attack plan is as advertised.

Apparently, one of Zimmerman's co-authors, Brooke Rogers, would like to see an intensive information campaign to keep the public informed and prevent panic.

We're doing our best on that one. It's hard to say that she and her co-authors are, though.



12

► Read the full paper at:

http://www.researchgate.net/publication/242298738_Beyond_the_Dirty_Bomb_Re-thinking_Radiological_Terror

A farewell to arms? Scientists developing a novel technique that could facilitate nuclear disarmament

Source: <http://www.sciencedaily.com/releases/2014/06/140625132404.htm>

A proven system for verifying that apparent nuclear weapons slated to be dismantled contained true warheads could provide a key step toward the further reduction of nuclear arms. The system would achieve this verification while safeguarding classified information that could lead to nuclear proliferation.

Scientists at Princeton University and the U.S. Department of Energy's (DOE) Princeton Plasma Physics Laboratory (PPPL) are developing the prototype for such a system, as reported this week in *Nature* magazine. Their novel approach, called a "zero-knowledge protocol," would verify the presence of warheads without collecting any classified information at all.

Alexander Glaser and Robert Goldston with the British Test Object.

"The goal is to prove with as high confidence as required that an object is a true nuclear warhead while learning nothing about the materials and design of the warhead itself," said physicist Robert Goldston, coauthor of the paper, a fusion researcher and former director of PPPL, and a professor of astrophysical sciences at Princeton.

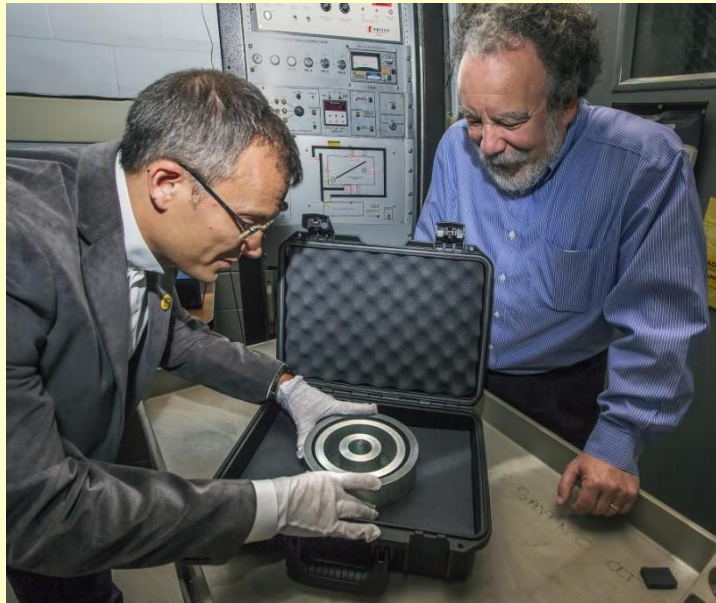
While numerous efforts have been made over the years to develop systems for verifying the actual content of warheads covered by disarmament treaties, no such methods are currently in use for treaty verification.

Counting warheads

Traditional nuclear arms negotiations focus instead on the reduction of strategic -- or long-range -- delivery systems, such as bombers, submarines and ballistic missiles, without verifying their warheads. But this approach could prove insufficient when future talks turn to tactical and nondeployed nuclear weapons that are not on long-range systems. "What we really want to do is count warheads," said

physicist Alexander Glaser, first author of the paper and an assistant professor in Princeton's Woodrow Wilson School of Public and International Affairs and the Department of Mechanical and Aerospace Engineering.

The system Glaser and Goldston are mapping out would compare a warhead to be inspected with a known true warhead to see if the weapons matched. This would be done by beaming high-energy neutrons into each warhead and recording how many neutrons



passed through to detectors positioned on the other side. Neutrons that passed through would be added to those already "preloaded" into the detectors by the warheads' owner -- and if the total number of neutrons were the same for each warhead, the weapons would be found to match. But different totals would show that the putative warhead was really a spoof. Prior to the test, the inspector would decide which preloaded detector would go with which warhead.

No classified data would be measured in this process, and no electronic components that might be vulnerable to tampering and snooping would be used. "This approach really is very interesting and elegant," said Steve Fetter, a professor in the School of Public Policy at the University of Maryland and a former White House official. "The main question is whether it can be implemented in practice."

PPPL project

A project to test this approach is under construction at PPPL. The project calls for firing high-energy neutrons at a non-nuclear target, called a British Test Object, that will serve as a proxy for warheads. Researchers will compare results of the tests by noting how many neutrons pass through the target to bubble detectors that Yale University is designing for the project. The gel-filled detectors will add the neutrons that pass through to those already preloaded to produce a total for each test.

The project was launched with a seed grant from the Simons Foundation of Vancouver, Canada, that came to Princeton through Global Zero, a nonprofit organization. Support also was provided by the U.S. Department of State, the DOE (via PPPL pre-proposal development funding), and most recently, a total of \$3.5 million over five years from the National Nuclear Security Administration.

Glaser hit upon the idea for a zero-knowledge proof over a lunch hosted by David Dobkin, a computer scientist, and until June 2014, dean of the Princeton faculty. "I told him I was really interested in nuclear warhead verification without learning anything about the warhead itself," Glaser said. "We call this a zero-knowledge proof in computer science," Glaser said Dobkin replied. "That was the trigger," Glaser recalled. "I went home and began reading about zero-knowledge proofs," which are widely used in applications such as verifying online passwords.

Disguising information

Glaser's reading led him to Boaz Barak, a senior researcher at Microsoft New England who had taught computer science at Princeton

and is an expert in cryptology, the science of disguising secret information. "We started having discussions," Glaser said of Barak, who helped develop statistical measures for the PPPL project and is the third coauthor of the paper in Nature.

Glaser also reached out to Goldston, with whom he had taught a class for three years in the Princeton Department of Astrophysical Sciences. "I told Rob that we need neutrons for this project," Glaser recalled. "And he said, 'That's what we do -- we have 14 MeV [or high-energy] neutrons at the Laboratory.'" Glaser, Goldston and Barak then worked together to refine the concept, developing ways to assure that even the statistical noise -- or random variation -- in the measurements conveyed no information.

If proven successful, dedicated inspection systems based on radiation measurements, such as the one proposed here, could help to advance disarmament talks beyond the New Strategic Arms Reduction Treaty (New START) between the United States and Russia, which runs from 2011 to 2021. The treaty calls for each country to reduce its arsenal of deployed strategic nuclear arms to 1,550 weapons, for a total of 3,100, by 2018.

Not included in the New START treaty are more than 4,000 nondeployed strategic and tactical weapons in each country's arsenal. These very weapons, note the authors of the Nature paper, are apt to become part of future negotiations, "which will likely require verification of individual warheads, rather than whole delivery systems." Deep cuts in the nuclear arsenals and the ultimate march to zero, say the authors, will require the ability to verifiably count individual warheads.



Nuclear deal boosts Cumbria's Moorside plant plans

Source: <http://www.bbc.com/news/business-28090612>

Plans to build Europe's largest new nuclear project in Cumbria have taken a step forward after Toshiba and GDF Suez signed a deal to develop the site.

The Japanese engineering giant will take a 60% stake in Nugen, the joint venture set up to develop the plant, with the French energy company taking a 40% stake.

The plans include three reactors at the Moorside site, next to Sellafield.

Final investment decisions should be made in about four

years, Nugen said.

"The Moorside new nuclear project will bring at least £10bn of investment and is expected to create up to 21,000 jobs, while also providing a reliable source of low carbon energy for over six million homes,"



said Energy Minister Michael Fallon.

"This announcement is a significant step towards new reactors likely to come online in 2024 and shows how attractive the UK is for investors." Work on more detailed plans will now begin, but questions remain about how the project will be funded.

The European Commission is currently investigating whether government support for the planned new £16bn Hinkley Point nuclear plant in Somerset breaches EU rules.

The government sees a new generation of nuclear plants as an important component of the UK's overall energy mix. They will also help the government meet its carbon reduction targets, proponents argue.

ISIS Threatens Israel With Nuclear Weapons

Source: <http://i-hls.com/2014/06/isis-threatens-israel-nuclear-weapons/>

An Islamic wind from the east threatens the world, while the Middle East is on the verge of a war of religions – Sunni Muslims murder Shiites in crumbling Iraq and the Western world looks away, lacking empathy or understanding, instead of making an effort to prevent the collapse. The ones who lead this fanatic force belong to the Sunni terror organization ISIS (Islamic State of Iraq and Syria), an organization with strong ties to al-Qaeda.

Over the years the west became used to Islamic use of fiery phrases and “Muhammad’s justice is carried out by sword” – words without actions to back them up. Unfortunately the season of violence is just beginning. One practical example for this new phenomenon is the murder of 1,700 Iraqi officers by ISIS

militants, with the organization’s warlike and terrible statements clearly presenting these murderer’s world view.

“After our major victories in Iraq, and the love of the Iraqi people given to us by Allah, we demand that every citizen of Iraq and all countries that follow give their unmarried daughters for the use of our warriors, so that they could fulfill the duty of Jihad through sex with our fighting brothers.” Avoiding this request will lead to a severe enforcement of sharia law.

In order to make the Islamic world believe they’re serious, ISIS leadership explained that while every Arab country in the Middle East is busy talking about the Palestinian issue, ISIS acts. The organization promised believers that

during the coming war Tel Aviv will fall as quickly as Mosul. In order to enhance the threat the fanatic organization also brought up the nuclear issue. In its public statement ISIS wrote: We despise the Zionist regime and

military and wish to fight them as soon as possible, despite assuming that the Zionists will use nuclear weapons. "The Zionists know we also have access to nuclear facilities, and if the Zionists will use theirs we will use ours."

Scaring The Japanese People With Radiation Is Criminal

By James Conca

Source: <http://www.forbes.com/sites/jamesconca/2014/06/25/scaring-the-japanese-people-with-radiation-is-criminal/>

I realize many journals and on-line publications need sensational headlines to attract readers. It seems necessary in these times of social media and 24-hour news cycles.

But it becomes unethical to push bad science without doing at least a little due diligence. I understand anti-nuke ideology cares little about science and is never held to any technical standard, but in some cases reporting bad science hurts people who need good science to make personal decisions for themselves and their families.

A recent textbook case of this malfeasance is the Fukushima-induced thyroid scare in Japanese children. There is no increase in thyroid health problems in Japanese children living in and around the Prefectures of Fukushima and it is unlikely there ever will be (UN Report; Nuclear News; J. of Am. Phys. and Surg.; CBCnews; Hiroshima Syndrome; National Geographic; Asahi Shimbun).

However, many so-called researchers, activists and reporters claim thyroid cancers have exploded in Japan and Japanese children are dying by the thousands (Business Insider; Eco Child's Play). They intentionally compared the wrong data sets, data sets that were not comparable, that used different methods, looked at different characteristics, even different ages. These news entities are not particularly known for their treatment of scientific issues and might be forgiven for not recognizing bad research, but just a phone call to a real scientist would have gone a long way to preventing this scare.

Unfortunately, these articles get picked up by other news outlets, lending them further legitimacy (Voice of Russia; CubaSi). And Eco Child's Play is supposed to care about children and parents, which they generally do. In this case, however, they have only caused grief and fear in thousands of parents in Japan.

The root of this thyroid cancer fear is the rapid and sophisticated screening of Japanese children for thyroid nodules and cysts after the Fukushima accident. The Thyroid Ultrasound Examination (TUE) Program was carried out as part of the Fukushima Health Management Survey, and uses the most sophisticated ultrasound technology that can detect thyroid growths better than previous methods.

The post-tsunami testing screened for all nodules of all sizes (Japan Probe; Fukushima Voice). Previous testing screened only for large nodules, greater than 5 mm, and large cysts, greater than 20 mm, since small ones are common in Japan and usually of no consequence. Hence, they didn't even write them down.

According to Dr. Jane Orient in an article just published in the *Journal of American Physicians and Surgeons*, "Modern ultrasound equipment, such as that used in the TUE study, is able to detect thyroid carcinomas as small as a few millimeters, long before these may come to clinical attention. Prior to the initiation of the TUE, no data existed to estimate the baseline frequency of thyroid cancer, detected by ultrasound, in a population of this age in Japan. Studies post Chernobyl show that radiation induced thyroid cancer has a minimal latency of around 4 years, so the initial screening carried out in Japan within 3 years of the accident would be predicted to give a measure of the background incidence of thyroid cancer in this population [and not any effect from Fukushima]."

So when comparing these data sets, you would obviously only compare those data for larger nodules, greater than 5 mm, since that's what the previous tests have data on.

However, these *we-want-to show-children-dying-so-everyone-will-hate-nuclear-energy* types have purposefully compared the total

data sets knowing full well that the recent ones would have thousands more small nodules not reported in the older data and, therefore, would make it appear that Fukushima had a huge health effect on children.

Scaring parents might be acceptable on Facebook, but in serious news outlets it's criminal.

There was never enough of an iodine-131 dose to children after the Fukushima accident to cause any problems because the Japanese government, for all their other issues, did the right thing in initially evacuating the region, and then preventing anyone from eating produce and drinking milk from that area until I-131 decayed away in the first two months. The Soviets did not do this after Chernobyl and that is the primary difference in the thyroid doses plus the vastly lower radiation emissions to the Japanese around Fukushima versus the Ukrainians around Chernobyl.

That's it. You can't get rad-induced thyroid cancer or tumors from anything else except radioactive iodine, and only from a dose in the first two months since I-131, with an 8-day half-life, dies away in that time. Cs-137 and Sr-90 don't affect the thyroid. They have a different biochemistry.

More importantly, you can't develop thyroid cancer this fast, it takes more than 4 years, and it's only been 3 years since the tsunami, and most of this screening was even earlier. So what has been measured so far in this screening is the *pre-Fukushima* baseline. It is good to do this extensive screening so that we can have a database to compare with the results several years from now when any Fukushima-induced thyroid cancers would actually show up.

The Japanese have a high level of iodine in their diet, which means that their thyroid glands are virtually saturated with non-radioactive iodine leaving little room for uptake of radioactive iodine. This is the reason for taking iodine pills before a plume of radiation hits you, but is only useful before it hits you. The areas around the Chernobyl power plant are naturally iodine deficient, and therefore uptake of radioactive iodine was greater in that population after Chernobyl.

The thyroid doses in Japanese children after Fukushima averaged 100 times lower than those after Chernobyl (4 mSv versus 500 mSv; UNSCEAR 2008). The WHO, UNSCEAR and the upcoming IAEA report state that no

increase in thyroid cancer will likely ever be discernible from Fukushima.

The results so far show no meaningful effect from Fukushima compared to previous data. Children from Fukushima have about the same number of thyroid growths as those in prefectures far away from Fukushima, in Aomori, Yamanashi, and Nagasaki prefectures, 0.7% versus 1%, respectively (*Hayashida et al, 2013*).

In addition, *"the overall rates of cysts (56.9%) and thyroid nodules (1.7%) as well as the proportion of ≤ 5 mm cysts (92%) and nodules (39%) are consistent with the cysts and nodules found in Fukushima children. Thus, crude comparison of rates in two pediatric populations suggests that thyroid lesions, particularly small thyroid cysts and nodules (≤ 5 mm), are common among children screened with sensitive ultrasound equipment"* (*Journal of American Physicians and Surgeons*).

So why are some unethical people declaring children are dying? Because they're unethical. And they don't care how many people they hurt as long as their political agenda is met. It's nasty, cruel and wrong.

Of course, the same names keep popping up with these stories, like Joseph Mangano, Harvey Wasserman and Helen Caldicott. These articles all say the same thing and reference the same debunked scientific studies that skew data to indicate a non-existent problem.

Since I subscribe to most of these environmental journals and have been a lifer for many groups such as NRDC, EDF, Sierra Club and Greenpeace, I am especially troubled. I understand the desire to reinforce a stereotype with data, but that is why being an actual scientist is important. We don't do that. It's why we have peer-review. By other scientists. *In that field*. Not editors, other writers or activists. A real scientist would have caught the disparity between these two incomparable data sets right off the bat.

Since few in the public read peer-reviewed journals or have the patience to plow through jargon-filled papers, it is the responsibility of scientists to communicate clearly and for journalists to have reputable sources.

Ironically, it has repeatedly been shown that the worst health effects from Fukushima have come from the fear of radiation and the forced evacuations, not from any radiation effects (Gaji 2013; Japan Daily Press; WHO Report;

NYTimes). Not one person has, or likely will, die from Fukushima radiation. But many people have died from the forced evacuations, fear and depression resulting from both well-intentioned and politically-motivated ignorance on radiation doses and effects following the accident.

Maybe *Business Insider* needs to follow up on their wanton contribution to this terrorism because, as we all know, radiation fear-mongering is an excellent weapon of terror. Why they would use it against our allies is confounding.

James Conca – I have been a scientist in the field of the earth and environmental sciences for 31 years, specializing in geologic disposal of nuclear waste, energy-related research, subsurface transport and environmental clean-up of heavy metals. I have found that important societal issues involving science and technology are rarely made on the basis of science, but on people's perception of science. Science is necessary but insufficient. It seems to be more important to understand Fareed Zakaria than Stephen Hawking, although you better understand both if you want to solve issues like sustainable energy development. Prior to my present position as Senior Scientist at UFA Ventures, Inc.. I was Director of the Center for Laboratory Sciences on the Campus of CBC, and Director of the WSCF at the Hanford Site. Before that, I was Director of the New Mexico State University Carlsbad Environmental Monitoring and Research Center, the independent and academic monitoring facility for the Department of Energy's WIPP site, a little-known deep geologic nuclear repository for bomb waste. I came to NMSU from Los Alamos National Laboratory where I was Project Leader for Radionuclide Geochemistry and oversaw data input into the Yucca Mt Project license application. Before that, I was on the faculty at Washington State University Tri-Cities. At the California Institute of Technology, I obtained a Ph.D. in Geochemistry in 1985 and a Masters in Planetary Science in 1981, and received a Bachelor's in Science in Geology/Biology from Brown University in 1979.

Ukraine crisis raises risk for nuclear reactors

Source: <http://www.dw.de/ukraine-crisis-raises-risk-for-nuclear-reactors/a-17694776>

Ukraine's volatility exacerbates the risk for the country's 15 Soviet-style nuclear reactors, warn German experts. They demand more attention for the country where the world's worst nuclear accident took place.



The recent news of a water shortage due to a broken pipeline affecting thousands in strife ravaged Eastern Ukraine spells trouble for the safety of the country's nuclear power plants.

That's because the security and reliability of a country's critical infrastructure like its electrical power and water grid is essential to safely run nuclear reactors.

"Once you have decided to operate a nuclear power plant or like in this case a nuclear reactor park, you must guarantee you don't have unstable social situations and you definitely can't have a war," Michael Sailer, chairman of the German Nuclear Waste Management Commission and member of the German Reactor Safety Commission, told DW.

Potential for human error

"We are talking about nuclear power plants that have a high risk even when they are constructed well and properly maintained," Sailer who also heads Freiburg-based environmental think tank Öko-Institut added. "And in the Ukraine we are talking about the additional problem that there is an increased

potential for human error due to less motivated nuclear operators than elsewhere and the fact that the security features of these reactors are a lot weaker than those of modern reactors."

Ukraine currently has four nuclear power plants with 15 reactors online providing roughly half of the country's energy needs which makes it practically impossible to shut them down during the crisis. All of the reactors stem from the Soviet era, went on the grid in the 1980s and are similar to the Chernobyl reactor that blew in 1986 causing the worst nuclear accident in history. Ukraine's largest plant in Zaporizhia is located about 200 kilometers from Donetsk, the epicenter of the clash between pro-Russian militants and the Kyiv government.

Danger of sabotage



Pro-Russian separatists have attacked public buildings in Eastern Ukraine

But it's not just the maintenance of the technical infrastructure and the motivation of the engineers operating the reactors that has the experts worried. The continued fighting between government and pro-Russian forces including the seizure of buildings raises the risk that the

country's nuclear plants could also be drawn into the mix.

The older Soviet-style reactors are already less safe than those in Western Europe, Lothar Hahn, former director of the Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Germany's leading nuclear safety research center, told DW. "But this is even overshadowed by the danger of sabotage or war. Then you would immediately have a dramatic situation on your hands."

The experts did not want to describe possible sabotage or war scenarios on the record, but stressed that they consider this a real danger. "You don't need an army, only 20 to 30 highly trained men," said Hahn. "These things are totally incalculable."

That's why NATO sent a small civilian expert team to Ukraine in April to advise officials on improving the safety of nuclear power plants and other critical infrastructure "in the context of possible threats". The experts then produced a confidential report that has been handed over to Ukrainian officials.

NATO role

One reason for Ukraine's request for NATO help was "possible destabilization" in the area where strategic infrastructure was located, the country's ambassador to the alliance told Reuters.

NATO's help is useful, but also limited, said Sailer. It can advise Ukrainian officials on how to improve its facilities to better defend against possible intruders. "But at the end of the day, if you have a team that is sympathizing with pro-Russian militants and the conflict escalates then this will become part of it. The second thing where NATO can't help at all is the safety and stability of the power grid."

"If you imagine Ukraine without clear command structures, this clearly means that the stability of the entire power grid is threatened," noted Sailer. "And a nuclear power plant without several connections to

a solid power grid is extremely dangerous."



More attention

The Chernobyl ruin serves as a reminder of the danger of nuclear energy

That the command structures particularly in the east of the country are already tenuous and embattled is evidenced by the ongoing fighting,

the hostage taking of OSCE observers and the seizures of public buildings. And that this can easily affect critical infrastructure is highlighted by the recent news of a broken water pipeline in Eastern Ukraine.

That's why - notwithstanding NATO's assistance - not enough attention is being paid to the security of nuclear power plants in Ukraine, argue the experts.

"It's really a problem, because only very few people think about this," said Sailer. Nuclear experts usually don't focus on such instable situations and the people who are concerned with instable situations like diplomats usually don't realize how sensitive a nuclear power plant is."

Chernobyl's arch: Sealing off a radioactive sarcophagus

Source: <http://www.bbc.com/news/magazine-25086097>

27 Nov 2013 – Work began in recent days to remove, bit by bit, the giant chimney protruding from the Chernobyl nuclear power station. It's one small part of a mammoth engineering project, now nearing completion, designed to slash the risk of another major release of radioactivity.

Massive and glittering in the weak winter sunshine, a half-built arch looms over Chernobyl's decaying industrial landscape of cooling towers and power lines.

One of the biggest engineering projects in history, it has been likened to a gigantic metal igloo, built to seal off hundreds of tons of nuclear fuel and dust buried inside reactor number four, which in 1986 blew up and burned for 10 days.

Everything about the project is epic: the size, the 1.5bn euro (£1.2bn) cost, the technical problems of working on a radioactive building site.



The ends of the arch will also be sealed

At 110m (360ft) tall, the structure could house the Statue of Liberty, and at 257m (843ft) wide, there would be room for a football pitch. There are acres of metal panels in the roof, to seal off the reactor and the dangerous mess inside. The whole lot will be held together by 680,000 heavy bolts.

With these gigantic dimensions the arch would be difficult to build anywhere, but it is being assembled in one of Europe's more remote corners, a site surrounded by forest and marsh in northern Ukraine, far from the factories of Western Europe where its component parts are made. This autumn, as the project reached the half-way point, it was more than a decade behind schedule, although engineers believe work will now go more quickly and it could be finished in 2015.

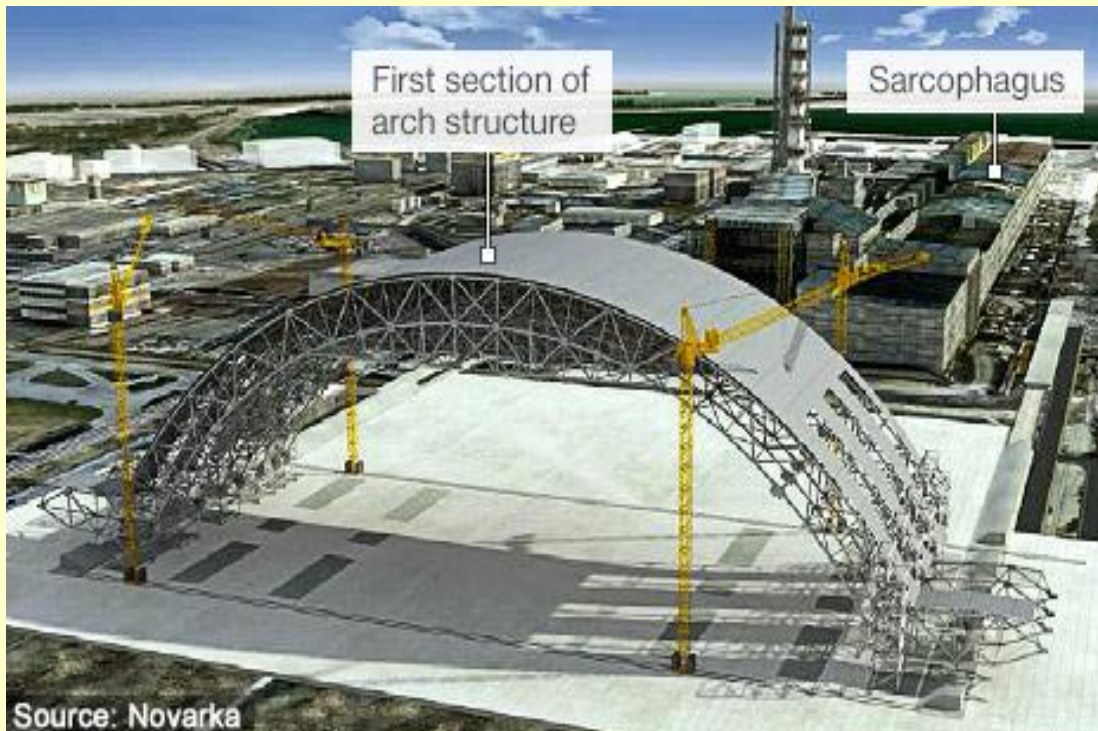
"Nothing like this has ever been attempted before," says Don Kelly, 57, a nuclear industry veteran from Washington State, as he walks under the arch. He works with foreign specialists from 24 nations, as well as hundreds of Ukrainian workers. Young French technicians, who monitor radiation, work alongside Ukrainian veterans of the 1986 disaster, former Soviet engineers who risked their lives battling to put the fires out after the reactor exploded, sending a cloud of radioactivity across Europe. Grinning with enthusiasm as he stares up at the roof, Mr Kelly points out Turkish workers in harnesses far overhead. "For anyone in the nuclear business, this is the place you want to be: the biggest, most exciting project in the world right now," he says.



Bolts used to assemble the Arch are some 15cm long and weigh more than 1kg

Every stage of the project has been a step into the unknown. Nobody has ever had to make a wrecked nuclear reactor safe before. Just preparing the site where the arch is being assembled required the removal of hundreds of

tons of radioactive topsoil, then laying concrete foundations 8m (26ft) deep. The reactor building itself, badly damaged in the 1986 explosion and fire, is still far too radioactive for people to work there assembling the arch above it. Instead the arch has had to be put together a few hundred metres away, at a safer distance from the reactor's intense radiation. Half of it is ready, and when the other half is finished, the two parts will be clamped together. Then, as nervous engineers look on, 29,000 tons of metal will slide along specially laid tracks, until the reactor is covered and sealed off.



The arch is being assembled in two halves in an area about 300m to the west of the sarcophagus, to protect workers from high levels of radiation. The project is due to be completed in 2015.

At present, it is contained by a shelter of concrete and metal panels called the sarcophagus, built in the months after the accident. It was supposed to have been replaced in 2006, and although it has been shored up, it is now rusting and in danger of collapse. Last February there was a radiation alert when part of the turbine hall roof next to the reactor collapsed. The site was evacuated, although nobody suffered harmful effects and work soon resumed.

Everyone hopes the arch will be completed before there is a major collapse. If this were to happen now, it would send a plume of radioactive dust into the sky, scattering radiation across a large area. It's one reason Ukrainians worry about the repeated delays to the project.

Radioactive dose limits at Chernobyl

The annual radioactive dose limit is 20 millisieverts (mSv).

Some parts of the Chernobyl site are more radioactive than others, so the time that workers are permitted to spend in any one place varies.

Three separate ways of reaching the annual dose limit would be to spend:

- **50,000 hours** at the on-site office
- **2,000 hours** in control room Unit 4
- **12 minutes** above the sarcophagus roof

The area under the arch is now safe enough for people to work unprotected, although dosimeters and breathing equipment must be carried at all times. But just a couple of hundred metres away, workers must wear white suits and hats, and breathe through masks.

This month, one of the trickiest operations in the whole project began, the removal of the old reactor chimney, which must be got out of the way before the arch can slide into place.

Work has started removing sections weighing up to 55 tons each. They must be cut off with a plasma cutter by teams of two workers and removed by crane - a nerve-racking process. If a crane fails, or an operator miscalculates, and a section falls into the reactor, this too could release a new cloud of radioactive dust into the atmosphere.

Anyone working on the chimney must also be carefully monitored. All staff working on the arch have an annual allowance of exposure to radiation. Once it has been used up, they are sent to work offsite. Around the chimney, an entire year's allowance will be used up in a few hours.

Engineers say the radioactive environment is why work has been so slow. "It's not dangerous, it's just very, very difficult," says Philippe Casse, 61, the site manager. "You have to organise everything to avoid the risk to people. But it is worth doing. I'm not just here to make a living, I'm here to make Chernobyl safe."

The cost of the project is being borne by some 40 countries, and the work is being done by Western corporations assisted by Ukrainian companies. Nearly three decades after the accident, the radioactive mess in Chernobyl remains a grave threat to the health of Ukrainians.

Eventually, when the arch seals off the reactor, the plan is for giant cranes to lift out the remains of the reactor and what's left of the fuel, which melted and flowed like lava into chambers beneath it. But there are fears the cranes would quickly become so radioactive they could not be maintained, and would gradually stop working. There is also still no suitable nuclear waste dump in the country.

Philippe Casse acknowledges that getting rid of all this highly radioactive material will be far more difficult than building the arch.

"Disposal will be an even bigger project," he says.

"There is no money at the moment.

"It could be done in 50 years' time. Perhaps there will be the technology to solve the problem then."

Chernobyl's radioactive trees and the forest fire risk

Source: <http://www.bbc.com/news/magazine-18721292>

Much of the 30km exclusion zone around the Chernobyl nuclear plant is pine forest, and some of it so badly contaminated that a forest fire could create a devastating radioactive smoke cloud.

Heading north from Kiev in Ukraine, you can see old ladies and their grand-daughters sitting waiting expectantly in the long grass, shaded from a sweltering sun, under the straight red eaves of tall, orderly Scots pines which line the road.

It is blueberry season, and they are selling them by the plastic pint glass. You could pull in to haggle, but Sergiy Zibtsev, a professor from the Forestry Institute at the Kiev University of Life Sciences does not recommend it. They are laced with radioactive strontium.

Berries are highly efficient at soaking up and storing radionuclides, huge quantities of which were dispersed over large parts of the Soviet Union and Western Europe by smoke plumes from the explosion.

Radiation measurement checks only take place in official markets, and usually only for caesium. As for the hundreds of makeshift fruit stalls, generally run by old ladies, these are never checked at all.

Having said this, the berries are not uniformly harmful. In an average pint of them, perhaps only a quarter will be contaminated. The main thing is to make sure you do not put them on your cereal every day.

Besides the blueberry sellers, the road on the fringes of the exclusion zone surrounding Chernobyl feels busier than when I first came here with Sergiy a couple of years ago.

There is a girl in high heels tottering along the verge, chatting on her iPhone. A large barley field ripples in the wind, ready for harvesting. A young couple shoot by on a moped.



Up to 80 forest fires are tended to each year

This region is slowly getting back to normal, says Sergiy. People are returning to farm this once booming agricultural area.

It is happening inside the exclusion zone too. Chernobyl Forestry Enterprise is now planting small new pine stands which it plans to harvest in 80 years' time. But there

are serious problems with the rest of Chernobyl's extensive pine plantations.

Pine damages easily. Wind blows it down. Insects infest it. Drought makes brush into perfect tinder which can all too easily catch fire. And these dying radioactive plantations are considered too



dangerous and expensive to clear.

If ignited, one expert likens the potential effect to setting off a nuclear bomb in Eastern Europe. Wind could carry radioactive smoke particles large distances, not just in Ukraine, but right across the continent.

To help establish or disprove such hypotheses, Sergiy

has come to Chernobyl to gather data about a very large fire which spread unchecked and destroyed a huge area of Scots pine in 1992. A colleague is preparing a scientific paper on the fire's consequences, which are still largely unknown.

Together, they hope to attract funding to model the danger represented by Chernobyl's forest.

If they can pinpoint the most vulnerable pine stands, the next step will be to persuade the Ukrainian government and other partners to invest in training and equipment to safeguard Chernobyl's firefighters, and perhaps eventually to clear parts of the forest considered to be at the most risk.

Firefighters in Chernobyl have one of the least enviable jobs in the world. They spend all day up rusty Soviet watchtowers, which sway in the wind like tin-box metronomes, and act as conductors to the huge lightning storms which swing across the land most afternoons in summer, often sparking fires.

When they spot a wildfire, the firefighters triangulate its location by radio. Teams jump aboard big, red, Soviet fire trucks, and lumber along cracked, overgrown roads to the source of the blaze.

Their equipment is very basic. They believe they know when they are fighting a radioactive fire - they experience a tingling, metallic sensation in their skin - but they do not fully understand the serious dangers of being exposed to superheated radioactive particles.

Their job description still belongs to heroic, Soviet ideals - they must put the blaze out, no matter the personal consequences.

Sergiy says more big wildfires in Chernobyl like the one in 1992 would be catastrophic for Ukraine's image, and potentially devastating for farmland right across Europe.

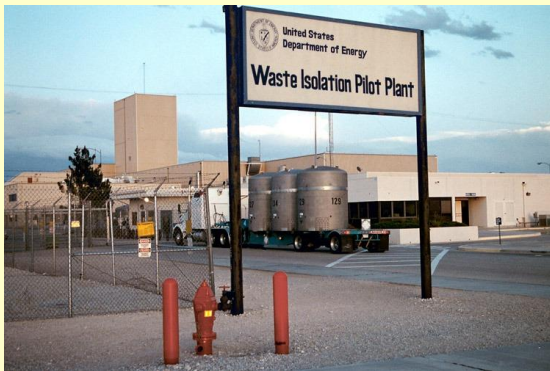
Lots of people are working on the problem, which continues with each new hot summer.

Sergiy and his colleagues need support, not just to save Chernobyl's firefighters from exposure to high doses of radiation, but to stop the particles migrating up into the air and away wherever the wind blows them, spreading the legacy of an accident which many people think we can already safely forget.

Los Alamos lab admits mishandling toxic waste, causing repository radiation leak

Source: <http://www.homelandsecuritynewswire.com/dr20140709-los-alamos-lab-admits-mishandling-toxic-waste-causing-repository-radiation-leak>

In a letter addressed to the New Mexico Environment Department (NMED), lab officials at Los Alamos

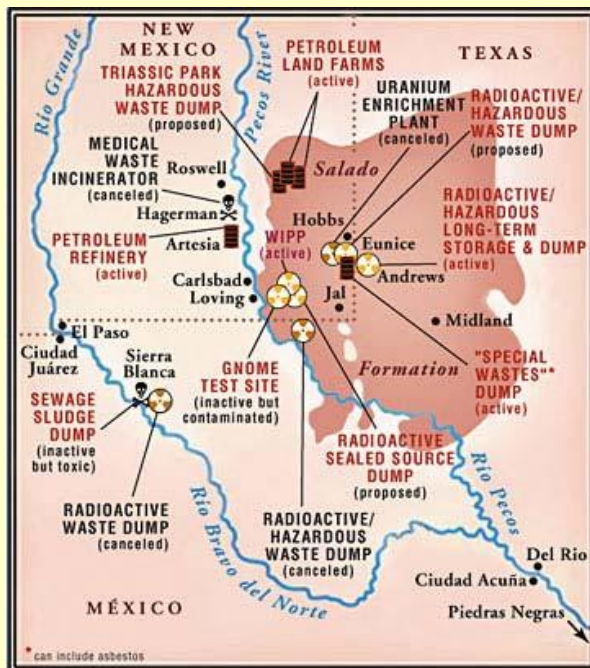


National Laboratory (LANL) have admitted to mishandling toxic waste shipped to the Waste Isolation Pilot Plant (WIPP) in Carlsbad, New Mexico, the nation's only permanent repository for plutonium-contaminated waste from government nuclear facilities. The letter, released by state regulators last Thursday, does not confirm whether the violations or LANL's use of an organic absorption material in waste containers is to blame for the underground radiation leak which occurred on 14 February,

contaminating twenty-two workers with low levels of radiation.

LANL failed to follow proper protocols when switching from inorganic absorption material to an organic substitute, and the lab also failed to follow up on waste which tests showed to be highly acidic, both in violation of its Hazardous Waste Facility Permit. Despite hundreds of experiments, investigators have been unable to confirm what actually caused the underground leak. In the meantime, the repository remains closed.

ABC News reports that Terry Wallace, LANL principal associate director for global security, told employees at a recent meeting that an in-house investigation is focused on sixteen barrels of highly acidic, nitrate-salt-bearing waste, including the drum that leaked at WIPP. Ten barrels under investigation remain underground at WIPP, while five are in temporary storage at a private waste facility in Texas. According to an internal-LANL memo obtained by the AP, Wallace noted that a



technical review “identified certain conditions that might potentially cause an exothermic reaction inside a drum. Among them are neutralized liquids, a low pH and the presence of metals.”

“The low pH findings should have prompted a pause in work to ensure appropriate technical and regulatory reviews of next steps,” Wallace said.

LANL is now focused on correcting the processes to prevent any recurrence. “We need to get this right and set best practices for the entire Complex,” Wallace said.

NMED is reviewing the “initial violations and plans to take appropriate actions once it concludes its independent review of the incidents at WIPP and LANL,” including an underground truck fire at WIPP six days before the radiation leak.

Game of marbles inspires nuclear-inspection protocol

Source: <http://www.homelandsecuritynewswire.com/dr20140709-game-of-marbles-inspires-nuclear-inspection-protocol>

Modern cryptography combined with simple radiation detectors could allow nuclear-weapons checks to be carried out with almost complete security. That is the conclusion of scientists in the United States,



who have used computer simulations to show how a beam of neutrons can establish the authenticity of a nuclear warhead without revealing any information about that weapon’s composition or design.

Current arms-control arrangements between the United States and Russia limit the number of nuclear warheads inside missiles. Future agreements, however, could require that all warheads be accounted for, including those in storage. This would rely on inspectors being able to tell a real nuclear warhead apart from a fake one — which would prevent a country from secretly stashing away some of its declared warheads.

Plutonium-239 in a concealed warhead can be revealed by exposing it to gamma rays or neutrons. This means of detection, however, would also reveal secret information about the design of the weapon, which must be kept from the inspectors to prevent nuclear proliferation.

Open to abuse

Proposed schemes to avoid this problem involve passing the detector’s output through an electronic device that strips the data of their sensitive elements, such as the precise amount of radioactive material contained in the weapon. Such techniques, however, are open to abuse. The inspector could syphon off sensitive data, while the weapon’s owner could interfere with the device and make innocuous objects appear to be nuclear warheads.

An IOP release reports that the newly proposed technique closes these loopholes by not producing any sensitive information in the first place. It is based on the “zero-knowledge proof,” in which two objects can be shown with near certainty to be identical, even though nothing is known about the objects themselves. In their work, Alexander Glaser of Princeton University and colleagues adapt a game in which a character known as Alice must prove to a second person, Bob, that the number of marbles in each of two cups she is holding is the same, without revealing what that number (N) is.

Alice empties the contents of each cup into a separate bucket, each of which she says already contains 100–N marbles. Bob then counts the number of marbles in each bucket to find out whether or not they add up to 100. Alice could try to deceive Bob by not putting the same number of marbles in each bucket. However, if Bob specifies which cup must be emptied into which bucket he has a 50-50 chance of discovering Alice’s deception. If the

process is repeated many times — and Alice continues to lie — it is unlikely that she can maintain her deception for long.

Arrays of neutron detectors

For weapons verification, the idea is for the host (Alice) to show the inspector (Bob) that an unknown, concealed object is identical to a known nuclear warhead. Both items are exposed to beams containing equal numbers of high-energy neutrons, with the transmitted radiation recorded by two separate arrays of simple detectors that cannot be tampered with clandestinely. Playing the role of the buckets, the detectors are set by the host to compensate precisely for the reduction in recorded intensity that the warhead in question is known to cause.

The inspector should find that all of the detectors display the same, maximum count that would be recorded if no object were to be placed in the neutron beam. To make sure that no cheating has taken place, however, the inspector chooses which detector array is assigned to which object. If the host has lied then some of the detectors will not show the maximum count — and if the process is repeated enough times, the chance of evasion is close to zero. The inspector can therefore establish whether or not the unknown object is a nuclear warhead, and does so without finding anything out about the weapon itself.

To investigate the feasibility of their technique, Glaser and colleagues carried out a Monte Carlo simulation in which neutrons with an energy of fourteen MeV irradiate a 19-cm-diameter ball containing concentric rings of

polystyrene, tungsten, aluminium, graphite and steel. This standard object is used to calibrate nuclear-weapon imaging systems. They found that their technique should reveal whether the tungsten had been removed or replaced by lead, even for relatively small neutron doses.

Cheating could leak information

John Finney of University College London believes that the new approach should be less vulnerable to cheating than existing techniques that rely on an information barrier. "It could potentially be a major step-change in improving confidence in inspections," he says, "as long as you work through to prove that the system works as designed." Another "nice twist" to the work, he adds, is that any attempt by a host to tweak pre-loaded data might actually lead to classified information leaking out. "It is an inherent property of the system that it goes against attempts to cheat," he says.

Glaser is now looking to reproduce his group's results experimentally, using neutrons from the Princeton Plasma Physics Laboratory and bubble chambers as detectors. One priority is ensuring the stability of the neutron source to guarantee that unknown and reference objects are exposed to equally large neutron fluxes. Also critical is establishing the consistency of the detectors. "Can we distinguish a fresh bubble from a pre-loaded bubble?" he asks. "If it turns out we can, then that is something we have to know." These tests should yield results within about six months, and then the technique will be evaluated using real weapons materials.

— *Read more in Alexander Glaser, "A zero-knowledge protocol for nuclear warhead verification," Nature 510 (26 June 2014): 497-502*

Iraq tells U.N. that 'terrorist groups' seized nuclear materials

Source: <http://www.reuters.com/article/2014/07/09/us-iraq-security-nuclear-idUSKBN0FE2KT20140709>

July 10 – Insurgents in Iraq have seized nuclear materials used for scientific research at a university in the country's north, Iraq told the United Nations in a letter appealing for help to "stave off the threat of their use by terrorists in Iraq or abroad."

Nearly 40 kilograms (88 pounds) of uranium compounds were kept at Mosul University, Iraq's U.N. Ambassador Mohamed Ali Alhakim told U.N. Secretary-General Ban Ki-moon in

the July 8 letter obtained by Reuters on Wednesday.

"Terrorist groups have seized control of nuclear material at the sites that came out of the control of the state," Alhakim wrote, adding that such materials "can be used in manufacturing weapons of mass destruction."

"These nuclear materials, despite the limited amounts mentioned, can enable terrorist groups, with the availability of the required

expertise, to use it separate or in combination with other materials in its terrorist acts," said Alhakim.

He warned that they could also be smuggled out of Iraq.

A U.S. government source familiar with the matter said the materials were not believed to be enriched uranium and therefore would be difficult to use to manufacture into a weapon. Another U.S. official familiar with security matters said he was unaware of this development raising any alarm among U.S. authorities.

A Sunni Muslim group known as the Islamic State is spearheading a patchwork of insurgents who have taken over large swaths of Syria and Iraq. The al Qaeda offshoot until recently called itself the Islamic State in Iraq and the Levant (ISIL).

"The Republic of Iraq is notifying the international community of these dangerous developments and asking for help and the needed support to stave off the threat of their use by terrorists in Iraq or abroad," Alhakim wrote.

Iraq acceded to the Convention on the Physical Protection of Nuclear Material on Monday, said the International Atomic Energy Agency (IAEA). The convention requires states to protect nuclear facilities and material in peaceful domestic use, storage and transport.

"It also provides for expanded cooperation between and among states regarding rapid measures to locate and recover stolen or smuggled nuclear material, mitigate any radiological consequences of sabotage, and prevent and combat related offences," according to the IAEA.

The Untold Story of China's Forgotten Underground Nuclear Reactor

By Jeffrey Lewis

Source:http://www.foreignpolicy.com/articles/2014/07/08/the_untold_story_of_chinas_forgotten_underground_nuclear_reactor_yichang_827_plant



Go to a conference about China's nuclear weapons and you will hear, over and over again, that China is not very transparent when it comes to its nuclear program. That's still true at a governmental level, but it is an increasingly

outdated assessment of other aspects of Chinese society, especially in the age of social media. Western analysts have more access to information on these topics than they have ever had access to before, even if much of it is in

Chinese. That has led to some startling discoveries.

For example, despite official secrecy about China's production of plutonium for nuclear weapons, my colleague Catherine Dill and I discovered an underground nuclear reactor that China attempted to construct near Yichang in Hubei province during the 1960s and 1970s. The Yichang reactor is different from the never-finished underground nuclear reactor near Fuling, in Sichuan province, which the government opened to tourists a few years ago. The reactor at Fuling was a surprise when Chinese authorities publicized it, but it was still only an unfinished copy of one of China's above-ground nuclear reactors. The reactor at Yichang, on the other hand, is a totally different design. As far we can tell, the existence of the Yichang reactor has never been written about in English.

We didn't start out looking for a secret underground nuclear reactor. I recently finished writing an Adelphi book for the International Institute for Strategic Studies on China's nuclear weapons program. My book makes extensive use of open sources. As part of the research, I was looking into part of China's nuclear industry called the "827 Plant." China has lots of factories associated with the nuclear industry, so an unidentified plant wasn't necessarily anything interesting.

I still wanted to know what role the 827 Plant played in China's early nuclear weapons program, even if it was boring. When we started looking into the 827 Plant, I hoped we might find something exciting, like an unknown fuel-cladding plant. (That's sarcasm, by the way. Not even nuclear-policy wonks think fuel-cladding plants are exciting.)

There is an enormous amount of open-source information available about China's nuclear programs. Of course, that information is encrypted in a kind of tonal and ideogrammatic code referred to as Chinese. But it is out there. I have to admit that my Chinese skills are pretty limited. I once made the mistake of joking with a Chinese friend that I can only order a beer and start a fistfight in Chinese, which pretty much makes me proficient in the language. He laughed and has now spent the past decade introducing me as a "proficient" speaker of Chinese, largely to make me tell that joke again and again. Fortunately, the Monterey Institute, where I work, has a large number of amazing students and researchers, such as Catherine

Dill, with both language skills and expertise in proliferation who can compensate for my deficiencies.

Searching for any reference to the 827 Plant, Catherine and I found a lot of references on resumes of Chinese nuclear engineers online. Plenty of Homer Simpsons worked there through the early 1980s, before finding employment in the civilian nuclear power program.

Then the resumes gave way to an amazing memoir we found online. Cui Zhaohui is a retired professor of nuclear engineering at Tsinghua University. He has written a very interesting memoir recounting his career, which started at China's original plutonium production reactor near Jiuquan. Jiuquan was the original source of China's military plutonium. While Cui never worked at the 827 Plant, he mentions in passing a colleague who was reassigned there. Almost as an afterthought, Cui mentions that the 827 Plant was "originally planned [as a] heavy-water nuclear reactor and reprocessing plant."

I had to read that again. Did he just tell me the 827 Plant was a secret nuclear reactor that I'd never heard about? Is this guy for real? Is he just pulling my leg? How does he know his friend wasn't pulling his leg?

Suddenly, I was very interested in the 827 Plant. The Chinese plutonium-production reactors we know about were based on a totally different Soviet design that used graphite and plain old "light" water. Did China try to build a second underground nuclear reactor with a completely different design at the same time? We kept finding more and more evidence to suggest that Cui was right. One academic paper about a nuclear research facility in Beijing, for example, explained that it was a sort of prototype for a much larger, never completed heavy water reactor called the 827 Plant.

Eventually, we decided to locate the 827 Plant site. Lots of sources said the 827 Plant was near Chinese city of Yichang, in Hubei Province. Since Yichang is just downriver from the Three Gorges Dam, we had a temporary panic that the remains of the reactor were now underwater.

Thousands of people lived and worked at the site before it was abandoned sometime in the 1980s. The children of those people are now adults. And like most grown-ups, they are nostalgic. They have reunions and even a blog.

They have posted many pictures of the abandoned site online. The local municipality is attempting to redevelop the abandoned site as an artist's community.

With so many pictures, it was easy enough to find the site in satellite images. The 827 Plant is located at 30°50'56"N, 111° 8'46"E, between Yichang and the Three Gorges Dam.

Then we noticed something amazing. If you look at the site in Google Earth with the Panoramio layer, there are a number of ground-truth images posted by the same person who maintains the 827 families blog. The title of one image (in Chinese) is "827 pump house." It appears to be the ruined pump house that brings river water for the secondary cooling loop for the reactor, which seems to have been constructed underground. Holy cow! Like the other reactor near Fuling, the paranoia of Maoist China had driven them to place the reactor underground to protect it from an attack that never came.

In the early 1960s, China had one plant to make highly enriched uranium near Lanzhou and was completing one nuclear reactor to produce plutonium at Jiuquan. In 1964, China began the "Third Line" effort -- a massive construction effort to relocate all of China's heavy industries, nuclear and otherwise, in the interior of the country. Often these factories, including things as mundane as steel mills, were placed underground to protect them from Soviet or American attack. As you might expect, the disruption of attempting to relocate the country's heavy industries to underground caverns in the rural interior was a complete and total cluster... well, you know. Wikipedia calls the Third Line "an economic fiasco," which seems to me to be an example of the wisdom of crowds.

As part of the Third Line effort, China's nuclear engineers were supposed to build a copy of the first reactor -- the one where Cui worked -- in an underground cavern being dug near Fuling. But placing a nuclear reactor under a mountain is about as slow and arduous as you might expect. At some point in 1969, with relations between Moscow and Beijing collapsing, Beijing decided it could not wait for the engineers to finish Fuling. The first proposal suggested physically picking up and moving the reactor near Jiuquan somewhere else. Eventually the technical personnel convinced the Chinese leadership this was total madness. So, instead, China started building a temporary

replacement above ground, near a place called Guangyuan in Sichuan.

I always wondered how, in the middle of the paranoia associated with the Cultural Revolution, Chinese leaders came to their senses and ditched the underground reactor at Fuling in favor of the above-ground copy at Guangyuan. It turns out they didn't. Instead of replacing one crazy project with a more sensible one, the Chinese doubled-down on crazy -- continuing the reactor project at Fuling, starting a new one at Guangyuan and, we now know, starting the underground reactor at Yichang. That, come to think of it, sounds more like Mao's China during the Cultural Revolution. Not many leaders respond to resource bottlenecks by tripling reactor construction, but Mao Zedong wasn't most leaders. As best we can tell, China never finished the heavy water at Yichang, just as it never finished Fuling or any other number of wildly implausible Third Line projects. Construction at Yichang lumbered on through the 1970s, before being shut down around 1980 or so. At this point, the Chinese government took a number of steps to transition its nuclear industry to civilian power generation, converting and eventually decommissioning the reactor near Jiuquan, as well as giving up on Fuling and Yichang. China would not build a heavy water reactor until it bought CANDU heavy water reactors from Canada, one in 2002 and another in 2003. (CANDU is a portmanteau of "Canada" and "deuterium oxide," better known as heavy water.) Yichang is just a footnote. A crazy, implausible footnote.

The failed effort to build an underground reactor near Yichang helps explain some mysteries about China's plutonium production. China didn't produce a ton of plutonium for a nuclear weapons state. (Well, it produced a ton -- like one, maybe two, but almost certainly not more than four.) That means China's nuclear arsenal cannot grow beyond a several hundred warheads unless it builds new reactors to make plutonium. One question has been whether there are, or were, other sites in China churning out plutonium in secret. That now seems unlikely. We now know that China, during the madness of the Cultural Revolution, tried to build several underground nuclear reactors in the 1970s and failed. During the 1980s, China ended these projects, converting and closing all of these facilities. Of the two plutonium production reactors that China

finished, Jiuquan closed in the late 1980s and Guangyuan closed sometime in the 1990s. China never finished the reactors at Fuling or Yichang. China's surprisingly small stockpile of plutonium isn't so surprising once we know this historical context. They tried to make more. They just couldn't.

Yichang also helps explain why China has been reluctant to negotiate to a treaty banning the production of fissile material for nuclear weapons purposes and cagey about the history of its plutonium production efforts. Secret projects like the underground nuclear reactor near Yichang may be one reason why. Publicizing this history, on the other hand, may provide an opportunity to engage the Chinese

government on the need, even inevitability, of becoming more transparent.

It is time for Beijing to understand that we now live in an era in which social media and Google Earth can reveal the existence of a long-secret underground nuclear reactor. This is a different world than in the past, one that will be far more transparent than most governments realize at the moment. And we are only at the beginning of this era. There will be more disclosures. Like yet another unfinished secret underground nuclear reactor that I haven't mentioned. That's right, there is a third underground nuclear reactor project that we've found. But I will keep that one a secret. For now.

Jeffrey Lewis is director of the East Asia Nonproliferation Program at the James Martin Center for Nonproliferation Studies.

Iran wants to expand its uranium enrichment capacity

Source: <http://www.homelandsecuritynewswire.com/dr20140710-iran-wants-to-expand-its-uranium-enrichment-capacity>

July 10 – Former Iran president Ahmadinejad reviews uranium enrichment facility // Source: vietbao.vn
Iran's Supreme Leader Ayatollah Ali Khamenei



said on Tuesday that Iran would need significantly to increase its uranium enrichment capacity for future energy needs, dealing a setback to negotiations between the country and world powers. Iran and the United States, Russia, France, Germany, China, and Britain have less than two weeks to agree on the future scope of Iran's enrichment program and other issues if they are to meet a self-imposed 20 July deadline for a deal.

Iran wants to expand its capacity to refine uranium to support a planned network of atomic energy plants, but other members of the negotiating nations insist Iran must reduce its capacity to prevent it from producing a nuclear bomb using highly-enriched uranium.

"Their aim is that we accept a capacity of 10,000 separative work units (SWUs), which is equivalent to 10,000 centrifuges of the older type that we already have. Our officials say we need 190,000 SWU. Perhaps this is not a need this year or in two years or five years, but this is the country's absolute need," Khamenei said in a statement published on his website late on Monday. SWUs are a measurement of the effort required to separate isotopes of uranium for use in nuclear power stations or nuclear weapons.

Western diplomats note that Iran had lowered its demands for the size of its future nuclear enrichment program, but Mark Fitzpatrick, director of the non-proliferation program at the International Institute for Strategic Studies (IISS), said Khamenei's statement "confirms what I have suspected: that although Iranian negotiators have leeway on some issues, such as transparency and the timeframe for lifting sanctions, they are not authorized to accept cutbacks to the enrichment program."

Yahoo News reports that Iran has more than 19,000 installed enrichment centrifuges, mostly old-generation IR-1 machines, with about 10,000 of them operating to increase the concentration of uranium fissile isotope U-235. Over the last decade, Iran has significantly expanded its centrifuge capacity, but the

country stopped doing so under a 24 November 2013 agreement between Iran and

the six nations in exchange for limited sanctions relief.

Life after a nuclear war revealed: Computer models reveal Earth would suffer a 20-year-long winter and worldwide famine

Source: <http://www.dailymail.co.uk/sciencetech/article-2699854/Life-nuclear-war-revealed-Computer-models-reveal-Earth-suffer-20-year-long-winter-worldwide-famine.html>

THE AFTERMATH OF NUCLEAR WAR ACCORDING TO THE STUDY

Year 0

Five megatons of black carbon released into the atmosphere, which absorbs sunlight and begins to cool the planet. Black carbon rain also kills millions.

Year 1

Average surface temperature drops by 1°C (2°F).

Year 2

Crop growing season is shortened by 10 to 40 days.

Year 5

Earth is an average of 1.5°C (3°F) colder than the present day, colder than it has been in 1,000 years. There is also nine per cent less rainfall. The ozone is also up to 25 per cent thinner, increasing UV rays on Earth.

Year 10

Ozone recovers slightly to just 8 per cent less than modern day.

Year 20

Planet warms slightly to 0.5°C (1°F) lower than the present day.

Year 26

Rainfall increases to about 4.5 per cent less than today.

They then used computer models to examine the impact on the planet and its environment - and it makes for grim reading.

The immediate result of 100 nuclear weapons roughly the size of those dropped on Hiroshima and Nagasaki being detonated would be the release of five megatons of black carbon into the atmosphere.

Black carbon, not too dissimilar to soot, would block out the sun and can also be fatal to humans.

Following a spell of black carbon rain, a deadly weather front that would devastate what remained of humanity following the nuclear war, the temperature of Earth would begin to drop.

After a year the temperature would fall by 1°C (2°F), while after five it would be 1.5°C (3°F) cooler than it is now.

About 20 years after the conflict it would warm again to just 0.5°C (1°F) below today's temperature.

Accompanying what the researchers call 'the coldest average surface temperatures in the last 1,000 years' would be a huge loss in ozone levels.

They say that global ozone losses of 20 to 50 per cent would occur over populated areas, 'levels unprecedented in human history'.

The immediate result of 100 nuclear weapons being detonated would be the release of five megatons of black carbon (shown) into the atmosphere, say researchers. Black carbon, not too dissimilar to soot and released from the burning of things such as fossil fuels, would block out the sun and can also be fatal to humans

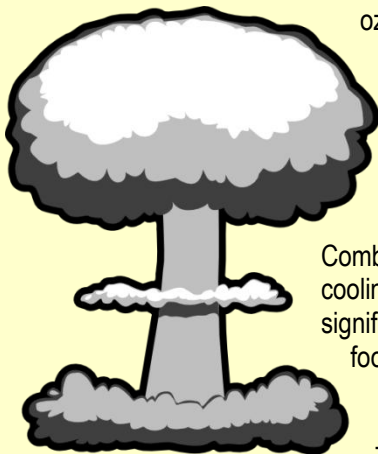


The drop in temperature would produce 'killing frosts' that reduce the world's growing season by 10 to 40 days.

Meanwhile the eradication of up to half of the ozone would increase UV rays in some locations by as much as 80 per cent, raising the chance of developing skin cancer for large swathes of humanity.

Combined with the global cooling, this 'would put significant pressures on global food supplies and could trigger a global nuclear famine.'

The planet's falling



temperature would also decrease the amount of rainfall.

Five years after the conflict Earth would see 9 per cent less rain, while 26 years after the war there would still be 4.5 per cent less rain.

The result of all this would be devastation and ultimately death for hundreds of millions, and perhaps billions.

But the researchers hope that their example of a relatively small nuclear war between two modestly armed nuclear nations, India and Pakistan, will encourage superpowers such as the U.S. and Russia to discuss nuclear disarmament.

'Knowledge of the impacts of 100 small nuclear weapons should motivate the elimination of more than 17,000 nuclear weapons that exist today,' they write.

► Read the full paper at: <http://onlinelibrary.wiley.com/doi/10.1002/2013EF000205/full>

Japan testing underground nuclear waste storage depot, despite local concerns

Source: <http://www.homelandsecuritynewswire.com/dr20140723-japan-testing-underground-nuclear-waste-storage-depot-despite-local-concerns>

Data is being collected at the Horonobe Underground Research Center, in Horonobe,



Japan to determine whether the site is able to begin storing radioactive waste in conditions which could last for 100,000 years. The sprawling laboratory, carved into the ground, is outfitted with cables and gauges that measure the movement of groundwater and tectonic shifting, given Japan's long history of ground fluctuation. Currently, if approved, the site is expected to begin operation in radioactive storage in 2015.

Japan Today reports, however, that some of the town's 2,500 residents are

worried about the possibilities of mismanagement and accidents.

"I'm worried," said Atsushi Arase, "If the government already has its eye on us as a potential site, it may eventually come here even if we refuse."

Others, such as the town mayor Akira Miyamoto have urged further development in the project, citing how it "helps revitalize our town."

Japanese utility systems have produced more than 17,000 tons of spent nuclear fuel rods from power plants which are no longer useful but are expected to remain radioactive for around several thousand years. The problem has been



a tough one for the Japanese government, which is currently debating the validity of nuclear power following the devastating tragedy of the 2011 disaster at the Fukushima-Daiichi power plant — a move that could ultimately result in much more spent fuel. Many are viewing the Hornobe Underground Research Center and its geological data



collection as a possible to solution to the growing crisis. To date, the facility has been given one billion yen in subsidies to finance the project. If selected to store waste, the site will eventually cost 3.5 trillion yen. Waste would be fused with melted glass before being inserted into stainless steel canisters

designed to last for 1,000 years. Following this, cylinders would be wrapped in a clay shield before lowered into deep tunnels.

Kazuhiko Shimizu, the general director for the lab, said that the overall plan is “A project that takes a lot of time and effort just get started. It’s not easy.”

Yet despite the likely solid scientific preparations for the storage center, cause for skepticism from local citizens comes from Shimizu’s logic that “exploring an alternative location would take another 20 years.”

Area farmer Satoshi Sumi said that “There is no guarantee this test site won’t turn into a final repository. I’ve been skeptical about the agreement and I still am.”

Sumi cites tricky deals with other nations involving underground nuclear storage that ultimately went in circles, including France and the United States — which waged a costly and complicated battle at the Yucca Mountain storage site in Nevada over several years.

The government began a study in April to test the feasibility of direct storage.

Fire shuts down nuclear repository, but DOE still recognizes operator for “excellent” performance

Source: <http://www.homelandsecuritynewswire.com/dr20140723-fire-shuts-down-nuclear-repository-but-doe-still-recognizes-operator-for-excellent-performance>

July 23 – Five days after an underground truck fire closed the Waste Isolation Pilot Plant (WIPP), the Energy Department (DOE) awarded Nuclear Waste Partnership (NWP), the operating contractor of the nuclear repository, \$1.9 million for “excellent” performance during the past year. Subsequent investigations of the fire and a later incident involving radiation leak have cited a history of poor attention to safety protocols. One investigation showed that operators allowed diesel fuel engine oil to build up on



the truck that caught fire. Yet, no individual or entity has been held accountable for the recent incidents at WIPP.

The remains of a salt-hauling truck that caught fire underground at WIPP, the nuclear waste repository near Carlsbad. (Courtesy of the U.S. Department of Energy)

“No federal or contractor official has lost their job, been transferred, been moved off the WIPP contract or otherwise held accountable. No leadership has changed at the federal level. No company has lost a contract,” wrote Martin Schneider, chief executive

of Exchange Monitor Publications, in an editorial in *Weapons Complex Monitor*. NWP has however assigned Bob McQuinn to head the recovery and cleanup effort.

The *Albuquerque Journal* reports that last month, DOE levied the only financial penalty against NWP since the February truck fire and radiation leak: a \$2 million, or 25 percent, reduction in the nearly \$8.2 million fee available in fiscal 2014, as a result of the fire. NWP is able to earn back 50 percent of that amount for good performance or corrective actions. "They've always gotten their full bonus," said John Heaton, head of the Carlsbad mayor's Nuclear Task Force. "The main focus of that bonus was getting waste into the facility and, in my opinion, there was very little emphasis on safety or training that will keep WIPP open 30 or 50 years."

The DOE compensates NWP through two channels: a performance-based incentive determined by meeting set goals; and an award fee based on an evaluation of NWP's performance. For fiscal 2013, DOE awarded NWP a \$5.9 million-performance-based incentive in addition to the \$1.9 million award fee issued in February for "excellent" performance. The *Journal* notes that these payments represent potential earnings above what DOE reimburses NWP for the annual cost of operating WIPP, budgeted at \$142 million for fiscal 2013 and \$158 million for fiscal 2014. Across the nuclear weapons complex, "it's become almost a ritual that the contractor gets its bonus no matter what," said Edwin Lyman, senior scientist with the Union of Concerned Scientists' global security program. "It became a standard accessory with the contract and totally nullified the idea of the performance bonus. This has been criticized for years and years. There is so little competition for management of these sites."

NWP, which has operated WIPP since 2012, is contracted to run the facility through 2017, with a five-year option for renewal. "We should not be paying them for work they haven't done," said Don Hancock, a longtime WIPP observer with the Southwest Research and Information Center. "Their contract is to certify the characterization of waste elsewhere (at generator sites) and have it disposed of safely at WIPP and they failed in that."

Heaton suggests that NWP's awards and incentives should be linked more directly to safety and maintenance protocol. "In the next 50 to 100 years, I doubt there will be another repository in the U.S.," he said. "This is the only show in town. And to not maintain it in pristine condition and keep it to a high standard doesn't make any sense."

DOE's Carlsbad Field Office, which pays NWP on behalf of the department, is not considering revision or termination of the contract "pending the results of the radiological release investigation," said spokesman Tim Runyon. WIPP is expected to be closed until 2016, as authorities complete their investigation of the truck fire and radiation leak.

NWP is set to make "dramatic" changes to its safety culture. "We didn't perform and we're going to get criticized," McQuinn said. "I'm spending a lot of time helping my team understand that we have to change and the change will be dramatic."

Emergency radiology response assessed after Boston Marathon bombings

Source: <http://www.medicalnewstoday.com/releases/279652.php?tw>

An after-action review of the Brigham and Women's Hospital emergency radiology response to the Boston Marathon bombings highlights the crucial role medical imaging plays in emergency situations and ways in which radiology departments can improve their preparedness for mass casualty events. The new study is published online in the journal *Radiology*.

"It's important to analyze our response to events like the Boston Marathon bombing to identify opportunities for improvement in our institutional emergency operations plan," said senior author Aaron Sodickson M.D., Ph.D.,

emergency radiology director at Brigham and Women's Hospital.

Lead researcher John Brunner, M.D., was an emergency radiology fellow working in the Brigham and Women's Emergency Department on April 15, 2013, when two bombs detonated near the finish line of the Boston Marathon. **As a Level 1 trauma center, the hospital received 40 of the wounded patients, most within hours of the bombing.**

"Imaging is one of the best ways to decide who needs attention most quickly," Dr. Brunner said. "The use of shrapnel-laden explosive devices resulted in extensive shrapnel injuries

that required evaluation with X-ray and computed tomography, or CT."

Of the 40 patients who arrived in the emergency department for care, 31 patients (78 percent) underwent imaging, including 57 X-rays performed on 30 patients and 16 CT scans of seven patients.



Additional staff was rapidly mobilized, including attending radiologists, radiology fellows and residents, and x-ray and CT technologists. In addition, the usual emergency radiology imaging equipment (two portable X-ray machines and two fixed digital X-ray units, an ultrasound machine and a CT scanner) were supplemented with additional imaging machines from elsewhere in the hospital, including two additional CT scanners and additional portable X-ray units.

The researchers studied the emergency radiology response by comparing turnaround times - or the amount of time taken to perform exams and to interpret the results - from routine emergency radiology operations with those during the mass casualty event. **CT exam turnaround time averaged 37 minutes during the mass casualty event, significantly lower than the annual median of 72 minutes during routine operations.** The researchers said the fast turnaround was

likely the result of having access to three CT scanners and stationing a radiologist at each.

"By having a radiologist stationed at each CT scanner, we could provide real-time protocols and preliminary interpretations of crucial results to help our trauma teams," Dr. Brunner said.

By contrast, the researchers found the X-ray turnaround time (median, 52 minutes) was longer than during routine operations (31 minutes), most likely due to a bottleneck created by the use of conventional radiography portable X-ray machines relying on a single x-ray plate readout device. To eliminate this technical bottleneck, these portable X-ray units have since been replaced by digital radiography equipment with wireless image transfer to enable faster exam completion and image availability.

"Imaging plays a vital role in all emergent situations, from everyday Emergency Department visits and trauma to mass casualty events," Dr. Sodickson said. "The surge in imaging utilization following the Boston Marathon bombing stressed emergency radiology operations but overall, things went smoothly in terms of patient care."

During the mass casualty event, the hospital's system for naming unidentified patients contributed to a large number of duplicative imaging orders and has since been overhauled. The new system, which includes a combination of a unique color, gender and numeral, (e.g. Crimson Male 12345) will reduce confusion that accompanied the influx of multiple patients following the Boston Marathon bombings.

"Hospitals need to have emergency operations plans in place, and emergency radiology is a crucial component of that preparedness," Dr. Sodickson said. "When an event occurs, it is important to direct a critical eye to the plan's operation in order to refine it for the future."

Institute of IED Management (IIM), Central Reserve Police Force, India

By CMDT Mohd Jamal Khan (IIM)

Source: <http://www.cbrneportal.com/institute-of-ied-management-iim-central-reserve-police-force-india/>



Improvised Explosive Devices (IED) remains the most potent weapon in the hands of terrorists. The IED menace is now rapidly increasing as a single largest abstract enemy of the security forces, cutting across geographical dimensions. Terrorists, today, are more educated, trained, technically sound and innovative. Easy availability of IED components and improved knowledge of fabrication has made it their favorite instrument. The IED threat has even challenged the mightiest armies of the World including that of USA and NATO in Iraq and Afghanistan. Hence countering IED threat has become top priority of every nation so as to reduce the losses due to IEDs/bomb blast. Therefore security apparatus across the globe needs improved counter IED techniques, training facilities and infrastructure to meet this challenge.

India has, simultaneously, suffered deeply by IED menace chiefly exercised by Maoists all across the Red Corridor Zone encompassing many States. The casualty figure on account of attacks by IEDs have progressively increased and adversely affecting the morale of the Security Forces. Existing training facilities in India for countering IED menace are inadequate to meet the challenge. Central Reserve Police Force (CRPF), being leading force in combating Naxalism in India and simultaneously facing the brunt of IED threat

resulting into colossal loss of men and material. CRPF evolved a mechanism for setting up a separate, dedicated institute for countering IED menace catering to needs and requirement of CRPF and other Police Forces of India and friendly countries. The mission of IIM,CRPF is to provide wide spectrum of specialized and technical training that involves all aspects of IED management including search, detection, identification and disposal through realistic, relevant and functional training with attention to details with a view to earn the reputation for excellence and high standards of knowledge and skills.

The Institute of IED Management was formally inaugurated by the Honorable Union Home Minister, Government of India, Sh. P. Chidambaram. The Honorable Union Home Minister applauded the efforts made by CRPF for starting the IIM with international infrastructure and facilities. **The salient features of IIM are:**

- High-tech Class Rooms
- State of the art Model Room :with models of all major IED incidents across India and even abroad
- IED training Lab: for hands on training on detecting, deactivating/ neutralising and destroying IEDs of various types.



- Sand Model Room: to help students training on planning counter IED operations.
- Counter IED range (Urban and Rural): with counter IED exercises, involving security forces, terrorists and by-standers. Use of RF wireless based IEDs which can be shifted from anywhere to anywhere to set new exercises every time.
- Latest counter IED equipments and devices
- Database of different IED incidents: facilities for data management and intelligent assessment/predictions.
- IED Archive :display recovered IEDs from fields to familiarize trainees
- Digital library: case studies and data on recovered IEDs

The IIM, CRPF, Pune (India), a counter IED training institute of CRPF is imparting training to all ranks of CRPF, other sister organizations and Security forces of other Asian countries. Initially IIM is focusing on ToT courses to disseminate and spread the flow of knowledge and skill to the very grass root level in the field areas as fast as possible thereby reducing the loss of men and property to the minimal.

IIM, CRPF, Pune is conducting courses and modules covering all aspects of training catering to the needs of every zone like different technique for J&K, different aspects for Northeast and altogether different approach for Naxal infested areas. IIM Pune also consults other specialized counter IED Institutions and facilities from time to time and conducts seminars and workshops to upgrade and hone the skills and techniques in countering IEDs. Improved efficiency comes from the improved training and IIM CRPF, Pune is evolving as a international centre of excellence by inculcating all ultra modern and latest techniques, tactics and procedures in the field of Counter IED training.

IIM, the brightest jewel in the crown of CRPF is though in its nascent stage nevertheless it has earned laurels and kudos from all quarters of the country. All the premier national investigating agencies look up to IIM for its assistance in different IED related circumstances. **In a very short span of two years the institute has achieved the following milestones:**

- Trained a more than 2000 trainees of all ranks of CRPF and other security forces of the country.
- Trained the Police Forces of all the Maoists affected states of India.

- Designed and conducted Capsule course for BDDS of various State Police Forces.
- IIM, Pune imparted training to 159 participants of Central Industrial Security Forces who are guarding the various vital installations of the country.
- IIM, Pune also trained senior scientists of Defense Research & Development Organization on Counter IED Trg.
- The Institute Played a pivotal role in cracking the Pune Blast that took place on 1st Aug.2012.
- The Institute contributed in the preparation of SOP of various Police Forces regarding Search, Detection and Neutralization of IEDs in different situations.
- Officers of the Institute visited the various blast sites in the field areas and prepared the instructions for different IED related situations.
- Instructors from the Institute visited the various Trg Centers of India and delivered the guest lectures and shared their rich experiences.
- IIM, Pune contributed in an IED awareness program for the common masses in cities The Institute believes that the society can play a key role in detecting, identifying and alerting the specialized security agencies in countering the IED threat.
- IIM, Pune assisted National Investigation Agency (NIA) in the investigation of Hyderabad twin Blast (21/02/2013) & Bangalore Blast (17/04/2013).
- Officers of the Institute participated in various National and International conferences/seminars and did value addition by sharing their rich experiences.
- Institute of IED Management played a key role in designing and imparting customized training on counter IED during State Assembly election of highly Naxal infested state of Chhattisgarh in India. In run up to the election security forces recovered more than 100 IEDs and more than 500Kgs explosive material because of effective training imparted by the Institute.
- Under the directions of CRPF Headquarters Institute of IED Management identified about 30 training nodes throughout India for conducting Counter IED Training programmes for all the security forces of India in the backdrop of General Parliamentary Election 2014 where speculation of use of IEDs by Maoists guerilla is very high.



India's quest for peace can only be realized once our country is free from all kinds of threats posed by different anti national forces. Here comes the role of CRPF and IIM. By our professionalism, vision and training we shall be able to defeat the dark forces which are acting against the very 'idea of India'. The Institute believes that the quality of training needs to be

constantly revised with the changing pattern of IED threat. The Institute looks forward to convert and transform the Red Corridor Zone into a No Fear Zone by eliminating IED menace and terrorism. We believe in the words **"COMING TOGETHER IS A BEGINNING, KEEPING TOGETHER IS PROGRESS, WORKING TOGETHER IS SUCCESS"**.

Managing Residual Clearance: Learning From Europe's Past

Source: <http://www.cbrneportal.com/managing-residual-clearance-learning-from-europes-past/>



Lessons learned from residual clearance in post-1945 Europe may apply to long-term clearance efforts after more recent conflicts – Geneva International Centre for Humanitarian Demining

In light of current conflicts, it is easy to forget that many European countries still manage World War I (WWI) and World War II (WWII) explosive-remnants-of-war (ERW) contamination. Over decades, these countries developed practices and policies that could help shape priority setting and risk management in countries more recently affected by ERW. Post-conflict countries could learn from the early mistakes in European responses and benefit from practical approaches that address residual threats at varying depths and with differing time frames. The historical evolution of best practices since WWII can also assist countries in policy design beyond the fulfillment of commitments under the international Convention on Cluster

Munitions (CCM) and the Convention on the Prohibition of Use, Stockpiling, Production and Transfer of Anti-personnel Mines (APMBC). Understanding when to start and stop the implementation of proactive clearance serves as an excellent foundation for residual clearance policies.¹

Understanding Before Acting

One of the immediate challenges facing countries recovering from armed conflict is the prevention of further casualties from ERW contamination. After addressing immediate concerns, including protecting citizens and critical national infrastructure from explosive hazards, governments strive to secure safe environments for daily life and socioeconomic recovery.² With internal and external pressures in play, the following limitations often characterize this early stage:

- No time for planning comprehensive surveys.



- Inadequate information on the scale and impact of ERW contamination.
- Policymakers' inability to approach the threat of ERW through risk management.

As a result, some countries provided ambiguous estimates regarding years of ERW clearance required, adding to the confusion.³

From Proactive to Responsive

Responsible governments logically adopt a proactive approach to ERW during and immediately after armed conflict. Implementation usually involves a rapid survey covering large areas with clearance operations aiming for exhaustive eradication of ERW, at least in priority areas. With time and progress, these operations usually report an accelerating decline in ERW encountered and make priority and highly contaminated areas safe from surface and shallow ERW. Meanwhile, institutional knowledge within the responsible authority improves on typology, extent and implications of the remaining contamination.⁴ With less ERW to address, the high costs of proactive clearance yields decreasing marginal returns and, in absolute terms, often debatable increases in public safety. The reduced threat from remaining ERW raises the need for the country to readjust its priorities and response policy to better reflect modern risk management.⁵

World War II Lessons

Several European and Asian countries experienced extensive and prolonged bombardments from air, sea and land during WWII, resulting in significant ERW contamination per square kilometer (247 ac) of territory.⁶ In fact, more than 30 countries continue discovering and clearing WWII-era ERW. For instance, the U.K. regularly recovers deeply buried bombs from the greater London area and many ERW remain at the bottom of the River Thames. Germany's experience of bombing during WWII was more intense and sustained, leaving a widespread legacy of surface and shallow contamination in cities and the countryside. Two million tons of ordnance were dropped, with an estimated 100,000 unexploded bombs remaining in present day Germany.⁷ Up to 10 aircraft bombs are still found yearly in Berlin alone. Meanwhile in Japan, there were more than 1,200 explosive ordnance disposal (EOD) call outs each year from 2008 to 2012.⁷

The intensity of the destruction in specific areas of the U.K. and Germany compares with the shelling and bombing of Laos and Vietnam, which began with the battle of Dien Bien Phu in 1954 and continued through the end of the Vietnam War in 1973.⁸ Sixty years after the First Indochina War and 40 years since the war in Vietnam, the management of residual ERW in this region is highly relevant and could benefit from a fresh perspective and transfer of knowledge.

After WWII, European governments had to make major decisions on prioritization and public safety, assessing economies of scale in dealing with residual abandoned and unexploded ordnance. The primary regulator for the evolution of policies prior to establishment of the International Small Arms Control or International Mine Action Standards was common sense; not every square meter could or should be cleared in each area suspected of containing ERW. The contamination had to be treated differently depending on if the ERW was at the surface or buried. Economic and infrastructural pressures often resulted in release of land to the population before it was guaranteed that the land was safe to a specified depth. It was, and still is every citizen's responsibility to be vigilant and report ERW findings to local authorities.

Evolution of Policies

Since 1945, countries' responses to ERW evolved through a series of reality checks. On the one hand, authorities had to weigh the extent and type of contamination with the de facto danger to population and infrastructure. On the other hand, they needed to assess available technical and human resources, as well as their efficiency and associated costs. The reality of these competing priorities was no more apparent than in post-WWII London, where more than one million destroyed buildings needed to be rebuilt.⁹

The policies of that era were guided by early applications of risk management and implemented by experienced, yet often poorly equipped operators and advisers. The first two decades after WWII could be described as a showcase of varying degrees of resilience in London and Berlin, learning from mistakes of unregulated work while pushing for new perspectives and procedures for ERW practices. During the 1970s,



civil-reporting mechanisms became more effective by moving data from war archives to the first interactive information-management systems. The management of residual ERW soon evolved as a mechanism of shared responsibility with specified tasks for armed forces, emergency services, civil servants, citizenry, and more recently for commercial contractors.

Proactive, Reactive, Responsive

Present ERW clearance in European countries is largely responsive compared to the proactive operations conducted immediately after WWII. Many of the affected countries now operate on the premise that ERW contamination cannot be totally eliminated, but the hazards associated with remaining ERW can be mitigated through risk education, responsive local threat assessments and EOD.¹⁰ This assumption of acceptance of long-term residual risk and differentiation between responses on surface, shallow and deep residual contamination starkly contrasts with the admirable yet abstract policies that continue advocating for total eradication of ERW.^{11,12}

Emerging countries that experienced major bombardments following the 1960s, such as Laos and Vietnam, completed most of their post-war reconstruction and now enter long-term development. However, some of their current contracting and budgeting modalities encourage continued proactive ERW clearance over less expensive survey activities, land-use assessments and risk reduction through spot EOD.¹³ Moreover, policymakers may overestimate the impact of ERW, in particular that of deeply buried bombs.¹⁴

For instance, the response requirements for ERW on the surface and at shallow depths vary significantly to that of the U.K.'s deeply buried bombs, wherein the latter are mitigated reactively by default. A good example of this policy's implementation is the construction project of the Queen Elizabeth Olympic Park in London prior to the Olympic games in 2012. The entire area was heavily bombed during WWII. Based on the bombing data, deeply buried ERW could emerge during the park's construction.¹⁵ A risk assessment deliberately avoided proactive clearance of the park. The level of preparedness was raised for the reactive EOD.

Lessons Learned

Central to managing residual ERW is strong national ownership of risk and response, and well-performing authorities with solid understanding of liability, operational efficiency and risk management. ERW tasks are best suited to be the shared function and responsibility of civil defense and military together maintaining the budgets and mobile response capacity.¹⁶

Following the organizational structure, suitable information management and reporting systems differentiate between surface (and shallow subsurface) contamination and deeply buried bombs. Deeply buried bombs cannot be easily surveyed over large areas nor can communities readily identify them; often they become a challenge only after being discovered during construction and development activities. Therefore, adopting a risk management approach and introducing more sustainable, commercially viable response models would better address most long-term contamination that does not pose immediate humanitarian danger. For financing institutions and donors, selecting such an approach would allow investment to focus on manageable and important tasks, not the all-encompassing clearance of countries.

Conversely, national authorities would be responsible for developing policies to manage long-term residual ERW. In such an environment, progress would be defined in other terms than the sum of square meters cleared and number of ordnance destroyed. Lessons from the European WWII experience advocate moving away from proactive clearance practices and policies to responsive long-term survey and clearance mechanisms that are sustainable, proportional to the reduced threat and appropriate to the intended use of the contaminated land. Adoption of such policies would enable efficient resource allocation while providing better developed perceptions of residual ERW and associated risks.

About the Study

The Geneva International Centre for Humanitarian Demining (GICHD) began a study of post-1945 ERW response policies and practices in 2013, focusing on management of residual risks. The research project extends to 15 countries and serves to facilitate knowledge transfer and



advise policymaking on residual ERW among national governments and donors. Beyond this study, GICHD assists in developing sustainable national leadership and capacities to confront

residual contamination while increasing the role, and sharpening the structure of national security services in ERW response.

► Endnotes are available at source's URL.

EDITOR'S COMMENT: Just a small addition to the above: recent Bosnia mega floods "relocated" thousand of buried landmines that might pose an evolving problem/threat in the years to follow.

New bomb scanners will reduce wait time at airports

Source: <http://www.counteriedreport.com/news/new-bomb-scanners-will-reduce-wait-time-at-airports>

Long queues and strict guidelines over liquids on board planes could soon be a thing of the past with the arrival of sophisticated bomb detection scanners at Dublin Airport. And baby food – an ongoing headache at security barriers for parents travelling with young children – can now be cross-checked without the need to open containers.

INSIGHT 100 Liquid Explosive Detection System (LEDS) uses laser-based technology to screen liquids, powders, aerosols and gels. It can investigate sealed containers for possible explosives within five seconds.



It's also possible to operate it in conjunction with standard X-ray security machines. Dublin Airport Authority (DAA) has purchased up to nine 'Insight 100' scanners – costing about €50,000 each – in a bid to make identifying liquids carried in hand luggage easier. The device works by shining a laser beam directly at the bottle, which returns a spectrum of light. The scanner then cross-checks the container against a library of recognised dangerous liquids deemed as potential threats. A foiled 2006 plot to blow up transatlantic flights leaving London for North America using explosives concealed in bottles led to restrictions on travellers taking drinks and toiletries on board planes.



EU guidelines stipulate that only liquids of 100ml, or less, are allowed on an aircraft. Thousands of containers that don't meet this ruling are abandoned every day at airports, resulting in lengthy queues at security.

But that could be set to change.

Industry experts envisage that emerging technologies will allow airports to end the ban in just 18 months, by 2016.

European airports are spending in excess of €150m in equipping passenger screening areas with the latest technology.

At present, any liquid items being transferred through another airport must be checked in these bomb detection devices.

Essential

The first phase of recent EU regulations is limited to the screening of 'transfer' duty free purchases carried in sealed bags, and liquids carried for medical and essential dietary purposes.

Baby foods are subject to this liquid detection also.

In a statement to the Irish Independent, the DAA said it had sufficient machines for the number of transferring passengers at the moment. "We keep this under review and, if required, we will purchase more as numbers increase."

Figures show that in the first three years of the ban, almost 33,000 items were surrendered to Dublin Airport security staff.

These included an estimated 4,000 bottles of wine, 6,500 bottles of spirits, 1,500 bottles of cream liquors, 14,600 bottles and cans of beer, 4,500 quarter bottles of wines and spirits. A further 750 perfume and body lotion gift sets were also seized.

Terrorists Team Up in Syria to Build Next Generation of Bombs

Source: <http://www.counieredreport.com/news/terrorists-team-up-in-syria-to-build-next-generation-of-bombs>

An alliance has been building inside war-ravaged Syria, with al Qaeda-linked terrorists there now working alongside hardened operatives from the prolific al Qaeda affiliate in Yemen to develop a new generation of bombs that could be smuggled aboard commercial planes, according to ABC News.

This potentially lethal partnership helps to explain why U.S. officials have so publicly expressed concern about thousands of Americans and other foreign fighters who joined terrorists in Syria, and it is at least part of what sparked a warning to airlines earlier this year to look out for explosives-laden toothpaste tubes, cosmetics and shoes.

The U.S. government had obtained intelligence that associates of an al Qaeda affiliate in Syria – the Al Nusrah Front – and extreme elements of other radical groups were being joined by operatives from al Qaeda in the Arabian Peninsula, the Yemen-based group behind the failed underwear bomb plot on Christmas Day 2009 and the plot a year later to take down

cargo planes over the United States with explosives packed into printer cartridges.

And the groups are jointly working to produce new and "creative" designs for nonmetallic explosives, leading U.S. analysts to believe that the group of radicals, who have worked with Al Nusrah Front, might be looking to target a U.S.- or European-bound plane, sources told. The intelligence obtained by the U.S. government did not indicate a specific target or a specific timeline. But groups like Al Nusrah Front and al Qaeda in the Arabian Peninsula are now "leveraging each other," as one source put it – with some linked to Al Nusrah Front leveraging their Yemen counterparts for their bomb-making expertise, and al Qaeda in the Arabian Peninsula leveraging Al Nusrah Front for its array of foreign fighters with U.S. and European passports.

Asked to comment, a Department of Homeland Security official issued a statement, saying, "DHS regularly monitors intelligence related to terrorist groups seeking to do us harm."



“At this time, however, there is no specific or credible indication of an active plot against the homeland,” the statement said. “DHS continually monitors intelligence and regularly reevaluates our security apparatus, which includes a number of measure both seen and unseen, to fit an ever evolving threat environment.”

Speaking in Washington Monday, FBI Director James Comey reiterated his concern about radicals operating in Syria.

“We’re spending a tremendous amount of time and effort trying to identify those who go, so we can know who they are when they come back,” Comey told reporters at an unrelated news conference. “The challenge for us is if we don’t know they’ve gone. ... American citizens travel back to the United States, hundreds of thousands on a regular basis every month. So it’s tougher to spot them that way.”

Asked about the deteriorating security situation in Iraq, Syria’s neighbor, Comey said the situation there changes the overall concern about foreign fighters “in degree, not in kind.”

“We’re still very concerned, as we’ve talked about before, about Syria as a breeding ground and a staging ground for terrorist groups,” Comey said. “To the extent that the activities of this [Iraqi terrorist] group expand that safe-haven – that launching ground – it’s obviously a [big] concern here.”

Nevertheless, it’s unclear whether al Qaeda in the Arabian Peninsula would ever share its bomb-making expertise with the group now wreaking havoc in Iraq, the Islamic State of Iraq and Syria, which has its sights on attacks against the West. Al Qaeda denounced and cut ties with the Iraq-based group earlier this year.

Israeli scientists develop nano-tech explosive detector

Source: <http://www.countriedreport.com/news/israeli-scientists-develop-nano-tech-explosive-detector>

The device has been successfully tested on both military explosive and peroxide-based explosives commonly used in home-made bombs.

Israeli scientists have developed an electronic chip with microscopic chemical sensors that can detect explosives in the air at concentrations as low as a few molecules per 1,000 trillion.

Developed by a Tel Aviv company called **Tracense**, the groundbreaking, nano-technology-based sensor was revealed in the journal Nature Communications on Tuesday.



The trace detector, which is still in the prototype phase, can identify several different types of explosives in real time, even at a distance of several meters from the source.

Sensing Chip – An array of two hundred nano-detectors on a tiny silicon chip

It is small enough to be portable yet so sensitive that it can pick out explosives traces that would otherwise be masked by stronger chemicals.

"Different explosive species display a distinctive pattern of interaction with the nanosensing array, thus allowing for a simple and straightforward identification of the molecule under test," the team wrote in the study.



Detection System – Able to detect minute quantities of explosives and other threats with high reliability and speed.

Existing detection methods can detect few explosive types and only at higher concentrations, the Israeli team said. They also require bulky equipment and tedious sample preparation by a trained operator.

The nanomaterials used by Tracense, on the other hand, "offer the ability of incorporating multiple sensors capable of detecting numerous chemical threats simultaneously on a single miniature array platform."

The clusters of nano-sized transistors used in the prototype are extremely sensitive to chemicals, which cause changes in the electrical conductance of the sensors upon surface contact.



The device has been tested with explosives like TNT, RCX and HMX, which are used in commercial blasting and military applications, as well as peroxide-based explosives like TATP and HMTD. The latter are commonly used in home-made bombs and are very difficult to detect with existing methods. TATP particles could be detected five meters from the source and TNT at four meters. Only five seconds of air sample collection was required through a paper filter.

"These promising results demonstrate the potential capability of our sensing platform for the remote detection of explosive species," the team wrote.

Sandia Labs-developed IED detector being transferred to the U.S. Army

Source: <http://www.homelandsecuritynewswire.com/dr20140627-sandia-labsdeveloped-ied-detector-being-transferred-to-the-u-s-army>

Though IED detonations have declined in Afghanistan since a peak of more than 2,000 in the month of June 2012, Department of Defense reports indicated IEDs accounted for about 60 percent of U.S. casualties that year. Detecting improvised explosive devices in Afghanistan requires constant, intensive monitoring using rugged equipment. When

(MiniSAR) system to do just that, some experts did not believe it.

Those early doubts, however, are long gone. Sandia's Copperhead — a highly modified MiniSAR system mounted on unmanned aerial vehicles (UAVs) — has been uncovering IEDs in Afghanistan and Iraq since 2009. Now, Sandia is transferring the technology to the U.S. Army to support combat military personnel, said Sandia senior manager Jim Hudgens.

A Sandia Lab release reports that the technology was developed with the Defense Department's Joint Improvised Explosive Device Defeat Organization (JIEDDO); the U.S. Army Engineer Research and Development Center/Cold Regions Research and Engineering Laboratory (CRREL); the Naval Air Systems Command (NAVAIR); Johns Hopkins University's Applied Physics Laboratory; the Naval Research Laboratory; and Florida-based force protection company AIRSCAN.

"JIEDDO tested a number of technologies and ours emerged as one that was viable," Hudgens said. "Today, we're acknowledged as the most successful airborne IED detection capability out there."

Department of Energy Secretary Ernest Moniz honored the team that developed Copperhead with an Achievement Award at a ceremony this spring in Washington, D.C.

Copperhead detects disturbances in the earth, for example, those made when IEDs are buried. It can find them day or night and in many weather conditions, including fog and dust storms. Extremely fine-resolution images are processed onboard



Sandia researchers first demonstrated a modified miniature synthetic aperture radar (MiniSAR) system to do just that, some experts did not believe it. Those early doubts, however, are gone. Sandia's Copperhead — a highly modified MiniSAR system mounted on unmanned aerial vehicles (UAVs) — has been uncovering IEDs in Afghanistan and Iraq since 2009. Now, Sandia is transferring the technology to the U.S. Army to support combat military personnel.

Detecting improvised explosive devices in Afghanistan requires constant, intensive monitoring using rugged equipment. When Sandia researchers first demonstrated a modified miniature synthetic aperture radar



UAVs and transmitted real-time to analysts on the ground. Those analysts pass the information to soldiers charged with destroying IEDs.

Though IED detonations have declined in Afghanistan since a peak of more than 2,000 in the month of June 2012, Department of Defense reports indicated IEDs accounted for about 60 percent of U.S. casualties that year.

MiniSAR legacy enables Copperhead’s rapid development

Sandia is a world leader in the development of



SAR systems, a history that grew out of its mission to develop radars for nuclear weapons. Recent SAR systems have vastly improved radar images from aircraft flying at great heights.

SAR and its descendent MiniSAR, the first system of its size to successfully transmit real-time images from UAVs in 2006, use small antennae that capture reflections of microwaves returned from objects on the ground, transmitting and receiving many radar pulses as the aircraft flies. The received pulses are integrated by signal-processing techniques to synthesize a fine-resolution image, hence the name “synthetic aperture.”

Hudgens and Sandia manager Bill Hensley say had it not been for Sandia’s research and development process funded, in part, by the Laboratory Directed Research and Development program, to reduce the size of the SAR that led to MiniSAR, Copperhead might never have been ready in time to help the Army.

“If we wouldn’t have made that investment, we wouldn’t have been in that position to be ready. Otherwise it would have taken us years,” Hudgens said.

MiniSAR, however, was still limited when it came to the real-world problem of IEDs. As Americans heard more reports of soldiers killed or maimed by IEDs in Afghanistan and Iraq, Sandia researcher Bryan Burns wanted to help.

“People were getting blown up driving along the road and I said, ‘We can help solve this problem,’” Burns said.

A few different demonstrations and tests were conducted to demonstrate the fundamental capability. Though some experts expressed doubt that any coherent change-detection system could detect IEDs, in 2007, the Sandia team connected with Mark Moran, director of the special projects office at CRREL. Moran’s team was running a series of scientific investigations to predict the operational ability of various technologies for JIEDDO. During

one of those tests, the team showed the value of the MiniSAR technology.

JIEDDO then became interested in the technology and assigned Moran’s team at CRREL as the developing and fielding program office. JIEDDO needed Copperhead developed in nine months, about half Sandia’s normal development period, Hensley said.

Focusing on mountaintops, valley floors simultaneously is solved

Just as cameras are limited by depth of field — where a near object is in focus but the background is blurry or vice versa — MiniSAR needed a way to keep the entire height of the terrain in an image in focus, for example, the top of a mountain and the valley floor.

So Bryan created advanced image-processing algorithms that focused the high and low terrain simultaneously while continuing to provide fine-resolution imagery. The new capability, which has been proven effective on slopes of more than 40 degrees, made Copperhead useful in the wide variety of terrain present in places like Afghanistan.

To make Copperhead a reality, more than 300 Sandia employees each spent at least three months on the project during development, including researchers with diverse areas of expertise and staff who helped with logistics, foreign travel and contracting, Hensley said.



Sandia and its partners had to quickly adapt and enhance the 30-pound MiniSAR so it could fly on NAVAIR's 17-foot Tiger Shark UAV and accomplish the mission JIEDDO had set.

When the modifications were made Copperhead's MiniSAR technology weighed about sixty-five pounds and was about one foot wide, it could do its entire image processing on board and was rugged enough for the environments it would face, Hudgens said.

Then the modified MiniSAR was integrated into the operational system known as Copperhead, which includes hardware and software tools to help radar analysts on the ground understand the data coming from the aircraft and a training program for them.

"We developed a flight planner and an exploitation tool that the analysts use in the ground station, and we had to develop all the concepts of operations to make it work and tactics, techniques and protocols for utilizing the system," Hudgens said. "While MiniSAR was a radar that we flew and used to collect data, Copperhead is an entire system, everything from communications to analyzing imagery to providing information useful to people who defeat IEDs."

Wartime conditions test a success

In 2009, JIEDDO sponsored a 30-day evaluation of the technology in wartime conditions and — despite doubts raised that all the images could have such fine resolution —

Copperhead has been fielded in Afghanistan ever since, Hensley said.

Copperhead uses a technology called coherent change detection, which compares a pair of extremely detailed SAR images taken of the same scene but at different times. The process allows analysts to detect minute physical changes on the surface.

"There are other approaches to change detection out there, but this is the only one that's all-weather," Hudgens said.

An earlier version of coherent change detection developed at Sandia showed images of a lawn taken 20 minutes apart from an aircraft flying 10,000 feet up and three miles away. The images revealed the path of a lawn mower due to the bending of the blades of grass.

Burns and the team are working with the Army to ensure that Copperhead continues to solve current problems. "We're helping them to use it in better and more effective ways, even when things change," he said. "The system is continuously adapting."

Sandia's transfer of the technology to the Army will take years to complete, but the Sandia team members say they are happy that they've provided the Army with a needed tool to detect IEDs.

Of the transfer to the Army, Hensley said, "We're making a positive, measureable impact right now on the security of U.S. people. This acknowledgement that it needs to be kept in the Army is very satisfying."

MINI Z: World's First Handheld Z Backscatter Imaging System

Source: <http://www.hstoday.us/single-article/as-e-introduces-the-mini-z-worlds-first-handheld-z-backscatter-imaging-system/108351ee9f4290221ae335009d2e3209.html>

American Science and Engineering, Inc. introduced the MINI Z, the world's first handheld Z Backscatter imaging scanner for fast, portable, real-time **detection of hidden organic threats, such as drugs, contraband, plastic guns, ceramic knives, and explosives.**



Designed for law enforcement, first responders, border control, event security, maritime police, and general aviation security, the MINI Z system's single-sided imaging and compact size offers unsurpassed operational flexibility — scanning effectively "on the go" in the hardest-to-reach environments.

"Leveraging the breakthrough capabilities of our Z Backscatter detection technology, the MINI Z system is AS&E's initial offering of

what will be a family of portable backscatter products," said Chuck Dougherty, AS&E's

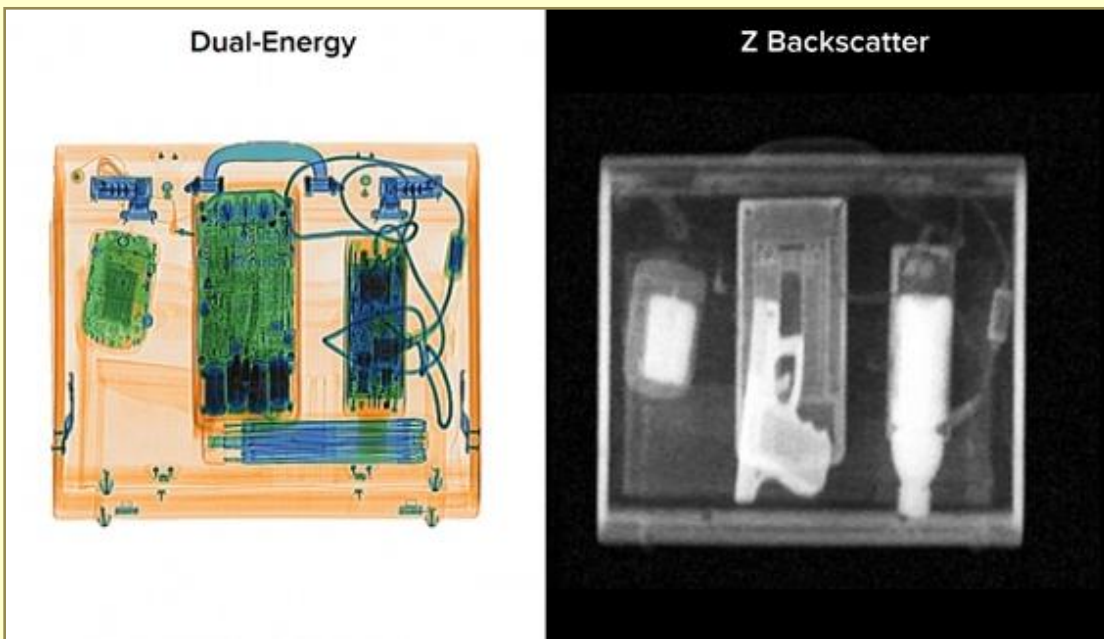


president and CEO. “We have taken the technology behind the success of the ZBV system and miniaturized it — making it more affordable and accessible to a broader range of customers. The MINI Z system is a game-changer for law enforcement and border security officials who are constantly challenged to quickly and accurately detect potential threats in hard-to-reach environments as they work to ensure the highest level of public safety.”



The MINI Z system is ideal for security and public safety officials for multiple applications. Examples include:

- Public Safety: Quick screening of unattended and suspicious bags and packages for potential terrorist threats in public spaces.
- Border and Security Checkpoints: Inspecting vehicle bumpers, tires, panels, and interiors for explosives, plastic weapons, and other concealed threats and contraband.
- Drug Enforcement: Investigating suspected drug labs for drugs or currency.
- Event Security: Screening hand baggage and deliveries to ensure public safety.
- VIP Security: Security sweeps of meeting rooms and furniture for organic threats and IEDs to ensure personnel safety.
- Maritime Security: Screening the hulls and bulkheads of suspected drug running boats for contraband or narcotics.
- General Aviation Security: Inspecting the seats, compartments, and panels of small planes for hidden contraband.



MINI Z — the World’s First Handheld Z Backscatter Imaging System:

- Scans in Places Other Systems Can’t Reach: The MINI Z system is a compact, single-sided imager that can be used to scan objects in hard-to-reach areas, such as unattended bags, backpacks, or packages in a subway or bus. Unlike density meters, trace detectors, or portable transmission X-ray systems, the MINI Z system produces an easy-to-interpret image to quickly detect organic threats and contraband behind non-metallic surfaces.



- Unsurpassed detection of organic threats: The MINI Z handheld system uses AS&E's signature Z Backscatter technology, an advanced X-ray imaging technology that produces a real-time image of the scan target, highlighting organic materials that transmission X-ray systems can miss, such as explosives, currency, and drugs.
- An easy to use, all-in-one imaging system: The MINI Z system is self-contained and does not require set-up, enabling immediate operation. The operator controls the scanning function using a simple, intuitive GUI on the system's dedicated tablet, upon which an image of the scanned target appears in real-time.
- Safe, secure and dependable operation: The MINI Z system is safe for operators, bystanders, and the environment. The system's X-ray dose conforms to the appropriate ANSI, ICRP, NCRP, and EURATOM radiation safety standards. Although the MINI Z is a low-energy and low-dose Z Backscatter system, it is not designed to scan people. The MINI Z system must be used in accordance with the manufacturer's instructions as well as applicable laws and regulations.

Airport Security May Tighten Due to Terrorist Bombs That Escape Detection

Source: <http://guardianlv.com/2014/06/airport-security-may-tighten-due-to-terrorist-bombs-that-escape-detection/>



48

The U.S. is concerned about reports that radical Muslim terrorist groups are getting more and more creative with their bomb making capabilities. According to the Department of Homeland Security (DHS), which monitors terrorist chatter, **there has been some intelligence that terrorists in the Arabian Peninsula have been building bombs designed specifically to target commercial air flights. Further, there is concern that these new and improved bombs are being constructed of non-metallic materials that**

may escape detection by current airport security measures unless tightened.

If the chatter is true and these "new generation" bombs come into play it could potentially allow would be suicide bombers to smuggle the explosive devices onto airplanes. As was tragically demonstrated by the events of September 11, 2001 airplanes can be extraordinarily effective weapons of mass destruction.

President Obama responded to the potential increased threat by



pursuing an examination and possible overhaul of current airport security systems. The tightened security measures would also need to be in place for overseas airports because, as Representative Peter King (R) from the House Homeland Security Committee states, "...a number of airports do not have the type of security that they should have." He further stated that the U.S. needs to be "very aggressive" in responding to the potential security risks overseas but declined to provide further details.

Terrorist chatter about the building of bombs that could potentially escape detection by airport security was intercepted as early as February of this year. Since then DHS and the Obama administration has been developing plans to enhance national security measures in airports and it appears, given the rising threat level, that those measures may soon be implemented. The new increased security measures for both national and overseas airports could include additional profiling and random checks of travelers although details as to the tightening methods have yet to be released.

Some of the chatter specifically relating to detection free bombs has been far more sophisticated than previous chatter related to underwear bombs or shoe bombs. This has senior intelligence agencies on high alert. According to a report by ABC News, the chatter

represents a threat that is "different and more disturbing than past aviation plots." However, DHS has not provided any information on possible credible chatter that identifies a time or location that represents a specific terrorist threat.

The Islamic State of Iraq and Syria (ISIS) has now claimed to be the leader of radical Islamic terrorism and has declared statehood for the areas it now occupies in Syria and Iraq. ISIS also claims to be ushering in a "new era of international jihad." In addition, these militants have put out the call for all terrorists to swear fealty to ISIS chief Abu Bakr al-Baghdadi. Of further concern are reports that al Qaeda connected groups in both Syria and Yemen have united in their cause to inflict terror on the west. According to ABC News, it may be this "potentially lethal partnership" that has prompted additional security concerns.

Regardless of the faction or allegiance, any radical Islamic terrorist group that has the ability to build bombs capable of escaping detection by U.S. and overseas airport security represents a huge threat. Tightening security by increased profiling and random security checks may not suffice to catch potential suicide bombers and the new generation of bombs could easily lead to an increased risk of an airplane being used, once again, as a weapon of mass destruction.

Dozens killed in north Nigeria as Boko Haram car bomb explodes in marketplace

Source: <http://www.homelandsecuritynewswire.com/dr20140701-dozens-killed-in-north-nigeria-as-boko-haram-car-bomb-explodes-in-marketplace>

Dozens of people were killed earlier today (Tuesday) when a car bomb exploded in a



market in Nigeria's north-eastern city of Maiduguri.

Maiduguri is the birth place of the Islamist Boko Haram group. Boko Haram has launched a series of deadly car bombs in public places in cities in north Nigeria, killing hundreds.

Last week, Boko Haram's explosions targeted the biggest shopping center in Nigeria's capital, Abuja, killing twenty-four people; a medical college in northern Kano city, killing at least eight; and a hotel brothel in north-east Bauchi city which killed ten.

Yesterday (Monday) night, the Nigerians military announced it had arrested a businessman



who, the military says, had “participated actively” in the mass abduction of more than 200 schoolgirls in April.

The Guardian reports that the explosives in Tuesday’s attack were hidden under a load of charcoal in a van.

Witnesses said they saw about fifty bodies, and also said that the death toll could have been worse but fewer traders and customers were around than normal because most people stayed up late to eat during Ramadan.

Boko Haram has adopted a two-pronged strategy this year of bombings in urban areas and scorched-earth attacks in north-eastern villages, where people have been gunned down and their homes burned.

In May 2013 the Nigerian president announced a state of emergency in three north-eastern states, and the Nigerian military deployed tens of thousands of troops to the area in an effort to fight Boko Haram. That campaign has been

a complete failure. The corrupt and inept Nigerian military proved unwilling to engage the Islamists, and those units willing to do so were too poorly trained and equipped to be a match for the dedicated Boko Haram fighters. Observers say that the Nigerian military has, in fact, exacerbated the situation by adopting heavy-handed tactics which resulted in the death of hundreds of civilians – in fact, the military has killed many more civilians than Boko Haram militants.

On Sunday, suspected extremists opened fire on worshippers in four churches in a north-eastern village and torched the buildings. At least thirty people were reported killed.

The *Guardian* notes that the extremists have been attacking with more frequency and deadliness in recent months, defying assurances by Nigerian security forces and government that they were getting the situation under control.

Dozens killed in north Nigeria as Boko Haram car bomb explodes in marketplace

Source: <http://www.homelandsecuritynewswire.com/dr20140701-dozens-killed-in-north-nigeria-as-boko-haram-car-bomb-explodes-in-marketplace>

July 01 – Dozens of people were killed earlier today (Tuesday) when a car bomb exploded in

eight; and a hotel brothel in north-east Bauchi city which killed ten.



a market in Nigeria’s north-eastern city of Maiduguri.

Maiduguri is the birth place of the Islamist Boko Haram group. Boko Haram has launched a series of deadly car bombs in public places in cities in north Nigeria, killing hundreds.

Last week, Boko Haram’s explosions targeted the biggest shopping center in Nigeria’s capital, Abuja, killing twenty-four people; a medical college in northern Kano city, killing at least

Yesterday (Monday) night, the Nigerians military announced it had arrested a businessman who, the military says, had “participated actively” in the mass abduction of more than 200 schoolgirls in April.

The *Guardian* reports that the explosives in Tuesday’s attack were hidden under a load of charcoal in a van.

Witnesses said they saw about fifty bodies, and also said that the death toll could have been worse but fewer traders and

customers were around than normal because most people stayed up late to eat during Ramadan.

Boko Haram has adopted a two-pronged strategy this year of bombings in urban areas and scorched-earth attacks in north-eastern villages, where people have been gunned down and their homes burned.



In May 2013 the Nigerian president announced a state of emergency in three north-eastern states, and the Nigerian military deployed tens of thousands of troops to the area in an effort to fight Boko Haram. That campaign has been a complete failure. The corrupt and inept Nigerian military proved unwilling to engage the Islamists, and those units willing to do so were too poorly trained and equipped to be a match for the dedicated Boko Haram fighters. Observers say that the Nigerian military has, in fact, exacerbated the situation by adopting heavy-handed tactics which resulted in the

death of hundreds of civilians – in fact, the military has killed many more civilians than Boko Haram militants.

On Sunday, suspected extremists opened fire on worshippers in four churches in a north-eastern village and torched the buildings. At least thirty people were reported killed.

The *Guardian* notes that the extremists have been attacking with more frequency and deadliness in recent months, defying assurances by Nigerian security forces and government that they were getting the situation under control

New U.S. Explosives Detector

Source: <http://i-hls.com/2014/07/new-u-s-explosives-detector/>

Though IED detonations have declined in Afghanistan since a peak of more than 2,000 in the month of June 2012, Department of Defense reports indicated IEDs accounted for about 60 percent of U.S. casualties that year.

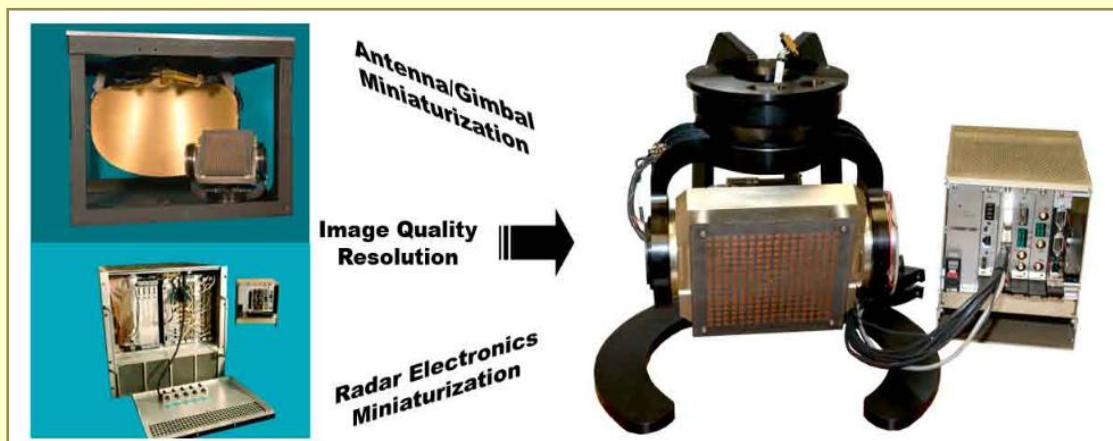


Detecting improvised explosive devices in Afghanistan requires constant, intensive monitoring using rugged equipment. When Sandia researchers first demonstrated a modified miniature synthetic aperture radar (MiniSAR) system to do just that, some experts did not believe it.

Those early doubts, however, are long gone. Sandia's Copperhead — a highly modified MiniSAR system mounted on unmanned aerial vehicles (UAVs) — has

been uncovering IEDs in Afghanistan and Iraq since 2009. Now, Sandia is transferring the technology to the U.S. Army to support combat military personnel, said Sandia senior manager Jim Hudgens.

A Sandia Lab release reports that the technology was developed with the Defense Department's Joint Improvised Explosive Device Defeat Organization (JIEDDO); the U.S. Army Engineer Research and Development Center/Cold Regions Research and Engineering Laboratory (CRREL); the Naval Air Systems Command (NAVAIR); Johns Hopkins University's Applied Physics Laboratory; the Naval



Research Laboratory; and Florida-based force protection company AIRSCAN. Copperhead detects disturbances in the earth, for example, those made when IEDs are buried. It can find them day or night and in many weather conditions, including fog and dust storms. Extremely fine-resolution images are processed onboard UAVs and



transmitted real-time to analysts on the ground. Those analysts pass the information to soldiers charged with destroying IEDs.

New bomb fear prompts TSA to boost security for U.S.-bound flights

Source: <http://www.freep.com/article/20140702/NEWS07/307020179/Airport-security-terrorism-al-Qaida>

Passengers flying to the U.S. from some airports in the Middle East and Europe will be put through tougher security screening in response to intelligence that a terrorist group in

In response to the information, Homeland Security Secretary Jeh Johnson ordered the Transportation Security Administration to take “enhanced security measures” in the coming days.



“We will work to ensure these necessary steps pose as few disruptions to travelers as possible,” Johnson said in a statement Wednesday. Johnson said details about the security concerns would be shared with foreign allies and airlines to protect passengers.

Yemen has developed a new method for smuggling a bomb onto a jetliner, two U.S. counterterrorism officials said Wednesday. Intelligence agencies learned that a bomb-maker working for al-Qaida in the Arabian Peninsula created a technique for hiding explosives that could evade metal detectors, body scanners and pat-downs, the officials said.

“Aviation security includes a number of measures, both seen and unseen,” Johnson said.

Officials are concerned that the method could be shared with Western fighters in Syria who might have valid passports and visas that would allow them to board a flight to the U.S.

In recent years, bomb-makers working for al-Qaida’s affiliate in Yemen have come up with sophisticated and unexpected ways to hide explosives. On Christmas Day 2009, a Nigerian passenger successfully concealed a bomb in his underwear on a Northwest Airlines passenger jet bound for Detroit. The device went up in flames but failed to explode. The assailant was sentenced to life in prison.

The agencies did not have details about a specific plot directed at U.S.-bound airlines, according to the officials, who were not authorized to speak publicly.

The al-Qaida cell in Yemen is also also blamed for a plan in October 2010 to hide bombs in printer toner cartridges and blow up two U.S. cargo planes. An informant tipped off Saudi intelligence officials, and the plot was disrupted.

UK terror alert: body searches at British airports

Source: <http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/10944978/UK-terror-alert-body-searches-at-British-airports.html>

July 03 – Holidaymakers face invasive physical checks and lengthy delays at Britain’s airports amid fears that jihadists returning from Iraq and Syria plan to target transatlantic flights with laptop explosives and “body bombs”.

Travellers at Heathrow were subjected to “vigorous” body searches and clothing and shoes were swabbed for traces of explosive. Passengers were ordered to switch on laptops, mobile phones and other electronic devices, and bags were taking twice as long to pass through scanners, according to reports.

A tough new security regime was imposed on passengers after American intelligence suggested that al-Qaeda was plotting to use Western fanatics to bring down a US-bound plane.

Passengers boarding American-bound planes were understood to



have undergone a second round of checks

before boarding their flights.

A memo sent to all airports by the Department of Transport urged staff to enhance checks, with laptops subject to particular scrutiny.

There has been a 70% rise in civilian casualties from IEDs around the world since 2011

Source:

<http://www.homelandsecuritynewswire.com/dr20140703-there-has-been-a-70-rise-in-civilian-casualties-from-ieds-around-the-world-since-2011>

July 03 – There has been a dramatic rise in civilian casualties from improvised explosive devices (IEDs) over the last three years, new data from Action on Armed Violence (AOAV) show.

Numbers compiled from English-language media reports show there was a 70 percent rise in the number of civilian casualties globally from IEDs like car bombs and suicide vests last year compared to 2011. In 2011 13,340 civilians were killed and injured by IEDs. 2013 saw this number shoot up to 22,735.

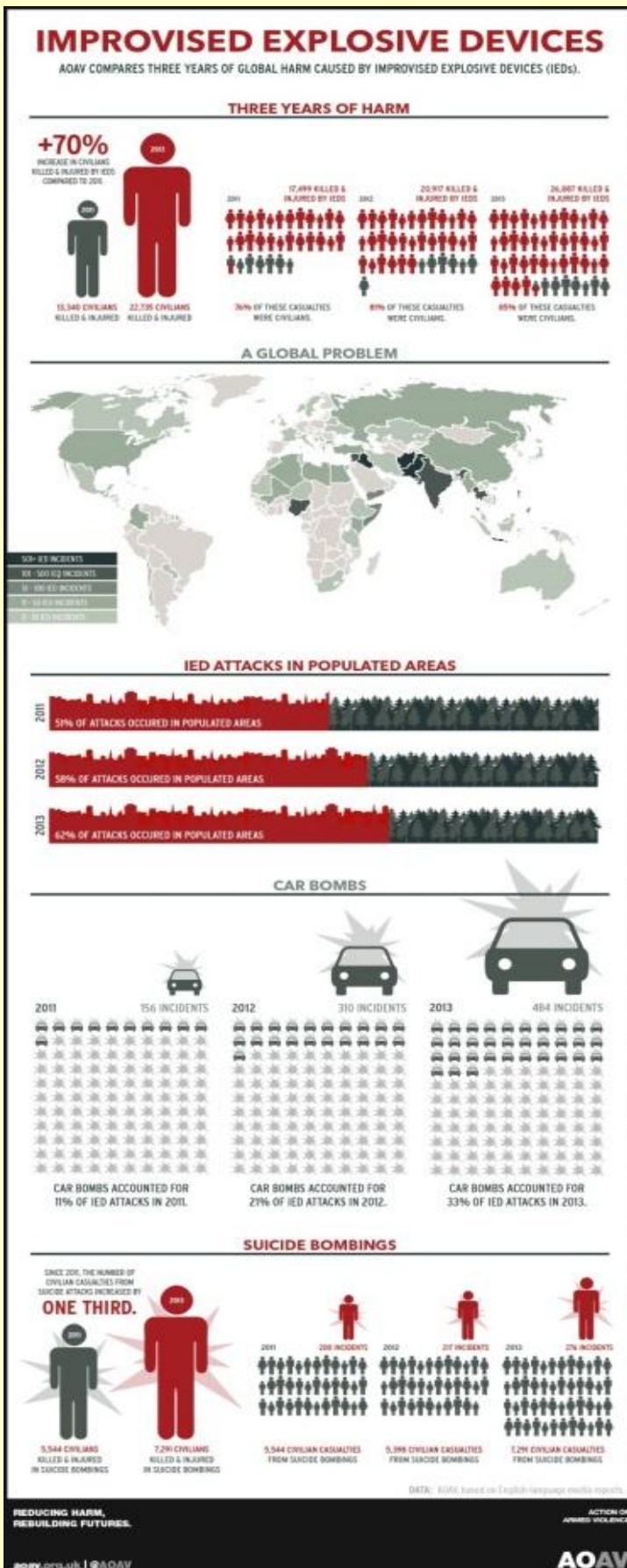
In total AOA's data, which has been compiled over the last three years and which is used by the United Nations for tracking explosive weapon harm, showed there have been over 60,000 deaths and injuries from IEDs in 2011-13, with civilians accounting for 81 percent of these casualties.

An AOA release reports that IEDs did not just impact Iraq and Afghanistan. AOA recorded IED incidents in sixty-six different countries and territories in the last three years. Of these countries, eight, including Pakistan, Nigeria, and Thailand, saw over 1,000 civilian casualties of IEDs.

New trends show that civilians are at greater risk due to the increased use of large vehicle-borne IEDs and the rise in the numbers of incidents occurring in populated areas.

The figures showed that:

- In 2013, 62 percent of all IED incidents took place in populated areas, like markets and cafes. This is compared to 51 percent in 2011.
- Civilians are at much greater risk from IEDs in populated areas. Ninety-one percent of casualties from IEDs in populated areas were civilians, compared to 42 percent in other areas.
- Car bombs are being used more frequently. The proportion of IED attacks



involving car bombs rose from 11 percent of all IED incidents in 2011, to 33 percent in 2013. Each car bomb incident caused an average of twenty-five civilian casualties.

- Over the last three years 34 percent of civilian casualties from IEDs were caused by suicide bombers. Suicide bombs were reported in twenty-six different countries, causing over 18,000 civilian casualties in the last three years.

“This huge increase in the number of innocent victims harmed and killed by IEDs is a terrible concern. Not only to those whose lives are transformed in an instant by these pernicious weapons, but to governments who have to bear the costs of the medical and security implications of these attacks. The use of suicide and car bombing as a major weapon is spreading, and fast. Countries that had not seen their use five years ago are experiencing their horrors now,” said Iain Overton, AOA’s Director of Investigations.

“Governments should wake up to this emerging reality. Explosive munition stockpiles should be better maintained to prevent explosives from

being smuggled out. Victims of IED attacks should receive proper medical and psychological help,” said AOA’s CEO Steve Smith. “And society at large should respond, condemning this rising use, just as they did on land mines and poison gas. Because if actions like these are not carried out then the use of IEDs in populated areas will continue its harmful and bloody ascent.”

The release notes that AOA’s data on IEDs is drawn from almost 500 different English-language media sources. It captures only a snapshot of worldwide explosive violence as reported in the news media. As such it presents only a low estimate of the real extent of suffering caused by explosive violence.

AOAV has also produced a film that counters the narratives used by violent extremists to justify suicide bombings. The film can be viewed [here](#).

AOAV has also carried out research on the long term impacts of IED attacks with a detailed examination of the aftermath of the Moon Market bombing in Lahore, Pakistan.

Afghan market car bomb kills 89 in Paktika province

Source: <http://www.bbc.com/news/world-asia-28307857>

At least 89 people have been killed and dozens injured in a suicide attack at a busy market in eastern Afghanistan’s Paktika province, local officials say.

They say the attacker drove a 4x4 vehicle into the market in Orgun district and detonated the explosives.



The market was full of people doing their shopping for the Muslim festival Ramadan at the time of the attack.

No group has claimed the attack, but Taliban insurgents said they had not carried it out.

“We clearly announce that it was not done by the Mujahedeen of the Islamic Emirate of

Afghanistan,” Taliban spokesman Zabihullah Mujahid was quoted as saying by Reuters news agency. Eyewitnesses and medical staff said local hospitals were overrun with casualties after one of the deadliest attacks in months in Afghanistan.

The eastern province of Paktika shares a border with Pakistan’s restive and volatile tribal areas.

Orgun is one of Paktika’s safest areas, though members of the Haqqani militant network are thought to have a presence there.



Analysis - Bilal Sarwary, BBC News, Kabul

Tuesday's attack is not a surprise for security forces in the border district with Pakistan's Waziristan region. The Pakistan-based Haqqani network is active in the area.



Last week, suicide attackers tried to assassinate local police commander Azizullah - who is widely credited with bringing security to the province, and what officials call breaking the backbone of the Haqqani network in the province.

Many car and truck bombs have been used by the Haqqani network in the province, where they have tried to target officials. But in recent years, most of the truck bombs were either defused, seized or could not

reach their targets.

For the Afghan civilians, Tuesday's attack once again brings to light how daily life is fraught with many dangers in Afghanistan. The Orgun district bazaar once a bustling town of shops and restaurants now

lies in ruin, and covered in blood. The attack will continue to undermine people's confidence in the Afghan government and the day-to-day security.



Ramadan shopping

A spokesman for Afghanistan's defence ministry told the BBC that most of the 89 bodies recovered from the rubble were women and children. There are fears that the death toll will rise further

The blast also destroyed dozens of vehicles and local shops

"ANA [Afghan National Army] soldiers are continuing their work of clearing rubble to look for possible survivors and victims," Gen Zahir Azimi said.

Some 42 injured people have been taken to hospital, he added.

The district governor of Orgun District, Mohammad Raza Kharoti, earlier told the BBC that most of those killed were shopkeepers and people doing their Ramadan shopping.

One man who witnessed the attack said the blast was huge and destroyed dozens of cars and shops.

"There is no room in the hospitals for the victims, people are treating the wounded people on the streets," he told AFP.

Eyewitnesses say police and security forces pursued the attacker before he entered the market.

One doctor at Orgun hospital, said it had become overcrowded with casualties. "We have got children, men and women injured and dead," he said.

The attack occurred hours after two men working for the media team of outgoing President Hamid Karzai were killed by a roadside bomb in Kabul.

The Taliban said it had carried out the attack, which targeted a vehicle carrying employees of the presidential palace to work.



It comes days after Afghanistan's two presidential candidates reached a deal to resolve a dispute over the results of last month's presidential election.

The contenders, Abdullah Abdullah and Ashraf Ghani, agreed to accept the outcome of a vote audit after earlier allegations of voter fraud.

The dispute had revived fears for Afghanistan's stability after the withdrawal of US-led forces later this year.

The First World War bombs that are still killing people in France

Source: <http://www.mirror.co.uk/news/world-news/first-world-war-bombs-still-3862370>

British and German forces launched more than a billion shells and bombs at each other as they fought in vain to break the stalemate in the mud on the Western Front.

The lethal ordnance killed millions on both sides during the First World War – and it continues to do so to this day.



Nearly 100 years since the conflict ended, an estimated 300 million unexploded bombs lie buried under farmland of Northern France and Belgium. As recently as March, two construction workers in Ypres died when a shell exploded.

The Belgians call it the iron harvest, and there is a team of army bomb disposal experts permanently stationed here.

In the past four years alone, they have removed some 629 tons of bombs, shells and other

explosives on former battle lines in Flanders. More and more are being found because of growing development in the region and modern tractors ploughing much deeper than in the past.

It is a constant fear for the people who live here. Farmer Wim Delputte, 46, tells me how he was ploughing his potato field when the blades got stuck on hidden metallic objects.

Jumping down from his tractor, he went to examine the obstruction – a cluster of rusted, mud-covered shells.

As he looked at the cache of unexploded munitions, he realised there were hundreds of bombs embedded in the earth.

Carefully he detached the plough and drove back to his farmhouse to alert his wife Hilde, 43, and their two daughters, eight and 11, who were playing nearby.



The devices, undisturbed since 1918, could go off at any moment. Most are not duds but live explosives which sank into the quagmire instead of detonating.

Bombs designed to kill in the four years of the Great War have killed more than 360 since, and injured more than 500 around Ypres alone.



And the danger does not just come from explosions. Many of the shells contain lethal poison gas. Chlorine, phosphene and mustard gas were all deployed by one side or another during the conflict.

"There is always a fear that we might tread on one and set one off," Hilde tells me, holding deactivated shells the family have kept as souvenirs. They also have some grenades – known to British soldiers as Fritz sticks – in an outhouse.

"I have had to explain to the children that if they see objects like this they don't go near," he says. "The dread is always there and it has definitely affected the girls.

"In total we have found about 400 on the farm. It must have been where some very heavy fighting happened.



57

"Every year we hear stories from the village, from our neighbours, of bombs that have exploded."

A few miles from the farm, in the village of Boezinge, is the base for a Belgian army unit permanently tasked with making the tons of unexploded bombs safe.

The bomb disposal experts are among the busiest in the world despite dealing with ammunition from a century-old war. They are called out every day by farmers and construction workers.

Dirk Gunst, 2nd Lieutenant with the 70-strong ammunition destruction squad, says the last year has been particularly hectic.

He was under pressure to ensure there were no bombs next to the Tour de France route when the cycling race passed through Ypres last week.

The Delputte farm is so peaceful it is hard to imagine the constant blasts which would have echoed across the flat fields a century ago.

Yet it was once on the frontline of the infamous Ypres Salient, where Allied troops endured four years of bombardment.

Fields as far as the eye can see across the flat terrain harbour a host of different, equally lethal bombs which were given grimly humorous nicknames by the Tommies in the trenches.

They called German artillery shells fired from 77mm field guns whizz-bangs and British trench mortars which were fired from Howitzers were toffee apples.

The bombs Wim discovered are probably German munitions which landed ineffectively on the British side of the line. He has also found detonators and fuses lying dormant in the soil.



Some shells he discovered were arranged in a heap, suggesting they were probably left over by a gun crew that had to retreat during one of the battles.

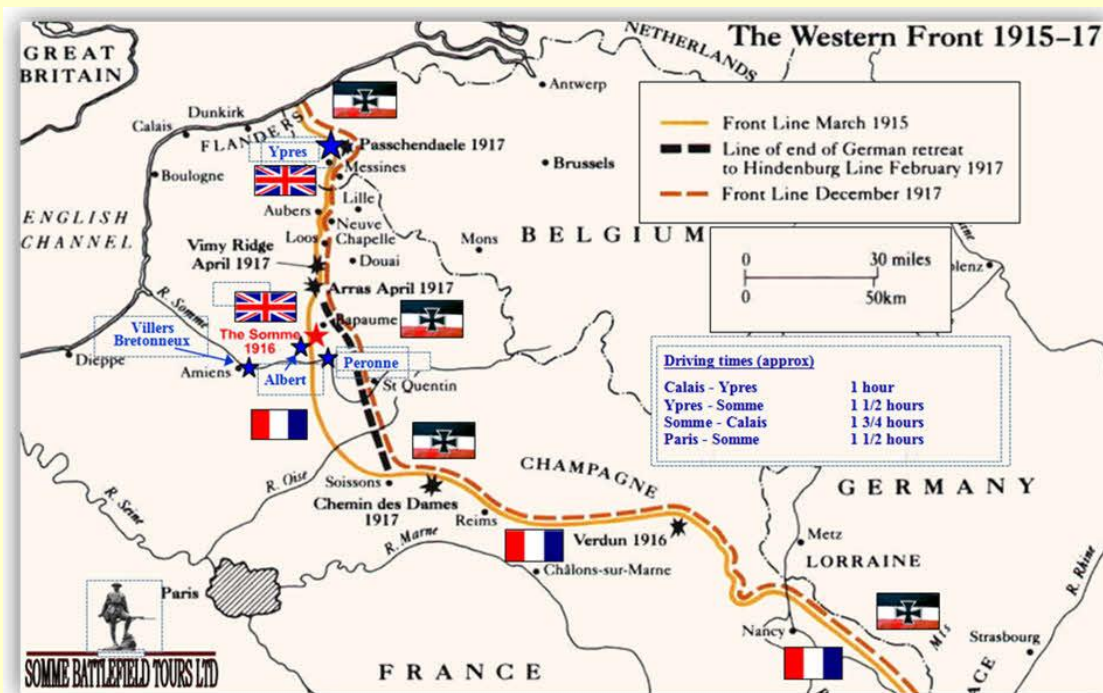
It took the army experts several hours to painstakingly remove the munitions and load them up to be safely exploded in a secured area.

Ypres was where trench warfare started in earnest, the scene of five costly battles.

Both sides dug in following the 1914 Race to the Sea – in which German forces were prevented from reaching the French ports of Calais and Boulogne.

The second Battle of Ypres in 1915 saw the first use of gas in the war and the almost total annihilation of the city itself.

At Passchendaele, the bloodiest offensive, in 1917, the British broke through German lines but rain turned the area into an impassable swamp.



The total number of Allied and German casualties exceeded 850,000; of these 325,000 were British soldiers.

Not surprisingly, people in the outlying villages of northern Belgium keep strictly to marked routes when they go for a Sunday afternoon stroll.

Lieutenant Gunst explains that more than 20 of his Belgian Army comrades have been killed since the unit was formed in 1919.

In 1986, a massive German mortar blew up after it was transported to the unit's depot near the small town of Poelkappele. His colleagues, who work in team of three, have suffered burns from mustard and phosphene gas shells.

"We fear no danger but we don't go in for heroics," the 41-year-old officer says. "We have a system in place with the police and fire brigade.

"Some calls are prioritised as urgent, say shells found near a school or busy crossroads. Or there are those churned out by a farmer and left lying on the edge of a lonely field which don't require much attention.

"No shell should be touched unless it is by us. Not only could the fuse suddenly decide to do its work, the shell might be toxic, or even the outside may be contaminated by chemical weapons that have lain in the soil next to it."

All munitions handled by the unit are placed in trucks that contain sand to reduce vibration. Once back at the deliberately obscure HQ, shells which are thought to contain chemicals are subject to X-ray.

If the shell is found to be toxic, the team identifies which type of poison lies inside the corroded casing.



They defuse some of the munitions by steaming out the explosives and making safe the fuses. The rest of the conventional shells are taken to a field bordered by earth banks to be detonated in controlled explosions.

A lump of explosive and an anti-tank mine are attached to the shell and a warning siren rings out. For the people of Ypres, the iron harvest is a constant reminder of the war to end all wars. Human remains are also regularly found. And Flanders' fields continue to offer up the skeletons of British soldiers who lost their lives in horrific circumstances and were left clinging to the barbed wire in no man's land.

But, incredibly, some people here actually did well from the inhuman conflict. Unexploded bombs were so plentiful in Belgium immediately after the war that one family even made a business out of recycling them.

Annemie Six runs a metal manufacturing company which was founded by her grandparents, who melted down munitions found on the land for scrap.

"After the war they needed a way of making a little money because they were not very well off," she explains.

"So my grandmother had the idea of collecting the scraps of war like shells made from lead and copper."

Unlike the hordes of British coach tourists who come to Ypres to visit the cemeteries, the people who live here do not think of the First World War as distant history.

It remains a very dangerous factor in their daily lives.

Bulgaria names Hezbollah suspects behind bombing of Israeli bus in Burgas

Source: <http://www.jpost.com/International/Bulgaria-names-2-suspects-in-Burgas-bus-bombing-321017>



Meliad Farah and Hassan El Hajj Hassan, who are suspected of involvement in the Burgas bus bombing. Photo: Bulgaria Interior Ministry

Bulgaria's Interior Ministry released on Thursday the names and photographs of **two people** believed to have carried out the Burgas bus bomb terrorist attack last year that killed five Israelis and their Bulgarian bus driver.

The powerful explosion at the Black Sea resort town wounded 32 Israelis.

The two suspects behind the deadly attack were identified as 32-year-old Australian citizen Meliad Farah, also known as Hussein Hussein, and 25-year-old Canadian citizen Hassan el-Hajj Hassan. In the days around the attack, the suspects had been noticed in Ruse, Varna and Nesebar, the Sunny Beach resort, and the village of Ravda, according to the ministry statement.

The alleged Hezbollah suspects are believed to be in Lebanon. In addition to their Canadian and Australian citizenships, Hassan and Farah are citizens of Lebanon.

A Bulgarian source familiar with extradition cases between Lebanon and Bulgaria told *The Jerusalem Post* that the Lebanese authorities have a lousy record in deporting wanted individuals to the Eastern European country.



The Lebanese government has refused to cooperate with a UN tribunal indictment seeking Hezbollah operatives charged with killing former Lebanese prime minister Rafik Hariri and 21 others in 2005. Hezbollah plays a central role in the Lebanese coalition governments and the country's parliament. The Bulgarian authorities were asking the

Farah sports a beard and has dark hair with thick black eyebrows and brown-colored eyes. His alleged accomplice – the 25-year-old Hassan – has a lighter skin complexion and a wears a goatee. His head is nearly shaven bald.

Bulgaria's Interior Minister Tsvetlin Yovchev said last week that his country has received



additional evidence implicating Hezbollah in the Burgas bombing. Fueled by concerns over Hezbollah's activities in Europe, European Union governments – in a reversal of past policy – agreed Monday to put the Lebanese organization's armed wing on the EU terrorism blacklist.

public for cooperation and suspect that the two men registered at hotels and rented cars in the area near Burgas under false names. Last July, according to the ministry, "it was established that Farah rented a Renault Clio in the village of Ravda."

The EU wrote it will review its proscription of Hezbollah's military wing as a terrorist organization on a six-monthly basis. Britain and the Netherlands had pressed EU peers since May to put the group's military wing on the bloc's terrorism list, citing evidence it was behind the bus bombing.

UPDATE (July 18): Bulgarian authorities have identified the **third perpetrator** of the 2012 Burgas bombing as Mohamad Hassan El Hussein or Mohamed Hassan El Hussein, a dual citizen of Lebanon and France who used a fake driving license in the name Jacque Felipe Martin.

Driverless cars could be used as bombs-on-wheels

Source: <http://www.homelandsecuritynewswire.com/dr20140721-fbi-driverless-cars-could-be-used-as-bombsonwheels>

Whether or not a driverless car, from Google or any other company, ever makes it to market, the FBI thinks it may be a "game changing" vehicle which could dramatically change high-speed car chases so that the pursued vehicle would have an advantage over the pursuing car. An agency report also warned that such cars may be used as "lethal weapons." In an unclassified but restricted report obtained by the *Guardian* under a public records request, the FBI predicts that autonomous cars "will have a high impact on transforming what both law enforcement and its adversaries can operationally do with a car." In a section called Multitasking, the report notes that "bad actors will be able to conduct

tasks that require use of both hands or taking one's eyes off the road which would be impossible today." One scenario could be suspects shooting at pursuers from getaway cars which are driving themselves. The newspaper reports that self-driving cars use lidar (laser ranging), radar, video cameras, and GPS technology to build up a digital 3D map of their surroundings, including buildings, roads, pedestrians, and other vehicles. The driverless cars can then be programmed to navigate safely so they reach their destination while avoiding obstacles and (usually) obeying the rules of the road.



The report, written by agents in the Strategic Issues Group within the FBI's Directorate of Intelligence, says, "Autonomy ... will make mobility more efficient, but will also open up greater possibilities for dual-use applications and ways for a car to be more of a potential lethal weapon than it is today."

"Dual-use" applies to the use of such cars by criminals, who might override safety features to ignore traffic lights and speed limits, or that terrorists who might program explosive-packed cars to become self-driving bombs-on-wheels.

Companies which look to produce automatic cars emphasize their safety. Google says of its latest driverless vehicles: "They'll be designed to operate safely and autonomously without requiring human intervention. Our software and sensors do all the work. The vehicles will be very basic but they will take you where you want to go at the push of a button."

The FBI report concedes that if operated properly, the fully autonomous vehicles will help to reduce the number of accidents. "The risk that distraction or poor judgment leading to collision that stems from manual operation would be substantially reduced," according to its report.

In the United States, about eighty people die every year in crashes involving emergency vehicles, while London's Metropolitan police cars have experienced as many as a dozen traffic accidents a day. The report says that the autonomous cars can "optimize" three-point turns and similar difficult maneuvers which

might otherwise delay responders pursuing a suspect or heading for a crime scene.

The FBI report also notes that tailing suspects will be simpler with the next generation of robot



cars. "Surveillance will be made more effective and easier, with less of a chance that a patrol car will lose sight of a target vehicle," says the report.

"In addition, algorithms can control the distance that the patrol car is behind the target to avoid detection or intentionally have a patrol car make opposite turns at intersections, yet successfully meet up at later points with the target."

The FBI says it is likely that autonomous cars could be approved by Congress for use by the American public within the next five to seven years.

The *Guardian* notes that at least for the time being, the FBI and other law enforcement agencies should not worry about chasing automatic cars: Google's current state-of-the-art vehicle is limited to just 25mph.

Tiny laser sensor increases bomb detection sensitivity

Source: <http://www.homelandsecuritynewswire.com/dr20140723-tiny-laser-sensor-increases-bomb-detection-sensitivity>

New technology under development at UC Berkeley could soon give bomb-sniffing dogs some serious competition.

A team of researchers led by Xiang Zhang, UC Berkeley professor of mechanical engineering, has found a way **dramatically to increase the sensitivity of a light-based plasmon sensor to detect incredibly minute concentrations of explosives**. The researchers noted that the sensor could potentially be used to sniff out a hard-to-detect explosive popular among terrorists.

The team's findings are published 20 July in the advanced online publication of the journal *Nature Nanotechnology*.

A UC Berkeley release reports that the engineers put the sensor to **the test with various explosives — 2,4-dinitrotoluene (DNT), ammonium nitrate and nitrobenzene — and found that the device successfully detected the airborne chemicals at concentrations of 0.67 parts per billion, 0.4 parts per billion, and 7.2 parts per million, respectively. One part per billion would be akin to**



a blade of grass on a football field.

They noted that these results are much more sensitive than those published to date for other optical sensors.

“Optical explosive sensors are very sensitive and compact,” said Zhang, who is also director of the Materials Science Division at the Lawrence Berkeley National Laboratory and director of the National Science Foundation Nanoscale Science and Engineering Center at UC Berkeley. “The ability to magnify such a small trace of an explosive to create a detectable signal is a major development in plasmonsensor technology, which is one of the most powerful tools we have today.”

The new sensor could have many advantages over current bomb-screening methods.

“Bomb-sniffing dogs are expensive to train, and they can become tired,” said study co-lead author Ren-Min Ma, an assistant professor of

trace vapor in the air of the explosive’s small molecules.”

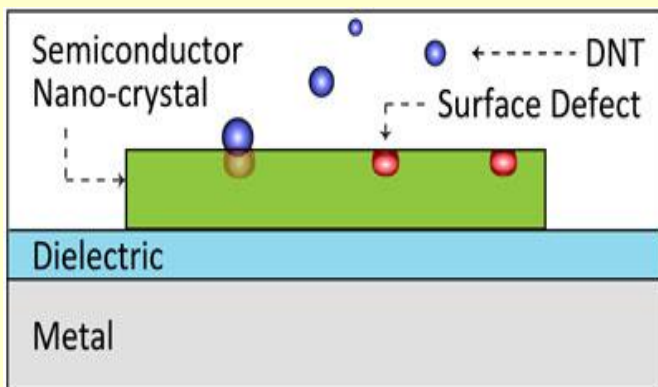
The sensor also could be developed into an alarm for unexploded land mines that otherwise are difficult to detect, the researchers said. According to the United Nations, landmines kill 15,000 to 20,000 people every year. Most of the victims are children, women and the elderly.

Unstable and hungry for electrons

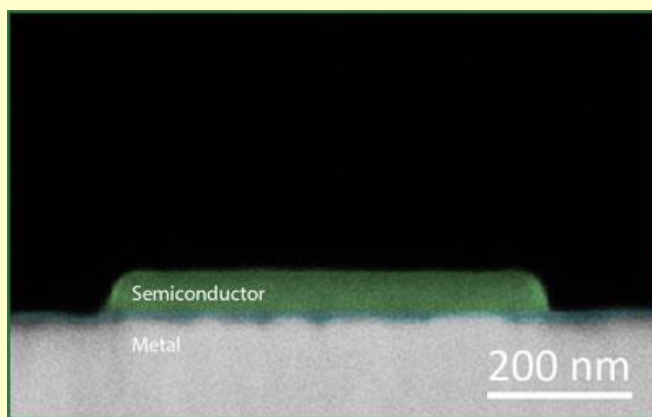
The nanoscale plasmon sensor used in the lab experiments is much smaller than other explosive detectors on the market. It consists of a layer of cadmium sulfide, a semiconductor, that is laid on top of a sheet of silver with a layer of magnesium fluoride in the middle.

In designing the device, the researchers took advantage of the chemical makeup of many explosives, particularly nitro-compounds such as DNT and its more well-known relative, TNT.

Not only do the unstable nitro groups make the chemicals more explosive, they also are characteristically electron deficient, the researchers said. This quality increases the interaction of the molecules with natural surface defects on the semiconductor. The device works by detecting the increased intensity in the light signal that occurs as a result of this interaction.



physics at Peking University who did this work



when he was a postdoctoral researcher in Zhang’s lab. “The other thing we see at airports is the use of swabs to check for explosive residue, but those have relatively low-sensitivity and require physical contact. Our technology could lead to a bomb-detecting chip for a handheld device that can detect the tiny-

The plasmon laser sensor consists of a thin slab of semiconductor separated from the metal surface by a dielectric gap layer. Surface defects on the semiconductor interact with molecules of the explosive DNT. (Image by Ren-Min Ma and Sadao Ota)

Potential use to sense a hard-to-detect explosive

“We think that higher electron deficiency of explosives leads to a stronger interaction with the semiconductor sensor,” said study co-lead author Sadao Ota, a former Ph.D. student in Zhang’s lab who is now an assistant professor of chemistry at the University of Tokyo.

Because of this, the researchers are hopeful that their plasmon laser sensor could detect



pentaerythritol tetranitrate, or PETN, an explosive compound considered a favorite of terrorists. Small amounts of it pack a powerful punch, and because it is plastic, it escapes x-ray machines when not connected to detonators. It is the explosive found in Richard Reid's shoe bomb in 2001 and Umar Farouk Abdulmutallab's underwear bomb in 2009.

U.S. Attorney General Eric Holder Jr. was recently quoted in news reports as having "extreme, extreme concern" about Yemeni bomb makers joining forces with Syrian militants to develop these hard-to-detect explosives, which can be hidden in cell phones and mobile devices.

"PETN has more nitro functional groups and is more electron deficient than the DNT we detected in our experiments, so the sensitivity of our device should be even higher than with DNT," said Ma.

Latest generation of plasmon sensors

The sensor represents the latest milestone in surface plasmon sensor technology, which is now used in the medical field to detect biomarkers in the early stages of disease.

The ability to increase the sensitivity of optical sensors traditionally had been restricted by the diffraction limit, a limitation in fundamental physics that forces a tradeoff between how long and in how small a space the light can be trapped. By coupling electromagnetic waves

with surface plasmons, the oscillating electrons found at the surface of metals, researchers were able to squeeze light into nanosized spaces, but sustaining the confined energy was challenging because light tends to dissipate at a metal's surface.

The new device builds upon earlier work in plasmon lasers by Zhang's lab that compensated for this light leakage by using reflectors to bounce the surface plasmons back and forth inside the sensor — similar to the way sound waves are reflected across the room in a whispering gallery — and using the optical gain from the semiconductor to amplify the light energy.

Zhang said the amplified sensor creates a much stronger signal than the passive plasmon sensors currently available, which work by detecting shifts in the wavelength of light. "The difference in intensity is similar to going from a light bulb for a table lamp to a laser pointer," he said. "We create a sharper signal, which makes it easier to detect even smaller changes for tiny traces of explosives in the air."

The researchers noted that the sensor could have applications beyond chemical and explosive detection, such as use in biomolecular research.

The U.S. Air Force Office of Scientific Research Multidisciplinary University Research Initiative program helped support this work.

— *Read more in Ren-Min Ma et al., "Explosives detection in a lasing plasmon nanocavity," Nature Nanotechnology (20 July 2014).*

Underwear bomber plot failed because he 'wore same pants for two weeks'

Source: <http://www.telegraph.co.uk/news/worldnews/al-qaeda/10989843/Underwear-bomber-plot-failed-because-he-wore-same-pants-for-two-weeks.html>

July 24 – The 2009 "underpants bomb" plot failed because the terrorist had been wearing his explosive-laden undergarments for more than two weeks and soiled the explosives, a senior US official said.

Umar Abdulmutallab sent shockwaves through US intelligence when he successfully smuggled a bomb onto a Detroit-bound airliner on Christmas day three years ago.

The British-educated Nigerian was able to light the bomb but it failed to explode, causing minor burns to the would-be bomber but sparing his fellow passengers.

John Pistole, the head of the Transportation Security Administration (TSA), said on Thursday that the bomb did not detonate because Abdulmutallab had been wearing the same underwear for more than two weeks.

"He had it with him for over two weeks," Mr Pistole said at the Aspen Security Forum.

Asked by his interviewer whether the bomb's fuse had become "damp" from two weeks of wear, Mr Pistole said: "Let's say it was degraded. We're getting kind of personal now."



Mr Pistole, who oversees the agency tasked with protecting America's civilian air traffic from terrorism, agreed with the interviewer when she remarked: "Thank goodness for bad hygiene, right?"

THE CHRISTMAS DAY PLOT THAT CAME SO CLOSE

1 Abdulmutallab, above, flew from Nigeria to the US via the Netherlands. At Schiphol airport in Amsterdam, he transferred to a Detroit-bound flight

2 Strapped to the student's leg was 80g of explosive powder, made from a mixture of PETN, or pentaerythritol tetranitrate, and the high explosive triacetone triperoxide (TATP)

3 Forty minutes from landing he tried to ignite explosive powder by injecting it with acid

4 There was a bang and flames burnt his leg, but the 'bomb' failed to detonate

Syringe containing acid

Explosive powder in pack sewn into underwear

Abdulmutallab, now 27, was sentenced to life in prison for attempted use of a weapon of mass destruction and attempted murder.

His bomb was made by al-Qaeda in the Arabian Peninsula (AQAP), the terror group's deadly Yemeni offshoot.

Western intelligence remains concerned that AQAP will try to find a European or American jihadist trained in Syria and supply them with a sophisticated bomb that can slip undetected onto a plane.

► Watch the full discussion on YouTube at:

<https://www.youtube.com/watch?v=hvVAgbyTqeA&feature=youtu.be&t=37m56s>



China's Tianhe-2 supercomputer, twice as fast as DoE's Titan, shocks the world by arriving two years early

By Sebastian Anthony

Source: <http://www.extremetech.com/computing/159465-chinas-tianhe-2-supercomputer-twice-as-fast-as-does-titan-shocks-the-world-by-arriving-two-years-early>



In a massive escalation of the supercomputing arms race, China has built Tianhe-2, a supercomputer capable of 33.86 petaflops — almost twice as fast as the US Department of Energy's Titan, and topping

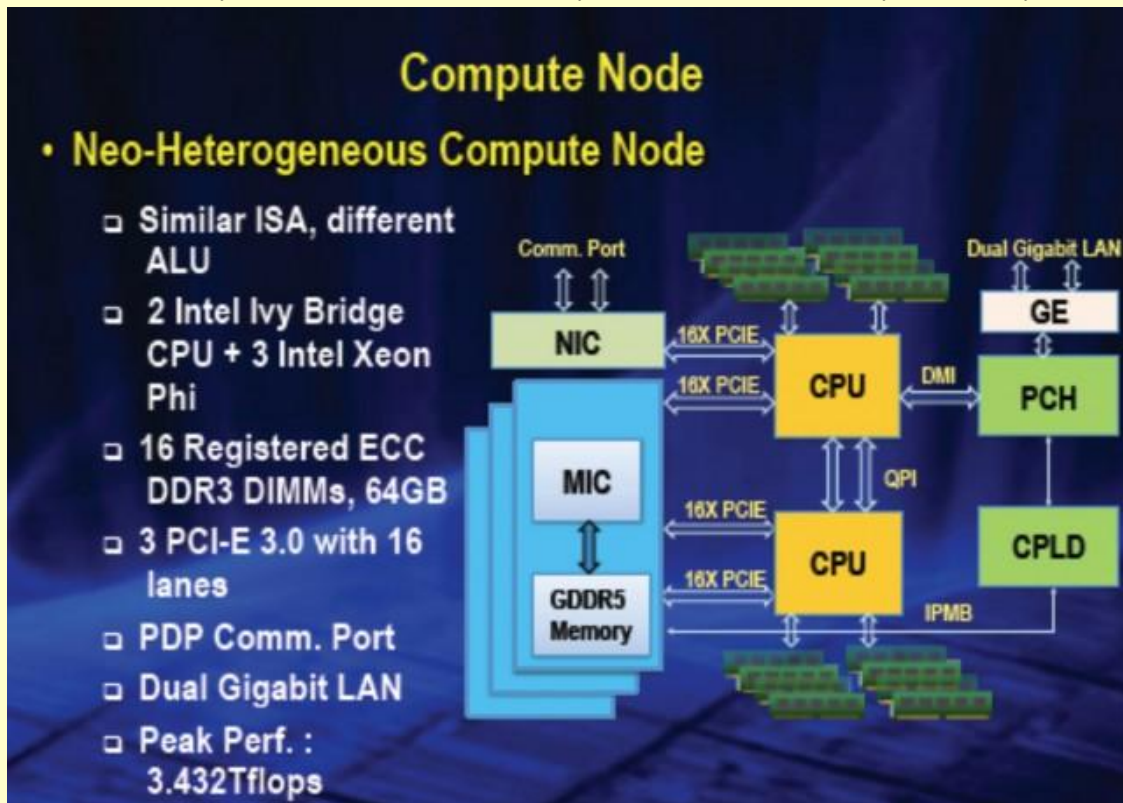
65



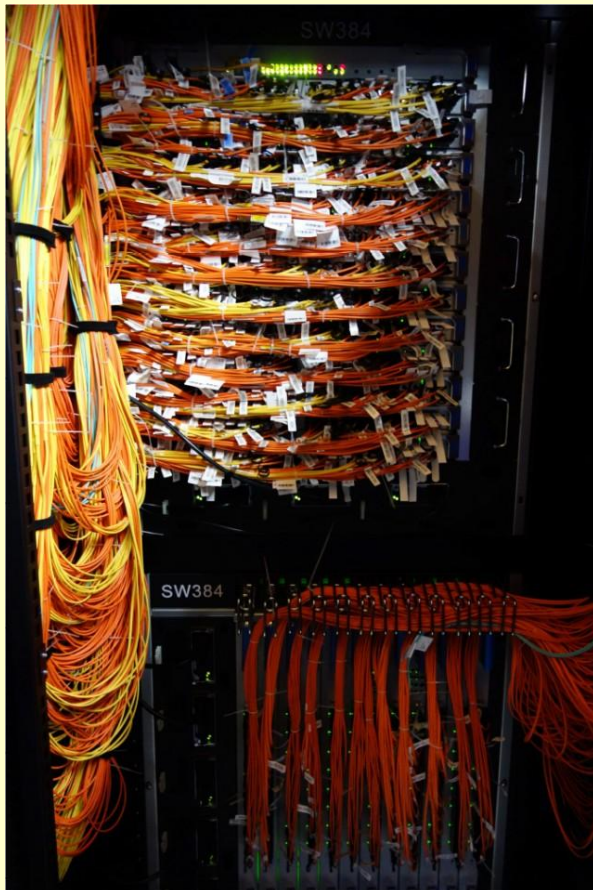
the official Top 500 list of supercomputers by some margin. The US isn't scheduled to build another large supercomputer until 2015, suggesting China will hold pole position for a long time to come. The computer has 32,000 Ivy Bridge Xeon CPUs and 48,000 Xeon Phi accelerator boards for a total of 3,120,000 compute cores, which are decked out with 1.4 petabytes of RAM. And of course the operating system is Linux.



The construction of Tianhe-2 (literally Milky Way-2) comes as a huge surprise, as it was originally scheduled for deployment in 2015. No one knows why China proceeded so quickly, but it's fairly safe to



assume that it's a reaction to the DoE's completion of Titan last year. Tianhe-2, which is currently being tested in a non-optimal space, is capable of 33.86 petaflops — when it's deployed in its final location,



however, and when any bugs have been ironed out, the theoretical peak performance will be 54.9 petaflops. Assuming that the US doesn't accelerate its own supercomputing plans, the final form of Tianhe-2 will be almost four times faster than any other supercomputer in the world.

To achieve a theoretical peak of 54.9 petaflops, Tianhe-2 has a mind-bogglingly insane hardware spec. There are a total of 125 cabinets housing 16,000 compute nodes, each of which contains two Intel Xeon (Ivy Bridge) CPUs and three 57-core Intel Xeon Phi accelerator cards. Each compute node has a total of 88GB of RAM. In total, according to a report by Jack Dongarra of the Oak Ridge National Laboratory, there are a total of 3,120,000 Intel cores and 1.404 petabytes of RAM, making Tianhe-2 by far the largest installation of Intel CPUs in the world. We believe it's also the largest amount of RAM for a single system, too.

Beyond the glut of x86 compute capacity, though, Tianhe-2 is notable for another reason: Except for the CPUs, almost all of the other components were



made in China. The front-end system, which manages the actual operation of all the compute nodes, consists of Galaxy FT-1500 processors — 16-core SPARC chips designed and built by China's National University of Defense Technology (NUDT). The interconnect (pictured below), also designed and constructed by the NUDT, consists of 13 576-port optoelectronic switches that connect each of the compute nodes via a fat tree topology. The operating system, Kylin Linux, was also developed by NUDT.

Tianhe-2 is currently located at the NUDT while it undergoes testing, but will be fully deployed at the National Supercomputer Center in Guangzhou (NSCC-GZ) by the end of 2013. The peak power consumption for the processors, memory, and interconnect is 17.6 megawatts, with the water cooling system bringing that up to 24MW — slightly below the gigaflops-per-watt efficiency record set by the DoE/ORNL/Cray Titan supercomputer. When Tianhe-2 is complete, its primary purpose will be as an open research platform for researchers in southern China.

Based in the middle of nowhere, England, Sebastian Anthony finds his lonely, friendless-hobo existence to provide the perfect vantage point for bias-free, objective opinionation. A gamer and engineer since a very young age (he famously took a VHS machine apart at the age of 18 months, and later started a school bus at 24 months), he not only likes to tear things to pieces, he also likes to find out what makes things tick. When not writing or editing, he travels, enjoys theatre and live music, sells his own fine-art photographs, and -- despite popular consensus, and his dark, grizzly visage -- he is actually quite young.

► **Read also (by same author) an interesting article on “The History of Super-Computers” at:**
<http://www.extremetech.com/extreme/125271-the-history-of-supercomputers>

ISIS jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter

Source: <http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-extremist-propaganda-on-twitter-9555167.html>

Islamists leading the jihadist advance in Iraq are using the World Cup and leading British football clubs to seek recruits and spread their propaganda via social media, *The Independent* can reveal.

Tweets sent from the accounts used by the propaganda operation of the Islamic State in Iraq and the Levant (Isis) and its supporters are being labelled with hashtags such as #Brazil2014, #ENG, #France and #WC2014 to try to hijack the World Cup tournament to spread their message.

The tactic, which allows Isis to access millions of World Cup Twitter searches in the hope that some will click on links to its propaganda material, was being deployed this weekend to disseminate a video showing British and Australian jihadists trying to persuade other western Muslims to join their ranks.

The use of hashtag links also extends to English Premier League clubs. In recent weeks, Isis accounts have used #MUFC, #WHUFC, #LFC and #THFC, among others, on tweets promoting vile “public relations”

material showing atrocities and beheadings committed by the extremist group's fighters in Syria and Iraq.

The use of Twitter hashtags is just one part of an increasingly sophisticated social media campaign by ISIS as it seeks to capitalise on its dramatic territorial gains in recent days and establish a puritanical Islamic state or “caliphate” across a swathe of Sunni-majority Iraq.

The militants have developed an Arab-language Twitter app which updates users on the latest ISIS developments but also requires signatories to surrender a large amount of personal data and gives the terror group the power to send tweets from that individual's account.

Charles Lister, a terrorism expert at the Brookings Doha Centre, said the ISIS had developed an “all-encompassing” media strategy which was allowing it to outperform longer-established extremist groups in its search for recruits and publicity.



He said: “The slick nature of ISIS media releases has undoubtedly allowed it to become somewhat the ‘celebrity’ actor within the international jihadist community. On social media, not a day goes by without a foreign supporter - from London, to Mogadishu, to

One account, @Alnhim, this weekend tweeted a link to the recruitment video entitled “There Is No Life Without Jihad”, featuring three Britons including Cardiff medical student Nasser Muthana, with seven World Cup-related hashtags.



With disenfranchised or disillusioned young Muslim men a priority for ISIS and similar groups when it comes to recruiting in the west, the harnessing of football-related tweets to its messaging strategy would seem to be a deliberate attempt to reach its target audience via their likely interests.

A screengrab of the Twitter account @Alnhim which is using hash tags associated with the World Cup to seek recruits and spread their propaganda via social media. But ISIS propagandists, who last weekend announced an attempt to **gain one billion supporters for an Islamic state on social media**, are also determined to simply reach as wide an audience as possible.

Manila - expressing their support and allegiance to ISIS’s cause.” Twitter and other social media providers have shut down a number of ISIS-affiliated accounts in recent days under rules which ban the use of threatening language and racial or religious hatred. But new accounts quickly take their place.

An analysis of social media tactics being used by the group by The Atlantic magazine last week found it was using an Arabic language twitter account - @ActiveHashtags - which advertises the most popular hashtags to get its own material on the feed. When this happens, ISIS receives on average 72 retweets for every tweet it sends.

Is Facelock the password alternative we’ve been waiting for?

By Philip Branch

Source: <http://www.homelandsecuritynewswire.com/dr20140626-is-facelock-the-password-alternative-we-ve-been-waiting-for>

One of the problems with using passwords to prove identity is that passwords that are easy to remember are also easy for an attacker to guess, and vice versa. Nevertheless, passwords are cheap to implement and well understood, so despite the mounting evidence that they are often not very secure, until something better comes along they are likely to remain the main mechanism for proving identity. But maybe something better *has* come along. In research published the other day in PeerJ, Rob Jenkins from University of York and colleagues propose a new system based on the psychology of face recognition called Facelock. But how does it stack up against existing authentication systems?



Exploiting the power of recognition

Our brains may not be wired to remember long strings of arbitrary characters, but they *are* wired to remember and recognize faces.

Our ability to recognize people we know — even when we haven’t seen them for a long time, even in a grainy photo with them looking the other way, even in sunglasses with a hat pulled low over their face — is quite extraordinary. Facelock tries to integrate this ability into an identity authentication system.

If we know someone well we can usually recognize them easily from an image, regardless of how poor the image is. However, this ability does not extend to unfamiliar faces. If we don’t know the person, we find identifying two different images of the same person very difficult.

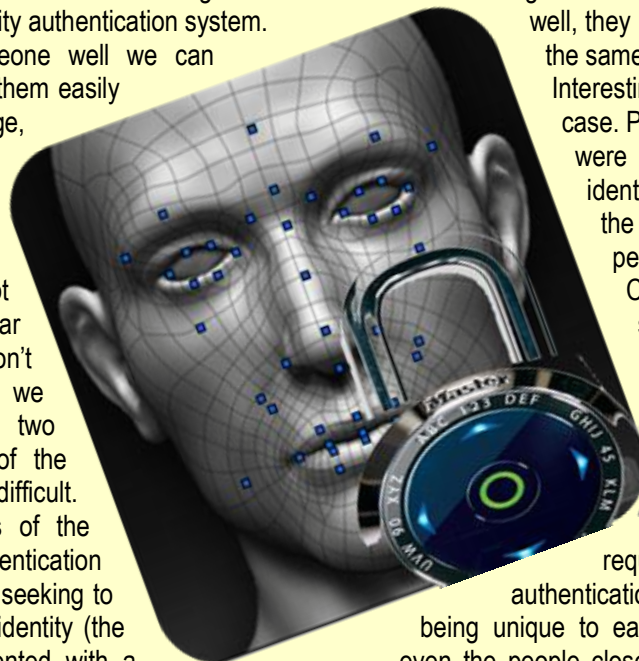
This is the basis of the proposed authentication system. Someone seeking to authenticate their identity (the “subject”) is presented with a succession of pages, each containing nine faces of which one is a person well known to the subject. To prove identity, the face of the familiar person in each grid is clicked.

It is worth pointing out that systems such as Passfaces already do something similar. In Passfaces, during the set up phase, the user selects a number of faces that are presented to them. When logging in, the faces previously selected must be chosen.

Facelock differs in that it allows the subject to choose familiar faces that others are unlikely to recognize. The subjects in this study were told to choose “Z-list celebrities” via Google Image Search, such as obscure musicians, sportspersons or otherwise little-known people but who are of interest to them.

So does it work?

The authors present impressive statistics to support their Facelock approach: subjects detected familiar faces with 97.5 percent accuracy, compared to less than 1 percent for would-be attackers.



Both our ability to recognize faces of people we know and our inability to identify faces of the same person when we do not know them are confirmed by the study.

But the study went further. By choosing faces of people of interest to the subject, even a year later subjects were able to recognize them with an 86 percent success rate.

A possible weakness of the approach was also tested. It might seem that if someone knows us well, they might also know many of the same faces.

Interestingly, this was not the case. Partners and close friends were surprisingly poor at identifying faces known by the study participants (a 6.6 percent success rate).

Colleagues of the subjects and people looking over their shoulder at their selections were even worse.

So this ability seems to satisfy the other requirement for an authentication mechanism, that of being unique to each person. That is, not even the people closest to us will be able to recognize the same faces that we can.

But there are downsides

Technical challenges are unlikely to limit such a system. As noted, systems such as Passface have been available for many years. But there are other issues that need solutions before such a system becomes a practical alternative to passwords.

The main issue is that setting up such a system will likely be very labor intensive. How would images be selected for the system? Images of well-known figures would be unsuitable; they would have to be people who are not widely known.

Additionally, images of the same person would need to be sufficiently different that identifying the person is a challenge for anyone unfamiliar with the faces. How could we determine if they are different enough?

It is hard to see how such a system could be set up with anything like the ease that a password is created.



There are other issues as well. Would the system be susceptible to a brute force attack where every combination is tried until the correct one is found?

Some systems force regular password changes on users — should images be changed frequently as well? How would the images be secured? Password files make use of many security features to secure them — what would be necessary for image files?

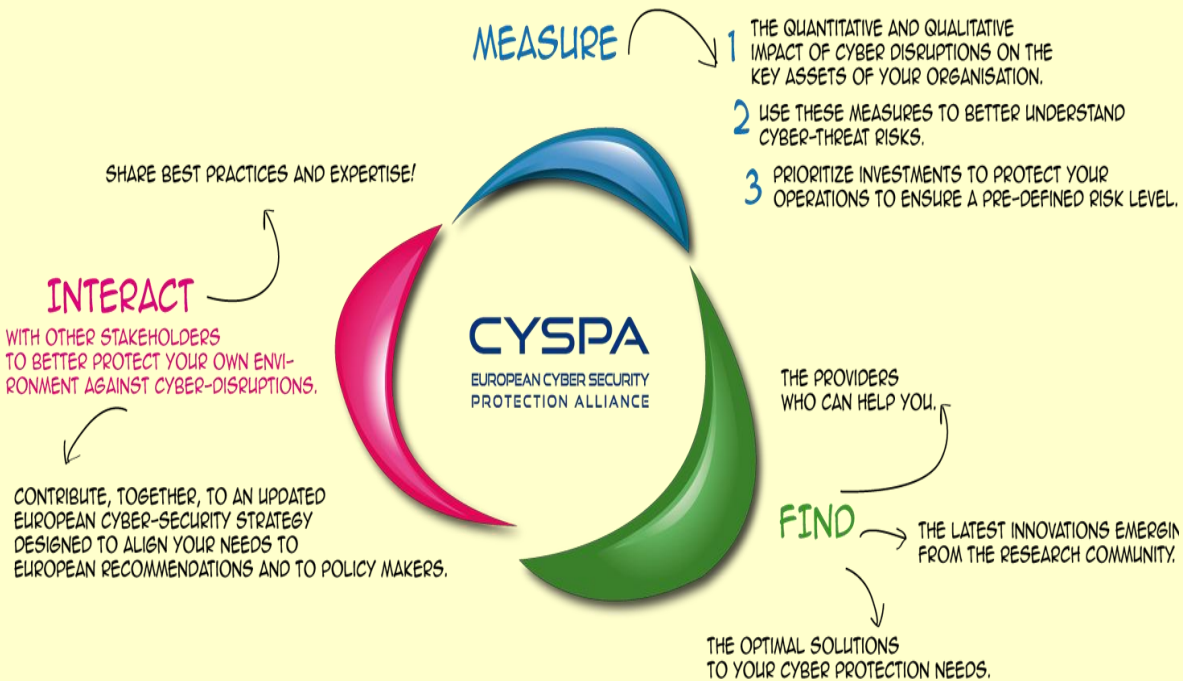
Could face recognition software be used to defeat such a system?

So has something better than passwords finally arrived? The idea certainly sounds interesting and the technical challenges in implementing such a system do not seem great. But there are difficult questions regarding cost, selection and security of images that need to be answered before it becomes a practical alternative to passwords.

Philip Branch is Senior Lecturer in Telecommunications at Swinburne University of Technology.

E-BOOK: Protecting European Organizations against Cyber Threats

Source: <http://edition.pagesuite-professional.co.uk/launch.aspx?pbid=fc8e2ca7-cfe6-455f-94e6-057d5e7298fe>



CYSPA is the **European Cyber Security Protection Alliance**, initiated by 17 founding organisations.

The aim of the Alliance is to **increase the capacity of industry to protect itself from cyber disruptions**. The strategy is to bring together EU stakeholders working together to articulate, embody and deliver the concrete actions needed to reduce cyber disruption.

The key drivers of the Alliance are to deliver **concrete results** to its members and to contribute to Europe's policy on cyber-security by **providing expert input** to the European Commission and the Member States.

The methodology of the Alliance is deliver results through clearly identified **action lines** and to operate both at



sectorial level in domains proposed by its members and at cross-domain level. The Alliance is **open to all stakeholders** impacted by cyber disruptions as well as solution providers



and researchers.

The Alliance is supported through a structured governance that includes a Board, Steering Committee, and selected Advisors; the different sectors are represented in working groups, while the action lines are implemented through task forces.

► Read more about CYSPA at: <http://www.cyspa.eu>

Cyber Deterrence and Its Challenges

By Dr. Vasilos Damiras

Source: <http://strategicri.com/newsAndPress/cyber-deterrence-and-its-challenges>

The United States' ability to deter and disrupt the start of a cyberattack is critical; however, questions remain about whether the U.S. government and private industry are ready to respond to the Top Ten Cyber Security threats. There are two dominant views about cybersecurity challenges.

Cyber deterrence is an important definition on the security lexicon. Nonetheless, various security experts and commentators argue that is extremely difficult to execute cyberspace deterrence, because it is difficult to identify the origins of threat that appears via the Internet.

Deterrence strategy planning goes back to the Thucydides and the Peloponnesian War, and the subject grew during the Cold War as the United States military structure faced the Soviet menace. As history indicates, deterrence is cheaper than its alternative to engage in a continuous conflict.

The new kind of virtual warfare can be also devastating. Cyber warfare like the 2007 attack on Estonia produced substantial economic damage on the victim. Georgia faced a similar cyberattack in 2008 as Russian forces advanced in her soil. In 2009, the United States and South Korea faced various cyberattacks. North Korea was the originator of this penetrating cyberterrorism.

Two Views

In this new cyberspace challenge, the United States is called to develop effective cyber deterrence and countermeasures. Nonetheless, it is pressing American homeland security and defense officials to understand the origins of the cyber threat. The main weapons of hackers are computers and handheld devices. **At least two views dominate the debate for defining the term cyberattacks:**

- **Effects-based:** Cyberterrorism exists when computer attacks result in effects that are

disruptive enough to generate fear comparable to a traditional act of terrorism, even if done by criminals.

- **Internet Effects:** Cyberterrorism exists when unlawful or politically motivated computer attacks are done to intimidate or coerce a government or people to further a political objective, or to cause grave harm or severe economic damage.

A well-targeted cyberterrorist act can inflict serious damage or



extensive destruction to infrastructure, and it can be coordinated to enlarge the effects of a simultaneous conventional physical or chemical, biological, nuclear, or radiological attack.

Four Objectives

The specific objectives of a cyberattack are four:

1. Loss of integrity, such that information could be modified improperly;
2. Loss of availability, where mission-critical information systems are rendered unavailable to authorized users;
3. Loss of confidentiality, where critical information is disclosed to unauthorized users; and,
4. Physical destruction, where information systems create actual physical harm through commands that cause deliberate malfunctions.

According to Richard Clarke, former Counter Terrorism Adviser and National Security Advisor to the Clinton and Bush administrations, if terrorists were to execute a large-scale cyberattack against U.S. national interests, the economy would be the main target for total disruption, while human casualties and building infrastructure destruction might be classified collateral damage.

Many American security experts fear that jihadist terrorists or terrorist groups can execute at the same time a cyber and chemical attack to inflict massive and extensive damage in the United States, or against American national interests across the globe.

Reports and Responses

Several recent studies by various global computer security firms discovered that the highest rates for cyberattack operations were targeted against critical and sensitive infrastructures, such as government agencies, financial services, manufacturing companies, and power plants. These reports also showed that the United States was the most frequent country targeted for computer attacks.

U.S. federal agencies have been criticized that they have not taken serious the new threat. In addition, a May 2005 report compiled by the Government Accountability Office (GAO) indicated that because of the evolving sophistication of malicious code on cyberspace, the American government may be

facing a serious challenge to identify and deter cyber threats in the future.

In response to that report, the Bush and Obama administrations authorized U.S. government departments and agencies to find and develop new ways to detect and deter cyberterrorism; hence, elevating cybersecurity as a national priority. Some analysts see the many federal organizations and programs as redundant and duplicative with the American government lacking a strong and coherent strategy for comprehending the true nature of cyber threat and security.

Protecting Critical Infrastructure

The Department of Homeland Security (DHS), despite serious delays executing cybersecurity in February 2006, participated in and organized exercise Cyber Storm which put to the test the ability of the American government, international agencies and partners, and the global private sector to identify, respond, and disrupt to cyberattacks. The exercise aimed to “enhance the nation’s cyber preparedness and response capabilities.” The results were mixed regarding the American response to cyberterrorism.

The Department of Defense (DOD) in August 2005 issued DOD Directive 3020.40, the “Defense Critical Infrastructure Program,” delegated specific and functional responsibilities within the DOD for coordinating the public and private sector during a cyberterrorist attack. DOD also formed the Joint Functional Component Command for Network Warfare (JFCCNW) which has the responsibility to protect and defend all DOD computer systems. Despite all these efforts, Chinese hackers have managed to penetrate its computer system.

FBI and CAEIAE

The Federal Bureau of Investigation (FBI) has created the Cyber International Investigative Program, which coordinated global agencies in the fight of cyber attacks. The National Security Agency (NSA) has established the National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program, which is aimed at diminishing the vulnerability of national information infrastructure by supporting higher education in information assurance (IA), and by creating



more professionals with IA experience and knowledge.

In February 2003, the aforementioned program was supported by DHS and the President's National Strategy to Secure Cyberspace. Under this federal program, four-year colleges and universities and graduate-level universities are able to apply to be qualified as a National CAEIAE. Students entering CAEIAE academic institutions can become eligible to apply for grants and scholarships via the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program (SFS).

CIA and Livewire

The Central Intelligence Agency (CIA) in 2004 organized a cyber exercise code name "Livewire". The exercise clearly stated there were serious questions over government's actions during a cyberattack depending on who was perceived as the perpetrator: terrorist, culprit, foreign government, or bored teenager. Moreover, it questioned the ability of the U.S. government to deter the beginning stages of a cyberterrorist act.

In 2005, the CIA conducted another exercise code name "Silent Horizon" to monitor how government and industry would react to a cyberattack. The main problem that the exercise wanted to address was in a cyber war attack, who will be in charge: the government or a private establishment, because the defense is controlled by a large number of civilian telecommunications firms. The cyberattacks were set five years in the future. The results did not give a clear picture of the situation.

Top Ten Cyber Security Threats

Jacqueline Dudman in her study regarding cyber threats vividly indicates **ten cyber security threats that will challenge the United States and rest of the developed world.**

1. ARM Hacking: Advanced RISC Machines are prevalent in cell phones and microcontrollers. As cell phones become more advanced more and more data is stored on mobile phones, since they are gaining in popularity as laptop replacements, they become a bigger target. More services run on mobile phones and some of them are vulnerable in the same way they are vulnerable

on PCs making it easier for hackers to exploit vulnerabilities on mobile phones.

2. Social Engineering Attacks: Social media adoption among businesses is skyrocketing and so is the threat of attack. Organizations can expect to see an increase in social media profiles used as a channel for social engineering tactics. Thieves will utilize clever tactics to coerce end-users into disclosing sensitive information, downloading malware or both. Attackers will increasingly make use of social-engineering tactics to bypass technological security controls, fine-tuning their techniques to exploit natural human predispositions.

3. Hactivism: Data thieves are simply looking for the path of least resistance, that path has been leading directly to SMBs (small businesses) that house large amounts of valuable data, but lack the data security budgets of their big business peers. Common modes of attack include everything from social engineering to SQL injection. Those leading the digital disruptions will join forces with physical demonstrators, and will target public figures, such as politicians, industry leaders, judges and law enforcement, more than ever before.

4. Cloud Computing: Companies are smartly embracing the cloud for the associated cost savings and ease of use. Unfortunately, current surveys and reports indicate that companies are underestimating the importance of security due diligence when it comes to vetting these providers. As cloud use rises, new breach incidents will highlight the challenges these services pose to forensic analysis and incident response and the matter of cloud security will finally get its due attention.

5. Industrial Attacks: Water, electricity, oil and gas are essential to people's everyday lives, yet many industrial systems are not prepared for cyber-attacks. Many of the environments where SCADA (supervisory control and data acquisition) systems are deployed don't have stringent security practices. As with recent incidents directed at water utilities in the U.S., attackers will continue to leverage this lack of preparedness, if only for blackmail or extortion.



6. Targeted Mobile Threats: Like ARM Hacking but with a specific target...Your Money! Expect mobile attackers to improve on their skill set and move toward mobile banking attacks. Techniques previously dedicated for online banking -- such as stealing from victims while they are still logged on, while making it

currencies, in order to steal money from unsuspecting victims or to spread malware.

9. Rogue Certificates: Untrustworthy and undetectable organizations and individuals tend to trust digitally-signed certificates; however, recent threats such as Stuxnet and Duqu used rogue certificates to evade



appear that transactions are coming from the legitimate user -- will now target mobile banking users. Attackers will bypass PCs and go straight after mobile banking apps, as more and more users handle their finances on mobile devices.

7. Embedded Hardware: Embedded systems are designed for a specific control function within a larger system and are commonly used in automotive, medical devices, GPS devices, routers, digital cameras and printers. Expect to see proofs-of-concept codes exploiting embedded systems to become more effective. This will require malware that attacks at the hardware layer, and will enable attacks to gain greater control and maintain long-term access to the system and its data. Sophisticated hackers will then have complete control over hardware.

8. Virtual Currency: A cyber-criminal payment plan Virtual currency, sometimes called cyber currency, has become a popular way for people to exchange money online. These online "wallets" are not encrypted and the transactions are public, making them an attractive target for cyber criminals. Expect to see this threat evolve into spam, data theft, tools, support networks and other associated services dedicated solely to exploiting virtual

detection. Expect to see the production and circulation of fake rogue certificates increase. Widescale targeting of certificate authorities and the broader use of fraudulent digital certificates will affect key infrastructure and secure browsing and transactions, as well as host-based technologies such as whitelisting and application control.

10. Insider Threats: You can have all of the best IT security practices in place; however, the biggest threat of all remains humans. The accidental insider breach will continue to be the primary source of compromise for the Advanced Persistent Threat (APT) and other attacks. Organizations need to focus on security awareness training and internal monitoring to detect intentional and accidental insider access.

The National Security Agency (NSA) and the Federal Bureau of Investigation FBI Strategic Information and Operation Center (SIOC) try to prepare and warn various American corporations for the major cyberattacks. It is evident that the American government still has difficulty in creating and establishing a clear and strong strategy regarding cybersecurity.

Some progress has been made to understand the threat and find



countermeasures. Yet it is imperative that current and future American administrations study and introduce new and capable ways

powerful enough to detect and thwart a cyberattack or attacks.

Dr. Vassilios Damiras is the CEO of Geostrategic Forecasting Corporation (GSFC) in Chicago, IL.

Syrian Electronic Army's attack on Reuters makes a mockery of cyber-security (again)

By Bill Buchanan

Source: <http://www.homelandsecuritynewswire.com/dr20140702-syrian-electronic-army-s-attack-on-reuters-makes-a-mockery-of-cybersecurity-again>

Marine website hacked by SEA, who left this defacing message // Source: shenidi.com
One big security issue that has arisen lately concerns control of news media. National

of the major media outlets. It did something similar to the *New York Times* last August. In this most recent case, the SEA appears to have redirected viewers to the bogus pages by compromising advertising hosted by a Reuters partner site called Taboola. This could have serious consequences for Taboola's other clients, who include Yahoo!, BBC Worldwide and Fox News; and will generally be great worry to many sites.



boundaries have become blurred on the Internet, and the control any nation can have over information dissemination has been eroded — on news Web sites but especially on open platforms such as Twitter and Facebook. Witness the activities of the Syrian Electronic Army (SEA), a pro-Assad group of “hacktivists,” which despite limited resources managed to compromise one of the leading news agencies in the world. It wasn't even the first time — it has already attacked the agency several times before, not to mention its other attacks on the *Financial Times*, *Washington Post*, *New York Times*, and *Associated Press*.

At midday on Sunday, people reading Reuters content found themselves redirected to a page which stated:

Where last year, for example, the SEA attack involved tweeting links to pro-Assad propaganda from the Reuters Twitter account, this time it targeted Reuters content directly. But instead of targeting the agency's site, the hack attacked the news content that it hosts on the sites of a large number of media outlets.

This is not the first time the SEA had attacked in a way that compromised the trusted partners

Look what the spear phishing dragged in ...

Another possibility for what lay behind the latest Reuters attack was one of the most common methods of compromise — a spear phishing e-mail, similar to the one that the SEA used to attack satirical site *The Onion* last year. This involved a person in the company clicking on what seemed to be a link to a lead story from the *Washington Post* but turned out to be malicious. It re-directed the user to another site and then asked for Google Apps credentials. Once these had been keyed in, the SEA gained access to *The Onion's* Web infrastructure and managed to post a story. While it took a while for *The Onion* to understand what had happened, Reuters quickly detected the compromise and had fixed the content within twenty minutes. But in classic form, when *The Onion* had got on top of the problem, it posted an article whose headline read, *Syrian Electronic Army Has A Little Fun Before Inevitable Upcoming Death At Hands of Rebels*.

These examples illustrate that organizations need to understand that there are new risks within the information age and there are new ways to distribute messages, especially from hackers skillful enough to be



able to disrupt traditional forms for dissemination.

The nature of the cause is likely to vary widely. In 2011, for example, Tunisian government Web sites were attacked by dissident group Anonymous because of Wikileaks censorship. The same year, the Sony Playstation Network was hacked after Sony said it would name and shame the person responsible for hacking its consoles. This showed that just because you are small on the Internet doesn't mean you cannot have a massive impact. Sony ended up losing billions on its share price and lost a great deal of customer confidence.

HBGary Federal vs Anonymous

The attack on security firm HBGary Federal is perhaps the best one in terms of how organizations need to understand their threat landscape. It started when Aaron Barr, the security firm's chief executive, announced it would unmask some of the key people involved in Anonymous, and contacted a host of agencies, including the U.S. National Security Agency and Interpol.

Anonymous bounced a message back saying HBGary shouldn't do this, as it would retaliate. As a leading security organization, HBGary thought it could cope and went ahead with its threat.

Anonymous then searched the HBGary content management system and found it could get access to a complete database of usernames and hashed passwords by inserting a simple [PHP](#) embed.

As the passwords were not encrypted, it was an easy task to reverse engineer the hashes back to the original password. Their target, though, was Aaron Barr and his chief operating officer, Ted Vera, each of which used weak passwords of six characters and two numbers, which are easily broken.

Having obtained their login details, Anonymous moved on to other targets. Surely they wouldn't have used the same password for their other accounts? Sure enough they had, including the likes of Twitter and Gmail, which allowed access to gigabytes of research information. Then the hackers noticed that the system administrator for their Gmail e-mail account

was called Aaron. As a result they managed to gain complete control of the company e-mail system, which included the e-mail system for the Dutch police.

Latterly they went after top security expert Greg Hoglund, who owned HBGary. This involved sending him an e-mail from within the Gmail account, from the system administrator, asking for him to confirm a key system password. After Hoglund replied back with it, Anonymous then went on to compromise his accounts.

HBGary Federal ended up being closed down due to the adverse publicity around the hack. Having said that, its partner company, HBGary, has gone from strength to strength. Hoglund is well known for making visionary presentations on computer security around the world. The word in the industry is that HBGary still did pass the Anonymous names to the American authorities, but no one knows for sure.

Conclusions

One lesson from all of this is that a focus of any attempted hack will be a spear phishing e-mail. Tricking users into entering their details may be simple, but it can be very serious. For example the Reuters site integrates more than thirty third-party/advertising network agencies into its content. A breach on any of these could compromise the agency's whole infrastructure. I'll end with a few straightforward pieces of advice that anyone who cares about security ought to follow:

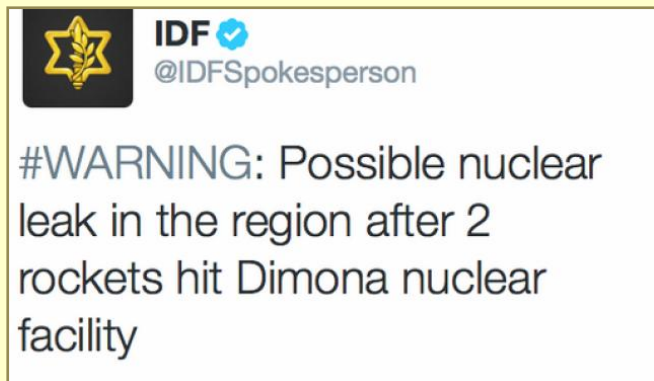
- Use strong passwords
- Never re-use passwords
- Patch systems
- Watch out for internal e-mails from bogus sources
- Beware external Web sites that integrate with your organization's site
- Get a service level agreement (SLA) from your cloud provider. This should state how quickly the provider will react to requests for a lockdown of sensitive information, along with providing auditing information to trace the compromise
- Don't store e-mails in the cloud
- Test your Web software for scripting attacks



IDF's Twitter account hacked: 'Rockets hit Dimona nuclear facility'

Source: <http://www.haaretz.com/news/diplomacy-defense/1.603040>

Hackers from the Syrian Electronic Army broke into the IDF Spokesperson's English-language Twitter account Thursday night, tweeting – among other hoax messages – "WARNING: Possible nuclear leak in the region after 2 rockets hit Dimona nuclear facility."



Following the Dimona message, the hackers posted another tweet reading "Long live Palestine." The tweets were deleted within minutes, but not before dozens of people already retweeted the hacked messages.

IDF officials confirmed that the account was hacked and shortly afterward the IDF Spokesperson tweeted an apology: "We apologize for the incorrect tweets. Our twitter account was compromised. We will combat terror on all fronts

including the cyber dimension."

The Syrian Electronic Army took responsibility for the hacking and tweeted about it on its page.

New Survey: Targeted Attacks on the Rise

Source: <http://i-hls.com/2014/06/new-survey-targeted-attacks-rise/>

According to a survey of nearly 4,000 IT managers across 27 countries targeted attacks are on the rise year-over-year. The survey also identified the business sectors most likely to be targeted.

Globally, 18% of organizations in the Government & Defense sector reported at least one targeted attack within the past 12 months. The rate of targeted attacks reported within the Government & Defense sector was the highest rate reported in this year's survey, a notable increase from the global average of 12% reported across all business sectors.

When looking at data across all business sectors, it's also clear that targeted attacks are not limited to the Government & Defense industry. Other business segments have felt the brunt of targeted attacks at a higher-than-average rate, including the Telecommunications industry where 17% of businesses reported targeted attacks, and the Financial Services and Transportation & Logistics sectors, both of which reported targeted attacks within the last 12 months at a rate of 16%.

The survey responses show the overall number of targeted attacks to be increasing as well.

The 12% of all businesses reporting a

targeted attack in 2013 has risen from the 9% average reported in 2013 and 2012.

Conducted in partnership with B2B International, these results have been published in Kaspersky Lab's 2014 IT Security Risks summary report, which outlines the types of internal and external security risks most often encountered by businesses across a variety of industries, along with the costs associated with an IT security incident, the types of data most lost as a result of these attacks, and more.

Perhaps unsurprisingly, 94% of companies reportedly encountered at least one externally-sourced data security incident within the past 12 months, including phishing attacks, DDoS attacks, and theft of mobile devices. In 28% of these instances, business reported the loss of sensitive business data.

The increase in the prevalence of targeted attacks, both in volume and in types of businesses being targeted, comes at a time when high-profile targeted attacks are being uncovered at an alarming pace. In September 2013, Kaspersky Lab released its analysis of the Icefog targeted attack campaign, a multi-year campaign which focused on



military, telecommunications, shipping and research organizations in South Korea and Japan. In February 2014 the company reported the discovery of The Mask cyber-espionage campaign, which included victims in 31 countries around the world, including governments and government-related agencies.

While the overall amount of data stolen from targeted attacks is lower than the losses that result from general malware attacks, it must be noted that general malware attacks themselves are much more common (an average of 61% of businesses reported malware attacks compared to an average of 12% reported

targeted attacks). However, the value of the data stolen from a targeted attack is much more likely to be highly valuable to the attackers, and the loss of this highly-sensitive data (future product plans, company financial statements, etc.) would cause more long-term damage to a company's business outlook.

A "targeted attack" typically consists of several malicious components that operate in tandem to bypass an organization's security measures, infect machines, and steal sensitive data. These attacks can implement unique modifications to common malware, or exploit specific vulnerabilities in targeted organizations.

Spain hit by Cyberwarfare attack

Source: <https://www.euroweeklynews.com/news/spanish-news/item/121378-spain-hit-by-cyberwarfare-attack>



Western energy companies in over 84 countries including Spain, France and USA are being targeted by Russian hackers who have threatened to disrupt power supplies.

The group called Energetic Bear have attacked more than 1,000 organisations since they were uncovered in 2012, according to cyber security researchers at CrowdStrike.

The hackers, nicknamed Dragonfly, have developed software that allows them to assume remote control over power companies and are able to disrupt power supplies to both private homes and businesses, but most recent attacks have been on government agencies and healthcare organisations.

A statement issued by computer security company Symantec said: "Among the targets of Dragonfly were energy grid operators, major electricity generation firms, petroleum pipeline operators, and energy industry industrial equipment providers.

"The majority of the victims were located in the United States, Spain, France, Italy, Germany, Turkey, and Poland."

Another security company F-Secure, based in Finland said that during the last six months the group has become increasingly sophisticated and aggressive, hiding behind encryption techniques.

The current cyberwarfare campaign is similar to one carried out in 2010 by Israel and the USA which attacked the Iranian nuclear industry.

Tunisian Hackers Announce Cyber Jihad Against US Banks, Airport Computer Systems

By Anthony Kimery (Editor-in-Chief HSToday.com)

Source: <http://www.hstoday.us/single-article/exclusive-tunisian-hackers-announce-cyber-jihad-against-us-banks-airport-computer-systems/7c3d2373e69fa9319e521816ce539b7d.html>

Beginning July 5, The Tunisian Hackers Team (THT), a group of Tunisian hackers known for its 2013 attempts to attack US banks, including Bancorp, announced via social media that it intends to launch a cyber attack on US banks and airport computer systems during the coming week, according to the Middle East

Media Research Institute's (MEMRI) Cyber Jihad and Lab Project.

MEMRI's cyber lab constantly monitors the activity of online jihadi and hactivists groups from the Middle East and South Asia.



MEMRI said, "In a video posted on the Internet on April 12, the Tunisian Hackers Team



threatened to attack the US financial sector and air traffic control in July unless US forces are withdrawn from Muslim lands. In an address to President Barack Obama, the Department of Homeland Security [DHS], the FBI and the CIA, the group claimed to have carried out cyber attacks in September 2013 and to have hacked into the Bancorp bank." "We first heard of The Tunisian Hackers Team in April when they announced in a video message directed to the U. government that the week of July 4th they would begin cyber attacks on US banks," *Homeland Security Today* was told by MEMRI Executive Director Steven Stalinsky. "These threats and the group itself are reminiscent of the Qassem Cyber Brigades," Stalinsky said. "It's unclear how strong the THT's capabilities really are -- but their warning that they will be working to gain control of American airport computer and communication systems should be taken seriously by homeland security officials. These types of threats by Middle East and South Asia cybergroups are the new norm and will only be increasing in the future." MEMRI's upcoming report on THT includes a transcript of a video the group released in April announcing what it calls the "Week of Horror," posts from its Twitter and Pastebin accounts

listing websites it has hacked; and similar threats posted to its Facebook page.

THT stated that its goal is to remove the US military from its "beloved lands of Muhammad." In the group's April video address to Obama, DHS, FBI and CIA in which it threatened attacks on US banks this month, a digital voice said: "Dear President of the United States, dear Department of Homeland Security, dear FBI administration in Washington, dear Central Intelligence Agency – this is the Tunisian Hackers Team."

"We warned you a few months ago, in Operation USA, released by our team, that if you keep ignoring us, we will carry out Operation Week of Horror in July 2014," the group continued, adding. "We promise that it will be more painful than a secret attack by Tunisian Hackers Team members in September 2013 against your financial sector. Today, the first Bancorp Bank has been hacked, and more than 12,000 users are in danger, and more ... So we repeat it again: If



you don't declare that you will remove your army from our beloved lands of Muhammad, we will increase the level of our operation. We will attack not only your financial sector, but next time, there will be an attack on your airness [sic]. We will work on gaining control of your airports' computers -- and you know very well that we can do this -- and of the electronic sector."

"So we will give you more and more time to think," the group said, "and reply to us on Twitter via @XhckerTN, or else we will realize our plan. Expect us. We are the cyber boss. We are the Tunisian Hackers Team."

According to the MEMRI Cyber Jihad and Lab Project, "The Tunisian Hackers Team Twitter



account, @XhckerTN, mentioned in its April video and on its YouTube page, has, as of July 2, 2014, 575 followers and 1,487 tweets. The group has tweeted numerous times about the 'Week of Horror' and about its their ability to hack into US government and other sites, such as the Atmospheric Radiation Measurement (ARM) Climate Research Facility, Homeland Guantanamo, and the State Department." The group's Pastebin account lists previous cyber attacks worldwide, including against the US government.

"The group's Pastebin account has, as of July 2, 2014, 30 pastes, 7,705 Pastebin hits and 20,526 total pastes hits," MEMRI reported. According to this account, it has targeted several US sites within the past three months, among them the Department of Agriculture and the Central Bureau of Statistics. They list a link to '12 Websites of the US government defaced,' most of them state government sites, including those of Roslyn, NY and Riverdale, NJ."

On its Pastebin account, THT posted its targets for its so-called "Week of Horror" cyber attacks,

including its schedule for the attacks the group said would begin July 5: Day 1, Whitney Bank; Day 2, Union Bank; Day 3, Zions Bank; Day 4, New York Community Bank; Day 5, TCF Bank; Day 6, Prosperity Bank; Day 7, Banner Bank.

According to MEMRI's Cyber Jihad and Lab Project, the group's official Facebook page, which, as of July 2 had 1,765 likes and was created April 10, 2013, posts reiterated threats against the US to be carried out during the "Week of Horror."

On its Pastebin account, THT has posted its targets for the Week of Horror, along with its schedule for the attacks beginning July 5: Day 1, Whitney Bank; Day 2, Union Bank; Day 3, Zions Bank; Day 4, New York Community Bank; Day 5, TCF Bank; Day 6, Prosperity Bank; Day 7, Banner Bank.

The group's official Facebook page, which, as of July 2, 2014, has 1,765 likes, was created April 10, 2013. The posts on the page reiterate threats against the US to be carried out during the "Week of Horror."

Anonymous Says it Will Attack Countries Supporting ISIS and 'Assault [American] Virtual Government Infrastructure'

By Anthony Kimery (Editor-in-Chief HSToday.com)

Source: <http://www.hstoday.us/single-article/exclusive-anonymous-says-it-will-attack-countries-supporting-isis-and-assault-american-virtual-government-infrastructure/7d7fa56b5cd3d6565c31ebcf70338fc7.html>

This week, the hacktivist collective known as Anonymous announced in a video on YouTube

that it will soon launch "Operation NO2ISIS," an attack on official websites of countries the group considers to be financially supporting the Islamic State of Iraq and Syria (ISIS).

According to the Middle East Media Research Institute (MEMRI) Cyber Jihad Lab Project that monitors the activity of online jihadi and hactivists groups from the Middle East and South Asia, "The name NO2ISIS is taken from #OPNo2ISIS, an anti-ISIS movement formed in reaction to ISIS's expansion into Iraq. Operation NO2ISIS's stated targets are Qatar, Saudi Arabia and Turkey, and Anonymous has said that it will also attack the US in the event of any attempt on its part 'to fuel [its] military industrial complex.'"

MEMRI will be releasing a report on the matter.



The following is a transcript of the video, as provided by Anonymous:

"To the citizens of the world, we are Anonymous. The events currently transpiring in Iraq have made us as a collective re-evaluate our priorities in regards to recent operations. The Iraqi people have gone through almost two weeks of sheer terror most of us will never



know nor experience. We are held by a code of honor to protect those who are defenseless, both in the cyber world and the real world.

"Before our inception, the Iraq war was well underway and crimes against humanity were rampant. The United States had no small part in this. When the United States government decided to begin an unnecessary war with the promise of oil and funds to the military industrial complex, it failed to realize the severity of taking out a leader who controlled a strong internal security force. This led to the power vacuum we witnessed after his capture. Yes, Saddam Hussein was ruthless and violent, but with this war, the US was guilty of the same crimes (i.e. Blackwater, Abu Ghraib, etc.).

"Fast forward to today, and Iraq is descending into chaos yet again thanks to the dastardly ruthless gang aiming to establish an 'Islamic'

state combining both Iraq and Syria, thus doing away with the post-WWI borders. They call themselves ISIS. These savages who have no religion or morality are bent on burning everything in their path, killing and pillaging as they go. They must be stopped.

"Several days ago, their electronic division assumed control of one of our twitter accounts (@TheAnonMessage) claiming it for themselves and releasing several graphic photos of their assault near Baghdad. These tweets have since been deleted. We sincerely apologize to the twitter followers who had to witness this without warning. This was an unfortunate, unprecedented takeover and steps have been taken to further secure this account from any future attempted hacks.

"We would also like to comment on the mainstream media who are pushing the division of Iraqis even further. The Iraqi public is made up of two Islamic sects: Sunnis and Shias. There are also other groups which include Kurds, Turkmen, Assyrians, Christians and others. The media would want us to believe that ISIS is made up of strictly Sunnis and the Iraqi army is a majority-controlled and operated Shia faction.



This is false. The groups that have been listed, including Sunnis, are enlisted in the Iraqi army and Sunni clerics in Iraq have also called for their followers to join ranks with their Shia brothers to defend their homelands.

"ISIS is a group made up of a Takfiri sect which is regarded by many prestigious clerics and organizations including Al Azhar, as un-Islamic. In fact, they have denounced them as 'Khawarij' and declared that they



must be exterminated from Islamic lands. This is why we urge the American mainstream media to stop releasing false information and further escalating the violence with their ignorant journalism.

"In conclusion, we stand by every righteous being when we say that we have also declared complete solidarity against those who affiliate themselves with ISIS and those who control them. Aljazeera; you have tarnished your reputation by spewing your lies and your treasonous support to ISIS. You will not escape us. To the state of Qatar, Turkey and the Kingdom of Saudi Arabia; you will not escape our wrath. Evidence shows your continued support and supply to ISIS. If this does not promptly stop, we will be forced to unleash our entire legion against your pathetic excuse of a cybersecurity. And to the United States; another attempt at fueling your military industrial complex for the sake of security and democracy will be grounds for our complete assault against your virtual government infrastructure. You have been warned."

MEMRI said, "The Twitter account, @TheAnonMessage, which Anonymous states in the video was hacked by ISIS and was now restored, was created in November 2011; as of July 1, 2014, that account had posted 3,378 tweets and had 16,000 followers."

"The @No2ISISofficial Twitter account," MEMRI said, "states that it is 'the official Twitter handle of the #No2ISIS campaign' and refers readers to an email account, No2ISISofficial@gmail.com for more information. As of July 1, 2014, this Twitter account had posted 51 tweets and had 285 followers; it also links to the Facebook page."

"In its 'About' section," MEMRI reported, "the #No2ISISofficial Facebook page states that it is the 'official Facebook page of the #No2ISIS campaign," which was established "by a group of grass-roots community activists concerned with the rising threat of foreign terrorists in Iraq, namely the Islamic State of Iraq and Sham who intensified their attacks from 5th June 2014."

Anonymous declared that its main aims are to raise awareness about:

- The brutality and savage crimes ISIS have committed;
- Possibility of ISIS recruitment from UK and potential attacks here;
- The threat it poses to the security and safety of civilians in Iraq;
- Inaccurate reporting of current events, relying on ISIS rumours & propaganda;
- Negative and inaccurate use of sectarian language in the media; and
- To show that Iraqis are united against ISIS terrorism.

Top FBI cybercrime expert was a discount furniture salesman before joining and thwarting online theft and fraud worldwide

Source: <http://www.dailymail.co.uk/news/article-2690798/Top-FBI-cybercrime-expert-discount-furniture-salesman-joining-thwarting-online-theft-fraud-worldwide.html>



J. Keith Mularski's world has expanded greatly since he stopped selling discount furniture to join the FBI 1998. Especially since he transferred from Washington, D.C., in 2005 to fill a vacancy in the Pittsburgh, Pennsylvania's field office's cyber squad - which he now heads.

Since then, Supervisory Special Agent Mularski has been recognized as a foremost expert on cybercrime. His profile has risen even more since the Justice Department used Mularski's sleuthing to bring two indictments with worldwide ramifications.

In May, five Chinese Army intelligence officers were charged with stealing trade secrets from

major manufacturers including U.S. Steel, Alcoa and Westinghouse.

In June, a Russian man was charged with leading a ring that infected hundreds of thousands of computers with identity-thieving software, then using the stolen information to drain \$100 million from bank accounts worldwide.

Mularski, 44, said in April during an oral history interview for the National Law Enforcement Museum that he became a furniture salesman out of college because jobs were hard to come by then. He spent about five years in the business before joining the FBI.

'I was in private industry beforehand. But I've kind of always liked computers,' said Mularski.



Mularski chose to join the Pittsburgh cyber squad largely because of family considerations - he grew up in suburban White Oak, Pennsylvania, the son of a steelworker.

'It kind of looked like cyber was the wave of the future,' Mularski said. 'The majority of all my computer training was just on-the-job training at the bureau.'

It has proved remarkably effective.

Even before the Chinese and Russian cases made worldwide headlines, Mularski was making cyber waves.

He made his reputation infiltrating Dark Market in 2006. The worldwide Internet forum allowed crooks to buy and sell stolen identity and credit card information.

Mularski infiltrated the network by pretending to be a notorious Polish computer hacker using the screen name 'Master Splyntr' - a takeoff on the cartoon rat who guides the Teenage Mutant Ninja Turtles.

Mularski was inspired while watching the cartoon character with his young son: 'He's a rat that lives underground. It was perfect,' he said.

Mularski befriended the criminal mastermind behind the site and persuaded him to let Mularski move the operation onto new computer servers. The servers happened to belong to the FBI, which led to more than 60 arrests worldwide.

Misha Glenny, a British journalist who specializes in cybercrime, wrote a book about the case called 'Dark Market, How Hackers Became the New Mafia.'

'Keith Mularski is not without technical ability, but his real talent lies in convincing experienced cybercriminals that he is one of them and not a law enforcement officer,' said Glenny.

His aw-shucks demeanor also makes him an ideal team player.

'He has an understanding of the whole grid, and then he develops relationships, whether it's with victims, the private sector, and our international partners,' said David Hickton, the U.S. attorney in Pittsburgh.

Those partnerships are important because the United States doesn't have extradition treaties to bring the Chinese and Russian suspects here for prosecution. Those defendants could be arrested if they travel into areas that cooperate with the U.S., but Hickton and Mularski said that's not the only purpose served by those indictments.

'The best result is to be able to get cuffs on a guy,' Mularski said. 'But you have to measure how you can impact each (criminal) organization.'

In the Russian case, Mularski got a federal judge in Pittsburgh to allow the Justice Department to monitor some 350,000 computers infected with malicious software, so the thievery could be stopped.

The Chinese indictment, meanwhile, was a 'put up' to the Chinese government's rumblings that the U.S. government should "shut up" about ongoing cyberspying allegations unless they could be proved, Mularski said.

Some cases produce a more tangible result.

The Dark Market case led Mularski to Max Ray Butler, a San Francisco hacker whose home computer was found by the FBI with 1.8 million stolen credit card numbers on it. Butler, who changed his name to Max Ray Vision, pleaded guilty and was sentenced to 13 years in prison - the longest sentence yet handed down in a U.S. hacking case. He was also ordered to repay banks \$27.5 million, the cost of replacing all the cards he stole.

'This was all just really organized crime with a computer,' Mularski said. 'It's traditional sleuthing but in a 21st-century way.'

'Terror texts' bring cyber warfare to mobile phones

Source: <http://www.jpost.com/Operation-Protective-Edge/Terror-texts-bring-cyber-warfare-to-mobile-phones-362756>

On the third day of Operation Protective Edge, a Haaretz news update on 29-year-old Sareena Denis's phone alerted her to horrifying news. Hamas had hit a chemicals plant in Haifa. The city was being evacuated. Twenty-five people were dead.

"I was so worried, I was so scared. It was this realization that the conflict escalated to a whole other level," said Denis, a Chicago native who made aliya in 2010, and had been taking the



semi-regular red alerts and trips to the bomb shelters in stride.

Yet none of the news sites was carrying the story, and none of her friends had heard about it. Soon, Haaretz clarified that the text messages sent to thousands of phones “were in fact sent from a fake account.” “I was relieved, but at the same time I was so upset, because it’s very disturbing to know that some hacker or Hamas has my phone number,” Denis said. “Something about having my emotions manipulated, it just felt like, as terrorists, they had really achieved their goals. I just started bawling when I realized what had happened.”

The false message, written in English, was one of several that made its way to people’s phones during the operation. Though police do not yet know if the texts originated from abroad or within Israel, they are perceived as part of a psychological war waged by Hamas or its supporters, akin to the cyberattacks on Israeli websites that have proliferated in recent years. According to Haaretz, the messages “were most likely sent from a pro- Hamas source as psychological warfare to instill fear and panic in Israeli citizens.”

On Monday, a message from “SMSQASSAM,” signed Izz ad-Din al-Qassam Brigades – Hamas’s military wing – vowed to keep firing on Israelis until its “legitimate demands” were met.

An earlier message, claiming to be from “SHABAK,” the Shin Bet (Israel Security Agency), stated that a suicide bomber was on the loose, waiting to blow up civilians hiding in bomb shelters. “Beware of strangers in shelters,” it warned.

Another, written in Hebrew and allegedly sent from Home Front Command, said the IDF was planning an attack in Gaza at 12:16, and instructed people to get to their bomb shelters near that time to avoid retaliatory rockets.

“In these instances the messages are false,” said an instructor on the Home Front Command hotline.

“We do not disseminate information on IDF activities. It’s preferable to ignore it and not pass it on.”

With the exception of an SMS survey it sent out last week, she said, Home Front Command had not made any attempts to communicate with the public via text message or the WhatsApp mobile app.

Yair Amichai-Hamburger, who heads the Center of Internet Psychology at the Interdisciplinary Center in Herzliya, calls the ruses an attempt at psychological warfare.

“Hamas is a very clever terror organization.

Psychology is the name of the game, and they want us to feel like they can reach us. It is a mosquito that is trying to pretend it’s a lion,” he said.

By playing on people’s fears during times of high stress and little information, he says, the culprits can strike raw nerves and toy with people’s emotions.

It is still unclear who is behind the messages, however, and Amichai- Hamburger notes that they could be coming from devious Israeli pranksters.

“If you want to believe that these are Hamas people, this is a possibility, but from other things happening on the Internet, it may not be the situation.” Plenty of hackers and trolls get a certain pleasure out of riling people up, he offered.

Indeed, the police have recently dealt with mean-natured pranks playing upon national security problems. After three Jewish teenagers were kidnapped last month, the police received several false alarms in the form of phone calls.

The cranks, mimicking a much-discussed call from one of the teens that failed to elicit a police reaction, claimed they, too, were being kidnapped.

“These people usually suffer from a strong need to justify their existence in a very distorted way. They get their self-esteem from doing these terrible things,” said Amichai-Hamburger.

“They’re normal people who look like you and me, but they find their fun in a very bizarre way.”

Text messages aside, cyberwarfare has not been confined to SMS-based misinformation.

Domino’s Pizza’s Hebrew Facebook page was hijacked for several hours on Sunday, allegedly by Palestinian hackers, who replaced the cover photo with Hamas fighters and anti-Israel messages. When they regained control of the page, Domino’s posted a photo of a terrorist saying, “You will not conquer the Israeli hunger for pizza!” Pro-Israel hackers also had a victory on the cyber-battlefield. A major hacking attack was carried out Monday against



some of Hamas's leading websites. For more than five hours, various sites were disabled and others displayed content against Hamas and its leaders. The leading Hamas site Shehab.ps displayed anti-Hamas headlines, which when clicked played a video from Egyptian television that was unfavorable to Hamas. In the video, from the Egyptian anti-Hamas website El Balad, Hamas leader Khaled Mashaal is seen living a life of luxury. The anchor on the video says: "If Mashaal is man enough, why doesn't he take a plane from Qatar to Egypt. We would gladly open our border and let him enter the Gaza Strip, and

then he can hide together with Hamas leader [Ismail] Haniyeh in a bunker underground." Later Monday, the site's Facebook page – which has more than a million followers – confirmed the "Zionist attack" and said it would "continue to expose the Zionist crimes." Other leading Hamas sites, such as Felesteen.ps and alsafa were hacked as well, and could not be accessed for more than four hours. Soon after the attack, Felesteen's Facebook page posted that the "occupation forces" had hacked the site, and that it was working to fix the page.

Social media and extremism – is Europe failing to tackle the issue?

By Chris Harris (Journalist)

Source: <http://www.euronews.com/2014/07/07/social-media-and-extremism---is-europe-failing-to-tackle-the-problem/>

Governments are at a loss over how to tackle

(ICSR) suggest there are up to 11,000 foreign fighters in Syria, including around 1,900 from Europe. Figures released by the UK's Metropolitan Police revealed 40 people had been arrested since the beginning of the year on suspicion of militant activity in Syria.



extremist groups' "highly-intelligent and unprecedented" use of social media, it's been claimed. Anti-extremism think-tank the Quilliam Foundation says authorities are failing to provide the counter-narrative to radical online propaganda. It comes as the likes of Germany, France and the UK meet in Milan today (Wed, July 8) to work out what to do about European-bred jihadists. They are fearful 'radicalised' Europeans will return home from places like Syria and carry out atrocities. There are reports the suspect behind a bombing at a Jewish museum in Brussels, which killed three people, had recently returned home from fighting in Syria.

Latest estimates from the International Centre for the Study of Radicalisation

In the Netherlands, where as many as 152 people are estimated to have gone to Syria to fight, social media is a key radicalising tool, according to AIVD, the country's general intelligence and security agency.

Ivo Opstelten, the Dutch minister for security and justice, has called on Twitter and other social media companies to delete propaganda posted by violent jihadists, according to the Wall Street Journal.

But Erin Marie Saltman, a senior researcher at Quilliam said censorship was not helpful.

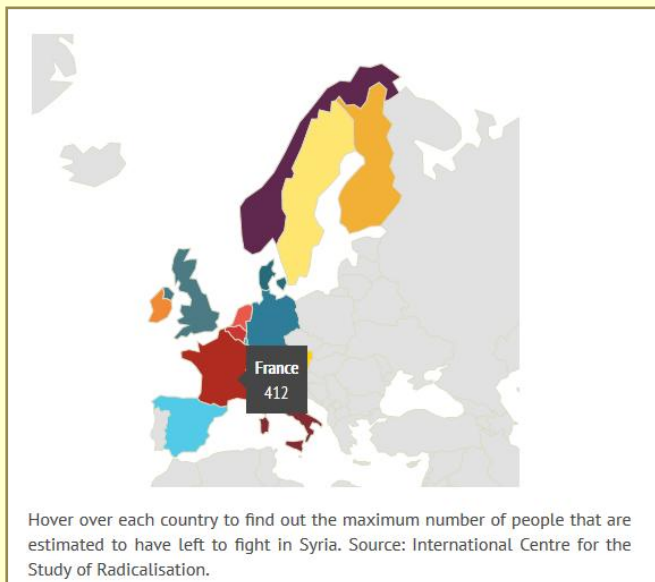
Dr Saltman, co-author of a report about how to tackle online extremism, said: "I would try and explain that negative messages are not the way forward – we should be better at engaging and realise the extremist propaganda does have a counter narrative."

Asked about how well authorities are responding to the challenge, she added: "Governments have been slow in taking social media seriously as a tool that is



legitimate and they are at a loss [at how to react]. They tend to target organisations – such as Twitter – but you’re attacking the system and not the root cause.”

Which countries have the most citizens estimated to have gone to Syria?



How big is the problem of extremism and social media?

Europol, the EU’s law enforcement agency, says social media-driven is a growing issue.

Wil van Gemert, its deputy director of operations, told euronews: “In the past there were preachers who reached out and they had maybe eight or 10 followers. But with the internet there’s the possibility to get to hundreds of people. Many more people can be radicalised.”

He added recruits to places like Syria had traditionally been young men – but Europol was now seeing women and girls as young as 16 going.

The report by AIVD on the situation in The Netherlands reads: “The effective use of social media has played a crucial role in the dissemination of jihadist propaganda. It has enabled jihadists to improve the effectiveness and speed of their communication within the Netherlands and abroad and fundamentally changed the characteristics of communication and interaction within the jihadist movement.”

“In the past, it was mainly a vertical process, with the messages intermittently emanating from one sender to multiple recipients (one to many). At present, it has become a much more horizontal movement, with multiple senders to

multiple receivers (many to many) – on a 24/7 basis, a permanent flow of Twitter, Facebook, and other messages, images, and reactions.”

A similar report from Italy, published on the European Foundation for Democracy’s website, claimed there had been a ‘remarkable increase’ in English and European-language jihadist websites.

It said: “While in the 1990s most jihadist websites were in Arabic or, to a lesser degree, other non-European languages, over the past 10 years there has been a remarkable increase in the number of websites in English and, albeit to a lesser degree, other European languages such as French, German and Dutch. Individuals throughout Europe, whose degree of proximity to ‘real’ terrorist networks ranges from close to nil, post online statements from jihadist groups, news about various conflicts, texts from prominent Salafist/jihadist clerics and commentaries on related issues.

Initially limited to websites and blogs, this material is now posted on more interactive platforms as well. Interactions on the many forums, Paltalk chat rooms, Facebook, Twitter and Instagram pages allow wannabe jihadists to feel part of a global community, largely increasing their belief in and commitment to the cause.”

Despite this, there is a degree of caution about social media’s influence.

Europol’s van Gemert said: “It’s the most popular tool but other tools will be used. Even if they are getting radicalised by social media you still have to travel there [to Syria] and there has to be a network for that.”

How are extremist groups using social media to radicalise?

Europol says groups such as ISIS focus on particular European countries, making it clear their compatriots are already in places like Syria.

But a report carried by ICSR suggests it is more sophisticated.

It said Al-Qaeda and its affiliates had realised an “entire media apparatus” was needed and now had a centralised hub where it can consolidate all its propaganda. Groups such as al-Shabaab, it claimed, are



producing lengthy English-language videos. Dr Saltman agreed over the level of sophistication. She said its use of social media was “highly intelligent and unprecedented”, citing a smartphone app from ISIS (The Islamic State in Iraq and the Levant) that automatically posts propaganda to the subscriber’s Twitter feed and reports extremists were hijacking World Cup and Premier League Twitter hashtags to promote their view of the world. But she rejected the idea it was social media alone that radicalised: “The idea of a lone wolf narrative is not true – you don’t go online to

buy a pair of shoes and then become radicalised. The first contact is a real world contact, like someone in your community or something in the media. After that people go online in a vacuum and search for the message they want.”

ISCR also monitored the Twitter accounts of Europeans fighting in Syria – to find out how they get their information and who inspires them.

The study – the subject of a report – identified two key people as being ‘influential’ in the social networks of foreign fighters in Syria, Musa Jibril and Musa Cerantonio.

ISCR said: “Jibril, a US-based preacher with Arab roots who is in his early 40s, does not explicitly call to violent jihad, but supports individual foreign fighters and justifies the Syrian conflict in highly emotive terms. He is eloquent, charismatic, and – most importantly – fluent in English. So is Musa Cerantonio, a 29 year old Australian convert to Islam who frequently appears on satellite television and has become an outspoken cheerleader for ISIS.

“Both men are very different and consequently have different appeals. Ahmad Musa Jibril is a subtle, careful, and nuanced preacher, while Musa Cerantonio is much more explicit in his support for the jihadist opposition in Syria.”



Twitter profile (left) – Musa Cerantonio

(scroll down at source’s URL to read complete dialogues)

WSJ's Facebook Page Hacked With Fake Air Force One News

Source: <http://mashable.com/2014/07/20/wsj-facebook-page-hacked/>



A false report about the loss of Air Force One was posted to *The Wall Street Journal's* Facebook page early Sunday morning. The newspaper later said its page had been "compromised."





The *WSJ* deleted the fake posts, but not before several users captured screenshots of the apparent hacking:

The newspaper then posted a message saying it was "looking into" the situation:

"We acted quickly to remove erroneous material and have secured the account," a *WSJ* spokeswoman said later on Sunday morning.

The incident echoed the hacking of the Associated Press' Twitter feed last year, when a false report of explosions at the White House was posted. That fake information was also quickly debunked. However, the AP episode occurred in the middle of the day on a Tuesday, so the tweet was widely seen and the Dow Jones Industrial Average briefly plunged before recovering. Since the *WSJ* hack happened overnight on a weekend, its impact will likely be more limited.

Representatives for the Secret Service, which would likely investigate this incident because of the nature of the posts, could not be reached Sunday morning.

President Barack Obama was spending the weekend at Camp David, far from the Russian airspace mentioned in the fake message.

The false report on the *WSJ*'s Facebook page comes just days after the downing of Malaysia Airlines Flight 17 near the Russian border in Ukraine on Thursday.



Innovative projects seek emergency housing alternative to FEMA's trailers

Source: <http://www.homelandsecuritynewswire.com/dr20140624-innovative-projects-seek-emergency-housing-alternative-to-fema-s-trailers>



Brownsville, Texas may soon become a model for other hurricane-ravaged cities as community groups institute new emergency housing measures in the wake of inexcusable hold-ups on the part of the Federal Emergency Management Agency (FEMA).

emergency housing for families in the wake of disasters, following FEMA's slow response in providing reconstruction support to the South Texas coast after \$1.35 billion in damage from Hurricane Dolly in 2008.

The results of this have manifested themselves

89



As the *Monitor* reports, groups like the Community Development Corporation (CDCB) in the city are assessing new ways to provide

in a 2009 act called HB 2450, which included recommendations for the "Lower Rio Grande Rapid



Re-housing Program,” or RAPIDO, which constructs simple, quick-construction house with a corrugated tin roof.

When implemented by groups like the CDCB, this replaces the slow turnaround time for many victims who languish in typical FEMA trailers, meant originally as a placeholder while homes are rebuilt. A further twenty RAPIDO projects are planned for construction with just a \$2 million portion of the \$130 million that has been spent on Hurricane Dolly response.

The focus of RAPIDO homes (p.7 – top), is on getting victims of federally declared emergencies as quickly as possible so that some semblance of a normal life may resume. Leo Barrera, CDCB’s housing coordinator, told the paper, “The concept is what’s the fastest way to get families back on their property after a hurricane, with a FEMA

trailer. Instead of having [one] sitting on your land or sitting out in a field somewhere, you get to the core. So this would serve as your temporary to permanent shelter.”

The government spends \$60,000 to \$70,000 per FEMA trailer (p.7 – bottom: N Orleans), with people like Barrera calling it a “complete waste of money,” with a RAPIDO house “being permanent, [constituting] a much wiser use of federal tax dollars.”

The goal of RAPIDO is not just to provide worthy homes to victims of disasters, but to influence policy and procedure for future events. The CDCB will monitor the progress of the effort for the next sixteen months in the hopes of developing a manual that can be approved by the state government and implemented during future emergencies.

A new way to detect leaks in pipes

Source: <http://www.homelandsecuritynewswire.com/dr20140624-a-new-way-to-detect-leaks-in-pipes?page=0,1>

Explosions caused by leaking gas pipes under city streets have frequently made headlines in recent years, including one that leveled an apartment building in New York this spring. But while the problem of old and failing pipes has garnered much attention, methods for addressing such failing infrastructure have lagged far behind.

Typically, leaks are found using aboveground acoustic sensors, which listen for faint sounds and vibrations caused by leakage, or in-pipe detectors, which sometimes use video cameras to look for signs of pipe breaks. But all such systems are very slow, and can miss small leaks altogether.

Now researchers at MIT and King Fahd University of Petroleum and Minerals (KFUPM) in Saudi Arabia have devised **a robotic system that can detect leaks at a rapid pace and with high accuracy by sensing a large pressure change at leak locations.** The concept was presented at two recent international conferences, and has been described in several recent papers.

This new system “can detect leaks of just 1 to 2 millimeters in size, and at relatively low pressure,” says **Dimitrios Chatzigeorgiou**, a Ph.D. student in mechanical engineering at MIT and lead author of the research papers. “We’ve proved that the concept works.”

The researchers have begun discussions with gas companies and water companies — the system can also detect leaks in water pipes, or in petroleum pipelines — about setting up field tests under real-world conditions.

Chatzigeorgiou presented the concept this month at the International Conference on Robotics and Automation in Hong Kong, and at the American Control Conference in Portland, Oregon.

Current acoustic tests are only effective for detecting sound and vibration in metal pipes, Chatzigeorgiou says; plastic pipes tend to dissipate the sounds too quickly. Such systems are also time-consuming and require expert operators, he says, whereas the small robotic device he and his collaborators have developed can move as fast as 3 mph through pipes, and are almost entirely automated. Ultimately, he says, such devices could be put into a system of pipes and left in place indefinitely, conducting automatic, nonstop monitoring of the system.

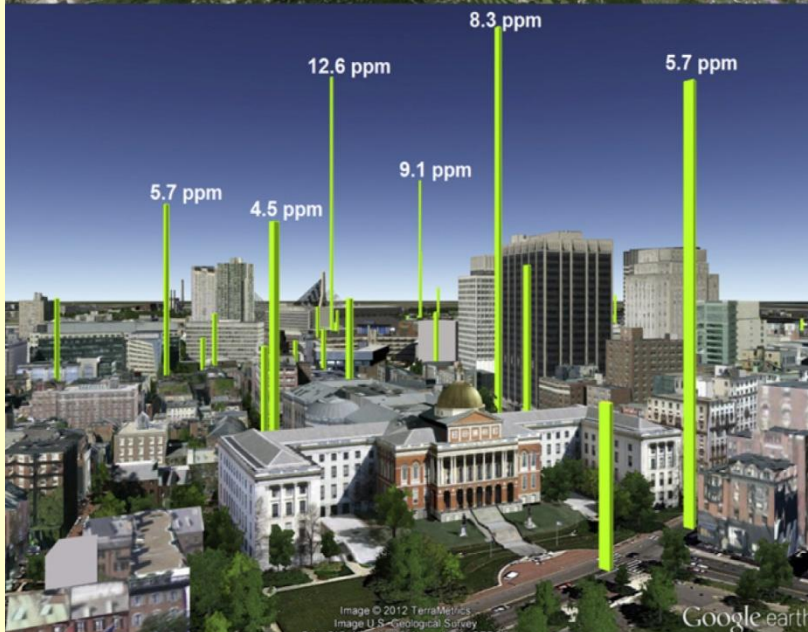
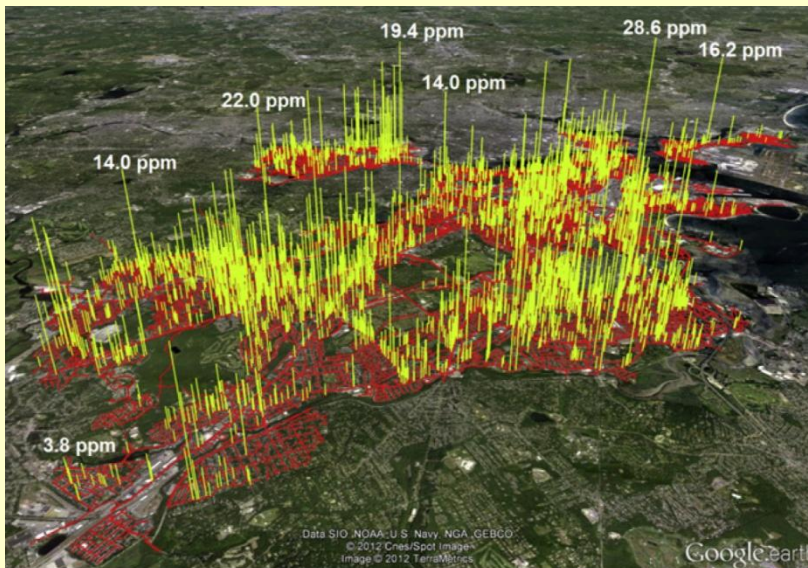
In addition to their potential for dangerous explosions, leaking gas pipes can be a significant contributor to global warming: Methane, the primary constituent of natural gas, is a greenhouse gas twenty-five times more potent than carbon



dioxide. Leaks in water pipes can waste up to half the water in a system; oil-pipeline leaks can lead to toxic spills and prolonged, expensive cleanup operations. All of these

small leaks that often go undetected for long periods of time.”

The current device consists of two parts: a small robot, with wheels to propel it through



pipes (or, in some cases, to simply be swept along by flowing liquid), and a drum-like membrane that forms a seal across the width of the pipe. When a leak is encountered, liquid flowing toward it distorts the membrane, pulling it slightly toward the leak site. That distortion can be detected by force-resistive sensors via a carefully designed mechanical system (similar to the sensors used in computer trackpads), and the information sent back via wireless communications.

Detecting leaks by sensing a pressure gradient close to leak openings is a novel idea, Chatzigeorgiou says, and key to the effectiveness of this method: This approach can sense a rapid change in pressure close to the leak itself, providing pinpoint accuracy in locating leaks. It also allows for relatively rapid monitoring of large systems: **At present, the 3 mph top speed of the device is imposed by the propulsion motors, not the detector itself, so faster surveying is possible.**

Boston’s street-level gas leaks

systems could benefit significantly from improved leak-detection methods, Chatzigeorgiou says.

While existing detection systems work under certain conditions, Chatzigeorgiou says, there is not yet an approach that can efficiently detect leaks in any of these pipe systems. “We believe this can solve the general problem,” he says: The new device could be produced in various sizes to fit different kinds of pipes, and should be effective in gas, water, and oil pipes. MIT mechanical engineering professor Kamal Youcef-Toumi, a co-author of the research papers, adds, “This technology allows for an unambiguous and reliable sensing of very

Because of the sensitivity of the membrane, Chatzigeorgiou and his colleagues believe the system can detect leaks one-tenth to one-twentieth the size of those that can be detected by most of the existing methods. At present, the system requires a fairly uniform pipe diameter, but the researchers are working on a version that will have more flexibility to deal with variations caused by damage, obstacles, or scale buildup inside pipes.

Co-author Rached Ben-Mansour, a professor of mechanical engineering at KFUPM, says that current leak-detection systems are quite expensive, typically costing \$250,000 annually to monitor 100 kilometers of pipe. “We’re hoping this system will be much more



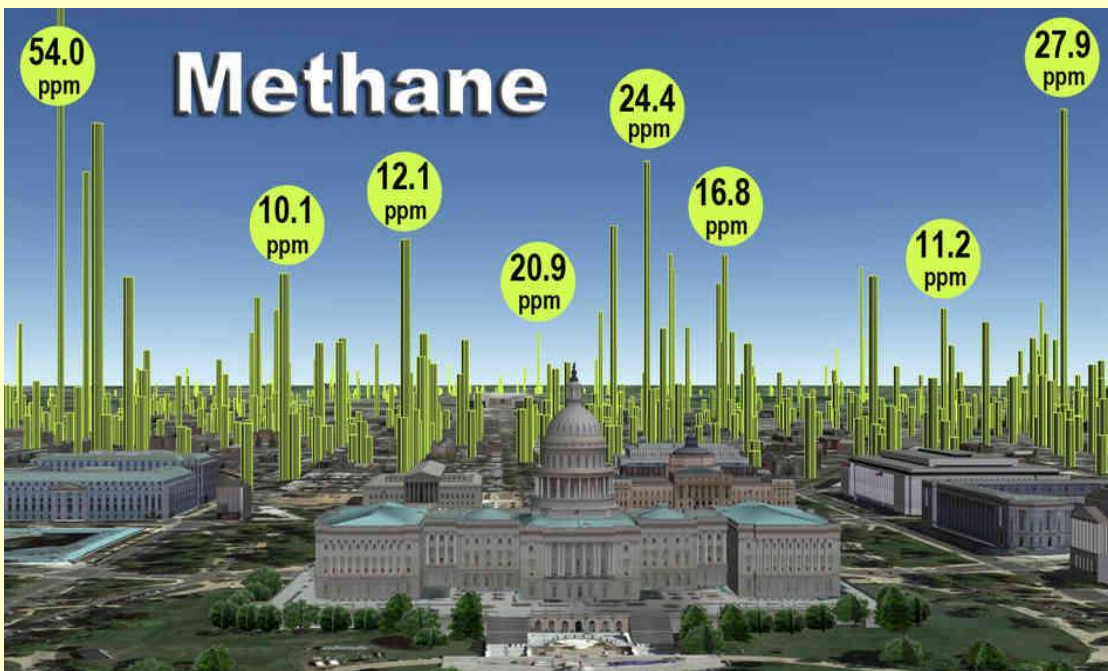
affordable,” he says, as well as faster and more sensitive.

Arnold Scott, vice chairman and director of First Commons Bank, who was not involved in this research but mentored the group in the MIT \$100K Entrepreneurship Competition, says this approach “is very important because of its size. It is the only [inspection device] small enough to fit inside of a 4-inch pipe.

Many modern water systems are built using 4-inch pipe, so being able to inspect this pipe diameter is very important. Another important element is the reporting mechanism. Using GPS, this [device] can specifically locate and report the location of a leak in a pipe.”

The research was supported by KFUPM through the Center for Clean Water and Energy at MIT.

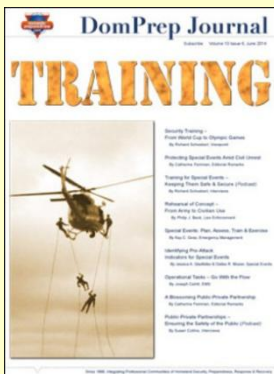
— Read more in Dimitrios Chatzigeorgiou, “Design of a Novel In-Pipe Reliable Leak Detector,” *IEEE/ASME Transactions on Mechatronics*, no. 99 (25 March 2014)



EDITOR’S COMMENT: Observing the photos from Boston or around US Capitol (DC), I wonder if someone has calculated this factor in case of a bomb detonation in urban environment. Can the already sub-explosive environment enhance the explosive effects and expand them to bigger distances than usual? Just a thought!

DomPrep Journal

Source: http://www.domesticpreparedness.com/DomPrep_Journal/



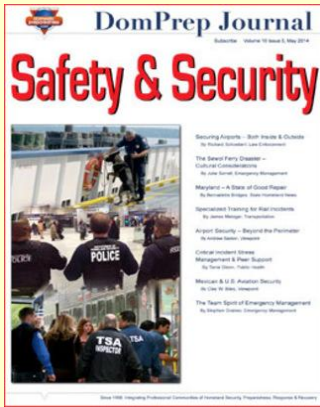
TRAINING

Wednesday, June 25, 2014

Featured in this issue: Security Training - From World Cup to Olympic Games, By Richard Schoeberl; Protecting Special Events Amid Civil Unrest, By Catherine Feinman; Training for Special Events - Keeping Them Safe & Secure, Richard Schoeberl; Rehearsal of Concept - From Army to Civilian Use, By Philip J. Beck; Special Events: Plan, Assess, Train & Exercise, By Kay C. Goss; Identifying Pre-Attack Indicators for Special Events, By Jessica A. Gladfelter & Dallas R. Mosier; Operational Tasks - Go With the Flow, By Joseph Cahill; A Blossoming Public-Private Partnership, By Catherine Feinman; and Public-Private

Partnerships - Ensuring the Safety of the Public, By Susan Collins





Safety & Security

Wednesday, May 28, 2014

Featured in this issue: Securing Airports - Both Inside & Outside, By Richard Schoeberl; The Sewol Ferry Disaster - Cultural Considerations, By Julie Sorrell; Specialized Training for Rail Incidents, By James Metzger; Maryland - A State of Good Repair, By Bernadette Bridges; Airport Security - Beyond the Perimeter, By Andrew Saxton; Critical Incident Stress Management & Peer Support, By Tania Glenn; Mexican & U.S. Aviation Security, By Clay W. Biles; and The Team Spirit of Emergency Management, By Stephen Grainer



UNTHINKABLE

Wednesday, April 30, 2014

Featured in this issue: The "Day After Disaster" - Revisited, By Craig DeAtley; Preparing for the Unthinkable, By Catherine Feinman; Nuclear Preparedness - Is the United States Ready?, By Craig DeAtley; Lessons Learned - Nuclear Devices & Nuclear Threats, By Stuart Cameron; The Emerging Nuclear Threat Environment, By Vayl Oxford; Nuclear Weapons - A Growing Security Threat, By Richard Schoeberl; The Dirty Details About Explosive Devices, By Courtney Gavitt; Radiological Detection - A Strategy for Changing Public Opinion, By Joseph Trindal; Civil Support Teams 101 - Removing Misconceptions, By Gordon Hunter; Illinois - Lessons From a Radiological Incident Exercise, By Curtis Hawk & Shay Simmons; and Death - Breaking the Bad News, By Joseph Cahill



EXTREMES

Wednesday, March 26, 2014

Featured in this issue: Natural Disasters: Challenges & Opportunities, By Stephen Grainer; Preparing for Extreme Weather Events, By Kay C. Goss; California - A Growing Response to Persistent Drought, By Mark Ghilarducci; Rising Waters & Tough Decisions, By Maggie Davis; Ten Winter Issues Every City Should Address, By Kim Fuller & Crystal Kline; Preparedness & Progress for Emerging Pathogenic Threats, By Robert C. Hutchinson; Preparing for the U.S. Tsunami Threat, By Christa Rabenold; Alaska - Building a Firm Foundation on Shaky Ground, By John W. Madden; Opioids - Overdoses & Antidotes, By Joseph Cahill; and Support to Local Authorities - Special Report, H. Steven Blum

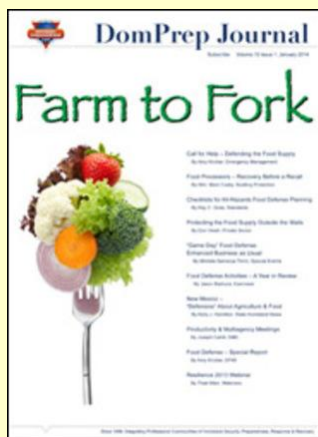


Connections

Wednesday, February 26, 2014

Featured in this issue: The Operational Imperative of Cybersecurity & Resilience, By Tom Ridge; Cyber Grand Strategies: Technology vs. Human Interaction, By Bonnie Butlin; The Real NCIS: An Interview With Thomas Betro, By Aaron Sean Poynton; Fusion Centers & the Public Health Advantage, By Raphael M. Barishansky & Seth J. Komansky; CHEMPACK 2.0: A Policy Roadmap, By Timothy Stephens; Preparing the Next Generation for War on the Virtual Battlefield, By Rodrigo (Roddy) Moscoso; Information Systems - Advancing Capabilities & Increasing Risks, By Craig DeAtley; Bridging the Medical Ladders, By Joseph Cahill; Virginia - Using Social Media the Right Way, By Tanya Ferraro; and Exercise Extent-of-Play Agreements, By Ken Lerner & George Yantosik





Farm to Fork

Wednesday, January 29, 2014

Featured in this issue: Call for Help - Defending the Food Supply, By Amy Kircher; Food Processors - Recovery Before a Recall, By Wm. Mark Cosby; Checklists for All-Hazards Food Defense Planning, By Kay C. Goss; Protecting the Food Supply Outside the Walls, By Don Hsieh; "Game Day" Food Defense: Enhanced Business as Usual, By Michèle Samarya-Timm; Food Defense Activities - A Year in Review, By Jason Bashura; New Mexico - "Defensive" About Agriculture & Food, By Kelly J. Hamilton; Productivity & Multiagency Meetings, By Joseph Cahill; Food Defense - Special Report, By Amy Kircher; and Resilience 2013 Webinar, By Thad Allen

► Download 2014 issues from source's URL.

Lesson Learned from Hurricane Sandy: Why Off-Grid Alternative Power Is Better

By LTC Robert L. Domenici (USA, Ret.)

Source: <http://strategicri.com/newsAndPress/lesson-learned-hurricane-sandy-why-grid-alternative-power-better>



Fossil fuel generators are not the best solution to the problem of power outages during disasters like Hurricane Sandy. Because they require resupply, these generators increase the burden on emergency managers. That's why responders are choosing off-grid power systems from SRI/ZeroBase.

Hurricane Sandy was a disaster of epic proportions for parts of New York, New Jersey, and Connecticut. Homes and buildings were destroyed. Thousands of lives were affected. High winds, heavy rains, and flooding were just the start of the region's problems. The damage to critical infrastructure, including the power grid, hampered the rescue efforts of first responders. Power outages also hindered the efforts of emergency managers who sought to start and then sustain the recovery.

The experience of Hurricane Sandy demonstrates the importance of emergency power during and after natural disasters. Emergency managers and first responders also need safe, reliable power sources in the event of man-made disasters such as a terrorist attack.

For a region that remembers the destruction of the World Trade Center on 9/11, the potential for both types of incidents isn't an abstraction. It's part of recent history.

The Limitations of Generators

Traditionally, fossil fuel generators have been used to provide emergency power. These devices are useful, of course, but only when there's an initial fuel supply on-hand. Moreover, generators may require supply lines during times of extended crisis. In turn, this



can create a logical support nightmare. Delivering fuel across a widespread area can take hundreds of hours. There are also equipment requirements such as fuel trucks and delivery systems to consider. Pumping the fuel itself may also present a problem. Unless gas stations can provide their own power, fossil fuels may remain trapped in underground storage tanks. During Hurricanes Sandy and Katrina, emergency managers faced this very problem. There's also an opportunity cost with generator resupply. Instead of delivering food, water, and other essentials to people in need, a limited number of responders must focus some of their efforts on supplying generators.

Three Goals and Over 100 Examples

It's time to end our dependence on resource-intensive generators during times of crisis. That's why Strategic Response Initiatives (SRI) and ZeroBase have developed and are now deploying hybrid systems that meet three goals.

1. Completely eliminate the need for fossil fuels whenever possible.
2. Otherwise, dramatically reduce fuel demand by connecting generators to SRI/ZeroBase hybrid systems that automatically start and stop generators in case of significant draw.
3. During normal operations, use these hybrid systems to send unused power back to the grid.

To date, SRI and ZeroBase have deployed over 100 new systems under the U.S. Army Rapid Acquisition program. Together, our companies provide systems that can produce from 1 KW to over 2 MW of clean, steady, sign wave power. By contrast, generators produce inconsistent sign wave power that can, and often does, reduce the operational lifespan of the equipment being powered.

Today and Tomorrow

In conclusion, SRI/ZeroBase systems can:

1. Support rapid deployment during and after times of crisis
2. Eliminate or reduce the need for fossil fuels
3. Extend the operational period of generators from hours to days.
4. Produce clean power in the range of 1 KW to 2 MW
5. Help extend the life of equipment by avoiding inconsistent sign wave power
6. Provide additional power to the grid during day-to-day operations
7. Reduce maintenance costs because, unlike traditional generators, SRI/ZeroBase hybrid systems do not have moving parts

In the near future, SRI/ZeroBase will seek to establish a manufacturing facility in New York State's Capital Region and begin to produce military units and a much-lighter civilian system. Together, our companies will replace generators whenever possible, and supplement power generation and energy storage to help support recovery from catastrophic events such as Hurricane Sandy.

LTC Robert L. Domenici (USA Ret.) is the founder and managing partner of Strategic Response Initiatives (SRI), a VA-verified Service-Disabled Veteran-Owned Small Business (SDVOSB) located in Schenectady, New York.

U.S. Northwest prepares for the Big One

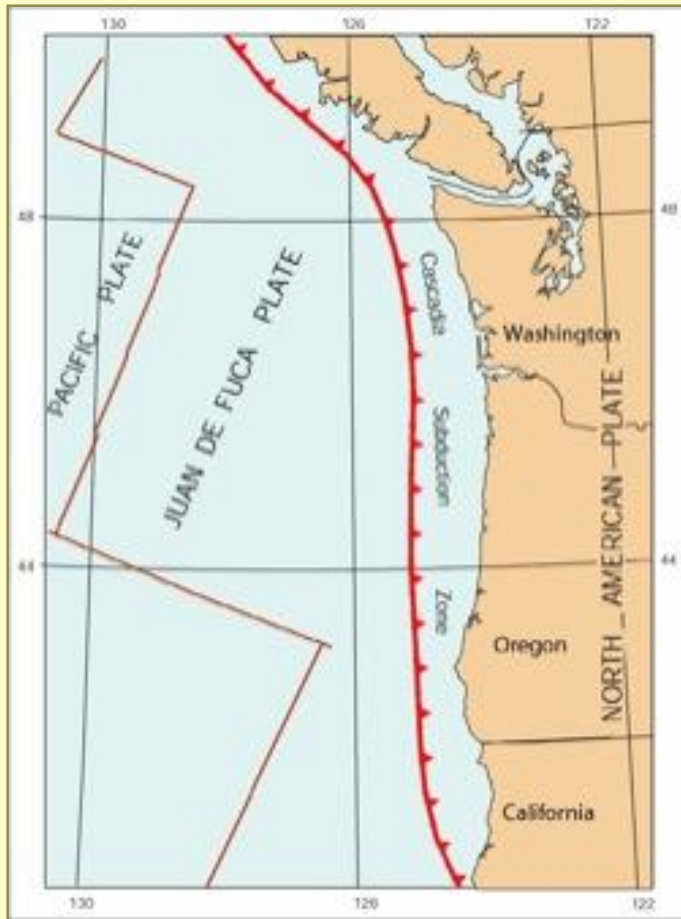
Source: <http://www.homelandsecuritynewswire.com/dr20140701-u-s-northwest-prepares-for-the-big-one>

Seismologists believe the Pacific Northwest is overdue for an earthquake that could register at over 8.0 on the Richter scale, leading many emergency management professionals in the region to anticipate and prepare for the devastating impact such an event would have on the local economy and quality of life. Last month, engineers, emergency managers, and public officials from across the region met at Centralia College as part of the Construction and Best Practices Summit hosted by the

college and the Pacific Northwest Center of Excellence for Clean Energy. The second day of the summit focused on how best to prepare for and recover from an earthquake along the Cascadia Subduction Zone, a 1,000-kilometer fault stretching from Vancouver Island to Cape Mendocino, California.

The *Chronicle* reports that that Matt Cutts, critical infrastructure program manager at the U.S. Army Corps of Engineers'





things are so tightly wrapped together, it's like a Gordian knot."

In the aftermath of an earthquake, aging buildings are likely to collapse, causing hundreds of deaths. Many roads would become impassable, and many businesses throughout the Pacific Northwest would cease to offer services for some time. "If we had this happen tomorrow, we'd be looking at thousands of people dead. You're also talking about months of recovery," Cutts said. "We really need to increase the public awareness of the possibilities. Emergency managers are always thinking about what could happen, but Joe Taxpayer doesn't spend a lot of time thinking about it."

Oregon Emergency Management director David Stuckey used the 2011 Japan earthquake and tsunami to signify the importance of educating the public. "Right after the 2011 Tohoku earthquake, I got a call from a commissioner on one of the coastal counties," Stuckey said. "There were people running to the

Portland District, discussed what he termed as the **Triple 3 Resilience Target — a goal of managing the aftermath of an earthquake to have emergency services running within three days, level of services to sustain the economy within three weeks, and a target of three years to stabilize the economy and prepare for future disasters.**

"We have such an interdependent nature to our infrastructure," Cutts said. "After an earthquake, roads are going to be down — but we need fuel and electricity as well. Those

beach with surfboards.... We have to create a broader perspective on how to educate people."

Efforts to retrofit buildings and critical infrastructure across the region have been made but emergency managers insist that the major focus now is how to restore critical infrastructure and the economy after a large earthquake. "If we can achieve the Triple 3 Resilience Target, we end up with a manageable disaster instead of a catastrophe that would take us months or even years to recover from," Cutts said.

Should States Take the Lead on Implementing Alert Systems?

By Justine Brown

Source: <http://www.emergencymgmt.com/safety/Should-States-Lead-Implementing-Alert-Systems.html>

As technology becomes cheaper, more sophisticated and easier to use, states have more options available to improve their public warning capabilities and integration with FEMA's Integrated Public Alert and Warning System (IPAWS). Some states are choosing to implement statewide systems while others are giving localities the lead and providing

statewide oversight and support. Iowa is one state that is pushing for a statewide alert system. The state previously left the deployment of alert systems to each county. But based on the results of a survey it conducted — which found that just 53 of the state's 99 counties had a public alert system



and that those counties were spending about \$600,000 a year on those systems — the state decided to investigate other approaches. In January 2013, the Iowa Homeland Security and Emergency Management Department (HSEMD) issued an RFI to investigate the feasibility of developing a statewide alert



system.

“We asked vendors what a statewide alert system might look like and cost,” said John Benson, spokesperson for the Iowa HSEMD. “Based on the responses, we recognized that if we did it right, we’d be able to provide statewide coverage for less than what those 53 counties were paying.” He said it would be a cost savings for those who were already paying and provide a new tool to the 46 counties that didn’t have a system.

Soon after, legislation was introduced supporting the implementation of a statewide system and requesting funds to support it. The request for funding was secured through the General Assembly this year. The Iowa HSEMD then issued an RFP, which was under review at press time. Once a vendor is selected, plans were to begin implementation July 1.

Benson said Iowa’s new alert system likely won’t be used on a statewide level, but decisions to alert residents would be made by local law enforcement and emergency management agencies.

“It’s basically a statewide system that retains its local control. It will be a statewide system, but the state will probably be the most limited user of it,” Benson said. “Our goal is to give local folks a tool to use and they would determine how and when to use it to send an alert for whatever emergency situations they have.”

The new system, which will be a Web-based SaaS application, will provide users a single Web page on which they can quickly compose a message and determine how they would like it delivered (text, email, voice mail, etc.). The system will also integrate with IPAWS and will include a special-needs advisory so someone with a mobility impairment can easily alert first responders of the need for assistance.

Local Control

Minnesota is taking a slightly different approach to its emergency alert system plans. Rather than implement a statewide system, the Minnesota Homeland Security and Emergency Management (HSEM) agency has asked counties to implement their own IPAWS compatible systems and is providing oversight and guidance from a statewide level.

“In 2010 we looked at doing a statewide system — what it would cost, what each county would gain from it, and where the funding would come from,” said John Dooley, communications and warning officer of Minnesota HSEM. “Third-party software just wasn’t sophisticated or available enough yet for us to pursue a statewide system.”

Minnesota HSEM then conducted a survey of public safety answering points (PSAPs) and decided to leave it up to the counties to determine and implement alert systems that would integrate with IPAWS (access to IPAWS is free; however, to send a message using IPAWS, an organization must procure its own software that’s compatible with the system).

“We thought, because pretty much all disasters are local, we wanted to keep the concept of operation local as well,” Dooley said.

At the same time, Minnesota HSEM formed a statewide IPAWS committee. The committee provides the counties with guidance, best practices, and education on IPAWS and how to use it.

“From our surveys, we found the PSAPs really wanted their alert systems to be simple, because when they get a call in and they are dealing with a disaster where they have to alert the public, there is already a flurry of things going on,” said Dooley. “They wanted to be able to choose a system they were comfortable with, and we felt allowing them to make that decision and providing oversight and support from a statewide level would put us miles ahead.”



Seven out of Minnesota's 87 counties are active on IPAWS, and several others are in the process of securing software and working with FEMA to complete a memorandum of agreement.

Mix and Match in Ohio

In Ohio, local governments have the option of using parts of the statewide system to address their alerting needs. Michael Swaney, communications infrastructure specialist for the Ohio Department of Public Safety, said Amber Alert origination capability and the availability of equipment gave the Ohio State Emergency Communication Committee a means to specify how to do a system at the county level with state government oversight. Swaney said most of Ohio's equipment was replaced in 2003 when the Emergency Alert System (EAS) replaced the previous Emergency Broadcast System. Today, local governments can use parts of the statewide system as they see fit.

In Texas, the Department of Public Safety (DPS) deployed a major upgrade to the Texas Emergency Alert System statewide this May. The new system will serve as the core of the state's public alert and warning system, simultaneously activating the state EAS relay to radio, TV and cable systems across the state. The new system will be the state's primary interface with the IPAWS network, giving the department synchronized access to EAS and enabling IPAWS to generate wireless emergency alerts to the cellphone systems.

In Texas, the size and geographic diversity of the state pose numerous hurdles to conventional EAS capabilities. The upgraded system addresses these challenges by allowing Department of Public Safety officials to create and issue alerts to both the existing EAS system and the IPAWS system. The system will allow Texas DPS to send statewide alerts or target the messages to any number of the state's 254 counties.

"By replacing its older equipment ... Texas now has a more robust, efficient and reliable way to spread lifesaving warnings to its citizens about emergencies via all modes of digital technology," said Edward Czarnecki, senior director of strategic development and global government affairs for Monroe Electronics, which provided the system.

Czarnecki added that because Texas DPS chose a standards-based approach, the system also sets the foundation for interoperability with future systems the department may consider.

Technology Tools

Benson said the technology has advanced by leaps in recent months, increasing its viability as a lifesaver.

"When you look back over the last 18 months, you can see a huge evolution in technology in terms of how it can be employed for mass notification and emergency alerts," Benson said. "With that has come recognition that this is something as emergency managers we really need to be leveraging."

Benson added that the system Iowa plans to deploy can also be used to more effectively manage and alert first responders. It can generate lists and first responders can designate which number should be called to summon them immediately in an emergency.

"You can set up a call list for a specific group of first responders so you can reach out and touch them all very quickly instead of doing the old call tree method," explained Benson. "It's another way to marshal your response force more effectively because it doesn't require human intervention."

Overall, Benson believes more states will choose to deploy statewide alert systems in the future.

"We are starting to see a lot of states lean this direction," he said. "With a statewide system, you have unified technology being utilized across the state, and that's always good in terms of being able to back people up. But there is also the cost that goes along with that, because generally the more you buy, the cheaper it gets. So when you talk about covering an entire state, a lot of times the cost savings really get your attention."

Several states are pressing forward with other types of early warning systems as well. For example, California is working on a statewide earthquake early warning system, though there is debate about how the system should operate and whether it will be strictly free or whether a more advanced, paid system will be incorporated.



Technology Plays an Increasing Role in Emergency Management

By Eric Holdeman

Source: <http://www.emergencymgmt.com/training/Technology-Increasing-Role-Emergency-Management.html>



Technology is at the heart of many emergency operations centers. In this image, the San Antonio and Bexar County, Texas, EOC bustles with activity in anticipation of Hurricane Ike in September 2008. *Jocelyn Augustino/FEMA*

99

Technology is beginning to dominate many aspects of the emergency management profession. This is particularly evident during disaster response. Today we have a number of large technology companies that offer their software or services for larger scale disasters. Chief technology officer for Microsoft Disaster Response, Tony Surma, answered questions about technology's use in emergency management.

Surma is responsible for the worldwide team and program at Microsoft focused on delivering technologies and technical assistance to communities, responders and customers both in response to natural disasters and in support of proactive resiliency efforts. He has been a part of the Microsoft Disaster Response team from the start — first as a volunteer global coordinator for solutions builds and deployments in time of disaster response and, more recently, as the lead for the program. Between response efforts, his focus is on building proactive partnerships and cross-organization initiatives, such as Humanitarian Toolbox, to operationalize innovations for use during response and leverage trends in technology and solution development to the benefit of response organizations and community readiness.

Surma answered the following questions in writing.

Where do you see technology being used today to advance the different missions of the emergency management community?

The role of technology in emergency management is to connect, inform and ultimately save the lives of those impacted by disasters. Technology restores connectivity to impacted areas so that governments can communicate with citizens and people can find their loved ones. Technology enables

responders to coordinate rescue missions and work efficiently from the minute they arrive in a disaster zone, and helps businesses recover so communities can begin to rebuild faster. Lastly, after and in between incidents, technology helps us analyze, track and study natural disasters so that we can always be learning and developing better solutions — and prepare to save more lives.



How is the cloud impacting emergency management?

The cloud has been transformational for preparation and management of disaster responses. Disasters can knock out or overload local infrastructure, making access to data and communication systems nearly impossible. The cloud works around this challenge because data is stored and kept accessible far from the disaster zone. The cloud can also be quickly scaled depending on traffic and volume, so local agencies' online presence after a disaster is secure from outages. For example, we help nonprofits and local agencies use the Microsoft cloud, Azure, with our ReadyReach portal solution, which allows sharing logistics quickly and broadcasting information to citizens, as well as informing those outside the disaster zone about ways they can help.

How is Microsoft trying to be proactive versus reactive when it comes to disasters?

The way we respond after a natural disaster is crucial, whether within the first few minutes or the months of rebuilding that follow. However, Microsoft Disaster Response emphasizes that the best disaster response begins before a disaster happens. As part of disaster preparedness, we are always learning from past experiences, building on solutions that worked and growing our network of partnerships so that all of these give responders what they need when disasters happen.

There is the concept of What's In My Back Yard (WIMBY)? Explain that concept and how it works with disasters and emergency management.

Rather than viewing disaster response as everyone trying to individually have 100 percent of what they need ready to go for themselves, we should think of WIMBY as preparation built from neighbors helping neighbors, sharing resources and being empowered to be first responders for each other. Emphasizing community is a key way to scale disaster response and preparedness to a backyard level, and communities should work together with emergency managers to jointly build resiliency before disaster strikes.

What solutions are out there today to obtain information faster and distribute it to the

correct people and organizations at the right point in time?

This reminds me of a really powerful statement made by the Red Cross in its World Disasters Report: When disaster strikes, access to information is "just as important as food and water" and is an increasing critical need.

The best examples of Microsoft getting solutions out there to fulfill critical needs are the times we have partnered with others to bring a solution that directly addresses the challenge. Let me give you a few examples: Microsoft was one of the partnering entities with the government of Luxembourg to develop emergency.lu, a satellite that can be rapidly deployed to a disaster zone within hours in order to bring high-quality Internet connectivity and low-bandwidth versions of Skype and Lync to areas where regular Internet connections have been downed. This satellite has been used successfully during Typhoon Haiyan, as well as by the World Food Programme in humanitarian situations such as the food crises in Sudan and Mali.

We were also involved with the deployment of another innovative connectivity solution during Typhoon Haiyan: TV White Space. We partnered with the Philippines government to leverage unused television channels, known as TV White Space, to enable connectivity in areas that lost Internet. Using TV White Space, Microsoft was able to provide Skype capabilities to the government and nongovernment agencies coordinating relief efforts, and citizens impacted by the Typhoon were able to use TV White Space Skype access to reunite with loved ones.

What role do you see big data playing in the future in regard to emergencies and disasters?

As greater volumes of data are generated and gathered during disaster response efforts, there is greater opportunity for research, analysis and visionary ways to build upon key lessons learned. As we are increasingly able to collect and extract more detailed assessments, we can proactively act before the next disaster. Working with our industry partners to build effective and collaborative ways to mine data, including social media, both during disasters and afterward is an important focus for us.



There are silos of data that are not being shared across the disaster enterprise today, because the right hand doesn't know what the left is doing in trying to help. What solutions do you see out there now that can help?

To us, it's about asking, "What role can technology play in improving logistics?" not asking "What role can Microsoft play?" When it comes to logistics, there needs to be a free flow of data during disaster response so that all people can access the information and play a part. We are talking about reconnecting loved ones, getting clean water where it needs to be, directing people to safety, and other tasks that transcend ownership. This is not an area to be competitive or closed to other organizations and businesses, which is why all of Microsoft's efforts involve building partnerships and sharing data, infrastructure and resources.

What is the future for information management during disaster response?

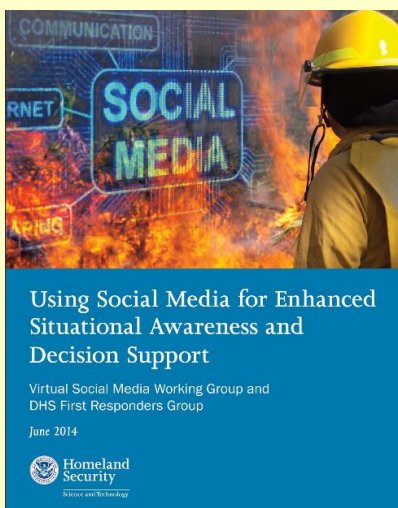
With the progressive, real-time open sharing of data during disasters, we expect to see a shift and rewiring of how disaster response is managed. Today we have phone calls, situation reports that come a day later, and a variety of data sources we rely upon to make critical decisions. An analogy I often use is the stock market. Think about an old-world model where you found out a stock's price a day later in the newspaper compared to today's integrated, immediate access that delivers the data needed to make important decisions nearly simultaneously to all involved. I see the future of disaster response similarly, that there will be a transformation in the way agencies exchange critical data in an open and real-time manner and make it available to people whose livelihood — and lives — rely upon it.

Eric Holdeman is a contributing writer for Emergency Management and is the former director of the King County, Wash., Office of Emergency Management.

NEW REPORT – Using Social Media for Enhanced Situational Awareness and Decision Support

By Brandon Greenberg

Source: http://www.disasternet.co/blog/2014/7/1/using-social-media-for-enhanced-situational-awareness-and-decision-support-new-report?utm_content=buffer7f622&utm_medium=social&utm_source=linkedin.com&utm_campaign=buffer



After a long effort by the DHS Virtual Social Media Working Group (VSMWG), the report *Using Social Media for Enhanced Situational Awareness and Decision Support* was just released on Tuesday. I was very happy to be a part of developing this report among many other talented people.

“The report introduces ways social media platforms can be used for situational awareness in public safety. It addresses various challenges associated with the use of social media for situational awareness, the integration of social media within the operational environment, and identifies areas requiring further consideration, research, and development.”

The report also discusses issues that extend well beyond social media. The report highlights many of the issues we face related to disaster information management as a whole. If you have questions about big data, social data, data interoperability, this report is your primer.

“[The report] also identifies critical areas requiring further consideration and research to address key technology, process, and policy gaps, including:”

- **Information Application:** *The ability to access, share, search, verify, contextualize, and manage available information. This concept also includes the identification of essential elements of information in social media as they relate to traditional public safety information requirements.*



- **Privacy, Legal, and Security Challenges:** There are several challenges associated with the use of social media for situational awareness, especially with regards to user privacy and the use of personally identifiable information (PII); the need to remove details when sharing information across multiple partners; and the security of networks, platforms, tools, and data.
- **Data and Open Standards:** To truly enhance situational awareness, social media must be integrated, both technically and contextually, within the larger information environment and into the public safety operational workflow. Additional considerations include event detection, data formats, data models, ontologies, semantic and linked data, automation, and artificial intelligence.
- **Technology Development:** Challenges associated with the use of third-party platforms, analytics tools, the development of operational requirements, the ability to geo-locate information published to social media, spatial-temporal characteristics (disparate and virtual communities, time decay of posts, etc.), and integration with NextGen911 will require further research. "

The DHS VSMWG also published a great report in May 2013: Lessons Learned: Social Media and Hurricane Sandy. This group is doing great things and trying to push the ball forward with social media and technology.

► **Read the report at:**

<http://www.firstresponder.gov/TechnologyDocuments/Using%20Social%20Media%20for%20Enhanced%20Situational%20Awareness%20and%20Decision%20Support.pdf>

Brandon Greenberg is a PhD student @GWEngineering | MPA from @NYUWagner | Researching & working btw Policy, Mgmt and Tech for Disaster

Health-Care System Needs to Prepare for Global Warming

Source: <http://www.emergencymgmt.com/health/Health-Care-System-Prepare-Global-Warming.html>

Climate change is happening, and with that will come more deaths from heat-related illness and disease, according to a report released Tuesday. The report, spearheaded and funded by investor and philanthropist Thomas Steyer, former Treasury Secretary Hank Paulson, and former New York Mayor Michael Bloomberg, examines many of the effects of climate change for business and individuals.

"One of the most striking findings in our analysis is that increasing heat and humidity in some parts of the country could lead to outside conditions that are literally unbearable to humans, who must maintain a skin temperature below 95°F in order to effectively cool down and avoid fatal heat stroke," the report's authors wrote. They use a "Humid Heat Stroke Index" that combines heat and humidity levels to measure how close they come to the point where the body is unable to cool its core temperature. So far the nation has never reached that level, "but if we continue on our current climate path, this will change, with residents in the eastern half of the U.S. experiencing 1 such day a year on average by century's end and nearly 13 such days per year into the next century."

Dr. Al Sommer, the dean emeritus of the Bloomberg School of Public Health at Johns Hopkins University in Baltimore, was on the committee that oversaw the development of the report. He says that often overlooked in the current debate about greenhouse gases and climate change is the effect of global warming on individuals and hospitals.

"There will be places that are heavily populated that will see four months in a row with 95 degree and over weather. You won't be able to let your kids play outside," he told KHN. "The average will be miserable. When your sweat can't evaporate, you have no way to moderate core body temperature, and some people will die. That's why you had 700 deaths in Chicago in a one week period in 1995. We're going to have a lot of those periods."

Sommer joined Lisa Gillespie and other Kaiser Health News reporters and editors in Washington to talk about the climate change report. Here is an edited transcript of his remarks.

What will the main health issues be as parts of the country get dangerously hot and humid, and others lose



coast line and experience drought?

The bottom line is that it's going to get more hot and humid in some areas ... you've got the South, the East Coast and Atlantic states, and the problem with hot and humid is that you can't control body temperature, because when it gets hot, you sweat, and when it evaporates, it cools the skin. But when it hits 95 or 102, and the humidity is such that you can't evaporate sweat, it just stays there, there is no way to cool the body temperature. You can bundle up against the cold, you can wrap up more blankets and you buy some down sleeping bags in freezing weather. But in heat, you can take off more clothes, but you're still stuck at that heat point index.

What are the challenges with getting this message out?

The challenge is like every challenge in public health. If we're successful, nothing happens. If you say, "Something is going to happen," [the public's] response will be "You know, who knows? I'm worried about my mortgage," and the average CEO is worried about making quarterly profits, so they don't care. Getting people to be concerned about the future is tough.

The person who is wealthy and can afford air conditioning doesn't have much to worry about. You'll have the deniers, and you can't talk to them, and then the people who just don't want to worry about it.

What challenges will health care systems face?

You have to pay attention to something that will dramatically impact the health care system. You have to deal with the poor who live in places that are getting the hottest, and won't necessarily be able to move up to other places where it's not so hot. And the health care system is going to have a surge where it'll have to deal with the problems of excessive heat. But who's going to pay them and who's going to warehouse the 25 percent increase in respirators, pumps, nurses and doctors

because 40 years from now something is going to happen? Health care systems would be happy to prepare if someone paid for it.

What do you think the health care system can do right now?

The health care system as a whole, knowing how much it will cost, can begin to put pressure and engage in climate discussion because [climate change] will end up driving costs. The hospitals have to be prepared, some hospitals may go out of business because there will be places where no one is left alive. Miami? Who's going to live in Miami? The heat is rising, the water is rising ... who's going to move the [health care] personnel [to another less hot state]? Will North Dakota build bigger hospitals to take up the surge of people who are moving up there?

Hospitals need to be able to pick up the slack, and plan for what they will do, and talk to the payers to [be able] to increase their surge capacity. Forty years isn't far away if you think about a cycle of a hospital. Hopkins just opened two new centers, and it took 25 years. They will have to start now.

Are there any benchmarks the health care industry can watch out for to know if there is enough being done to stop or slow climate change so that these health care crisis strategies will not be needed?

What would be terrific is if medical CEOs get into a discussion about this. I'm sure they've talked about pandemic flu, but I doubt they've talked about this. The fact that you can predict the amount of people who will show up in ER with heat stroke, [then] you can start assessing it. You guys and gals who run health care systems know what that will do. What would we really need? That's what this study is about -- to put data on the table at a granular level so people can begin to have informed discussions, which will lead to thoughtful ideas on how you respond and maybe lead to momentum.

► **Read more at:** <http://riskybusiness.org/report/overview/executive-summary>

Kaiser Health News is an editorially independent program of the Henry J. Kaiser Family Foundation, a nonprofit, nonpartisan health policy research and communication organization not affiliated with Kaiser Permanente.



Online Hurricane Evacuation Tool Helps with Decision-Making

Source: <http://www.emergencymgmt.com/training/Online-Hurricane-Evacuation-Tool-Helps-with-Decision-Making.html>

If you need help deciding whether to evacuate for major hurricane, state officials want you to punch your address into a new online tool.

It will suggest the best routes out of town. It will also show you, based on the hurricane's strength, a dramatic computer simulation of what the storm might look and sound like in your neighborhood.



Imagine whistling wind, cracking thunder, flashes of lighting, flying shingles, uprooted trees, flooded streets and, if the hurricane is bad enough, water pouring through holes in the roof.

Tropical Storm Arthur probably won't be strong enough for people to consider evacuation. The program is called the Hurricane Evacuation Encouragement Demonstrator, or HEED. Developers at the Virginia Modeling, Analysis and Simulation Center at Old Dominion University created it for the Virginia Department of Emergency Management.

"One of the big problems is the state can say, 'A hurricane is coming! A hurricane is coming!' and people don't leave," said Sol Sherfey, a project manager who helped develop the tool.

He said it's important to understand the videos don't reflect a weather prediction.

"We're not saying the video you're watching is what's going to happen to your house. It's meant to encourage people to leave."

► **Read more about HEED at:** <https://heed.vmasc.odu.edu/about.html>

Are Drones the Future of Firefighting?

Source: <http://www.emergencymgmt.com/disaster/Drones-Future-Firefighting.html>

In 2013, a California National Guard Predator



drone aided firefighting efforts during the Rim Fire. In this photo, an Army National Guard member throws a RQ-11 Raven drone during a field training exercise at the National Training Center in Fort Irwin, Calif. *Army National Guard/Spc. Grant Larson*

When it comes to analyzing dangerous wildfires, could a sensor attached to a drone ever replace a human eye connected to an intellect shaped by experience and intuition? That's one of the many questions federal wildland firefighting officials are asking as drones become increasingly popular in warfare and commerce.

The wildfire drone conversation comes on the heels of a national reminder about the human cost of firefighting after one of the deadliest seasons in recent memory. Nineteen firefighters died a year ago Monday at the Yarnell Hill Fire in Arizona. **In all last year, 38 firefighters were killed in the line of duty as fire burned 4.1 million acres and more than 1,000 homes.**

Drones with infrared capability could help where thick smoke keeps manned helicopters from gathering fire information. They also could keep people out of risky situations, provide real-time information to firefighters on the ground and alert officials when



conditions change or the fire jumps the line. While drones have been used in rare cases already, managers with the U.S. Bureau of Land Management and U.S. Forest Service say the headlines are ahead of technology and the agencies' comfort zone and pocketbooks.

"I think you are going to see them sooner than you think," said Rusty Warbis, flight operations manager at the BLM's National Aviation Office. "Right now it is procedures, policy and regulation that's really holding it up."

What's more, Warbis said, the BLM isn't quite sure how to incorporate drones into an already busy wildfire airspace without creating a hazard. More complex is the task of taking the drone's information and communicating it in a way helpful to planners and tacticians, he said.

Predator to the Rescue

Last year, a California National Guard Predator drone was dispatched to aid firefighters battling the Rim Fire, which burned 257,314 acres in the Sierra Nevada Mountains and Yosemite National Park.

The drone "proved particularly effective for perimeter and spot fire detection," says a report by Josh McDaniel of the Wildland Fire Lessons Learned Center. It was the first and most



significant launch of a drone in wildfire history and "could point the way to how these assets are used on future fires."

"Fire managers on the Rim Fire say that the (drones) also have potential application in a wide range of missions related to communication crew, safety and night ops," McDaniel wrote.

The drone picked up a critical spot fire that could have spread into a populated area. It also had the technology to identify the precise

latitude and longitude of such spot fires for an airdrop of water or retardant, he reported.

The drone could fly from one side of the fire to the other in about 15 minutes and could see more than two helicopters monitoring opposite ends of the blaze. It easily saw through light and dry smoke, but it was grounded when the Rim Fire experienced inversion, trapping smoke near the ground.

The drone was operated by a military crew completely unfamiliar with fire behavior, requiring a fire behavior specialist to gather and interpret the information.

A Range of Capacities

Other drones have been used since, including one from the University of Alaska Fairbanks that flew a "Scan Eagle" into the Funny River Fire on the Kenai Peninsula in May.

Recently, Oregon's Department of Forestry — which has its own firefighters — approved one forester's idea of using a much smaller drone. The state plans to equip a small, remote-controlled helicopter with video, infrared cameras and GPS systems at a cost of about \$5,000.

Firefighters hope to fly it into smoke-choked canyons when helicopters are unable, then share the information with firefighters and other agencies. In a decade, Warbis said, firefighters could be equipped with such small drones as regular field equipment.

The Oregon drone is only cleared to fly 400 feet above the ground and holds enough gas to run for 30 minutes. One Predator drone costs \$17 million, can stay in the sky 20 hours and operates at 18,000 feet altitude.

The Forest Service has "dabbled" in using drones while a committee of specialists works on a report examining their use in all of the agency's programs, not only wildfire, said Mike Ferris, spokesman for the fire aviation management division.

"We're not going to run out and buy something without understanding things like cost, storage, maintenance, deployment and training," he said. "There are so many components to taking on a program of that nature that you really have to turn it out first."

Warbis said the BLM is further along in its use of drones. It has 16 ongoing projects that employ two drone types for anything from



data collection on wildlife to aerial surveys and archaeology.

"Technology is getting way out ahead of us, and we're working to catch up with it," Ferris said.

Hot Costs

Warbis said he doubts the BLM will create its own firefighting drone division, instead contracting that work out with private groups that would respond to a la carte orders for services on specific fires.

"I may have 20 (drone types) on your shelf and go, 'Yes, I can fill that need with this (drone).' That keeps me from having to come up with pilots that are qualified to fly technology that's moving so fast that it is obsolete by the time I buy it. ... You'd have to put up a full-blown unit with the training and standardization and everything. And in this day and age of government budgets, it's going to be hard-pressed."



Indeed, wildland firefighting costs are a major issue these days. Many members of Congress released a joint statement Friday, reaffirming their support for sweeping changes in how firefighting is funded and placing more money in coffers for prevention.

McDaniel's report, however, notes the reduced hourly cost of the Predator drone, at \$770 an hour, compared with a Type 3 helicopter at \$3,500 an hour.

Human vs. Artificial

Drones could help in one of Idaho's most treacherous fire sites, the Salmon River Breaks, where helicopters often can't fly into smoke-filled canyons, said Randy Skelton, deputy fire staff officer for the Payette National Forest. In 2003, two firefighters were killed in

the Breaks, an area known for high and erratic winds and frequent lightning strikes.

"I'm all for advancing technology if it is going to help out," Skelton said "If you don't need to expose firefighters and pilots to that hazard, it'd definitely be worth exploring."

But Skelton said he's not ready to replace experienced human eyes with drone sensors. Drones may be useful to cheaply monitor fires that the Forest Service lets burn in accordance with management objectives, he said.

"It is just not as 3-D as you'd like it to be like seeing it in person," he said of infrared, video and other imagery captured from the air. "It is better intel than not seeing it at all. But a tactician being able to fly over the fire and being able to give you real time feedback (is better) versus trying to decipher what you are seeing on a camera or infrared image."

Warbis agreed that a drone would lack the intuition many experts rely on when seeing a fire from the air.

"With someone trying to make decisions from data through a drone, you are not in the scene," he said. "You are observing the scene, and there is a risk there. ... You get a sense, a full, overall picture and awareness. When you are looking at a screen, I think it would be too easy to sit back and not have as much of the picture as you might like."

Connectivity from those receiving the drone's data with command on the ground may be complicated, too, Ferris said.

"Do we tap into their iPads? ... If we are in the urban interface, there is pretty good connectivity. But once you get out into the central mountains of Idaho, well, good luck."

In the meantime, all fire officials interviewed agreed that the biggest concern about drones is not whether they'd be effective in fighting fires. Rather, they worry about private drones interfering with air attack operations.

The BLM and Forest Service issued a safety alert June 25 after a private citizen launched a DJI Phantom to film the Two Bulls Fire northwest of Bend, Ore. Warbis said the BLM is working hard to get the word out about the dangers private drones pose while meddling inside a fire's airspace.

"It's bad enough if you hit a bird. Think if you hit a 40-pound piece of metal — not going to be good," he said.



Lessons Learned from the Response to the Oso, Wash., Mudslide

By Jim McKay

Source: <http://www.emergencymgmt.com/disaster/Lessons-Learned-Response-Oso-Wash-Mudslide.html>

Thomas Richardson is a battalion chief for the Seattle Fire Department, and Washington Task Force 1 Urban Search and Rescue Task Force leader. He was recently deployed to the site of the massive



107

mudslide near Oso, Wash., on a recovery mission where at least 42 people were killed. He has previously been deployed to missions during Hurricane Katrina, 9/11 and the Oklahoma City bombings. He took time to discuss lessons learned from the mudslide. This interview has been edited for clarity and length.

Emergency Management: What did you see when you got to the scene?

Thomas Richardson: Eight hundred acres of landslide. The mountain had come down and had taken out a good chunk of [State Route] 530 and with the flooding had spread out more than a couple of miles because it had blocked the river and backed things up — a little bit of housing debris on the outskirts of it but really just a mountain, dirt, water and broken trees was what was visible.

EM: Did anything surprise you about what you saw?

TR: Honestly there were no surprises. We knew we were on a recovery mission. We were not deployed until Monday night and Tuesday morning [the mudslide occurred Saturday, March 22] and given the conditions — freezing rain and pretty bad conditions — we expected we were just going to be there for a recovery. I've been deployed to Oklahoma City, the World Trade Center and Hurricane Katrina, so it's not a big surprise.

EM: What were the difficulties in this effort compared to others?

TR: The main challenge was the scale of the site. Think about 9/11: That was around 16 acres and it took them more than six months to get to native soil, down to the foundation of the World Trade Center. They were dealing with a couple of 110-by-110-[story, 10 million]-



square-foot buildings; we were dealing with 800 acres. A vastly larger scale with a small number of people we were looking for.

It turned out that we were able to recover a little more than 95 percent of the remains — not too bad considering the problem.

EM: What do you take away from this effort?

TR: If you're ever going to search a landslide or an avalanche, search the leading edge. People were not found where they live. They were found half a mile-plus away from where their houses used to be. Apparently landslides tend to push people toward the leading edge.

The second thing would be to do really good documentations of your finds because you can put together a picture; once you've found enough, you can start creating trajectories. We ended up creating trajectories based on where people used to be and where they were found. That allowed us to focus our efforts on our search so that we weren't having to search the entire site and were being successful within a couple of weeks, where my original projection was, "We're going to be here for months to years if you really want us to dig out all the bodies, and it's going to cost a billion dollars." It didn't cost quite that much and didn't take that much time.

GPS is critical. Using devices where you can connect data points and put that together with bodies so that you have an understanding of where you're looking, where you need to look and you can plan your future searches. We incorporated volunteers as a base instruction from the local incident management team. That was, in part, because they couldn't keep them away, but in the end it was a really good thing. The volunteers were critical in the success of the mission.

There were hundreds of volunteers out there and many of them worked for CERTs [Community Emergency Response Teams]. They found and helped recover a significant number of the remains, and it was volunteers who brought in dump trucks and heavy equipment. Usually our task forces come in with relatively small hand tools to do a rescue of a structural collapse. We're not really set up to do a large 800-acre site search. We really needed the heavy equipment and that was provided by volunteers. Really a success story of this evolution was that we not only incorporated the civilians into our response but of the hundreds of civilians there was just one problem with one person who was posting stuff online and that was quickly resolved.

There are independent activities going on where firefighters prepare for disasters and civilians prepare for disasters, but rarely do we actually tie the civilians in with the training of the firefighters. We have CERTs in Seattle and around the state, but very frequently you'll find that firefighters are not expecting them to be a participant. Even in my department there's no master plan in our policy and operating guideline on how we're going to use CERTs. We need a better incorporation of them, officially, into our plans and so that we can, among other things, take the civilians and trust them not only with doing the work but with the intelligence.

We ultimately got trajectory maps, but people were really possessive of those maps and concerned that if they got released to the public what would be the political ramifications of a map showing body parts. We need to let go of that and recognize that there's a grim reality to a disaster and either people are going to face those realities and be a part of the recovery or we're going to exclude them. But I don't think it's appropriate to exclude them and therefore we need to incorporate them in our intelligence.

EM: Did it slow the response down to try to coordinate all the volunteers?

TR: Not at all. Mostly we ended up the recipient of volunteers and were told to use them, but they didn't really report to us. We need to do a better job of putting them officially in our briefings and including them in our overall plans so they understand.

As it was, I had to go tell people out in the field what they could have gotten in a briefing. You get a lot more buy-in if somebody understands: "We're finding all the bodies here. I know that Steelhead Drive used to be over there, but that's not where the people are and here's why we believe we're searching in the right place."

We were actually not supposed to release that information, but in the end you're either a responder or you're not, so we treated all responders the same. Just because you're a civilian doesn't mean you don't have the capability of dealing with exposure to traumatic events. Responders are just people who happen to have a job, and yes, we have some training but we're really not any more equipped to deal with that stuff than Joe Civilian.



We've dealt with it before, but we need to realize that if people are stepping up to the plate and they understand the difficulties of the mission, we have to just trust that they can be a part of it.

We also need to do a better job of incorporating modern technology into our responses. Specifically we need to start to see official applications coming out where a person can report needs and impacts of the disasters so it can be tabulated automatically whether the person is in need of power, food or water, or their house is destroyed. We can help people report that stuff, and with an app we could incorporate volunteers more efficiently by allowing people to volunteer their resources by saying, "I have an excavator or a shovel and a strong back or a house where I can provide shelter."

Then as emergency managers we can connect the dots between the needs and the capabilities. But right now we kind of exclude them and frequently, not in this case, but the government response is promising to take care of everything without the capabilities.

There were also many things that needed to be addressed by the incident management team. There was a road that needed to be addressed; upstream flooding; hazardous materials; debris and personal belongings; people were displaced. There were many things that needed to be addressed other than the missing victims, but they were never incorporated in the incident action plan. We need to do a better job of looking at the big picture and beyond just the first few victims. We relied on the volunteers. If we had waited on the incident command system to supply us all the resources, we would have been waiting a much longer time.

Jim McKay is the editor of Emergency Management. He lives in Orangevale, Calif., with his wife, Christie, daughter, Ellie, and son, Ronan. He relaxes by fly fishing on the Truckee River for big, wild trout.

Language Barrier Complicates Emergency Response Scenarios

By Sarah Hadley (Waterloo-Cedar Falls Courier)

Source: <http://www.emergencymgmt.com/safety/Language-Barrier-Complicates-Emergency-Response-Scenarios.html>

Emergency dispatchers and response teams are struggling with a widening language divide as they attempt to service Waterloo's growing population of non-English speakers.

The communication barrier creates problems for all parties involved, from the dispatcher deciphering a 911 call to the officer trying to put together an accurate police report to the concerned resident trying to communicate a problem with little to no knowledge of the English language.

Over recent years, Waterloo Police have dealt with a slew of languages including Bosnian, Spanish, Serbian, Croatian, Burmese, French and Vietnamese.

In 2006, Burmese refugees began settling in Waterloo for the employment opportunities at Tyson's meat plant, and the community has been growing ever since.

Dispatchers at the Black Hawk Consolidated Communications Center receive about a half-dozen calls a day in foreign languages.

But resources for interpretation are slim, a Courier investigation shows.

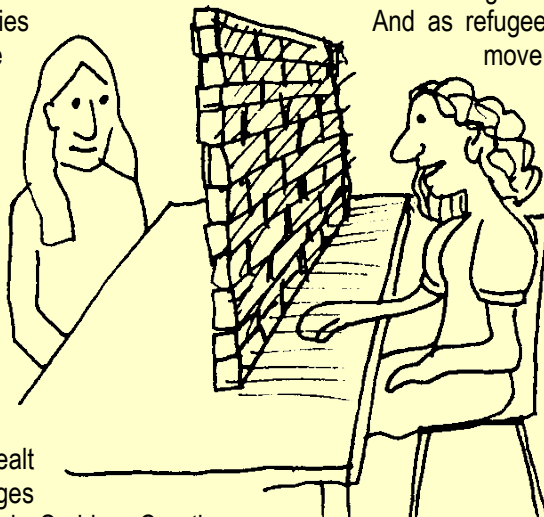
And as refugees from Burma continue to move to the area at a steady pace, bringing with them five vastly different languages, it has quickly become a complex problem to solve.

Nearly 1,500 Burmese refugees have planted roots in the Waterloo area, according to local estimates.

That population is expected to reach 2,000 in the next year.

In summer months, about two to four households migrate to the area each week.

Stephen Schmitz, who resettles new refugees through Catholic



Charities in Cedar Rapids, estimates that more than half of these incoming refugees are illiterate.

"It's a huge burden," said Waterloo Police Capt. Joe Leibold. "We just don't have the resources available to speak every language known to man."

A total of 14 different dialects are being used by Burmese refugees in this area. Often responders can tell someone is Burmese but are not able to determine which dialect they're speaking.

"For a mother to feel powerless to explain what's going on with her child is a scary, scary thing," said Ann Grove, case manager and site supervisor with the Cedar Valley Refugee Newcomer Services.

Interpreters can help, but law enforcement officials say they are hard to come by. Waterloo police have just two people they can call on to translate Burmese refugee languages.

One of them is Ivan Soe Myint, who recently began interpreting for the department. Soe Myint said he gets calls all the time to interpret on scene, often in the early morning hours.

But even interpreters don't know every dialect and are still developing their own knowledge of English.

"Sometimes we need an interpreter for the interpreter," Leibold said.

Black Hawk CCC has one dispatcher who is fluent in Spanish but no one who can speak Bosnian or languages of Burma.

Missing Details

Grove remembers one scenario from years ago in which a male client from Burma arrived at the police station after being assaulted.

"It was not handled adequately," she recalled.

A report of the crime was filed, but according to her, it lacked key information because officers didn't have the language capacity to do it properly.

In the case of an emergency, details can make all the difference.

For example, when dispatchers field a domestic abuse call, they are trained to seek answers to questions: where is the subject located, are there any weapons involved and is the attacker there currently. Judy Flores, director of Black Hawk CCC, said details are important with every call. They are intended to keep officers safe and help the paramedics know what equipment to bring in.

Usually, even those who can't speak English are able to say "police" and "help," she said.

But when that's all the detail dispatchers can prep responders with, it's problematic.

"Any time you don't get the details, you're kind of going blind into something," Flores said.

In that case, the emergency response process happens somewhat backwards. Responders arrive first, then attempt to grasp what the problem is.

That can be an issue for ambulance crews who rely on people to communicate any internal pain. Specifics like whether someone is experiencing a throbbing pain versus a dull, steady pain are lost.

Therefore paramedics struggle to determine internal problems like chest pain on a subject who has no obvious injuries and whose vitals are fine.

"It's difficult to relay on to the hospital what we're actually bringing in," said Pat Treloar, chief of fire services for Waterloo.

In many cases, children actually help to fill in those blanks. Young people tend to spend more time around other English speakers and adapt to a new language quicker.

"Right, wrong or indifferent, we use the kids to translate in those situations," Leibold said.

Another resource for getting adequate information is Language Line, a popular over-the-phone interpretation service that gives users access to more than 200 languages. But at about \$4 per minute, the service gets pricey fast, and it does not provide all of the dialects spoken by Waterloo's refugees.

The Black Hawk County sheriff's office and Black Hawk CCC have a contract with the service, but dispatchers rarely use it because of its steep cost. Waterloo police are currently working to get a contract.

Recruitment Struggle

Refugees-turned-police officers can be a strong asset for language barrier support. Leibold sees this as a good solution because it helps to "bridge the gap."

But getting foreign officers on board is a struggle.

When the last language barrier popped up in the late '90s with the influx of Bosnian refugees, emergency responders struggled with many of the same issues. It wasn't until 2007 that the first Bosnian officer arrived on staff with Waterloo police.

110



Leibold said that is because the police training is extensive, lasting five years. Not to mention that in order to enter the program, foreign applicants must pass English proficiency exams.

"It's not just learning the language to do our job, you've also got to learn American culture," Leibold said.

Currently the Waterloo police have one officer fluent in Bosnian and one officer fluent in Spanish. Those officers' interpretation abilities are in high demand within the department.

Hawkeye Community College has several bilingual Bosnian students in its police science program currently, but no Burmese are enrolled.

Building New Trust

Many times, the first hoop for refugees to jump through in an emergency is simply reaching out to law enforcement — an extremely daunting task to refugees who come from areas of widespread corruption.

"It's scary for families to trust that the American systems will not be corrupt, that they will do their best to help them out," Grove said.

Waterloo police have to assure refugees that they won't enter their home unless there is an emergency or they have a search warrant.

Some scenarios reveal a cultural divide.

Once a Burmese parent tried to have her 19-year-old daughter's boyfriend arrested because she did not approve of the two living together.

In Burma, that parent would have bribed the police to complete the arrest. But here in

Waterloo, officers are left explaining that they can't do anything about it.

Program Support

One local group is doing its part to better the language barrier situation: the Cedar Valley Refugee Newcomer Services. CVRNS, housed in First United Methodist Church, was created in May after the U.S. Committee for Refugees and Immigrants closed its Waterloo office.

Training sessions between police, dispatchers and refugees have helped to communicate emergency response issues and train refugees to be able to say their address and the words intruder, ambulance and fire.

The organization hopes to hold another session in the fall.

But resources are slim with just two employees and a survival budget goal they are only halfway toward reaching with grants and contributions.

"The city of Waterloo really needs to put money in the budget for interpretation," Grove said.

"We hope that would be done by the city, by the county, that would be a huge help."

In the meantime, Grove hopes cue cards with translation and pictures could help emergency communication. She has been working with Waterloo paramedics for eight months to get the cards into ambulances. But it has turned out to be a tedious task with the 14 different dialects and widespread refugee illiteracy.

"I'd say we could be better equipped, but we've managed to this point," fire chief Treloar said.

No Power? No Problem, \$75 P2P goTenna Lets You Text w/out Cell Network

Source:<http://www.dailytech.com/No+Power+No+Problem+75+P2P+goTenna+Lets+You+Text+wout+Cell+Network/article36236c.htm>

GoTenna is intended for both recreational use (backpacking, etc.) and emergency use. Having filed its final paperwork necessary to receive approval from the U.S. Federal Communications Commission (FCC), a small startup called "goTenna" is almost ready to make a bold debut two years in the making.

Designed primarily for emergency use -- but doubling as a recreational device -- the low power antenna communicates with a smartphone via the Bluetooth Low Energy (BTLE) specification. The antenna uses low-frequency radio waves to send peer-to-peer text message via goTenna's proprietary apps and antenna hardware.

GoTenna has a patent pending on the device.

Founder Daniela Perdomo said in a recent *Wired* interview that Hurricane Sandy, in part, inspired the new app:



I was thinking, 'Is there any way to make cell phones communicate, so even in the worst case scenario like Sandy, when you have no power or Wi-Fi, you can still communicate?'



The only thing that does that is Bluetooth, and for that you have to be within 20 feet, so you might as well just speak loudly. We figured out that the only way to do that was an external piece of hardware.

In terms of people communicating when they don't have service, on one end of the spectrum are walkie-talkies, and on the other are satellite communication devices, which are super expensive.

Walkie-talkies are big clunky devices that people use at Disney World. You have to

carry them in addition to your phone, they only let you do voice communication, you have to make sure you're on the same channel, you hear everyone's' conversations—they're annoying.

I do think there is something to decentralizing communication, to the idea that every person can be their synonymous node, and that you can create a communications system on your terms, on need as opposed to access.

He said he worked carefully to craft a device that was portable and rugged enough for a disaster use, but also attractive enough to be an item carried daily and employed in recreational uses, as well. He fashioned the device's final design by studying the look of various popular recreational gear at REI.

The finished device is made mostly of nylon and aluminum, with built in transmission and storage circuitry for

the messages, plus the antenna. It weighs ~2 oz. (56.7 g) and is 5 inches long (possibly the height of your Android smartphone). It has a strap to easily attach to a backpack or purse:



Here are the key details of the functionality and hardware spec:

Key hardware specs

- Antenna
- 2-watt radio
- Flash memory good for 1000's of messages
- Rechargeable Lithium-ion battery
- Micro-USB connector
- BluetoothLE data interface
- Status indicator lights
- Water-resistant
- Dust-tight

Key app features

- Send & receive text messages for free
- Share locations on detailed offline maps
- Instantaneous transmission within range



- Automatic message retry & delivery confirmation
- Individual & group messaging
- "Shout" broadcasts to anyone within range
- Proximal friend map & location pinging
- Emergency chat
- End-to-end encryption (RSA-1024) & self-destructing messages
- Compatible with iOS & Android

To get started you download an app on your phone and program the antenna to have your number so it can properly route user-specific messages to you. The app allows you to restrict access to it with a password on the device. The phone stores the messages in the antenna memory, transferring them to the logged in user. Aside from the shout and emergency messaging modes -- which are anonymous, open, and multi-user -- the device offers full 128-bit end-to-end encryption to protect your data.



The rechargeable battery lasts for up to 3 days on, or up to a year off. GoTenna includes a range calculator which allows you to estimate your range in various environments at elevations. In urban areas it appears you'll get 10-20 miles of range. In outdoor environments the range may be as long as 40-50 miles in ideal conditions.

While the device would clearly be useful for texting nearby loved ones in a disaster situation, it's important to remember that they

must have a goAntenna and they must be in range as the device does not use traditional cellular networks or frequencies. Aside from emergency use, goAntenna believes the device will be popular with users travelling in foreign countries (where messaging on traditional networks can lead to massive overages), users at concerts/social gatherings (perhaps looking to meet people), and hikers (in the backcountry where there's no power and little cellular coverage).

GoAntenna is selling antenna pairs for \$150 USD (\$75 USD per antenna) in a pre-order. After the FCC approval and official launch, the price will jump to \$299 (\$150 USD per antenna). Customers will also have the opportunity to receive and email to refer their friends. For each friend they refer they get \$10 off, up to the full cost of the antenna pair (so currently: refer 15 friends and you get a free pair). You can buy the device in Green + Blue or Purple + Orange.

113

There Are No Victims Here: Creating an Empowered Survivor Culture

By Charisma Williams

Source: <http://www.emergencymgmt.com/training/Creating-an-Empowered-Survivor-Culture.html>

"Be your own hero." The words hit me like a bolt of lightning (I'll explain why later). I was at my office having coffee with a colleague and discussing the changing (declining) status of the world we live in. We started talking about the rash of random shootings and how they have, ironically, improved our nation's geographical knowledge. Very few people had ever heard of Aurora, Colo.; Isla Vista, Calif.; or Newtown Conn., before deranged gunmen

decided to take their personal grudges out on innocent people. Now the names evoke equal parts sympathy and infamy in the minds of many Americans.

The conversation then turned to how to use these situations to encourage general preparedness. For example, countless times people have gone to the movies and texted or talked their way through



the “Please take time to make note of the nearest exit” message displayed before the feature presentation. After the shooting in Aurora, however, patrons were discreetly and



independently scoping out the nearest exits well before being prompted to do so.

Why the shift?

Although the threat of fire breaking out in a theater may not be at the forefront of many theatergoers’ minds, the thought of a lunatic bringing in a gun and shooting unsuspecting patrons certainly still is. And the response to both incidents is essentially the same: get out as quickly and safely as possible. An emergency is an emergency is an emergency, and in the aftermath of an event, preparedness professionals (like myself) get hung up on the details and sometimes miss out on valuable opportunities to use recent tragedies to train the public in an attempt to prevent additional tragedies.

Too often the public has to be “humbled” by a tragic or devastating event before many people start to see the validity in the safety and preparedness measures that those of us in the emergency management/preparedness community work so hard to promote both in our professional and personal lives. However, once they do, it is our job to use these events to help foster the safety culture we strive for daily. In my professional career, I have encountered companies that have chosen either ineffective preparedness education and training measures, or outright inaction for fear of “spooking” their employees. In order to be effective, we must push past the barrier of fear. The public is already scared, and the only way to combat that fear is with knowledge. How

many times have we heard on the news, “I didn’t think these kinds of things could happen here.” Tragedy happens everywhere, and the onus is upon us to make sure that the communities and constituencies we represent, and are responsible for, are both knowledgeable and resilient.

So what’s missing? Messaging that speaks the language of not just a privileged few but to the masses. While I have a great deal of respect for the recent Get a Kit, Make A Plan, Be Prepared campaign, I think the ambiguity of it confused a great deal of people. “Where can I get a kit?” “What kind of kit do I need?” “What kind of plan am I making?” “Be prepared for what?” It fell short of

glory by not addressing critical questions in the print ads. Granted, the ambiguity may have been intentional: either to pique interest and encourage those with the Internet access to log on and learn more, and maybe, esoterically, to reflect the fact that a good kit is supposed to be somewhat generic and unencumbered. The ideal preparedness kit addresses all hazards, and maybe that’s what the creative minds that devised this ad campaign were going for. And it would have worked had this been an ad exclusively for those of us within the community. Instead, for the more vulnerable populations — those who are struggling to make ends meet and are concerned with more imminent and pressing issues such as missed bill payments, late rent or mortgage and how to keep food on the table — this ad was likely received as little more than people of privilege speaking to people of poverty. The urgency of the preparedness message doesn’t take precedence in the face of other everyday obstacles.

Often the task of preparation seems so daunting (and expensive) that most people don’t even try. A poll released in 2012 showed that 44 percent of people reported not having first aid kits. Forty-eight percent said they did not have emergency supplies. Another 53 percent said they did not have the recommended three-day supply of food and water on hand in case of an emergency. So what do we do to get people on board? What do we do to encourage them to get



prepared and at the same time form a more productive partnership with our public? We can't do it for them — but we can show them how they can do it themselves.

Going back to my colleague's comment. While we were having our discussion, he said that in the face of tragedy, instead of trying to come in and fix everything on our own, we in the emergency management/preparedness community need to teach people to "be your own hero." What a brilliant strategy and a heck of a tagline, if you ask me. The same 2012 poll revealed that more than half of Americans believe that local authorities will still be available to assist them in the event of a disaster. What many of them fail to realize is that rescuers and local authorities are not superheroes working from impenetrable fortresses of solitude. They are our colleagues and neighbors and may likely be similarly impacted and incapacitated by the same disruptive incident.

By teaching our community members how to use what they have and tap into the resources that are already available to them (friends, family members, churches and community centers, for example) should the unthinkable occur, we better utilize both our time and their resources. By breaking the preparedness process into tangible tasks, members of the public will not feel so overwhelmed or pressured to buy the hundreds of dollars worth of supplies toted on many preparedness sites. No one person can do everything, but if everyone contributes something, then the

community is better equipped and able to assist itself (and us!) post-disaster. Finally, by promoting community-based response and resiliency efforts, we teach community members to fend for themselves and care for each other until help arrives. We give them ownership of the problem and charge them with seeking out the solutions that work best for their own unique surroundings. We teach them not to stand by and wait for help, but to be their own heroes.

A former boss once told me, "The worst plans you can make for yourself are often better than the best plans that other people can make for you." I have no problem asking members of the public if, during a disaster, they would rather sit on the cold hard floor of a dingy recreation center surrounded by several hundred of their closest (and equally miserable) friends, eating stale peanut butter sandwich crackers, or if they would prefer to stay in their own (less miserable) homes, on their own couches eating fresh peanut butter sandwiches. When the situation is presented in that way, the answer becomes obvious. Similarly, when we give the public a reason to care, candidly share the likely outcomes of inaction and provide them feasible ways to prepare for whatever is on the horizon, we are taking significant steps to quashing the so-called "victim culture" that many emergency management professionals have become accustomed to interacting with. More importantly, we are training, encouraging and empowering our valuable public partners to become their very own heroes.

Charisma Williams is an emergency preparedness professional in Washington, D.C. In her spare time, she preaches "the gospel of preparedness," helping to promote a culture of personal resiliency and responsibility.



As Violence Grips Iraq, Fears of Pre-Emptive Flooding Arise

Source: <http://www.enevspf.com/latest-news/latest-national/latest-national-news/53997-as-violence-grips-iraq-fears-of-pre-emptive-flooding-arise.html>



The Haditha Dam in Iraq as seen in 2004.

The possibility of potentially catastrophic flooding has emerged following reporting that either Iraqi military forces or Sunni militants would open the floodgates of a dam on the Euphrates River.

Citing statements by Iraqi security officials made Wednesday, the New York Times reported that ISIS forces "were advancing on the Haditha Dam," located roughly 120 miles from Baghdad.

The dam is the country's second largest and generates hydroelectric power.

The Times does not cite a specific threat made by ISIS forces that they would open the floodgates, but notes that ISIS fighters in April seized the Falluja Dam and unleashed flooding.

The Times reporting adds that Iraqi government forces were responding to the possibility by being prepared to open the dam's floodgates themselves. From the Times:

"This will lead to the flooding of the town and villages and will harm you also," the [dam] employee said he told the [army] officers.

Regardless of which side might open the floodgates, it is the civilian population who would suffer in such an event, Peter Bosshard, Policy Director of International Rivers, an organization that works to protect rivers and

the rights of communities that depend on them, explained to Common Dreams.

"Dams have been used as weapons of mass destruction through the ages," Bosshard continued. "In the first recorded water war, the army of Umma, a Sumerian city state, drained irrigation canals against their enemies of Lagash in present-day Iraq, not far from Haditha Dam, 4,500 years ago. In the most infamous case, the nationalist army of Chian Kai Shek destroyed the dikes of the Yellow River in 1937 to slow the advancing Japanese army, thereby flooding hundreds of thousands of square kilometers of land and killing at least 800,000 of its own people," he added.

Khalid Salman, head of the Haditha local council, told the Washington Post that ISIS would want take over the dam not to unleash flooding but to control the power plant powered by it, thus being able to provide a service to the local population.

"Of course they want to control the dam, which is very important, not only for Anbar, but for all of Iraq," the Post quotes Salman as saying.

Meanwhile, violence continues to erupt in the country. Reuters reports that on Thursday battles were "raging" in the city of Tikrit, where Iraqi forces are launching a



counter-attack on Sunni militant forces.

And on Wednesday, Shiite cleric Moqtada al-Sadr rebuked gains made by ISIS, and said his supporters "will shake the ground under the feet of ignorance and extremism," Agence France-Presse reports.

Iraq's Prime Minister Nour al-Maliki has told the BBC that he welcomed strikes against ISIS carried out by Syria, which hit within the Syrian side of the Iraq/Syria border. He said they were carried out without coordination, but added, "We actually welcome any Syrian strike against ISIS."

Amidst the official comments by leaders and new gains in territory by ISIS, a humanitarian

crisis continues to unfold, as over one million Iraqis—including half a million children—have been forced to flee their homes.

"Yet again, another humanitarian crisis hits war-torn Iraq, disproportionately and negatively impacting the hungry poor," reads a statement issued Wednesday by United Nations World Food Programme Executive Director Ertharin Cousin.

"The UN and the entire humanitarian community are surging staff, releasing funds and drawing on all available stocks to assist people affected by the fighting and meet the urgent growing needs," Cousin added.

Did climate deniers just admit they don't know what they're talking about?

By Dawn Stover

Source: <http://thebulletin.org/did-climate-deniers-just-admit-they-don%E2%80%99t-know-what-they%E2%80%99re-talking-about7261>

The war on climate science has evolved rapidly over the past decade, with talking points surging and subsiding in wave after wave: The planet is not warming. The planet might be warming, but the scientific uncertainty is too great to be sure. The planet was warming, but the warming stopped. The planet is warming, but not because of anything that humans are doing. The planet is warming, but that could be a good thing. The planet is warming and not in a particularly good way, but there's not much we can do about it. The planet is warming and possibly in a very bad way, maybe even because of human activities, but fixing it would be much too expensive.

Just when it seemed that climate deniers might finally be coming to their senses, several leading voices began backpedaling. But instead of asserting that global warming isn't occurring or isn't human-caused, they came up with a sly new way to suggest that the scientific jury is still out: total ignorance. As in *ignorance*.

The recent rash of ignorance started with a few Republican politicians who proclaimed that their lack of scientific training makes it impossible for them to determine whether scientists are telling the truth about global warming. By last week, Republicans in Congress were even ignoring experts from their own party: the heads of the Environmental Protection Agency under four Republican

administrations, who testified that global warming is real, humans are causing it, and action is needed. Republican congressmen responded by trying to block funding for EPA's proposed carbon pollution standards. Of course they did. The only science that interests them is political science.

Weasel words. "I'm not a scientist," said Florida Governor Rick Scott on May 27, when asked whether human activities are significantly affecting the weather. Asked whether he is now less doubtful about the human influence on climate than he was in 2011, Scott simply repeated himself: "Well, I'm not a scientist."

On May 29, House Speaker John Boehner spouted a slight variation on the theme: "Listen, I'm not qualified to debate the science over climate change."

"Neither he nor I are a climate scientist," said Tennessee Republican Marsha Blackburn in a debate with television personality Bill Nye "The Science Guy" three months earlier. "He is an engineer and actor. I am a member of Congress."

Koch Brothers spokeswoman Melissa Cohlmiya was on message, too, in a recent email to *The Wichita Eagle*: "We are not experts on climate change," she wrote.

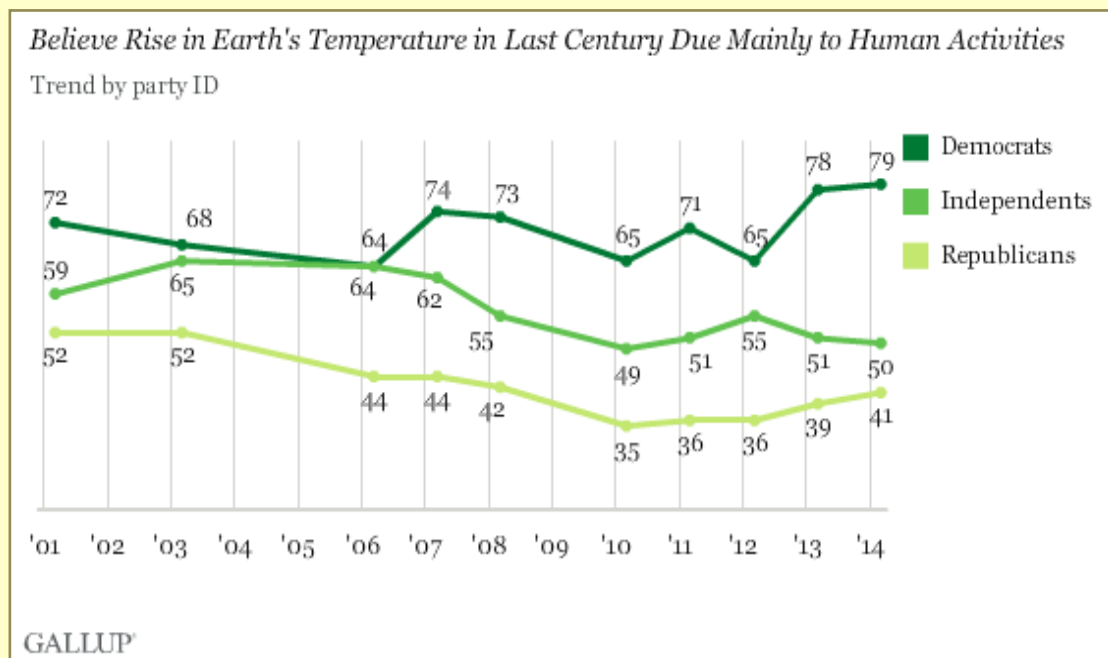


The “I’m not a scientist” mantra dates back to at least 2010, when Florida Senator Marco Rubio—who recently said he’s ready to be president—questioned the human contribution to climate change. “I’m not a scientist,” he told *The Miami Herald*. “I’m not qualified to make that decision... there’s a significant scientific dispute about that.” In a 2012 interview with *GQ* magazine, Rubio gave a similar answer when asked how old the Earth is: “I’m not a scientist, man. I can tell you what recorded history says, I can tell you what the Bible says, but I think that’s a dispute among theologians, and I think it has nothing to do with the gross domestic product or economic growth of the United States.”

Gosh, who knew that Rubio is an economist,

Mutism also makes the skeptic sound humble and respectful toward science. “The beauty of the line,” writes Jonathan Chait in *New York* magazine, “is that it implicitly concedes that scientists possess real expertise, while simultaneously allowing you to ignore that expertise altogether.”

Although professing respect, “I’m not a scientist” is actually a way of marginalizing scientists and relegating climate dialogue to elite scientific gatherings rather than making it part of broader public policy discussions. As Pat Cunningham points out in his blog at *The Oak Ridger*, Republicans “should say, in effect: We’re just like you. That science stuff just confuses us. But, by God, we’re not going to let the smarty-pantses tell us how to live.”



an historian, and a theologian? His resume reveals only that he is a scholar of politics and the law. Perhaps an advanced degree isn't necessary, after all, to understand (or claim to understand) the most elementary findings in an academic field.

Ignorance is bliss. It's easy to see what climate skeptics like about the not-a-scientist line, which the website DailyKos labeled as “climate change-mutism.” It allows them to beat a quiet retreat from earlier, scientifically dubious statements on climate change while dodging uncomfortable questions. And “I’m not qualified to debate” tacitly implies that there is a serious scientific debate about global warming.

When know-nothings know something. Unfortunately for Boehner and buddies, it doesn't take a smarty-pants to see the complications that result from pleading ignorance about science. If non-scientists can't understand science, what's the point of inviting scientists to testify at congressional committee hearings on climate science? And how can congressmen understand their own handpicked witnesses well enough to form any opinions on climate policy?

Imagine if politicians applied not-a-scientist reasoning to other areas of expertise: “I’m not a doctor, so I can't comment on the Affordable Care Act.” “I never served in the military, so I can't take a position



on nuclear weapons.” “I’m not an economist, so I’ll recuse myself from voting on the proposed federal budget.” “I’m not an engineer, so don’t expect me to have anything intelligent to say about whether my state needs any new roads or bridges.”

Even people who *are* scientists aren’t necessarily experts on climate. But that doesn’t prevent them or anyone else from reading and comprehending reports such as the Intergovernmental Panel on Climate Change’s latest assessment or the one the National Climate Assessment recently released by a team of more than 300 experts. The fact that most of us aren’t climate scientists is precisely *why* we rely on such people for credible information and authoritative analysis—and public policy makers should do the same.

Has climate denial become cheesy? Most Republicans aren’t making a point of being non-scientists, especially after President Obama skewered the phrase in a commencement speech on June 14, offering

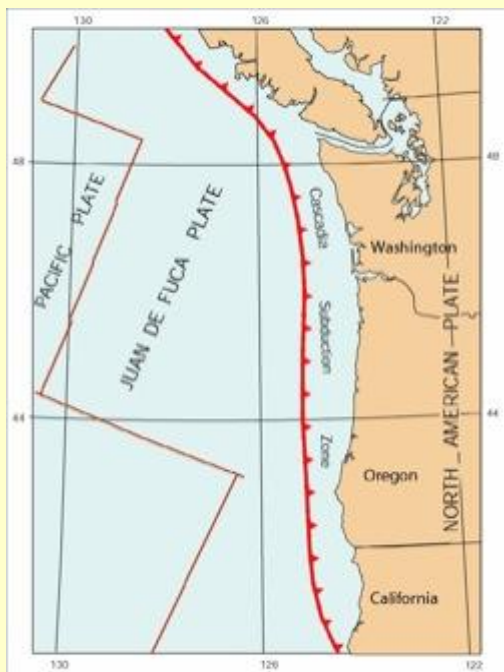
his own translation of “I’m not a scientist”: “I accept that man-made climate change is real, but if I admit it, I’ll be run out of town by a radical fringe that thinks climate science is a liberal plot.” Had climate deniers been around at the dawn of the space program, Obama said, they would have told John F. Kennedy that the moon “was made of cheese.”

We can’t get a taste of the moon, yet most of us trust science enough to believe that it’s not cheddar. With climate change, we *can* see for ourselves: coastal flooding, melting glaciers, extreme weather. Most Americans are not as clueless about what’s causing these changes as some of their elected representatives claim to be. A Gallup poll in mid-March (chart in previous page) reported that nearly six in 10 Americans believe that pollution from human activities, rather than natural causes, is responsible for the rise in global temperatures over the past century. Even among Republicans, 41 percent agree. And most of them aren’t scientists.

Dawn Stover is a science writer based in the Pacific Northwest and is a contributing editor at the Bulletin. Her work has appeared in Scientific American, Conservation, Popular Science, New Scientist, The New York Times, and other publications. One of her articles is included in the 2010 Best American Science and Nature Writing, and another article was awarded a special citation by the Knight-Risser Prize for Western Environmental Journalism.

U.S. Northwest prepares for the Big One

Source: <http://www.homelandsecuritynewswire.com/dr20140701-u-s-northwest-prepares-for-the-big-one>



Seismologists believe the Pacific Northwest is overdue for an earthquake that could register at over 8.0 on the Richter scale, leading many emergency management professionals in the region to anticipate and prepare for the devastating impact such an event would have on the local economy and quality of life. Last month, engineers, emergency managers, and public officials from across the region met at Centralia College as part of the Construction and Best Practices Summit hosted by the college and the Pacific Northwest Center of Excellence for Clean Energy. The second day of the summit focused on how best to prepare for and recover from an earthquake along the Cascadia Subduction Zone, a 1,000-kilometer fault stretching from Vancouver Island to Cape Mendocino, California.

The *Chronicle* reports that that Matt Cutts, critical infrastructure program manager at the U.S. Army Corps of Engineers’ Portland District, discussed



what he termed as the Triple 3 Resilience Target — a goal of managing the aftermath of an earthquake to have emergency services running within three days, level of services to sustain the economy within three weeks, and a target of three years to stabilize the economy and prepare for future disasters. “We have such an interdependent nature to our infrastructure,” Cutts said. “After an earthquake, roads are going to be down — but we need fuel and electricity as well. Those things are so tightly wrapped together, it’s like a Gordian knot.”

In the aftermath of an earthquake, aging buildings are likely to collapse, causing hundreds of deaths. Many roads would become impassable, and many businesses throughout the Pacific Northwest would cease to offer services for some time. “If we had this happen tomorrow, we’d be looking at thousands of people dead. You’re also talking about months of recovery,” Cutts said. “We really need to increase the public awareness of the possibilities. Emergency managers are always thinking about what could happen, but Joe Taxpayer doesn’t spend a lot of time thinking about it.”

Oregon Emergency Management director David Stuckey used the 2011 Japan earthquake and tsunami to signify the importance of educating the public. “Right after the 2011 Tohoku earthquake, I got a call from a commissioner on one of the coastal counties,” Stuckey said. “There were people running to the beach with surfboards.... We have to create a broader perspective on how to educate people.”

Efforts to retrofit buildings and critical infrastructure across the region have been made but emergency managers insist that the major focus now is how to restore critical infrastructure and the economy after a large earthquake. “If we can achieve the Triple 3 Resilience Target, we end up with a manageable disaster instead of a catastrophe that would take us months or even years to recover from,” Cutts said.

U.K. infrastructure facing tough challenges as extreme weather events multiply

Source: <http://www.homelandsecuritynewswire.com/dr20140702-u-k-infrastructure-facing-tough-challenges-as-extreme-weather-events-multiply>

The U.K. Institute of Civil Engineering’s (ICE)



State of the Nation: Infrastructure 2014 report has highlighted the fact that more frequent extreme weather events will make it increasingly difficult to operate U.K. infrastructure networks in all conditions at the level of service U.K. residents have come to expect, and people’s expectations of availability will need to change. The report grades the U.K.’s Transport, Energy, Flood, Waste, and Water networks from A to E, highlighting the progress since 2010 in improving infrastructure and positioning it as a core enabler of economic growth, but suggests more needed to be done if the United Kingdom is to have world class infrastructure — in

particular on the issue of resiliency, given its impact on the economy and the major challenges ahead. This was highlighted by the “at risk” or “requires attention” grades for Flood Management, Energy, and Local Transport networks, due to the narrowing gap between supply and demand for energy, inadequate resilience to flooding, and the decline in maintenance of both flood defenses and local roads following investment cuts.

An ICE release notes that the report said resilience — including the “domino effect” where the failure of one system can affect the operation of another — should be embedded into the criteria used as a basis for making decisions on priority infrastructure projects, better to reflect future challenges.

It also warned, however, that while the United Kingdom needs to build resilience, the U.K. infrastructure cannot be resilient to every eventuality, and that it will become more difficult to operate all infrastructure networks, at all times, in all conditions. The reports says that a shift in the public’s expectations on infrastructure availability would be needed.



State of the Nation report chair and ICE vice president Keith Clarke CBE, said: “As the 2013-14 winter floods showed, unplanned interruptions in our networks are costly to society and the economy. They happen because we are trying to run all services at all times, and are deemed unacceptable as the public expect a certain level of service. Government ultimately bears the risk for the resulting impact.

“It is becoming clear that extreme weather events will become more frequent, and it is time that factors such as availability, resilience and the “domino effect” across the networks when one network fails — as we saw recently when our flood defenses were overwhelmed and this in turn disrupted transport, energy, water and waste networks - are rooted into the criteria used to make decisions on which projects go ahead so new infrastructure is more ‘future proofed’.

“But, importantly, we must all recognize that our infrastructure cannot be resilient to everything and it will become more difficult to

run all services in all conditions — it will also not be cost effective. Funding will always be constrained as there are only two sources — tax and user charging — both ultimately falling on the consumer. The balance between the two is a choice for the government of the day, but irrespective of where it comes from, both are constrained resources and must be used efficiently.

“Clearly there are some difficult decisions ahead regarding just how resilient the U.K. should be, and also what networks can and should operate 24/7 in what conditions. We can then plan more effectively — avoiding costly unplanned disruptions — and adapt. Management of the public’s expectations on availability during adverse conditions will need to form a key part of this process.

“The onus is on government to make these choices for public sector infrastructure, and it must also build on its efforts to provide the right regulatory incentives to improve resilience within private sector infrastructure.” he added.

Key ICE recommendations

On strategic decision making and leadership, government should:

- Expand the criteria used as a basis for making decisions on priority infrastructure projects to reflect major future challenges— criteria should include resilience, availability, the pathway to a low carbon economy and better acknowledge “interdependencies” across networks — or how one sector impacts on another.
- Be prepared to make tough choices regarding the levels of resilience in the U.K.’s infrastructure networks and the appropriate levels of service/availability - and work with industry to manage public expectation.
- Ensure the right regulatory environment exists to incentivise private infrastructure operators to build resilience into infrastructure.
- Be appropriately resourced to make and implement decisions on key issues affecting the U.K.’s resilience or competitiveness, such as aviation capacity
- Provide more clarity, certainty and transparency for potential investors through the regularly published National Infrastructure Plan project pipeline — by including more detail on investable projects, their status, planning approval, ownership structure and revenue streams.

On Energy, Local Transport and Flood Management sectors:

- The Environment Agency and Lead Local Flood Authorities should fully implement a holistic approach to flood management, which includes a wider range of measures in addition to conventional flood defences — including building the physical resilience of communities by making property and infrastructure more resistant
- Government should provide the longer term certainty needed to improve flood resilience by committing to a long term capital and maintenance programme for Flood Management which protects funding beyond the current 5 year cycle
- Government should enact the secondary legislation to implement EMR by the end of this Parliament, establishing long-term investor confidence and entrenching cross-party support for electricity decarbonisation
- Government should extend devolved transport powers and funding through the creation of more powerful, fully integrated transport authorities in city regions.



- Government and local authorities must establish a more ambitious joint programme to clear the road maintenance backlog, and commit to a more cost effective planned, preventative maintenance regime.

— *Read more in State of the Nation: Infrastructure 2014 (Institute of Civil Engineering, 2014)*

Japan exceedingly vulnerable to sea level rise

Source: <http://www.homelandsecuritynewswire.com/dr20140717-japan-exceedingly-vulnerable-to-sea-level-rise>

Scientists say that Japan might be one of the most at-risk nations when it comes to the consequences of sea-level rise.

Japan Times reports that the most recent UN Intergovernmental Panel on Climate Change (IPCC) assessment predicts that sea levels will “rise by 1-3 feet by 2100.” Even more troubling, should Antarctic ice loss exceed expectations — of which there is evidence that the article cites — then these estimates would have to be “revised upward.”

This forecast proves to be exceptionally dangerous for Japan, a nation that has a coastline 30,000 km long, much of it in largely low-elevation regions. Additionally, about 80 percent of the country’s industry and population are located in these zones.

Multiple studies, some by scientists, other by economists such as those at the Asian Development Bank, concluded in 2013 that storms with higher seas could lead to thousands of deaths, the destruction of 1.4 million homes, and damages in a range from billions of dollars to hundreds of billions of dollars.

Environmental researcher Masahiko Isobe came to the conclusion in a 2013 study that a two-foot rise in sea levels would lead to a wave height which would be three times larger by the time the wave met the coast. Further, there is an elevated risk of liquefaction – in which soil becomes oversaturated and loses strength — which would be particularly devastating on

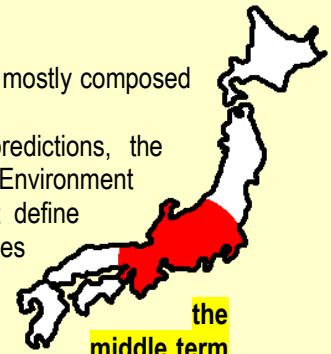
Japan’s coasts which are mostly composed of granular soil types.

Given these worrying predictions, the Japanese Ministry of the Environment is working on plans that define which issues are priorities for a range of time windows. **These include the short term (ten years), middle term (10-30 years), and long term (30-100 years), beginning in 2015.** Some methods include reducing greenhouse gas emissions, identifying at risk areas, and elevating or remodeling facilities.

The government has pledged one trillion yen for nationwide disaster prevention, which includes the strengthening of levees in port cities such as Tokyo with an eye toward the next 200 years.

Much of these measures come in the face of the 2011 Great East Japan Earthquake and tsunami, which devastated facilities like the Fukushima Daiichi nuclear power plant — largely regarded as one of the most devastating natural disasters the country had faced.

Kazuya Yasuhara, a professor at Ibaraki University’s Institute for Global Change Adaptation Science, told the paper that **preparing for a 3-foot sea level rise is possible**, provided further disasters of that magnitude do not divert the appropriation of funding and attention which are needed to ensure future coastal safety.



Microgrids offer cities resiliency, reliability, accessibility

Source: <http://www.homelandsecuritynewswire.com/dr20140709-microgrids-offer-cities-resiliency-reliability-accessibility>

A majority of the world’s population now lives in cities, which consume 75 percent of the world’s resources and emit most of its greenhouse gases. The United Nations estimates that by 2050, an additional three billion people will move into these dense, resource-intensive urban environments.



“Projecting from current trends, you realize that we should have a plan for how this change unfolds,” says Mike Corradini, director of the Wisconsin Energy Institute and professor of engineering physics. As urban growth increases stress on global systems, Corradini is among a team of University of



Wisconsin-Madison researchers working to develop solutions that contribute to the livability of future cities. When it comes to urban energy – and its ever-increasing consumption — Corradini believes resiliency, reliability and accessibility will be critical factors in ensuring a sustainable supply.

“When you’re talking about a livable city, you’re not just talking about energy or energy use,” he says. “It’s a combination of how we use water, create food, construct buildings, and transport people or goods. These are all largely connected

and interdependent.”

Of course, different cities have different energy needs, which means that livable city solutions tend to vary according to local need.

Eric Anderson writes in *In Common*, published by the Nelson Institute for Environmental Studies at the University of Wisconsin-Madison, that in the United States, for example, where infrastructure and utility support have made access to electricity nearly ubiquitous, plans for the future tend to focus on creating energy systems with greater efficiency and reliability. The focus in cities like New York or New Orleans is on building infrastructure to make cities more resilient when faced with extreme weather or natural disasters — by providing backup power during outages, as well as helping to ease systems back online as outages end.

In developing countries, however, electrification systems are often weak or nonexistent and the focus tends to lie elsewhere. In Uganda, where less than nine percent of the population has access to electricity, communities prioritize the development of individual off-grid solutions that have the flexibility to grow and meet future needs.

What is certain is that worldwide growth of urban centers will continue to pose energy challenges. And these challenges carry with them an opportunity to amplify the impact of livable-solutions planning and policy. By improving the places people already reside and preparing early for where they will live in the future, we can improve how we interact with the environment on a very large scale.

Microgrid researchers in the UW-Madison College of Engineering and the Wisconsin Energy Institute are taking up this challenge by developing an energy solution with the potential to strengthen all three critical factors of energy in a livable city: resiliency, reliability and accessibility. The microgrid, in other words, may offer a powerful, versatile and wide-ranging solution to a variety of energy challenges at different scales and under a range of conditions.

Resiliency

A microgrid is a small, self-contained electric-power system with the capability to seamlessly connect to and disconnect from the traditional grid, the network of power lines that move electricity from generating stations to users. It includes all of the components of the traditional energy infrastructure (generation, distribution and consumption) consolidated to accommodate smaller consumer base loads such as individual buildings, hospitals or campuses.

Many cities consume their energy predominantly from fossil fuel sources distributed through centralized generation systems. This type of expansive infrastructure, however, also comes with some risk.

“It’s unlikely that, particularly in the United States, we’ll completely replace the bulk power system,” says Paul Meier, a Wisconsin Energy Institute scientist and Nelson Institute alumnus (Ph.D. Land Resources and Energy Analysis and Policy ‘02). “It’s a vast infrastructure and, right now, there is little in the way of incentives to change it.”



“But, there are opportunities to improve how the system operates or where our energy comes from that could benefit cities,” adds Meier, whose research focuses on the economic feasibility and impacts of resource planning models.

The U.S. Department of Energy estimates that power outages and grid failures cost American businesses \$100 billion annually. When these interruptions occur, however, microgrid consumers can switch to electricity generated or stored locally, creating a more resilient and stable energy supply. In the case of hospitals, where the system can be designed to be even more robust and self-sustaining, key health services can be maintained throughout an outage.

Microgrids also create the flexibility to integrate energy from rooftop solar installations, nearby wind turbines or other distributed sources. These small-scale renewables have struggled to become cost-competitive with energy-dense fossil fuels at a utility scale. The microgrid can thus serve as a more immediate conduit between alternative energy resources and consumers.

Reliability

In India, rolling blackouts — an intentional shutdown of electricity distribution in certain areas to avoid overstressing the grid and creating a total system blackout — affect both rural and urban populations. In 2012, India experienced a massive electricity outage that affected more than 600 million people for many days. The outage crippled much of the country, bringing trains to a halt and leaving hospitals in the dark.

“At night you might see the factories shut down, so that power plants can divert electricity to people’s homes. They’re trying to be as equitable as possible,” says Giri Venkataramanan, a UW-Madison professor of electrical and computer engineering. “For example, during irrigation season, more power will be transmitted to rural regions for pumping water out of the ground for the crops. At those times cities suffer, but people have adapted.”

In many Indian cities where households or businesses have grid access but are forced to live “off-grid” throughout the day, a home energy system combining their own generation and storage capacity fills in for the prescheduled gaps. This system is essentially an incomplete microgrid, and provides a particularly possibility-rich opportunity for improvement in the future.

“Currently there is no interconnectivity among these makeshift microgrids,” Venkataramanan says. “We know it can be done. The challenge is in figuring out how to use the assets that people have already invested in to help the grid during peak demand times.”

Accessibility

Microgrids can complement a grid system by providing backup power for planned or unplanned outages. But in rural communities throughout the developing world, where there is neither a grid system nor a backup plan, microgrids provide an opportunity for people to develop energy systems structured to their own needs.

In Uganda, a team of UW-Madison researchers hopes to help curb reliance on traditional energy sources that can be harmful to human health and the environment by developing a system that Venkataramanan describes as a wireless microgrid.

The project brings together collaborators from the Nelson Institute and the College of Engineering to expand from existing biogas systems and create electricity in a way that is accessible and useful for community members. Their system captures and uses biogas from an anaerobic digester to fuel a generator that charges batteries. The batteries can then be used to power lights and charge cellphones in homes throughout the community, without a grid.

The problems associated with growing cities will challenge how we build, plan, support and improve this uniquely human environment. The study of microgrids and other micro-scale energy systems is just one part of a broadening spectrum of UW-Madison research meant to help urban populations adjust and react with solutions right for them.



6 Great Disaster Infographics

By Brandon Greenberg

Source: <http://www.disasternet.co/blog/2014/6/29/4-best-disaster-infographics>

Disaster statistics and information have been around for while, but rarely have they been presented in such ways that grabs people's attention. Infographics are a new visual way of presenting information in a easily digestible graphic. They are usually static in nature, but present a finite set of information in some sort of story line and are a great way to connect with your audience!

Brandon Greenberg is a PhD student @GWEngineering | MPA from @NYUWagner | Researching & working btw Policy, Mgmt and Tech for Disaster.

► View the rest of Indographics at source's URL.

Calculating the Cost of Doing Nothing for Disaster Recovery

Source: http://www.peak10.com/blog/post/calculating-the-cost-of-doing-nothing-for-disaster-recovery?utm_source=News&utm_medium=cpc-pk10mkto-2988&utm_campaign=datasecurity2#.U7p5KbFs5cp

There is no easy way to quantify the financial benefits of investing in backup and recovery. That's why with many companies, funds and resources for a backup and recovery solution are only allocated as part of another project. Too often the costs aren't fully understood until after a company faces a major data loss. Can you afford to do nothing?

What Does Nothing Cost?

Doing nothing seems surprisingly inexpensive at first glance. There is no equipment or software to purchase, no annoying project plan to set up, and no overtaxed personnel to re-allocate.



Who could argue with a strategy that has a cost of zero? Regardless of currency fluctuations or foreign exchange rates, zero is a very manageable number!

Unfortunately, doing nothing only works until the moment something happens. Just like it's efficient not to carry an umbrella – right up until the day it rains. In the IT field, something is definitely going to happen. The only question is, "When?"

Once something happens, doing nothing starts to look more costly. To put it in mathematical terms:

Expected loss = Probability of incident x Cost of incident

A simple example: if the probability of rain is 50% per week (weekly probability of 0.5) and the cost of being in the rain is the price of a suit (\$250), your weekly expected loss for not carrying an umbrella is $0.5 \times \$250$, which is \$125. Given that calculation, I'd keep an umbrella in my briefcase. Doing nothing could be rather expensive.

125

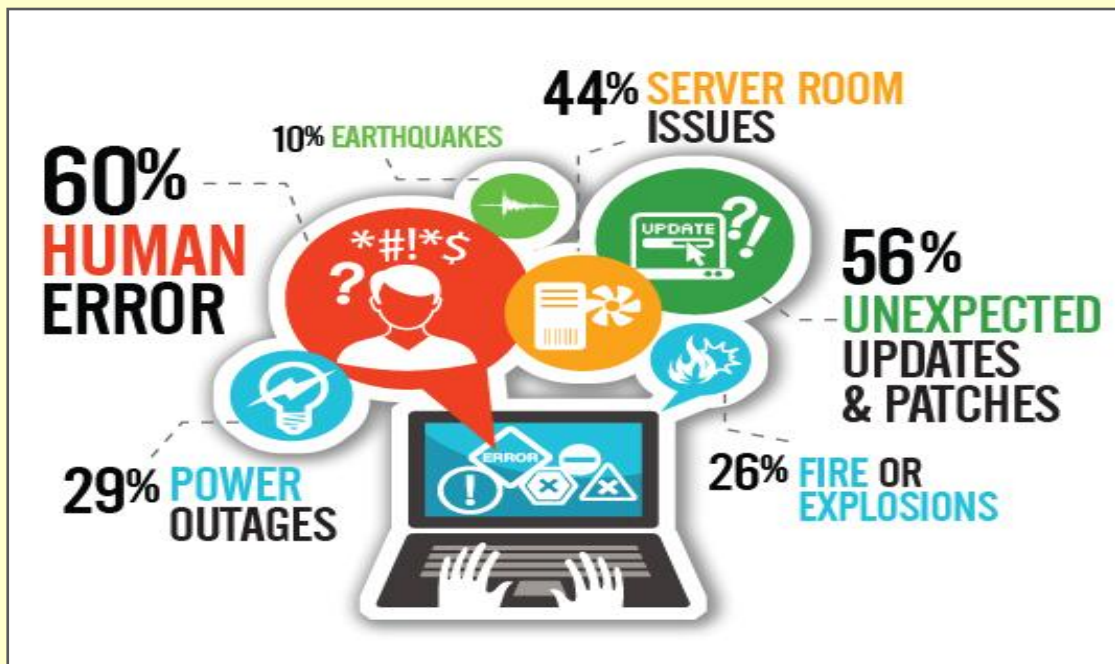


When Will Something Happen?

In disaster recovery (DR) terms, the first thing we need to know is the probability of a disaster. The fact is that unwanted stuff happens all the time. If you're counting on zero downtime or data loss, prepare to be disappointed. While the frequency of data center disasters varies by company and location, a 2012 Aberdeen Group report found that the average company reported 2.3 business interruptions each year, averaging one hour of downtime per event. And outages are only one class of potential disaster.

Weather-related disasters have been making headlines for several years, wiping out businesses in dramatic and unpreventable ways. In 2013 alone there were seven weather or climate disasters resulting in loss of one billion dollars or more. But it turns out that far more likely risk is presented by power/UPS failures, human error and the steadily growing threat of cybercrime.

Risk assessment is a scientific endeavor, since calculations need to be individualized to your company. While broad generalizations can be found, you're best off engaging with an expert consultant. In your organization's setting, there may be specific factors that influence your risk. Your geological location,



local infrastructure, nearby hazardous businesses and even the appeal of your company to hackers can magnify or reduce your disaster risk.

You get to define "disaster" in a way that's meaningful to you. You'll probably look at circumstances that interrupt your operations, cause you loss or damage your organization's reputation. There are lots of these. A recent Computing magazine survey of IT professionals in the UK identified the obvious disaster risks – natural disaster, system downtime and malware – as well as some you'd probably not think of – like disgusting smells from animal and human sources that necessitated equipment shutdown. A risk assessment consultant will help you factor in all pertinent categories of disasters, each of which has a different probability of occurring. For example, the probability of misplacing my umbrella is pretty high, based on experience. The probability of misplacing my toaster: negligible.

Totaling up the list of incidents and probabilities quickly eliminates the advantages of doing nothing – unless the probability of all disasters is zero.

What Will It Cost?

The second part of our loss calculation is the cost of each incident type.

Costs calculations for various disasters are readily available. In the category of data center outages, Gartner offers a detailed Downtime Cost Calculator. The Aberdeen Group report declares that the average annual cost of business interruption is \$418,071. Forrester Research calculates the cost of typical email and web outages between \$11,142 and \$47,662 per incident.



Those calculations only scratch the surface of what you might lose. Only some costs of a disaster are tangible, as history enlightens us. Memorable recent data breaches at major retailers have created quantifiable data center and customer retention costs, to be sure. In addition, senior managers' reputations were damaged, profits dropped, shareholders became militant and employee morale deteriorated.

It's difficult to assign a dollar figure in such cases. Some consequences cannot easily be remediated, particularly in the personal lives of those affected. But the dismay they cause us indicates that we cannot overlook qualitative losses in a review of the costs.

Make your own list of tangible and intangible costs, based on your business. Lists of likely categories are available from many reputable sources. You'll want to consider the hard and soft costs of remedying all types of calamities and their consequences. A partial list, as starting point:

- IT failures: servers and monitoring, databases, applications, infrastructure and networks
- Environmental disasters: fire, flood, earthquake, hurricane and tornado
- Utilities: HVAC failures, power outages, telecommunication failures
- Human error and accident: data corruption, file deletion, database record loss
- Cybercrime: in-house sabotage; efforts to steal, corrupt or destroy data; denial of service (DoS); malware, organized criminal activity
- Physical Break-ins: theft, destruction, vandalism, terrorist attacks
- Performance guarantees to your clients and related fees
- Local and regional disruption: strikes, legal actions, shutdown orders, ripple effects from neighboring crime or disaster
- Loss of business and customer retention, specific customer and vendor liability, consumer credit monitoring
- Regulatory compliance costs and penalties
- Company reputation, valuation, future business, impact on employee recruitment
- Community relations: local town/state goodwill, political considerations
- Lost productivity, employee morale
- Senior management's lost reputation: internal, external, future employment
- Shareholder value, disgruntlement, lawsuits

What Will It Cost to Mitigate?

Disaster cannot be prevented. Weather events, for example, can often be predicted but rarely avoided. Cybercriminals, regrettably, are moving faster than our ability to identify and prevent them.

But a good disaster recovery plan mitigates the cost impact of disasters and their consequences. To revise the previous mathematical formula, your budget for mitigation and recovery is the value of the losses the DR plan prevents.

Preventable loss = Probability of incident x Preventable cost of incident = DR budget

For most businesses, that's a sizeable budget.

But first, couldn't you save a lot of trouble merely by getting insurance? The answer depends on how willing you are to pause or close your business. After Hurricane Sandy's tragedy along the Jersey Shore, some small businesses that were insured were able to rebuild and eventually reopen – after a significant pause in operations. Others, even though insured, closed their doors forever. The damage done to property, customer continuity or morale exceeded their owners' physical and emotional resources to recover.

They just walked away.

So if you're willing to shut down your business in exchange for any insurance proceeds after the next significant incident, that strategy works. However, organizations with commitments to large customer and employee populations will not find this an attractive approach. Would you?

That's where disaster recovery comes in. A well-designed recovery plan assesses what you most need to protect, identifies your objectives for recovery, then designs technology and processes to reach these objectives. A good DR process also minimizes the duration of outages and follow-on consequences, so that you're back on your feet far sooner.

Planning and building a DIY disaster recovery is perfectly possible but complex. Frequently, the simplest solution is outsourcing with an experienced DR partner. Unless



you already have secure redundant data centers in place, a colocation or cloud recovery partner will get your plan up and running faster than you could. Plus, the expertise and processes that they bring to the table makes your DR plan more robust. If you're daunted by DR, it's worth finding out who can help.

Doing Nothing Costs Too Much

To paraphrase the bumper sticker, unwanted incidents happen. In the real world, putting your head in the sand simply makes the problem worse. The unplanned disaster throws business into a panic, wreaks havoc on the revenue, deflects personal careers and conceivably terminates the business. Doing nothing is expensive. Planning for recovery can pay for itself. To be sure, it's easy to postpone action when the choices are confusing or the justification is complex. But the ideal time to act is before the disaster develops. Now, for instance.

NOW WHAT?

TRENDS IN EMERGENCY MANAGEMENT
Expect the Best, Prepare for the Worst

Emergency management, most simply defined as the discipline dealing with risk and risk avoidance, is undergoing some dramatic changes.

WHERE WE'VE BEEN: A HISTORY OF EMERGENCY MANAGEMENT

1803 The US government's emergency management efforts begin when Congress passes an act providing financial assistance to rebuilding New Hampshire after a fire.	1934 President Franklin D. Roosevelt initiates programs that focus on disaster preparedness and relief, including the Federal Civil Defense Administration.	1974 April 1981 Indian Agent 11 plane being shot down over the LA area by a hijacking, the "Cherokee" hijack is averted.	1979 The Three Mile Island plant suffers a partial meltdown, which causes a release of radioactivity into the atmosphere.
1992 Hurricane Andrew hits Florida, causing widespread destruction.	2001 As a result of the 9/11 terrorist attacks, the Office of Homeland Security is created.	2005 Hurricane Katrina hits the Gulf Coast and FEMA's failure to respond to the disaster becomes a major focus of the federal government.	2013 The Ebola virus outbreak in West Africa causes a major public health crisis and a global health emergency.

WHAT LIES AHEAD: 21st-CENTURY EMERGENCY MANAGEMENT

Evidence indicates that there are more flooding episodes today than in the past. Even worse, they're occurring in places where they never have before.

Rising climate changes will increase episodes of both flooding and drought.

The increased reliance on computers will result in more technological disasters as times goes on.

New biological hazards such as SARS and avian flu continue to loom as potential pandemics.

Future terrorist attacks could be even more devastating than 9/11, especially if they involve weapons of mass destruction.

FACT LOSSES OWING TO NATURAL HAZARDS TOTAL MORE THAN **\$1 BILLION PER WEEK**

YOU CAN RUN, BUT YOU CAN'T HIDE: WHICH DISASTER WILL AFFECT YOU?

EARTHQUAKES **FLOODS** **FIRES**
TORNADOES **DROUGHT** **HURRICANES**
SNOWSTORMS
HUMAN ACCIDENTS

FACT THERE ARE NO HAZARD-FREE AREAS. YET TIME AND AGAIN, PEOPLE ARE UNAWARE OF OR UNPREPARED FOR COMING DISASTERS.

Danger? What danger?

Disasters are acts of God. There's nothing I can do about them.

Those threat warnings are overblown. I'm staying put.

WHY?

If disaster strikes, there's no way to be prepared, so what's the point?

I'm sure we can handle it...

Why spend money on preparedness measures that may not ever be needed?

FACT EMPHASIS ON HAZARDS INSTEAD OF VULNERABILITY IS A MAJOR ERROR AMONG SCHOLARS AND PRACTITIONERS.

Today's hazardous political climate is riskier than ever. Many believe that we will experience more attacks on a more frequent basis, and with more impact and complexity.

An attack involving biological agents could kill thousands, hundreds of thousands, or even millions of people.

A chemical release would be less deadly, but an effective response requires specialized knowledge, resources, and personnel.

FACT BECAUSE OF INCREASED VULNERABILITY, EMERGENCY MANAGEMENT MUST MEET NEW AND MORE COMPLEX NEEDS.

The US population is not only aging, it's shifting to the southeast. In some areas, it's even growing in hazardous and hazardous.

Our infrastructure is also aging. Bridges, highways, railroads, dams, and the electrical grid are all becoming.

America's population is shifting south and west. Several areas prone to hurricanes, drought, and earthquakes.

The current budget deficit means communities must do more with less.

OKAY, SO WHAT KIND OF CHANGES ARE BEING MADE?

The Bill and Melinda Gates Foundation's Emergency Response grant funding program aims to reduce suffering, disease, and death in countries affected by natural disasters and complex emergencies. Three areas of funding are:

- FAST-OCKET EMERGENCIES:** Focuses on funding to address high-impact disasters within 24 to 48 hours. Funding is required for prevention and early response efforts when the ability to intervene after the fact is limited.
- SLOW-OCKET EMERGENCIES:** Address long-term issues such as drought and famine.
- COMPLEX EMERGENCIES:** Focuses on long-term relief, support, and recovery for natural disasters, including those that are complex and multi-faceted.

BROUGHT TO YOU BY EMERGENCY-MANAGEMENT-DEGREE.ORG

