March 2016

CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

www.cbrne-terrorism-newsletter.com

British scientists designing cement to safely store nuclear waste for 100,000 years

Source: http://www.ibtimes.co.uk/british-scientists-designing-cement-safely-store-nuclear-waste-100000-years-1543754

Feb 14 – **A team of British scientists are working on designing a form of cement which could safely withstand the harmful effects of nuclear waste for thousands of years.** The team at the UK's synchrotron science facility, Diamond Light Source, said the project will be vital as Britain looks to expand on its nuclear industry.

The team believe the new material is 50% better at reducing the impact of radiation than current storage solutions. The government is set to choose a location of where to store the estimated 300,000 cubic metres of radioactive waste which is estimated to have been accumulated by the UK by 2030.

Part of this strategy for disposal is the plan for a Geological Disposal Facility (GDF) where highly radioactive waste, immobilised in cement, would be interred deep underground. However, before a location can be agreed, the government will need to be assured the waste will remain safe for at least 100,000 years.

Knowing how to store nuclear waste safely has become an important issue as approximately 11% of the world's electricity is produced through nuclear fission power, and it is an increasingly important factor in helping to reduce CO_2 emissions in line with international targets. Britain has previously announced to build several nuclear power stations over the next decade to phase out power provided by gas, coal and oil.

Dr Claire Corkhill from the University of Sheffield is using Diamond's unique Long-Duration Experiment (LDE) facility to study the way that cement reacts with water as it becomes hydrated over a period of hundreds of years. The team at Diamond Light Source now believe following a two-year long experiment that they have discovered new cement material that contains mineral phases known to absorb highly radioactive elements.

Corkhill said: "Armed with the knowledge that these phases form, and knowing how quickly, supports the use of our new cement material in the GDF. We hope that these results will influence the design of the GDF and help improve its long term safety."

Diamond's Director of Physical Sciences, Trevor Rayment: "Timescales are crucial when it comes to nuclear research. Any facility expected to contain highly radioactive waste will need to remain functional for an extremely long period of time. Until recently, it's been impossible to use synchrotron light to study interactions that take place over extended timescales.

"But, in a world first, Diamond has engineered a long-duration experimental facility that allows users to study sample behaviour in the intense detail afforded by synchrotron light but over a two-year period: much longer than has ever before been possible."

Truck carrying toxic nuclear materials stolen in Mexico

Source: http://www.homelandsecuritynewswire.com/dr20160301-truck-carrying-toxic-nuclear-materials-stolen-in-mexico

Mar 01 – **Five Mexican states have been placed on a state of alert after a truck carrying a container of dangerous radioactive material was stolen,** the Mexican Interior Ministry has said. The material could cause permanent or serious injury to a person who is in contact with it for a short time, and is fatal when exposure lasts for more than a few hours.

AFP reports that the Office of National Co-ordination of Civil Protection issued the warning after a truck carrying radioactive **iridium-192** was stolen from a company in the central state of Queretaro,

The radioactive material is understood to be contained in a device used for industrial radiography, according to CNN.

The police say that it is not yet clear whether the radioactive material was the target of the people who stole the truck.

The Interior Ministry said in a statement that such material "can be dangerous for people if not handled safely" and could cause "permanent or serious injury to a person who is handling or in contact with it for a short time." Officials added that the radioactive material could pose serious health risk if taken out of its container.

The *Daily Mail* reports that the truck and the radioactive material belonged to the company Industrial Maintenance Center, located in the city of San Juan del Rio. In addition to Queretaro, the states of Hidalgo, Guanajuato, San Luis Potosi, and Michoacan were also put on alert.

Experts note that iridium-192 can cause burns, radiation sickness, and permanent injury if a person comes into contact with it. Exposure to the material for more than few hours is fatal.

The Mexican authorities have urged people who spot the truck or the radioactive material to stay at least thirty meters away from it, and notify officials immediately.

CBS News reports that theft of radioactive material is common in Mexico, with this latest incident being the fourth such theft since 2013.

2014 French nuclear accident more serious than official reports suggested

Source: http://www.homelandsecuritynewswire.com/dr20160304-2014-french-nuclear-accident-more-serious-than-official-reports-suggested

Mar 04 – **German newspaper *Süddeutsche Zeitung* and public broadcaster WDR claim that both the French nuclear authority (ASN) and French energy giant EDF, which operates the two Fessenheim nuclear reactors, concealed the seriousness the 19 April 2014 incident at the site, when one of the reactors had to be shut down after water was beginning to leak from several places in the facility.**

The nuclear incident at Fessenheim, located in Alsace near the border with Germany, may prove to be one of "most dramatic nuclear accidents ever in Western Europe," researchers for *SZ* say. The researchers obtained a document which was sent by ASN to the then-head of the facility on 24 April 2014.

Yahoo News reports that the letter and subsequent reply show **that the reactor could not be shut down in accordance with the routine procedure because the control rods were jammed. The reactor had to be shut down by adding boron to the pressure vessel, an unprecedented procedure in Western Europe, nuclear experts say.**

"I don't know of any reactor here in Western Europe that had to be shut down after an accident by adding boron," Manfred Mertins, expert and government advisor on nuclear reactor safety, told WDR and SZ.

The media reports note that the official report on the incident, which ASN released weeks later, did not mention the adding of boron or the jammed control rods. The International Atomic Energy Agency (IAEA) requires that details of every nuclear incident be submitted to the agency, and ASN and EF submitted such a report – but it, too, failed to mention the boron and the jammed control rods.

The Fessenheim reactors, which went online in 1977 and 1978, are France's oldest nuclear reactors. French politicians, energy experts, and neighboring Germany and Switzerland have been pressuring the French government to shut down the aging facility, and the government has said it would.

Yahoo News quotes Eveline Lemke, environment minister for the German state of Rhineland-Palatinate, which borders Alsace, who called for Fessenheim to be shut down immediately. She said she was "dismayed to hear about yet another incident involving a French reactor," adding that France's nuclear watchdog was "evidently failing."

Germany is facing a similar problem with Belgium, where the aging Thiange nuclear reactor, located near the Belgium-Germany border, is reaching the end of its operational life. The reactor was shut down in March 2014, but went back online in December last year, in the face of mounting concerns over cracks in its containment vessels.

About three-quarters of France's energy needs are met by nuclear power, but last summer the government passed legislation to reduce France's dependence on nuclear energy.

Bird droppings caused N.Y. nuclear reactor power outage

http://www.homelandsecuritynewswire.com/dr20160307-bird-droppings-caused-n-y-nuclear-reactor-power-outage

Mar 07 – On 14 December, one of the nuclear reactors at Indian Point nuclear power plant outside New York City was safely shut down for three days, following an electrical disturbance on outdoor high voltage transmission lines. Outside experts investigating the incident found the bird droppings were the cause of the electrical disturbance.

On 14 December, one of the nuclear reactors at **Indian Point nuclear power plant** outside New York City was safely shut down for three days, following an electrical disturbance on outdoor high voltage transmission lines. Entergy Corp., which operates the power plant, hired outside expert to analyze the incident, and they found that the culprit was what the experts call bird "streaming."

NBC News reports that in a report to the Nuclear Regulatory Commission (NRC) last month, Entergy said the automatic reactor shutdown was apparently the result of bird feces which caused an electric arc between wires on a feeder line at a transmission tower.

"If it has nowhere to send its electricity, the generator senses that and automatically shuts down," Entergy spokesman Jerry Nappi said.
Plant managers told the NRC that the plant was revising preventive maintenance procedures, additing inspections and cleaning, and installing bird guards on transmission towers.
Nappi told reporters that said he could not recall a similar incident in the past several years at Indian Point, which is located along the Hudson River north of New York City.
NRC spokesman Eliot Brenner said it was not unusual for wildlife to trigger electrical outages on transmission lines, regardless of the generation source of the electricity. "Squirrels are the biggest offenders," he said.
He said he did not know whether the NRC was tracking animal-related reactor outages. "They're kind of few and far between, but they're not uncommon," he said.

Fukushima five years on: Three lessons from the disaster

Source: http://www.homelandsecuritynewswire.com/dr20160308-fukushima-five-years-on-three-lessons-from-the-disaster

Mar 08 – It has been five years since the emergency sirens sounded at Japan's Fukushima Daiichi power plant following the massive 2011 earthquake and subsequent devastating tsunami. The partial meltdown of three reactors caused approximately 170,000 refugees to be displaced from their homes, and radiation releases and public outcry forced the Japanese government to temporarily shut down all of their nuclear power plants. The events at Fukushima Daiichi sent waves not only through Japan but also throughout the international nuclear industry. Rodney Ewing, an expert on nuclear materials, outlines three key lessons to be taken from the tragedy at Fukushima.

Lesson One: Avoid characterizing the Fukushima tragedy as an "accident"

One of the biggest lessons to be learned from Fukushima Daiichi revolves around the language used to describe nuclear disasters**. In the media and in scientific papers, the event was frequently described as an accident, but this does not properly capture the cause of the event, which was a failure of the safety analysis.**
As an example, Ewing points specifically to the domino chain of events that led to the partial meltdown at reactors 1 and 3. Following the powerful magnitude 9.0 earthquake, the power plant automatically shut down its reactors, as designed. Emergency generators immediately started in order to maintain circulation of coolant over the nuclear fuel, a critical process to avoid heating and eventual meltdown. But the tsunami that followed flooded the diesel engines that were supplying power, and so cooling could no longer be maintained.

"The Japanese people and government were certainly well acquainted with the possibility of tsunamis," said Ewing, the Frank Stanton Professor in Nuclear Security and senior fellow at the Center for International Security and Cooperation in the Freeman Spogli Institute. "Communities had alert systems. But somehow, this risk didn't manifest itself in the preparation and protection of the backup power for the Fukushima reactors. The backup power systems, the diesel generators for reactors 1 through 5, were low along the coast where they were flooded and failed. They could have been located farther back and higher, like they were at reactor 6. These were clearly failures in design, not an accident.
"This is why when I refer to the tragedy at Fukushima, it was not an accident," said Ewing, who is also a professor of geological sciences in Stanford's School of Earth, Energy & Environmental Sciences.
"When some speak of such an event

as an 'act of God,' this has the effect of avoiding the responsibility for the failed safety analysis. We need to use language that doesn't seek to place blame, but does establish cause and responsibility."

Lesson Two: Rethink the meaning of "risk"

Shortly following the disaster at Fukushima, Tokyo Electric Power Company (TEPCO) received heavy criticism for its lack of planning and response. For Ewing, this criticism speaks to a larger issue: "We need to rethink what we mean by 'risk' when we perform risk assessments. Risk is more than the loss of life and property."

Reassessing risk also begins with changing our language, Ewing said. When we say a risk like an earthquake or tsunami is rare or unexpected, even when the geological record shows it has happened and will happen again, it greatly lessens the urgency with which we ought to act and prepare.

"It can be that the risk analysis works against safety, in the sense that if the risk analysis tells us that something's safe, then you don't take the necessary precautions," he said. "The *Titanic* had too few lifeboats because it was said to be 'unsinkable.' Fukushima is similar in that the assumption that the reactors were 'safe' during an earthquake led to the failure to consider the impact of a tsunami."

When evaluating risk, Ewing recommends that we carefully consider the way in which we frame the question of risk. For example, a typical risk assessment usually only considers the fate of a single reactor at a specific location. But perhaps that question should be asked in a different way. "You could ask, 'What if I have a string of reactors along the eastern coast of Japan? What is the risk of a tsunami hitting one of those reactors over their lifetime, say, 100 years?'" he said. "In this case, the probability of a reactor experiencing a tsunami is increased, particularly if one considers the geologic record for evidence of tsunamis."

Ewing acknowledges that incorporating geological hazards into a standard risk assessment has proved to be difficult because of the long recurrence intervals of damaging events. Stanford U notes that ongoing research at Stanford Earth continues to analyze the seismic and tsunami risks around Japan and over the entire world. Professor Paul Segall and graduate student Andreas Mavrommatis analyze dense GPS networks and small repeating earthquakes to better understand unprecedented accelerating fault slip that took place in advance of the surprisingly large 2011 earthquake. Associate Professor Eric Dunham, graduate student Gabe Lotto and alum Jeremy Kozdon create mathematical models to better understand the relationships between fault motions, ocean floor properties and tsunami generation. And Assistant Professor Jenny Suckale is working to improve tsunami early warning messages that will allow populations in Indonesia to receive the specific information they need to prepare. This research, and more, helps quantify some of the geological risks that should have been considered.

Lesson Three: Nuclear energy is strongly linked to the future of renewables

In the five years since the tragedy at Fukushima, Ewing has seen a number of **ripple effects throughout the nuclear industry that will have a great impact on the future of renewable energy resources.**

In the United States, the Nuclear Regulatory Commission (NRC) has required that all reactor sites reassess risks from natural disasters. This includes not only earthquakes and tsunamis, but also flooding risks, particularly in the central United States. But this reaction wasn't shared globally.

"In countries like Germany and Switzerland, the Fukushima tragedy was the last straw," Ewing said. "This was particularly true in Germany, where there has always been a strong public position against nuclear power and against geologic waste disposal. Politically, Germany announced that it will shut down its nuclear power plants."

In a region like Germany, which is far more seismically stable than Japan, this move away from nuclear power marks an important — and expensive — transition for global energy systems. During the recent 21st Conference of the Parties meeting in Paris, Germany and a large number of other countries pledged to reduce carbon emissions.

"To me, Germany is a wonderful experiment," Ewing said. "Germany is a very technologically advanced country that is going to try to do without nuclear energy while simultaneously reducing its carbon emissions. This will require a significant investment in renewable energy sources, and that will be costly. But it's a cost that many

Germans seem willing to pay."

As recently as ten years ago, nuclear energy was quickly gaining support as a carbon-free power source. While the costs of renewables such as solar and wind remain more expensive than some fossil fuels, the steady decline in their costs and the boom of natural gas combined with the tragedy at Fukushima has once again muddied the waters of many countries' energy future.

"The biggest need for the U.S. right now is to have a well-defined energy policy," Ewing said. "With an energy policy, we would have a clear picture of how our country will address its energy needs."

Secretive Area 6 used to test aerial radiation detection equipment

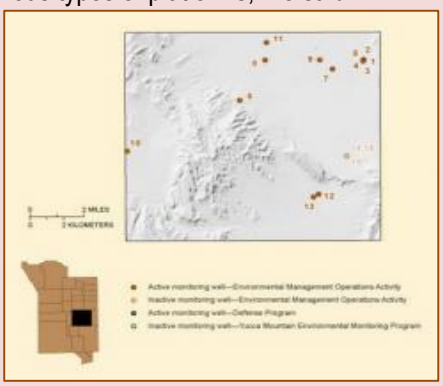
Source: http://www.homelandsecuritynewswire.com/dr20160308-secretive-area-6-used-to-test-aerial-radiation-detection-equipment

Mar 08 – Area 6, located in Nevada's Yucca Flat, once served for underground nuclear testing. The Nevada National Security Site saw more than 1,000 nuclear tests between 1945 and 1992, and information from the U.S. Department of Energy shows that four tests and six detonations took place in Area 6.

The *Las Vegas Review-Journal* reports that now, the airbase at the site, which has a 5,000-feet runway, is home to aircraft tests for federal agencies such as the Department of Defense and DHS.

National Nuclear Security Administration (NNSA) spokesman Darwin Morgan told the *Review-Journal* that the federal agencies use Area 6 to test drones equipped with sensors and away from the public eye — and to avoid being spied on in space. "We have controlled airspace and that gives them opportunities to test various types of platforms," he said.

"We do a wide variety of work for others — supporting people with sensor development activities. It evolved from the nuclear testing program. We had to have very good sensors to collect data in a split second before they were obliterated."



Map of active and inactive monitoring wells // Source: usgs.gov

The Nevada National Security Site, of which Area 6 is a part, is run by the NNSA field office in Nevada. The office works with other federal agencies to develop counterterrorism technologies. One task is developing technologies to detect radioactive materials, which terrorist could use in dirty bombs.

Tim Brown, an imagery analyst at defense information website GlobalSecurity.org, told the *Review-Journal* that based on the length of the runway, Aera 6 could be used to test drones such as Predator and Reaper drones. The area's hangar could house 15 Reapers, he estimated.

Records show that Area 6 was built in the 1950s for $9.6 million and the runway was added in 2005. The site also includes a large hangar and several smaller buildings.

The newspaper notes that the site is located a dozen miles northeast of the secretive Area 51, the existence of which was only acknowledged by the U.S. government in 2013.

The lasting legacies of Chernobyl and Fukushima

Source: http://www.homelandsecuritynewswire.com/dr20160311-the-lasting-legacies-of-chernobyl-and-fukushima

Mar 11 – It is thirty years since the Chernobyl nuclear disaster. It is also five years since the Fukushima disaster. Greenpeace says that to mark these anniversaries, the organization has commissioned reviews of scientific studies examining the continued radioactive contamination in the affected areas, and the health and social effects on the impacted populations. Greenpeace has also carried out radiation field work to study the affected areas in Russia, Belarus, Ukraine, and Japan where thousands of people still live with the effects of radiation.

Greenpeace says that there is no simple or easy way to clean up an aftermath of a nuclear accident. Indeed, this report shows that there is no such thing as a complete decontamination of radioactively contaminated areas. The disasters at Chernobyl Nuclear Power Plant (NPP) in 1986 and at Fukushima NPP in 2011 have demonstrated not only the initial consequences of major nuclear accidents, but they also left long-term consequences for human health and the environment. "These scars are still with us today and will be with us long after tomorrow," Greenpeace say.

The organization also challenges the way the nuclear industry frame these accidents by downplaying the numbers of deaths. Greenpeace says that reality is more complex. "Following a nuclear disaster, people are put under overwhelming pressures. They must evacuate their communities to avoid radiation risks. They are displaced from their friends, families, and communities for years," Greenpeace notes.

"The real risk of nuclear power, however, is inescapable for hundreds of thousands of Chernobyl and Fukushima survivors. Despite the immense suffering that accompanies losing your home or living in a contaminated environment, the scale and seriousness of these effects continue to be played down or misrepresented," Greenpeace asserts.

This report seeks to clarify how governments, reactor operators, and nuclear regulators were unprepared to deal with not only emergency evacuations immediately after the accidents, but with the long-term management of hundreds of thousands of displaced persons, as well as with the contaminated communities and agricultural lands.

— Read more in: Nuclear scars:The Lasting Legacies of Chernobyl and Fukushima (Greenpeace, 2016).

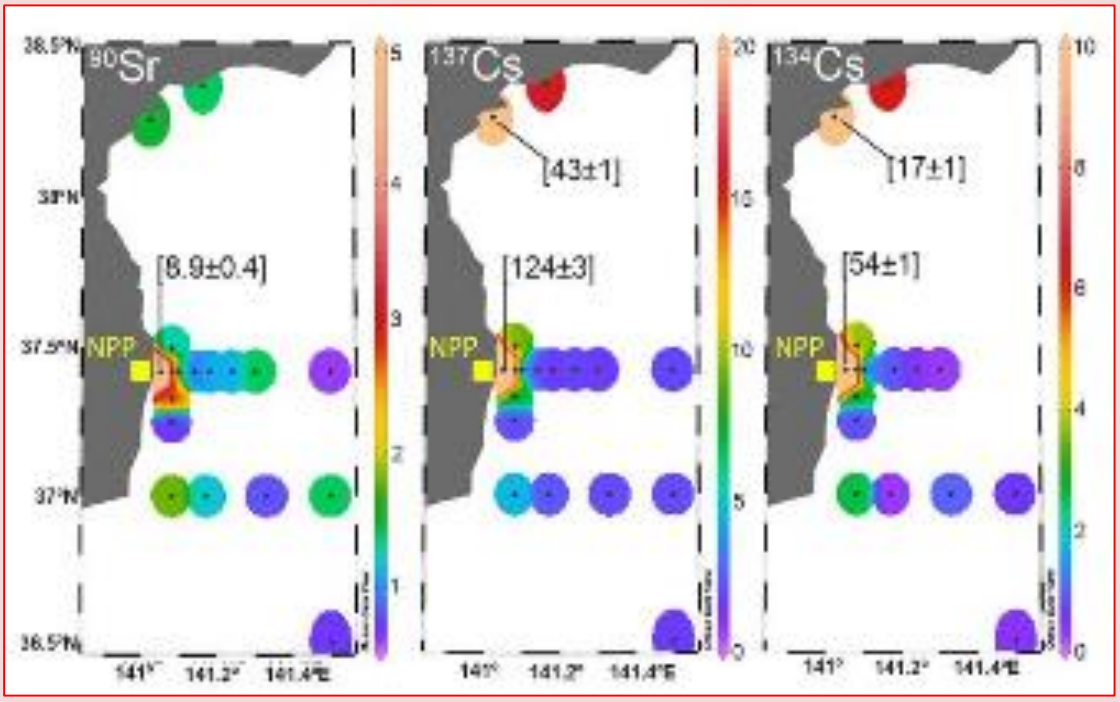
Radioactive strontium, cesium from Fukushima continue to leak to the ocean

Source: http://www.homelandsecuritynewswire.com/dr20160311-radioactive-strontium-cesium-from-fukushima-continue-to-leak-to-the-ocean

Mar 11 – Scientists from the Universitat Autònoma de Barcelona (UAB) investigated the levels of radioactive strontium and cesium in the coast off Japan in September 2013. **Radioactive levels in seawater were 10 to 100 times higher than before the nuclear accident, particularly near the facility, suggesting that water containing strontium and cesium isotopes was still leaking into the Pacific Ocean.**

Today, 11 March, is the fifth anniversary since the nuclear accident in Fukushima, Japan. The Tohoku earthquake and the series of tsunamis damaged the Fukushima Dai-ichi Nuclear Power Plant (FDNPP) causing a massive release of radioactivity into the atmosphere and the Pacific Ocean. Since then, the Tokyo Electric Power Company (TEPCO) and the Japanese authorities have focused on controlling the water flowing in and out of the FDNPP and on decontaminating the highly radioactive water used as coolant for the damaged reactors (about 300 m3 a day, cubic meter = 1000 L). This cooling water is then stored in tanks and, to some extent, being decontaminated.

UAB reports that a new study recently published in *Environmental Science & Technology*, uses data on the concentrations of 90Sr and 134,137Cs in the coast off Japan from the moment of the accident until September 2013, and puts it into a longer-time perspective including published data and TEPCO's monitoring data available until June 2015.



Concentrations of 90Sr, 137Cs and 134Cs in surface seawater in September 2013 (in Bq·m−3).

This study continues the work initiated after the accident in 2011 by some of the authors. These and other partners from Belgium and Japan are currently involved in the European FRAME project lead by Dr. Pere Masqué that aims at studying the impact of recent releases from the Fukushima nuclear accident on the marine environment. FRAME is encompassed within the European COMET project.

Seawater collected from the sea surface down to 500 m between 1 and 110 km off the FDNPP showed concentrations up to 9, 124 and 54 Bq·m−3 for 90Sr, 137Cs and 134Cs, respectively. The highest concentrations, found within six km off the FDNPP, were approximately 9, 100, and 50 times higher, respectively, than pre-Fukushima levels. Before the accident, the main source of these radionuclides was atmospheric deposition due to nuclear bomb testing performed in the 1950s and 1960s. The presence of 134Cs (undetectable before the accident) and the distinct relationship between 90Sr and 137Cs in the samples suggested that FDNPP was leaking 90Sr at a rate of 2,3 – 8,5 GBq d-1 (giga-Becquerel per day) into the Pacific Ocean in September 2013. Such a leak would be 100-1000 times larger than the amount of 90Sr transported by rivers from land to ocean. Additional risk is related to the large amounts of water stored in tanks that have frequently leaked in the past. These results are in agreement with TEPCO's monitoring data which show levels of 90Sr and 137Cs up to 10 and 1000 times higher than pre-Fukushima near the discharge channels of the FDNPP until June 2015 (most recent data included in the study).

The researchers say that the presence of 90Sr and 134,137Cs in significant amounts until 2015 suggests the need of a continuous monitoring of artificial radionuclides in the Pacific Ocean.

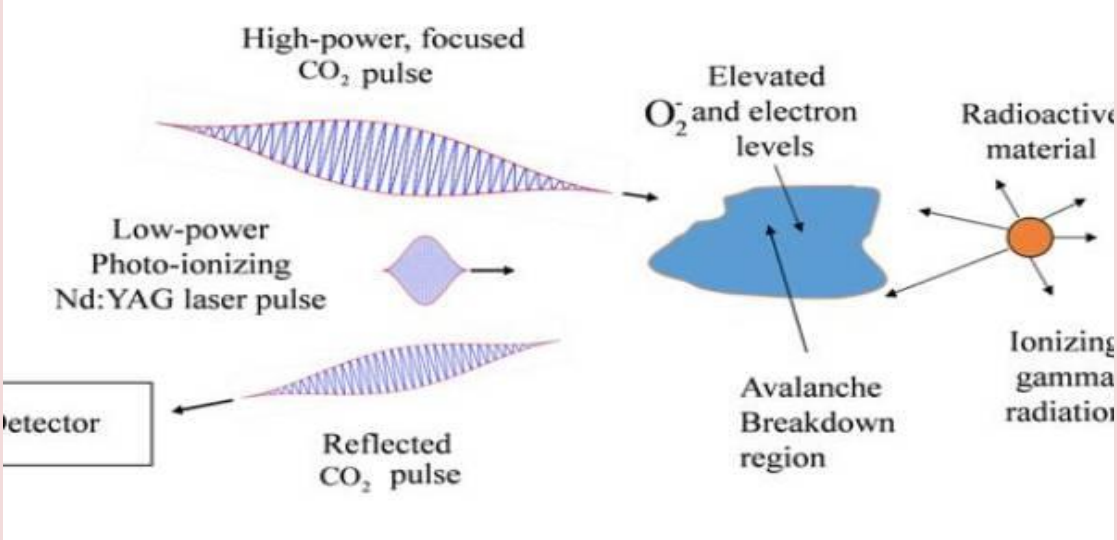
— Read more in Maxi Castrillejo et al., "Reassessment of90Sr,137Cs, and134Cs in the Coast off Japan Derived from the Fukushima Dai-ichi Nuclear Accident," Environmental Science & Technology *50, no. 1 (2016) 173-80.*

.

Remote detection of radioactive materials

Source: http://www.homelandsecuritynewswire.com/dr20160316-remote-detection-of-radioactive-materials

Mar 16 – In 2004 British national Dhiren Barot was arrested for conspiring to commit a public nuisance by the use of radioactive materials, among other charges. Authorities claimed that Barot had researched the production of "dirty bombs," and planned to detonate them in New York City, Washington D.C., and other cities. A dirty bomb combines conventional explosives with radioactive material.



Although Barot did not build the bombs, national security experts believe terrorists continue to be interested in such devices for terror plots. AIP reports that now **researchers from the University of Maryland have proposed a new technique remotely to detect the radioactive materials in dirty bombs or other sources.** They describe the method in a paper in the journal *Physics of Plasmas*, from AIP Publishing.

While the explosion of a dirty bomb would likely cause more damage than the radioactive substances it spreads, the bombs could create fear and panic, contaminate property, and require potentially costly cleanup, according to the U.S. Nuclear Regulatory Commission.

Radioactive materials are routinely used at hospitals for diagnosing and treating diseases, at construction sites for inspecting welding seams, and in research facilities. Cobalt-60, for example, is used to sterilize medical equipment, produce radiation for cancer treatment, and preserve food, among many other applications. In 2013 thieves in Mexico stole a shipment of cobalt-60 pellets used in hospital radiotherapy machines, although the shipment was later recovered intact.

Cobalt-60 and many other radioactive elements emit highly energetic gamma rays when they decay. The gamma rays strip electrons from the molecules in the surrounding air, and the resulting free electrons lose energy and readily attach to oxygen molecules to create elevated levels of negatively charged oxygen ions around the radioactive materials.

It is the increased ion density that the University of Maryland researchers aim to detect with their new method. They calculate that a low-power laser aimed near the radioactive material could free electrons from the oxygen ions. A second, high-power laser could energize the electrons and start a cascading breakdown of the air. When the breakdown process reaches a certain critical point, the high-power laser light is reflected back. The more radioactive material in the vicinity, the more quickly the critical point is reached.

"We calculate we could easily detect ten milligrams [of cobalt-60] with a laser aimed within half a meter from an unshielded source, which is a fraction of what might go into a dirty bomb" said Joshua Isaacs, first author on the paper and a graduate student working with University of Maryland physics and engineering professors Phillip Sprangle and Howard Milchberg. Lead could shield radioactive substances, but most ordinary materials like walls or glass

do not stop gamma rays.

UMD notes that the lasers themselves could be located up to a few hundred meters away from the radioactive source, Isaacs said, as long as line-of-sight was maintained and the air was not too turbulent or polluted with aerosols. He estimated that the entire device, when built, could be transported by truck through city streets or past shipping containers in ports. It could also help police or security officials detect radiation without being too close to a potentially dangerous gamma ray emitter.

The proposed remote radiation detection method is not the first, but it has advantages over other approaches. For example, terahertz radiation has also been proposed as a way to breakdown air in the vicinity of radioactive materials, but producing terahertz radiation requires complicated and costly equipment. Another proposed method would use a high-power infrared laser to both strip electrons and break down the air, but the method requires the detector be located in the opposite direction of the laser, which would make it impractical to create a single, mobile device.

So far the researchers at the University of Maryland have analyzed the feasibility of the new approach and experiments are underway to test it in the lab.

Isaacs said it would be difficult to estimate when a detection device based on the new method might be commercialized, but he didn't foresee a specific manufacturing challenge that would stand in its way.

"We specifically chose well developed technology for each component of the proposed system," he said.

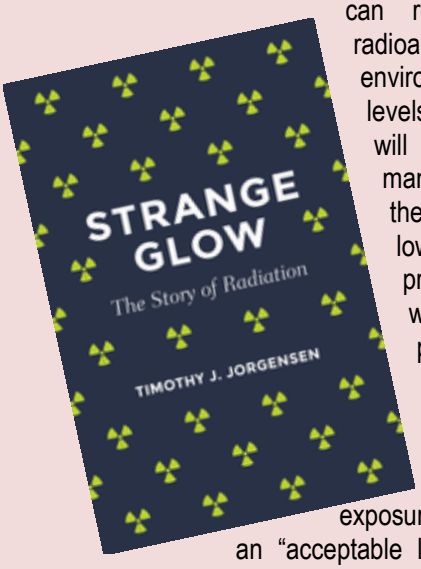
— Read more in Joshua Isaacs et al., "Remote Monostatic Detection of Radioactive Materials by Laser-induced Breakdown," Physics of Plasmas 23 (15 March 2016).

"Acceptable risk" is a better way to think about radiation exposure in Fukushima

By Timothy J. Jorgensen

Source: http://www.homelandsecuritynewswire.com/dr20160316-acceptable-risk-is-a-better-way-to-think-about-radiation-exposure-in-fukushima

Mar 16 – Five years after the Fukushima disaster, many of these people remain refugees, unable to return home for fear of radiation exposure. As the radioactivity cleanup continues, people are coming to an uncomfortable realization: although cleanup can reduce the level of radioactive contamination, the environmental radiation dose levels within the prefecture will remain elevated for many generations before they finally reach the very low levels that existed prior to the accident. So, when will it be safe for people to return to their homes and to normal life in the Fukushima Prefecture? With regard to radiation exposure, "safe" really means an "acceptable level of risk," and not everyone agrees on what is acceptable. Providing people with this risk characterization information, at the very least, is within the power of all radiation regulatory agencies, even if achieving complete cleanup of the environment is beyond their reach. This public information void about radiation risks needs to be filled. People can make their own decisions once they're empowered with credible and intelligible risk information.



On 11 March 2011, the Fukushima Prefecture of Japan experienced multiple nuclear reactor meltdowns as a consequence of an earthquake and a subsequent tsunami. **The meltdowns resulted in the release of radioactivity into the environment and 150,000 people were evacuated from their homes specifically due to radiation concerns.**

Now, five years later, many of these people remain refugees, unable to return home for fear of radiation exposure. As the radioactivity cleanup continues, people are coming to an uncomfortable realization: although cleanup can reduce the level of radioactive contamination, the **environmental radiation dose levels within the prefecture will remain elevated for**

many generations before they finally reach the very low levels that existed prior to the accident.

So, when will it be safe for people to return to their homes and to normal life in the Fukushima Prefecture? As I explain in my book, *Strange Glow: The Story of Radiation*, there may be 150,000 different answers to that question.

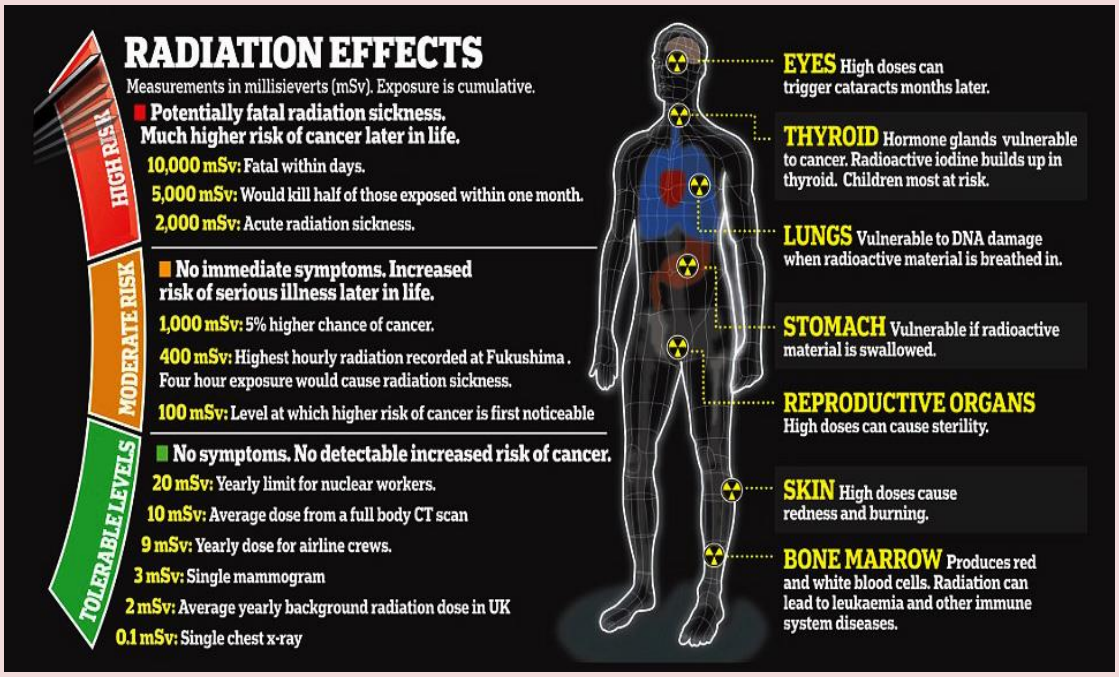
"Safe" has a fluid meaning

With regard to radiation exposure, "safe" really means an "acceptable level of risk," and not everyone agrees on what is acceptable. **The Japanese government has set an annual effective dose limit to the public of 20 millisieverts (mSv) per year above background as its remediation goal for the Fukushima Prefecture – up from one mSv per year, which was the official limit for exposures to the public prior to the incident. Although accurate numbers are hard to come by, it's been estimated that about 50 percent of the original evacuation zone remains restricted because its radiation levels still exceed 20 mSv per year, and for half of this restricted half (about 25 percent of the total evacuated area) annual dose levels still exceed 50 mSv per year.**

To the Japanese people, this raising of the annual safety limit from one to 20 mSv appears like the government is backpedaling on its commitment to safety. They suspect it's because the government knows it is not technically or financially feasible to deliver on any cleanup commitment to reduce the annual effective dose below 20 mSv, and that, of course, is true. This is the problem with moving regulatory dose limits after the fact to accommodate inconvenient circumstances; it breeds distrust.

These arbitrary-feeling radiation levels can seem very abstract to the general public. Rather than moving the dose limits around, the Japanese authorities would be better off to just explain what the actual cancer risks are at the various radiation doses and let people decide for themselves if they want to go back to their homes.

For example, receiving an annual environmental dose of 20 mSv is similar to having a single annual whole-body CT scan for medical diagnostic purposes. Epidemiological evidence indicates that the lifetime cancer risk from a single whole-body dose of 20 mSv is about 0.1 percent (or odds of 1:1,000). Put another way, if 1,000 people received a dose of 20 mSv, just one would be expected to develop cancer.



Now ask yourself: would it be worth it to me to go back to my home knowing I was facing this level of personal cancer risk? How you answer probably depends upon what you stand to lose by not returning home, in terms of your livelihood, possessions and finances. It also may depend upon what other personal behaviors you have that

affect your cancer risk, such as smoking.

Letting individuals choose

Providing transparent risk characterizations for various radiation doses and allowing people to decide for themselves what radiation dose they are willing to accept is better than setting opaque "safety limits" that are enforced uniformly upon everyone. That way, individuals can choose their own "acceptable risk."

And this is particularly true if regulatory agencies are going to start moving those safety limits around to suit the circumstances. The risk estimates for 20 mSv were the same before the Fukushima accident as they were after the accident. The risk per unit dose doesn't change with the circumstances.

Regulatory limits don't represent thresholds for safety. The limits are merely arbitrary lines that are drawn in the sand by some regulatory body, marking the fuzzy border between the dose levels that entail "acceptable" versus "unacceptable" amounts of risk. If you don't like where that line has been drawn, pick up a stick and draw a different line for yourself. When it comes to risk tolerance, different people will always draw different lines.

These are the issues the people from the Fukushima Prefecture are now facing with regard to radiation. It's not necessary that all of them arrive at the same conclusion about their personal safety. Whether or not to return should be an individual choice, and people can make different decisions, all equally valid. But they do need the facts to make a credible assessment of their personal risk level, in accord with their individual circumstances.

Providing people with this risk characterization information, at the very least, is within the power of all radiation regulatory agencies, even if achieving complete cleanup of the environment is beyond their reach. The mayor of one town, where 14,000 people were evacuated after the accident, was quoted in *Science* saying:

There has been no education regarding radiation. It's difficult for many people to make the decision to return without knowing what these radiation levels mean and what is safe.

This public information void about radiation risks needs to be filled. People can make their own decisions once they're empowered with credible and intelligible risk information.

***Timothy J. Jorgensen** is Associate Professor of Radiation Medicine, Georgetown University.*

We still don't really know the health hazards of a nuclear accident

By Claire Corkhill

Source: http://www.homelandsecuritynewswire.com/dr20160317-we-still-don-t-really-know-the-health-hazards-of-a-nuclear-accident

Mar 17 – Five years after the nuclear disaster in Fukushima and thirty years after the Chernobyl accident, scientists are still disagreeing about the impact on human health — such as how many people have got cancer as a result and how dangerous the exclusion zones currently are.

In Fukushima, residents are forbidden to permanently return to their homes within the exclusion zone. And in Ukraine the city of Pripyat, 4 km from Chernobyl, still remains largely deserted. While some experts have recently said that the areas surrounding these accidents are not as dangerous as previously thought, others are concerned about the high levels of radiation remaining in plants and animals, particularly seafood.

It is true that large doses of radiation can be fatal. Marie Curie, who carried radium in her pockets, eventually died of cancer. But small doses of radiation are all around us, every day. They are measured in millisieverts (mSv). **The average person in the United Kingdom receives a dose of 2.7 mSv per year (or 7.8 mSv per year if you happen to live on top of granite in Cornwall, which emits radon gas).** A transatlantic flight will give you a dose of 0.08 mSv from cosmic radiation. Even eating a humble banana will expose you to 0.001 mSv of radiation, from the tiny amount of radioactive potassium inside. But it is only really when you are exposed to annual radiation doses of more than 1,000 mSv that things start to get a bit hairy.

The type of radiation you are exposed to matters too. Some types only cause severe damage when ingested (lodged in the stomach or lungs). Other types can penetrate the body from outside, putting you at risk just walking by the source.

In the case of an accident, we have to take into account what sort of radiation is released – and how much – to take the right precautions. When radioactive gas from the Three Mile Island reactor in the United States was released after an accident in 1979, people were advised to stay indoors and to keep farm animals under cover. Later, pregnant women within a 20-mile radius of the reactor were recommended to evacuate. Within three weeks, 98 percent of the evacuees had returned. These were sensible precautions — after eighteen years of monitoring, no unusual health trends were reported. People only received an average dose of 0.08 mSv.

In the far more severe Chernobyl accident, radioactive elements including iodine-131 and cesium-137 were spread by graphite fires across a wide area. People in the vicinity of the fires (mainly firefighters) were exposed to fatal doses of radiation (300,000 mSv per hour). Nearly a third of them died in the months following the accidents.

But for people who have lived in the most contaminated areas of Belarus, the Russian Federation and Ukraine at some point since the accident it is more difficult to estimate the impact. They have received relatively low doses of radiation over a long time, estimated as 1 mSv per year on average. While there was an initial spike in thyroid cancer cases, it is difficult to work out whether other cancers in this population are due to radiation or other lifestyle factors.

So is Chernobyl now safe? If you take a tour of it today, expect radiation doses of 0.2 to 20 mSv per hour depending on how close to the reactor you go. The levels of radioactivity from radioactive cesium and strontium have already dropped by half – and in 30 years time they will half again. After ten "half-lives" (300 years) the radioactivity would decayed to normal background levels.

Relocation versus radiation

But the effect of radiation is not everything. **More than 116,000 people from the area surrounding Chernobyl were evacuated but about 1,200 refused.** These so-called "Babushkas of Chernobyl," all over 40 at the time of the accident, defiantly ignored the law

and decided to take their chances against the radiation rather than being displaced from their beloved homes and communities. More than 200 of these remain living in the area today.

And perhaps they were right to stay — the World Health Organization (WHO) cites relocation from Chernobyl as a cause of stress, anxiety, mental illness and "medically unexplained physical symptoms". To this day, we do not know the true cost of relocation on lives because it was not formally measured.

The radioactive fallout at Fukushima was less than 10 percent of that at Chernobyl. A number of scientists have suggested the evacuation was therefore too cautious. Others recommend that the acceptable radiation dose to the public set by international organizations is too conservative and could be significantly increased without causing harm.

There seems to be little evidence to suggest that lower doses of radiation causes a big risk. It has even been suggested that the body may have some sort of cellular repair mechanisms to deal with lower doses. The problem is we simply just don't know for sure – the only way to find out is to study the people who have been exposed to these low doses over their entire lives, an enormous task that not everyone is willing to take part in.

The people of Fukushima, except those in the worst contaminated areas, will eventually be encouraged to return to their homes. In the absence of better understanding, scientific and political arguments about how safe the radiation levels are will continue. What is abundantly clear, though, is that we need to understand the comparative health effects of radiation versus relocation. Developing a new approach in our response to nuclear accidents and the decisions

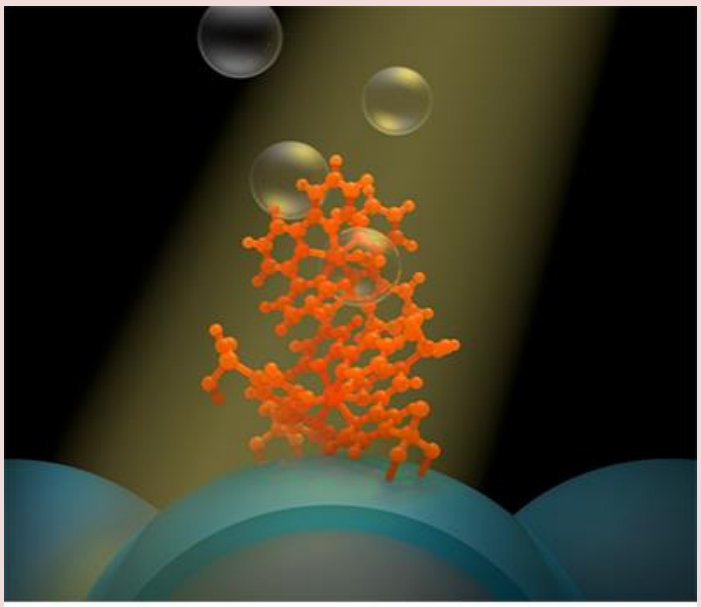
that are made in their immediate aftermath is vital so that we can avoid unnecessary panic and evacuation — something virtually all scientists agree on.

Claire Corkhill is Research Fellow in nuclear waste disposal, University of Sheffield.

Researchers crack 50-year-old nuclear waste problem, making waste storage safer

Source: http://www.homelandsecuritynewswire.com/dr20160318-researchers-crack-50yearold-nuclear-waste-problem-making-waste-storage-safer

Mar 18 – **Researchers at the University of North Carolina at Chapel Hill have adapted a technology developed for solar energy in order to selectively remove one of the trickiest and most-difficult-to-remove elements in nuclear waste pools across the country, making the storage of nuclear waste safer and nontoxic — and solving a decades-old problem.**



Solar fuel. Tom Meyer's new system generates hydrogen fuel by using the sun's energy to split water into its component parts. After the split, hydrogen is stored, while the byproduct, oxygen, is released into the air. Image courtesy: Yan Liang

The work, published in *Science*, not only opens the door to expand the use of one of the most efficient energy sources on the planet, but also adds a key step in completing the nuclear fuel cycle — an advance, along with wind and solar, that could help power the world's energy needs cleanly for the future.

"In order to solve the nuclear waste problem, you have to solve the americium problem," said Tom Meyer, Arey Distinguished Professor of Chemistry at UNC's College of Arts and Sciences, who led the study.

UNC notes that americium does not have the same name recognition as a plutonium and uranium, but researchers have been trying to remove it from nuclear waste for decades. Several groups initially succeeded, only to be met with several subsequent problems down the line, rendering the solution unfeasible. Meyer and his team, including Chris Dares, who spearheaded the project, have found a way to remove the radioactive element without encountering downstream problems that have hindered progress.

The technology Meyer and Dares developed is closely related to the one used by Meyer at the UNC Energy Frontier Research Center of Solar Fuels to tear electrons from water molecules. **In the americium project, Meyer and Dares adapted the technology to tear electrons from americium, which requires twice as much energy input as splitting water. By removing those three electrons, americium behaves like plutonium and uranium, which is then easy to remove with existing technology.**

Dares describes that nuclear fuel is initially used as small solid pellets loaded into long, thin rods. To reprocess them, the used fuel is first dissolved in acid and the plutonium and uranium separated. In the process, americium will either be separated with plutonium and uranium or removed in a second step.

Meyer and Dares worked closely with Idaho National Laboratory (INL), which provided research support and technical guidance on working with nuclear materials. Most of the experiments were carried out in the laboratories at Idaho, which provided a safe area to work with radioactive material. At present, INL and UNC-

Chapel Hill are in discussion about extending the research and to possible scale up of the technology.

"With INL working with us, we have a strong foundation for scaling up this technology," said Dares. "With a scaled up solution, not only will we no longer have to think about the dangers of storing radioactive waste long-term, but we will have a viable solution to close the nuclear fuel cycle and contribute to solving the world's energy needs. That's exciting."

Hezbollah threatens it will attack Israel's nuclear facilities in future war

Source: http://www.homelandsecuritynewswire.com/dr20160322-hezbollah-threatens-it-will-attack-israel-s-nuclear-facilities-in-future-war

Mar 22 – Hassan Nasrallah, Hezbollah leader, on Monday threatened that in the event of another war between Hezbollah and Israel, his Iran-supported Shi'ia Lebanese militia will strike all targets in the Jewish state "without any limits."

"If the Israeli army escalates its aggression against Lebanon, Hezbollah will strike all the strategic targets in the occupied Palestinian territories, including the nuclear facilities," Nasrallah said in an interview with Hezbollah-leaning TV station Al Manar.

Nasrallah stated that Israel is aware of the quantity and quality of Hezbollah's rocket arsenal.

In addition, he claimed that "Hezbollah possesses all the details about the positions of the petrochemical, biological and nuclear facilities across Palestine."

The *Jerusalem Post* reports that Nasrallah stressed that Hezbollah does not want to start a war with Israel, but that his organization "does not grant Israel any security guarantees."

Nasrallah criticized the six-member Gulf Cooperation Council (GCC) for their 11 March decision three weeks ago to designate Hezbollah as a terrorist organization.

"Israel does not respond to the Arab regimes' demands, but some Arab countries work for the sake of the Israelis," he said.

The Sunni Muslim-dominated GCC — Saudi Arabia, the UAE, Bahrain, Kuwait, Oman, and Qatar – in 2013 imposed sanctions on Hezbollah after the Lebanese militia began to send its fighter to Syria to help the beleaguered regime of President Bashar Assad.

New sensor rivals dogs in detecting explosives

Source: http://www.homelandsecuritynewswire.com/dr20160222-new-sensor-rivals-dogs-in-detecting-explosives

Feb 22 – Dogs have been used for decades to sniff out explosives, but now a University of Rhode Island scientist and his team have come up with another way to detect bombs: sensors.

Otto J. Gregory, professor of chemical engineering and co-director of URI's Sensors and Surface Technology Partnership, has developed a sensor that can detect explosives commonly used by terrorists. One of these explosives is triacetone triperoxide, or TATP.

Triacetone triperoxide has been used by terrorists worldwide, from the 2001 "shoe bomber" Richard Reid to the suicide bombers who attacked residents of Paris in November. The explosive is relatively easy to make with chemicals that can be bought at pharmacies and hardware stores, attracting little attention from authorities.

URI reports that Gregory's work focuses on creating a sensor that continuously detects vapors emitted by the explosive.

Here is how it works: A tin oxide catalyst in the sensor causes the triacetone triperoxide molecule to decompose at a specific temperature. The sensor monitors the amount of heat released by the decomposition and triggers an alarm.

"We initiate the decomposition of the molecule using a catalyst and then measure the heat released,'' says Gregory, of Kingston. "If the amount released can be measured, we can identify the molecule responsible.''

What makes Gregory's research — published in the journal Electrochemical Society Transactions — even more significant is that his sensor could be used round-the-clock in various public places, from boarding areas in airports and subways to ports of entry for cargo containers.

"If someone carrying TATP were to walk by in a relatively confined space, the sensor could detect it,'' he says. "It works 24/7.''

Gregory says sensors are the future of trace explosive detection systems. Not only does his sensor detect TATP, it can also determine if ammonium nitrate, TNT and other explosives are present.

Dogs can still be trained to track down explosives at very low levels, but sensors are a better long-term solution to continuous screening of these substances, Gregory says.

"Dogs have short attention span and can be distracted,'' he says. "For the first hour or so, they're really good at detecting explosives. Then their minds wander. It's like a little kid. What our sensors do is continuously sniff 24/7. Dogs need to rest for periods of time."

The next step is to reduce the sensor to a manageable size — maybe the size of a shoebox or smaller. Meanwhile, Gregory and his colleagues at URI will continue to play a key role in making the world a safer place.

"URI professors and students are doing cutting edge research in the areas of explosive characterization and detection,'' he says. "We're trying to make buildings, stadiums, airports and subways safer for the traveling public. Our research will go a long way in achieving this goal.''

URI notes that Gregory's work is funded by the U.S. Department of Homeland Security. In 2008, URI was awarded $5.15 million from the federal agency to launch a Center of Excellence in Explosives, Detection, Mitigation, Response and Characterization for research on explosives and detection of explosives. URI has received additional funding since then.

"Faculty and students at URI have partnered with the Department of Homeland Security to research explosives and explosive detection methods,'' Gregory says. "In the process we have addressed some of the safety and security concerns, both here in the United States and abroad.''

Gregory's research team is also working on sensors for jet engines that would make aircraft safer and more reliable. Part of this research focuses on ways to eliminate messy wiring by relying on wireless sensor technologies.

Isis making deadly suicide bombs and IEDs using freely available civilian components from around the world

Source: http://www.independent.co.uk/news/world/middle-east/isis-deadly-suicide-bombs-ieds-legal-civilian-components-from-world-islamic-state-daesh-a6893856.html

Feb 25 – Isis is manufacturing ever more sophisticated and devastating suicide bombs and improvised explosives using civilian components from countries around the world, an investigation has revealed.

Most of the equipment, including chemicals, fertilisers, wire and electronics, is being funnelled through Turkey to the group's territories, according to a report by Conflict Armament Research (CAR).

White petroleum drums manufactured in Iran found near the Mosul Dam in Iraq, February 2015

The EU-funded group analysed improvised explosive devices (IED) collected over 20 months on Iraqi and Syrian frontlines to reveal how the so-called Islamic State has been able to amass its arsenal at an unprecedented speed.

James Bevan, executive director of CAR, told the *Independent*militants are using explosives in terror attacks, military offensives and to defend territory.

He said the group was continually experimenting, refining and creating new types of IEDs ranging from suicide and car bombs to landmines, booby traps and improvised mortars.

The inventions have taken a heavy toll on the Peshmerga, Shia militias, Kurdish YPG, opposition rebels and other forces attempting to take back Isis territory.

"Whenever they try to liberate an area, that area is absolutely littered with IEDs and they are causing the greatest amount of casualties," Mr Bevan said. "It's on a larger scale than we've seen in recent conflicts."

The report found that most of the components are gained by exploiting legal agricultural and mining sectors where the necessary chemicals and parts are freely available.

A white petroleum drum manufactured in Iran found in Makhmour, Iraq, in January 2015

It identified 51 companies in 20 countries involved in the deadly supply chain, including Nokia, which is now owned by Microsoft, and firms headquartered in Europe and the US.

Although CAR concluded that issues stretched far beyond the nations surrounding Iraq and Syria, Turkey was found to be the

main "choke point" in the enterprise.
Mr Bevan said: "There is a lot of farming and a lot of demand for chemicals, some of which are precursors in the manufacture of explosives.
"There's certainly a requirement to tighten up regulations and government oversight, and if the companies themselves didn't know their products were being used, they should be aware now."
He claimed that CAR investigators had seen cars, lorries, food, oil and people crossing parts of the border between Turkey and northern Syria in recent months.
"If you are in YPG-controlled territory, the border is virtually hermetically sealed, whereas if the border is with Isis-controlled areas it was and still is virtually open," Mr Bevan added.
The Turkish government failed to respond to CAR's requests for information but other mentioned parties, including Nokia, aided the non-governmental organisation with documents and invoices.
All companies and countries named have been informed of the findings as investigations continue in Ramadi and other territory recently retaken from Isis.
The *Independent* had not received a response from Nokia or Microsoft at the time of going to press.

The report's key findings:

- **Turkey:** 13 companies - components including chemical precursors, containers, detonating cord, cables, and wires, which Turkish companies either manufactured or sold in Turkey before Isis forces acquired them in Iraq and Syria.
- **India:** Seven companies - manufactured most of the detonators, detonating cord, and safety fuses documented by CAR's field investigation teams. Under Indian law, transfer of this material requires a licence and all components documented by CAR were legally exported to entities in Lebanon and Turkey.
- **Japan, Switzerland, and the United States:** Same electronic components consistently used in the construction of one type of remote-controlled IED used in Iraq. Companies headquartered in Japan, Switzerland, and the United States manufactured the microcontrollers and transistors used in the devices.
- **United Arab Emirates and Iraqi Kurdistan:** Isis in Iraq uses 105 Type RM-908 Nokia phones to manufacture of a specific type of remote-controlled IED. Of 10 such telephones documented by CAR, eight had been supplied to intermediaries in the United Arab Emirates and two had been sent to distributors in the city of Irbil, Iraqi Kurdistan.

Why ISIS Is Building Mad Max Truck Bombs

Source: http://www.popularmechanics.com/military/weapons/news/a19555/why-isis-is-building-mad-max-truck-bombs/

Feb 22 – The members of ISIS have more in common with the war boys of *Mad Max: Fury Road* than ruthless violence, desert surroundings, and a yearning to die in combat ("I live, I die, I live again!").

Robert Bunker, a counterterrorism expert at TRENDS Research & Advisory, warns that the latest ISIS tactic is to field car bombs fitted with Mad Max-style improvised armor to carry out suicide attacks on protected targets, and that such tactics might spread to the U.S. and Europe.

The Evolution of the Car Bomb

This new development represents a third wave of vehicle-borne bombs. The first wave consisted of stationary vehicles. That goes all the way back to "Buda's Wagon," a horse-drawn wagon packed with explosives and metal, which anarchist Mario Buda used for an attack on Wall Street that killed 40 people in

1920. Notorious "Type 1" attacks also include the World Trade Towers bombing in 1993 and the Oklahoma City bombing in 1995. I was in London during the Staples Corner bombing carried out by the IRA, and like thousands of people I had my commute disrupted by a white van left on the road by an overpass. Several hours later the van exploded.

The stakes were raised in the 1980s with a new style of vehicle bomb attack, when Shia militias and Hezbollah started using moving vehicles with suicide drivers. Their initial targets were Israeli military convoys, but this sort of "Type 2" attack was employed against the American embassy in Beirut in April 1983, killing 63 people, and also six months later in the attack on a Marine barracks, which killed more than 200 U.S. servicemen. Type 2 tactics have grown more sophisticated, too, with the use of multiple vehicles, sometimes one to break through perimeter defenses and another to attack the installation behind, or with several vehicles attacking at the same time supported by gunman.

Clearly, the best way to stop such an attack is to blow up the vehicle before it can get close enough to do any damage to the target. And that explains the rise of this new kind of vehicular warfare: "Type 3" vehicle bombs that are protected by armor. The vehicles involved in previous attacks have been, for the most part, civilian cars and trucks that are vulnerable even to small-caliber fire. Not so for armored cars. Bunker describes this threat in detail in a new report on "Daesh/IS Armored Vehicle Borne Improvised Explosive Devices."

Bunker calls the devices "armored vehicle-borne improvised explosive devices" (AVBIEDs), and notes reports of their use by ISIS in Iraq and Syria since 2013. Such vehicles include cars and trucks with "applique armor" welded on, as well as armored bulldozers, dump trucks, and even captured armored Hummers and M113 personnel carriers.

ISIS lacks heavy artillery and airpower, but of late it's been using these robust vehicle bombs as a substitute. For example, during fighting in Ramadi, an armored bulldozer led the assault, followed by thirty other vehicles with improvised armor. Ten of these were said to be as being as powerful as the Oklahoma City bomb, which had an explosive equivalent to 5,000 pounds of TNT and leveled entire city blocks.

Now, the tactic is spreading.

"No evidence exists that AVBIED manuals or instructions are shared online," Bunker tells Popular Mechanics. "However the existence of IS videos and still photos of these devices online and in social media suggest that knowledge of AVBIEDs has now widely proliferated amongst insurgent and terrorist groups."

Rolling, Armored IEDs

The AVBIEDs come with different levels of protection depending on the environment and the need to operate covertly. Bunker says the heaviest versions are those that have been seen in Syria and Iraq. "These are full-out armored vehicles like armored bulldozers with explosives on them," he says. "Mad Max vehicles with heavy armor plate"

With such thick armor, they're difficult to stop: "7.62 armor-piercing is probably useless, and .50 caliber is questionable. You have to go for the tracks or wheels." Instead, he recommends using shoulder-fired anti-tank weapons to destroy these vehicles.

These "Type 3" attacks aren't limited to warzones. The lightest level of improvised armor theoretically might be used in future attacks in the U.S. or Europe. Think of covert, interior armor that would not be obvious on the street. Such a vehicle could get close enough so that defensive fire from carbines and handguns would not be enough to stop it. "In such a scenario, the AVBIED has a much greater likelihood of reaching its intended detonation," says Bunker. The most likely use for such a vehicle would be to clear the way for bigger and more conspicuous AVBIEDs following in a second wave.

This isn't the final stage of vehicular warfare. A recent "Jihadi University" video shows ISIS working on a driverless car for terror attacks.

"From a martyrdom perspective, a driverless AVBIED makes little sense," Bunker says. "Where it might make sense is against a heavily defended target in which the driver—even a fanatical one in an armored cab—has little hope of surviving the assault on the way to the target."

Still, there is a counter to every weapon, and it is entirely possible that incoming armored, driverless truck bombs will be identified and taken out at a safe distance by defensive bazooka drones. *Mad Max* had better raise his game.

Suicide bomb detector moves close to commercialization with Sandia engineer's help

Source: http://www.homelandsecuritynewswire.com/dr20160226-suicide-bomb-detector-moves-close-to-commercialization-with-sandia-engineer-s-help

Feb 26 – **On the chilling list of terrorist tactics, suicide bombing is at the top. Between 1981 and 2015, an estimated 5,000 such attacks occurred in more than 40 countries, killing about 50,000 people. The global rate grew from three a year in the 1980s to one a month in the 1990s to one a week from 2001 to 2003 to one a day from 2003 to 2015.**

Terrorism experts say suicide bombings are pervasive because they generate publicity and require little expertise, resources or planning. Perhaps most importantly, they are almost impossible to prevent.

Until now, said Albuquerque businessman Robby Roberson. Sandia Lab reports that this company R3 Technologies and a

group of other small businesses are developing a way to prevent suicide attacks by detecting concealed bombs before they go off. After a frustrating start, the group decided it needed more technical help and turned to the New Mexico Small Business Assistance (NMSBA) program, which pairs entrepreneurs with scientists and engineers at Sandia and Los Alamos national laboratories.

"The suicide bomber can walk into a crowded place unnoticed and inflict a horrifying amount of death and destruction," Roberson said. "It's very hard to stop. There was no technology to deal with it."

R3 found a partner in Sandia sensor expert JR Russell who has helped bring the company's **Concealed Bomb Detector, or CBD-1000,** close to commercialization over the past two years. "JR has been all over it and really turned things around for our company," Roberson said. "He brings in sharp people from Sandia. I love working with those guys."

Russell said his role largely has been to develop ways to measure how well the technology works. He zeroed in on the device's accuracy by analyzing false positives and pushed to redevelop software so it would more reliably detect a bomb threat. "After getting to know Robby and the team I got more and more interested in the problem," said Russell, who enlisted Sandia engineers Matt Erdman and Michael Bratton in the project. "The technical part of me took over. Engineers want to validate the model and we needed to validate the performance of Robby's system. We threw out a lot of the existing technology. Early versions were a good start, but not where the technology needed to be."

The CBD-1000 bomb detector (left) is trained on a mock suicide vest

Screening for bombers in public places

The CBD-1000 uses X-band radar to detect metallic and nonmetallic explosives. Roberson said it can detect ball bearings, glass, nails, ceramics, rocks and other materials frequently used as shrapnel in suicide vests.

The device is designed to detect bombs that current metal detector technology would miss and is intended for screening areas, such as airports, embassies, public and government buildings, border crossings, transportation hubs, and military compounds. It is portable and could also be used at large special events.

The CBD-1000 is the size of a cereal box, weighs about 13 pounds and is mounted on a tripod. It is electric or battery powered and works with proprietary embedded software. The device uses a spread spectrum, stepped, continuous wave radar to bounce a signal off a subject. The software analyzes both horizontal and vertical polarized signals to determine the presence of a potential threat. "If the person is not carrying a threat, the return signal is in the same polarity as when it was transmitted," Roberson said. "A threat will rotate the polarity of the signal, and it comes back differently."

The system sets up in about fifteen minutes and an operator, who does not need a working knowledge of radar, can be trained in thirty minutes. The scan takes about 1.3 seconds from nine feet away. Roberson said the team is refining algorithms that will allow people in motion to be scanned at greater distances.

"We're working toward an instantaneous scan so a person can be checked while moving through the beam field. And we hope to extend the range to 100 feet," Roberson said. "We want to take movement out of the equation. People who want to

protect their citizens want to detect at a distance, keep the threat away. They want to scan crowds and stop threats before they get too close."

First system didn't work

Sandi Lab notes that the original technology was developed by another Albuquerque company in the early 2000s as a hand-held, radar-based sensor that police could use to scan people moving at a distance who they suspected might be armed. It evolved into a stationary system. After years of development, the technology just didn't work. "It became apparent that the system was not completely accurate," Roberson said.

Roberson and his father, Coda Roberson, founded R3 Technologies to further develop and commercialize the technology. They approached Sandia for help through NMSBA and added partners including Manuel Rangel of APPI Inc. in Las Cruces, the acclaimed radar scientist Don McLemore of McLemore Enterprises LLC in Albuquerque, Lawrence Sher of Wind Mountain Research Associates in Albuquerque and Julie Seton of Indelible Enterprises in Las Cruces.

"When JR came onboard we all took a hard look at what we had, what it did and how it worked," Roberson said. "JR came at this problem from a different point of view. He wanted to know everything about it. He helped us realize we had to go in a completely different direction. We reverse engineered the hardware and software. I can't stress enough how important JR was."

Russell said the Sandia employees studied noise surrounding the radar signal and how it impacted true positives and true negatives. They found a way to reduce noise and strengthen the signal, improving accuracy by minimizing false positives. "If the signal is bigger than the noise, it can scan people as they're walking. They don't have to stop," he said. "These breakthroughs will enable new applications in security of the future and will increase the marketability and desirability in the field of the CBD-1000."

Continuing the NMSBA collaboration

Roberson hopes to go to market this year after working with Sandia to further improve the machine's speed, distance and accuracy. He said **the CBD-1000 will cost about $50,000 and that several hundred units have been produced.** The device is patented, and the company has received inquiries from Pakistan, Afghanistan, Singapore, Kuwait, Saudi Arabia, and Nigeria, he said.

Russell said he enjoys helping a small business. "It's good for our community," he said. "Helping someone succeed helps us succeed, too, as a lab. I get to see science though the eyes of business people. And I've learned things that will help me in my work."

Russell said R3's suicide-bomb detector resonates with Sandia's national security mission. "We want to help our nation protect our people, our assets," he said. "If we can save one life, we can make a difference. The opportunity to make us safer from attacks is one of the idealistic things that drive us."

Sandia Lab notes that NMSBA was created in 2000 by the state legislature to bring national laboratory technology and expertise to small businesses in New Mexico, promoting economic development with an emphasis on rural areas. The program has provided more than 2,300 small businesses in all 33 New Mexico counties with $43.7 million worth of research hours and materials.

"The project between Sandia and R3 Technologies is a compelling example of how NMSBA is not only helping a New Mexico small business but also helping Sandia's national security mission," said Jackie Kerby Moore, Sandia's manager of Technology and Economic Development. "We applaud JR and his team for helping the company commercialize its technology."

IS suicide bombers penetrate Iraq army HQ, kill general

Source: http://www.terrorismwatch.org/2016/03/is-suicide-bombers-penetrate-iraq-army.html

Mar 01 – **Four Islamic State group suicide bombers infiltrated an army headquarters west of Baghdad, killing an Iraqi general and five other soldiers,** army and police officers said on Tuesday.

The bombers attacked a regimental headquarters in the Haditha area of Anbar province late on Monday, **killing Staff Brigadier General Ali Aboud, Lieutenant Colonel Farhan Ibrahim and four others, the sources said.**

Major General Ali Ibrahim Daboun, the head of the Al-Jazeera Operations Command, said one suicide bomber blew himself up inside Aboud's office, while the other three detonated explosives elsewhere inside the headquarters.

Seven soldiers were also wounded in the attack, Daboun said.

Colonel Faruq al-Jughaifi, the Haditha police chief, confirmed the attack, saying it took place near a major dam in the area, and that the bombers were dressed in military uniforms.

Jihadist group IS claimed the attack in a statement posted online but mentioned only two suicide bombers saying they were Syrian nationals.

IS overran swathes of Iraq, including large parts of Anbar, in a sweeping offensive launched in June 2014, but has largely been on the defensive in the province since the middle of last year.

Iraqi tribesmen and security personnel defending Haditha, which lies near the country's second largest dam, have held off IS for more than 18 months with the help of air strikes by a US-led coalition.

The war with IS has taken a heavy toll on senior Iraqi officers in Anbar.

Two heads of the Anbar Operations Command were wounded in 2015, while the commanders of a division and a brigade were killed in Anbar in April of that year. The province's governor was wounded in 2014. Senior army and police commanders have also been killed in other provinces.

The Animals That Sniff Out Tuberculosis, Cancer, and Landmines

Source: http://www.psmag.com/health-and-behavior/the-animals-that-sniff-out-tuberculosis-cancer-and-landmines

Feb 27 – In a small, hot room in a compound located in Tanzania's lush southern highlands are three white-clad technicians, a glass-and-metal chamber, and a large brown rat named Charles.

After being gently dropped into the chamber, Charles aims his long snout toward the first of a series of 10 sliding metal plates in the chamber's base. A technician swiftly opens it, revealing a small hole. Charles sniffs at it ... and moves on. The hole is re-closed, and there's a clink of metal as the next plate is yanked back. This time, Charles is gripped. He sniffs hard, scratching at the metal, the five claws on each paw splayed with the pressure. The technician calls out "Two!"

Over by the window, her colleague is holding a chart, which he keeps raised so the others cannot see it. He inserts a tick. I glance over. The chart is a grid of small boxes, 10 across

by 10 down, each marked with an alphanumeric code. Two of the boxes in each line are shaded grey. The tick has been placed in one that is white. It's highly possible that Charles has just saved someone's life.

Charles is an African giant pouched rat, a species endemic to sub-Saharan Africa. He's also a pioneer, one of 30 of his species that live and work here in Morogoro, a few hundred kilometers west of Tanzania's largest city, Dar es Salaam, on a program to sniff out tuberculosis (TB).

TB is a disease that can destroy the lungs. About nine million new cases are diagnosed worldwide every year, one-quarter of them in Africa. Africa also has the highest TB death rate per head of population. Antibiotics can cure TB, but it's fatal if untreated, and many patients are never diagnosed. This is partly because the 125-year-old microscope-based test used across Tanzania (and in many other cash-strapped countries) picks up only about 60 percent of cases, a figure that drops as low as 20 percent for people also infected with HIV.

This is where Charles the rat comes in. Charles and his rat colleagues sniff cough-and-spit samples provided by suspected TB patients. The rats aren't infallible, but they do detect about 70 percent of cases, and it doesn't matter to them if a patient has HIV—which matters a great deal in Tanzania, where about four in every 10 people with TB are HIV positive.

This particular morning Charles has sniffed 100 samples, missing one that has been identified as positive by the public clinic—shaded grey on the chart—but identifying 12 new suspected cases, which will now go for secondary checking.

The next rat brought into the testing room, a sleeker, bigger-eared, three-and-a-half-year-old named Vladić (after a Bosnian Croat footballer; many of the rats are named after footballers), is even speedier than Charles. There's a rapid clatter of metal plates being pulled back and replaced. The two technicians manning the chamber call out numbers: "Three! ... Nine!" Ticks rapidly accumulate on a fresh copy of the same chart. About 15 minutes later, Vladić has correctly identified eight out of 10 clinic-positives, and also 15 new suspects.

Fidelis John, the training supervisor, is looking on. Unlike the standard lab rat, *Rattus norvegicus*, the African giant pouched rat (*Cricetomys gambianus*) is not a species that has been bred over many generations to cooperate well with people. Is it very hard to train them to perform like this? "It's not easy," he says, smiling. "But it's possible. When a rat doesn't perform well, it is usually the trainer who is to blame."

Around the world, other animals—mostly dogs—are being used experimentally to screen human samples for disease; the TB-sniffing rats of Tanzania are the only animal disease-detectives in routine use. When medics first hear about the program, they are often skeptical about the idea of using rats rather than machines, says Christophe Cox, CEO of Apopo, the Belgian-based organization behind the project. But then they are shown the case detection data. The rats are saving lives every day, and, argue some advocates, the time has now come for dogs to do the same.

★ ★ ★

The first *Lancet* letter came in 1989. Writing, as the name suggests, in the *Lancet* medical journal, a pair of dermatologists reported the case of a patient whose dog constantly sniffed at a mole on her leg, on one occasion even trying to bite it off. The woman sought medical advice. Tests showed it was a malignant melanoma, almost two millimeters thick. It was removed, and she remained well.

The second *Lancet* letter (as they're known in the dog-cancer-detection community) was published in 2001. John Church, a British doctor, and his colleague reported the case of 66-year-old man whose pet Labrador, Parker, kept pushing his nose against the man's leg, sniffing at a rough patch of skin that had been diagnosed as eczema. The man went back to his doctor. The "eczema" was found to be a basal cell carcinoma, which was swiftly removed.

"This is how it started," Church told the inaugural international conference on medical biodetection, held in Cambridge, United Kingdom, in September 2015. "It was all anecdotal."

At least, that was how interest in using dogs to sniff out cancer began. But the idea of smelling breath, urine, and stools to diagnose disease goes back millennia. In the time of Hippocrates, around 400 B.C.E., it was reportedly common for patients to cough and spit on hot coals to generate a smell that the physician would sniff to aid diagnosis.

Methods for disease diagnosis have clearly come a long way. But the *Lancet* letters got some, including John Church, thinking: Might animal noses be quicker, or more accurate, and/or cheaper—and so able to be used more widely—than some high-tech cancer-

screening techniques? If dogs really could sniff out cancer, what other diseases might they smell? And might the noses of other animals be useful too?

Over the past decade, there have been projects investigating the use of bees to sniff out cancer, for example, but that research hasn't advanced very far. The overwhelming focus in the field now is on dogs—and the African rats.

When someone with TB coughs, he or she exhales compounds produced by the bacterial pathogen *Mycobacterium tuberculosis.* If the TB is advanced enough, the smell of these compounds can even be detected by people. In 2002, when research to investigate the potential of using dogs in cancer diagnosis was in its embryonic stage, a former product designer from Belgium called Bart Weetjens began wondering about African giant pouched rats and TB.

Weetjens already knew that TB has a distinctive smell. "There is a lyric of a Van Morrison song: 'I can smell your TB sheets'—your bedsheets." Also, "in my native language, Dutch, the name for TB traditionally is *tering*, which etymologically refers to the smell of tar." Weetjens also knew that these rats are superlative sniffers. More than that, he understood how to breed them and how to train them, and his track record of using this species to save lives, albeit in a very different setting, was well-established.

★ ★ ★

As a boy, growing up in Antwerp, Belgium, Weetjens had kept pet rats. "Not only rats—I was very fond of all kinds of rodents. Hamsters and mice, and then rats. I tried gerbils and squirrels as well." He bred them in his bedroom. "I learned that they smell very well, but I was not occupied with that. I was simply breeding these animals to give offspring to the pet shops. It was a way to get pocket money. I gave up all rat breeding in my bedroom when I was 14."

After graduating and starting work as a product designer, Weetjens found himself increasingly preoccupied with the problem of landmines. "I saw a documentary about Cambodia, and also Princess Diana in Angola visiting mine-extraction operations. These two things triggered in me the magnitude of the problem." He began to consider landmine-detection systems: in theory, what kind of engineering solution would work best? Then he met a Dutch researcher who had come across stalled plans to try to use cockroaches to detect TNT exuding from buried landmines. "I thought, yes—this was the way forward: using local resources, a solution based on what was available in the context. This was for me an a-ha moment."

Except that Weetjens didn't think cockroaches. He thought rodents. In 1997, at a time when the local military academy was working on a landmine-detecting robot, he secured his first research grant, from the Belgian Development Cooperation, a government agency. "The secretary for the Development Cooperation had been a director of Doctors Without Borders. He knew the African realities much better than the army folks, actually. He immediately said to one of the professors in our team: 'This is a stupid idea, let's do it!'"

Car bomb kills dozens in Turkish capital

Source: http://www.usatoday.com/story/news/world/2016/03/13/large-explosion-turkey-capital-ankara/81729364/

Mar 13 – A large car bomb explosion killed at least 34 people and wounded scores more (~164; 12 in critical condition) in the Turkish capital of Ankara on Sunday, the governor's office said.

The bomb exploded close to bus stops near a park at Kizilay, Ankara's main square, NTV television reported. The news channel said the explosion occurred as a car slammed into a bus.

Mehmet Muezzinoglu, Turkey's health minister, said 125 people were wounded, 19 of them seriously. He said 30 of the victims died at the scene, while another perished at hospitals. Two of the dead were believed to be bombers, The Associated Press reported.

The BBC reported that several vehicles at the scene were reduced to burnt-out wrecks, including at least one bus.

No group immediately claimed credit for the attack, but a senior government official told the AP police suspected that Kurdish militants carried out the attack. Kurdish militants and the Islamic State group have carried out bombings in the city recently.

Dogan Asik, 28, said he was on a bus when the explosion occurred.

"We were thrown further back into the bus from the force of the explosion," said Asik, who sustained injuries to his face and arm.

Police sealed off the area and pushed onlookers back, the AP reported, warning there could be a second bomb. Forensic teams were examining the scene.

Prime Minister Ahmet Davutoglu was convening an emergency security meeting and President Recep Erdogan, who has been in Istanbul, was briefed on the attack by the interior minister, the newspaper *Hurriyet* reported. Erdogan was expected to return to Ankara.

Turkey's state-run news agency reported that Davutoglu had postponed a visit to Jordan.

The explosion came just three weeks after a suicide car bombing in the capital targeted buses carrying military personnel, killing 29 people. A Kurdish militant offshoot of the

outlawed Kurdish rebel group the Kurdistan Workers' Party, or PKK, claimed responsibility for that attack.

But on Sunday, the Peoples' Democratic Party, or HDP, issued a statement saying it shares "the huge pain felt along with our citizens."

In a statement, White House National Security Council spokesperson Ned Price on Sunday said the U.S. condemns the attack "in the strongest terms," adding, "This horrific act is only the most recent of many terrorist attacks perpetrated against the Turkish people. The United States stands together with Turkey, a NATO ally and valued partner, as we confront the scourge of terrorism."

One of the suicide bombers - Seher Çağla Demir (student at Tourism and Hotel Management section, Balikesir University City)

Sunday's attack came two days after the U.S. Embassy issued a security warning about a potential plot to attack Turkish government buildings and housing in one Ankara neighborhood and asked citizens to avoid those areas.

Hundreds of people have been killed in Turkey in renewed fighting following the collapse of the peace process between the government and the PKK in July. Authorities on Sunday had declared curfews in two towns in the mainly Kurdish southeast region in anticipation of large-scale military operations against PKK-linked militants.

Turkey also has been struck by several bombings in the last year that were blamed on the Islamic State as the government joined efforts led by the U.S. to fight the extremist group in Syria. The deadliest came in October when a peace rally outside Ankara's main train station killed 102 people.

EDITOR'S COMMENT: Despite this unfortunate event it is impressive that within 2 min, 112 ambulances rushed to the incident's site. A reminder that preparedness can save lives! **UPDATE** (17/3): The Kurdish Freedom Falcons, an offshoot of the separatist group PKK, have claimed responsibility for a car bomb attack in the Turkish capital.

Sheriff: Duo used 'weapons of mass destruction' on mailboxes

Source: http://www.theleafchronicle.com/story/news/2016/03/10/sheriff-duo-used-weapons-mass-destruction-mailboxes/81593596/

Mar 10 – **A Clarksville man and Fort Campbell soldier are both accused of using weapons of mass destruction after breaking into several barns in Christian County and then using homemade explosives to destroy mailboxes.**

According to a Christian County Sheriff's Department new release, on Feb. 25, suspects broke into several barns on John Rives Spur belonging to Garnett Farms and destroyed property, including a pickup and two tractors. The release does not say how the property was destroyed.

The following night, suspects used **homemade explosive made of PVC pipe and gunpowder** and destroyed three mailboxes in the Long Pond Road area.

Evidence was traced back to a Clarksville man and a soldier from Fort Campbell, the news release states.
Christian County Sheriff's Office Department Detective Sgt. Mark Reid worked with the Army's Criminal Investigation Division to interview the suspects. One gave a full confession and the other admitted to some involvement, the release states.
Daniel Kordis, 21, of Clarksville was arrested Wednesday and charged with use of a weapon of mass destruction, third-degree burglary, first-degree criminal mischief, third-degree criminal mischief and possession of a destructive device.
Ethan English, 19, of Fort Campbell was arrested Friday and charged with use of a weapon of mass destruction, first-degree criminal mischief, third-degree burglary, third degree criminal mischief and possession of a destructive devise.
Kordis, who gave a Barrywood Circle Clarksville address and English, a Tennessee Avenue Fort Campbell address were booked into the Christian County Jail on $10,000 cash bonds

EDITOR'S COMMENT: Perhaps it is time to use terms the right way: weapons of mass disruption – YES! Weapons of mass destruction – NO! Keep this for nuclea weapons only! Are they terrorists? Of course they are – what else?

Murder investigation after car bomb kills driver in Berlin

Source: http://www.bbc.com/news/world-europe-35810521

Mar 15 – **Berlin police** have launched a **murder inquiry** after **car bomb** exploded in a travelling vehicle, killing the driver.
The explosion occurred as the car moved through the western Charlottenburg district **towards the centre**. It flipped the vehicle into the air, police said.
They have identified the victim as a 43-year-old **man of immigrant background**.
Officials believe the blast was linked to organised crime and say there is no evidence of any link with terrorism.

However they do not know if the driver of the car was the intended target, a police spokesman said,

quoted by German media.
The explosion happened **"in or on" the front part of the Volkswagen Passat** as it travelled along the Bismarckstrasse during the **morning rush hour,** a police spokesman said.
Police told residents in the area to close their windows and stay in the back of their apartments.
But bomb disposal teams later said there was no risk of more explosions.

EDITOR'S COMMENT: Put all the yellow highlighted words together and you will understand why I love BBC so much! And then the Berlin Police assessment (in red): "No! Not in our safe city!"
Just a reminder: In Sept 17, 2015 a known Islamic extremist has been shot dead by police in Berlin after he stabbed and seriously wounded a woman officer in an apparent terror attack. The woman officer's partner immediately drew his gun and shot him four times. The assailant has been identified as Rafik Mohamad Yousef, a 41-year-old Iraqi citizen who had already served a prison sentence in Germany for his part in a 2004 terror plot. He was one of three men found guilty of a plot to assassinate the former Iraqi prime minister Iyad Allawi during a visit to Berlin in 2004. The terrorist was wearing an electronic surveillance bracelet/device that he removed beforehand.

Suspected Istanbul suicide bomber - A said ISIS terrorist known to Turkish authorities

Source: http://www.jpost.com/Middle-East/ISIS-Threat/Suspected-Istanbul-bomber-an-ISIS-terrorist-known-to-Turkish-authorities-448540

Mar 20 – **Savaş Yıldız, a 33-year-old Turkish national from the southern city of Adana, is the man authorities believe carried out the suicide bombing on Istanbul's Istiklal Avenue on Saturday, killing five people and wounding 39 (at least 24 foreign nationals).**
Yıldız was reportedly known to the security services as a follower of the jihadist organization Islamic State.
Local media reported on Sunday that Turkish law enforcement officials took fingerprint samples from Yıldız's father.

Authorities in Turkey also believe that Yıldız was involved in the October 2015 Ankara bombings, which killed over 100 civilians.

Yıldız had been on a terrorism watch list run by Turkish intelligence services, who reportedly monitored him during the time he spent on the Turkish-Syrian border. While there, Yıldız is believed to have been associated with jihadists.

Despite being under the watchful eye of the authorities, Yıldız managed to flee to Syria. After returning from Syria, he carried out the bombing in Istanbul.

Prime Minister Benjamin Netanyahu said on Saturday that officials in Jerusalem were in contact with their counterparts in Turkey in an attempt to clarify whether the suicide bombing in Istanbul was aimed at Israeli tourists. Israel has confirmed that three of its citizens died in the blast. Two of them held dual citizenship with the United States. Among the injured were 11 Israelis as well. An Iranian was also killed, Turkish officials have said.

Turkish official fired after tweeting she hoped Israelis injured in Istanbul terror attack "were dead"

Source: http://www.homelandsecuritynewswire.com/dr20160321-turkish-official-fired-after-tweeting-she-hoped-israelis-injured-in-istanbul-terror-attack-were-dead

Mar 21 – **A Turkish official has been sacked over a tweet in which she expressed her wish that a dozen Israeli tourists wounded in a bomb attack in Istanbul "were dead."**

The suicide attack by what the Turkish government described as a follower of ISIS, killed five people, including the bomber, three Israelis, and an Iranian, and injured thirty-nine, of which eleven were Israeli nationals.

According to the *Jerusalem Post*, shortly after details emerged of the victims of the attack, **Irem Aktas, a board member in the women's branch of the ruling AK Party for the Istanbul district of Eyup,** posted a tweet which read: "I wish that the wounded Israeli tourists were dead."

The tweet triggered a wave of outrage by both Turks and Israelis on social media, and appears to have prompted an angry personal intervention from Israeli Prime Minister Benjamin Netanyahu.

Netanyahu had instructed Israel's Foreign Ministry to demand an official condemnation and apology from the Turkish government. Foreign Ministry spokesman Emmanuel Nachshon told the *Post* if it was legitimate, the tweet was a "shocking and ugly statement".

Times of Israel reports that Aktas's account has been deleted in the wake of the post, and that she has since been fired from the AK Party.

415 children under 10, 1,424 secondary school children, referred to U.K. anti-extremism program

Source: http://www.homelandsecuritynewswire.com/dr20160321-415-children-under-10-1-424-secondary-school-children-referred-to-u-k-antiextremism-program

Mar 21 – **Almost 4,000 Britons have been referred to the U.K. government's counterterrorism program last year, among them children under nine.**

The rise in the number of referrals to the government's Channel program follows instructions by the government to prisons, NHS Trusts, and schools to tackle extremism more vigorously.

***International Business Times* reports that in 2015, 3,955 people were reported to Channel — up from 1,681 in 2014.**

The figures, which were obtained by the *Guardian* through Freedom of Information Request, are the first since the new counter-extremism rules came into force in July last year.

Analysts say that the data suggest the U.K. law enforcement authorities have become more vigilant about tackling extremism.

Recent cases such as a 3-year-old child being referred to the service have highlighted the anxiety over the number of both families and lone fighters travelling to Syria to fight in ISIS ranks.

Dr. Erin Saltman, a senior counter-extremism researcher at the Institute for Strategic Dialogue, told the *Guardian* the figures were "highly significant."

She said: "It's indicative of a couple of things. One is that there's a huge amount of awareness around **radicalization** that just didn't exist before — it's now a buzzword whereas five years ago it wouldn't have been.

"The other is an increase in fear. We are seeing an increase in fearful rhetoric around radicalization, particularly when we see foreign terrorist fighters and females in unprecedented numbers joining ISIS." The figures released in January show 415 children aged 10 or under and 1,424 secondary school aged children had been referred to the program in England and Wales since July.

Read also this: http://www.theguardian.com/uk-news/2016/mar/11/nursery-radicalisation-fears-boys-cucumber-drawing-cooker-bomb

Not with a bang, but a meltdown – Andy Oppenheimer looks at cyber-attacks on nuclear power plants

By Andy Oppenheimer

Source: http://www.cbrneportal.com/not-with-a-bang-but-a-meltdown-andy-oppenheimer-looks-at-cyber-attacks-on-nuclear-power-plants/

Feb 29 - Attacks by computer hackers on the IT systems of government and commercial organisations have become commonplace, and cybercrime is arguably the fastest growing new crime in the 21st century. Attacking lines of communications and vital infrastructure became a classic military and insurgent tactic in World War II by British Special Operations Executive (SOE) and resistance groups in Europe – and later, terrorist groups, most notably the IRA – set the stage for mass sabotage of infrastructure. With the dawn of digital communications and globalized commerce all countries became inexorably linked and hence, infinitely more vulnerable to infrastructure attack.

And among the most dangerous is a cyber-attack on a nuclear power plant (NPP) or nuclear reprocessing plant such as Sellafield, due to the possible release of radiation from reactors or spent fuel ponds. A cyber-attack by terrorists on NPP systems and back-ups powering reactor cooling systems could trigger a meltdown incident similar to Fukushima Daichi in 2011. According to Director of the International Atomic Energy Agency (IAEA), Gen. Yukiya Amano, in August 2015, "reports of actual or attempted cyber-attacks are now virtually a daily occurrence."

As a state-launched attack, the Stuxnet worm set back Iran's nuclear programme in 2009 by instructing 1,000 centrifuges to self-destruct – and has since escaped into programmes in other countries. In March 2015 the South Korean government accused the North Koreans of carrying out cyber-attacks in December 2014 on Korea Hydro and Nuclear Power (KHNP).

Nuclear industry "barely grappled with cyber"

In October 2015 a Chatham House report, *Cyber Security at Civil Nuclear Facilities: Understanding the Risks*, based on an 18-month study on cyber defences in NPPs, stated that UK's plants and associated infrastructure "were not well protected or prepared because the industry had converted to digital systems relatively recently." Based on 30 interviews with senior nuclear officials at plants and in government in Canada, France, Germany, Japan, the UK, Ukraine and the US, the researchers found that risks were compounded by increased digitisation and the industry's growing reliance on commercial software.

▶ **Read the rest of this article at sourc's URL.**

Andy Oppenheimer AIExpE MIABTI *is Editor of CBNW (Chemical, Biological & Nuclear Warfare) journal and a consultant in CBRNE and counter-terrorism. He is author of IRA: The Bombs and the Bullets (Irish Academic Press, 2008) and of the CBRN and IEDs module courses for the St Andrews University Certificate in Terrorism Studies.*

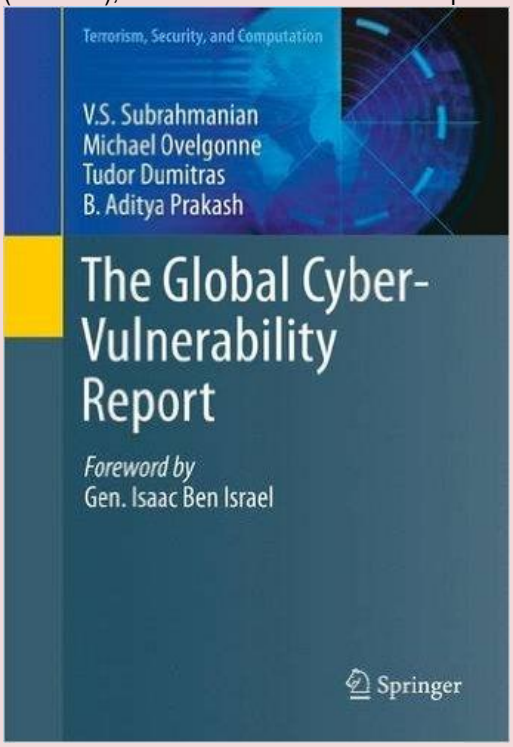
Nations ranked on vulnerability to cyberattacks

Source: http://www.homelandsecuritynewswire.com/dr20160316-nations-ranked-on-vulnerability-to-cyberattacks

Mar 16 – Damaging cyberattacks on a global scale continue to surface every day. Some nations are better prepared than others to deal with online threats from criminals, terrorists, and rogue nations. Data-mining experts ranked the vulnerability of forty-four nations to cyberattacks. **The United States ranked 11th safest, while several Scandinavian countries (Denmark, Norway, and Finland) ranked the safest.**

Damaging cyberattacks on a global scale continue to surface every day. Some nations are better prepared than others to deal with online threats from criminals, terrorists, and rogue nations.

Data-mining experts from the University of Maryland and Virginia Tech co-authored a recent book that ranked the vulnerability of forty-four nations to cyberattacks. On 9 March, lead author V. S. Subrahmanian, a UMD professor of computer science with an appointment in the University of Maryland Institute for Advanced Computer Studies (UMIACS), discussed this research at a panel



discussion hosted by the Foundation for Defense of Democracies in Washington, D.C.

The United States ranked 11th safest, while several Scandinavian countries (Denmark, Norway, and Finland) ranked the safest. China, India, Russia, Saudi Arabia, and South Korea ranked among the most vulnerable.

"Our goal was to characterize how vulnerable different countries were, identify their current cybersecurity policies and determine how those policies might need to change in response to this new information," said Subrahmanian.

UMD reports that the authors conducted a two-year study that analyzed more than twenty billion automatically generated reports, collected from four million machines per year worldwide. The researchers based their rankings, in part, on the number of machines attacked in a given country and the number of times each machine was attacked.

Machines using Symantec anti-virus software automatically generated these reports, but only when a machine's user opted in to provide the data.

Trojans, followed by viruses and worms, posed the principal threats to machines in the United States. However, misleading software (that is, fake anti-virus programs and disk cleanup utilities) is far more prevalent in the United States compared with other nations that have a similar gross domestic product. These results suggest that U.S. efforts to reduce cyberthreats should focus on education to recognize and avoid misleading software.

In a foreword to the book, Isaac Ben-Israel, chair of the Israeli Space Agency and former head of that nation's National Cyber Bureau,

wrote: "People — even experts — often have gross misconceptions about the relative vulnerability [to cyberattack] of certain countries. The authors of this book succeed in empirically refuting many of those wrong beliefs."

The findings include economic and educational data gathered by UMD's Center for Digital International Government, for which Subrahmanian serves as director. The researchers integrated all of the data to help shape specific policy recommendations for each of the countries studied, including strategic investments in education, research and public-private partnerships.

Subrahmanian's co-authors are Michael Ovelgönne, a former UMIACS postdoctoral researcher; Tudor Dumitras, an assistant professor of electrical and computer engineering in the Maryland Cybersecurity Center; and B. Aditya Prakash, an assistant professor of computer science at Virginia Tech.

A related research paper on forecasting the spread of malware in forty countries — containing much of the same data used for the book — was presented at the 9th ACM International Conference of Web

Search and Data Mining in February 2016.

Another paper, accepted for publication in the journal *ACM Transactions on Intelligent Systems and Technology*, looked at the human aspect of cyberattacks — for example, why some people's online behavior makes them more vulnerable to malware that masquerades as legitimate software.

— Read more in V. S. Subrahmanian, M. Ovelgonne, T. Dumitras, and B. A. Prakash, The Global Cyber-Vulnerability Report (Springer, 2015); Chanhyun Kang et al., "Ensemble Models for Data-driven Prediction of Malware Infections" (paper presented at the 9th ACM International Conference of Web Search and Data Mining, San Francisco, California, 22-25 February 2016); and Michael Ovelgonne et al., "Understanding the Relationship between Human Behavior and Susceptibility to Cyber-Attacks: A Data-Driven Approach," ACM Transactions on Intelligent Systems and Technology 7, no. 3 (March 2016)

Identifying national security threats posed by everyday commercial technologies

Source: http://www.homelandsecuritynewswire.com/dr20160315-identifying-national-security-threats-posed-by-everyday-commercial-technologies

Mar 15 – For decades, U.S. national security was ensured in large part by a simple

advantage: a near-monopoly on access to the most advanced technologies. Increasingly, however, off-the-shelf equipment developed for the transportation, construction, agricultural, and other commercial sectors features highly sophisticated components, which resourceful adversaries can modify or combine to create novel and unanticipated security threats. DARPA says that to assess this growing security challenge and identify specific potential risks, a new DARPA effort will ask experts across multiple disciplines to look at today's bustling tech marketplace with an inventor's eye and imagine how easily purchased, relatively benign technologies might be converted into serious security threats. The endeavor is dubbed "Improv," an abbreviated reference to the potential for improvising with widely available technology to create new and unanticipated risks.

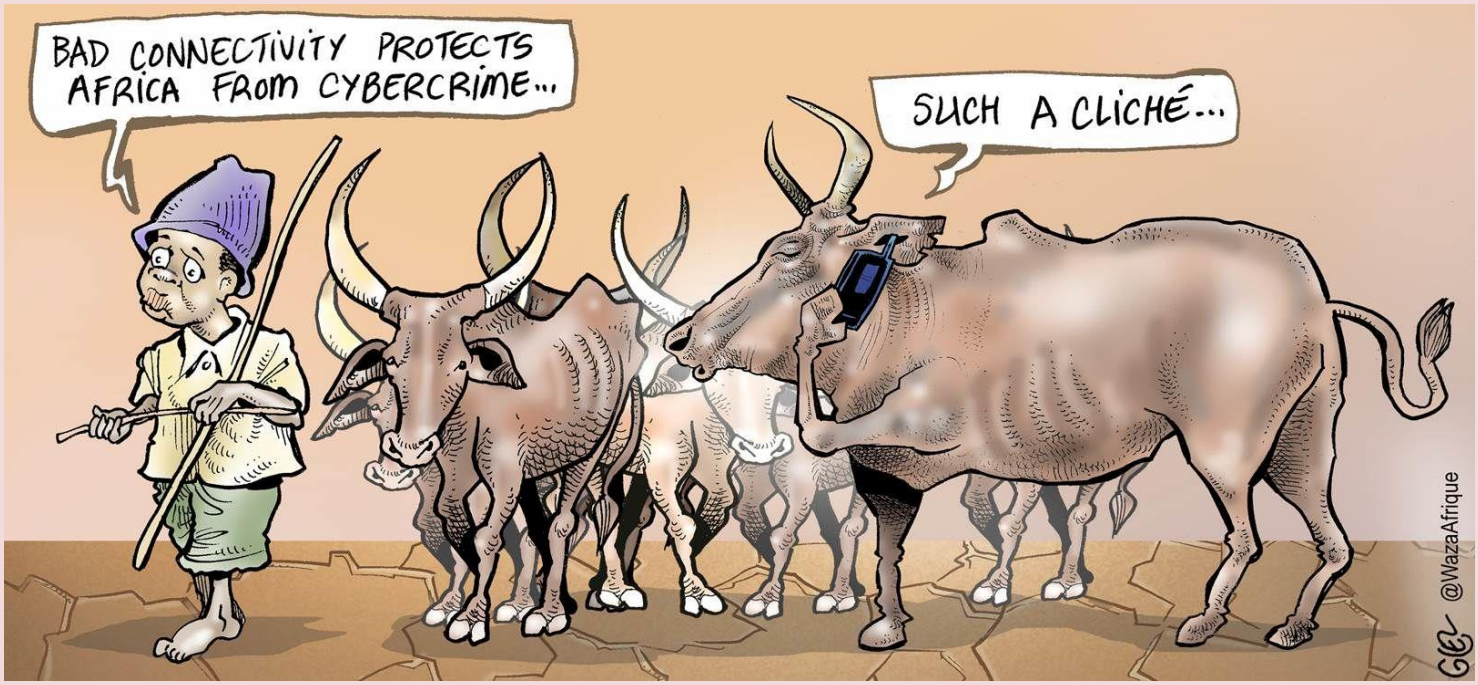
"DARPA's mission is to create strategic surprise, and the agency primarily does so by pursuing radically innovative and even seemingly impossible technologies," said program manager John Main, who will oversee the new effort. "Improv is being launched in recognition that strategic surprise can also come from more familiar technologies, adapted and applied in novel ways."

Improv will explore ways to combine or convert commercially available products such as off-the-shelf electronics, components created through rapid prototyping, and open-source code to cost-effectively create sophisticated military technologies and capabilities. To bring a broad range of perspectives to bear, DARPA is inviting engineers, biologists, information technologists and others from the full spectrum of technical disciplines — including credentialed professionals and skilled hobbyists — to show how easily-accessed hardware, software, processes and methods might be used to create products or systems that could pose a future threat. DARPA will assess candidate ideas and offer varying levels of support to develop and test selected proposals. The emphasis will be on speed and economy, with the goal of propelling winning submissions from concept to simple working prototypes within about ninety days.

"DARPA often looks at the world from the point of view of our potential adversaries to predict what they might do with available technology," Main said. "Historically we did this by pulling together a small group of technical experts, but the easy availability in today's world of an

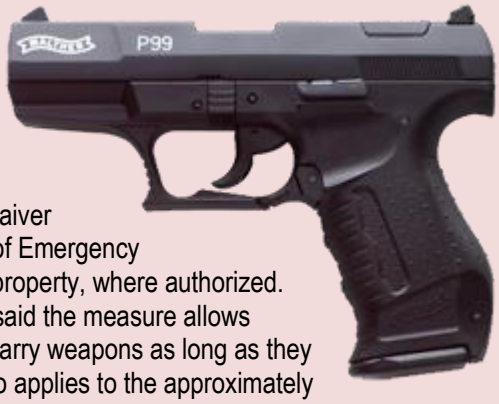
enormous range of powerful technologies means that any group of experts only covers a small slice of the available possibilities. In Improv we are reaching out to the full range of technical experts to involve them in a critical national security issue."

DARPA notes that it intends to fund selected Improv proposals through a short feasibility-study phase, during which performers will refine their ideas and compete for the opportunity to build prototypes. DARPA will evaluate the results of that work, and a subset of the prototypes will proceed to a detailed evaluation regimen. If performance warrants, DARPA may advance the relevant capabilities in separate follow-on efforts.



Emergency Management Personnel Get Green Light to Carry Firearm

Source: http://www.emergencymgmt.com/safety/Emergency-management-personnel-get-green-light-to-carry-firearms.html



Feb 24 – **A resolution to allow personnel from the Pittsburg County Office of Emergency Management to carry firearms has been locked, loaded and passed.**

During their regular Monday meeting at the Pittsburg County Courthouse, county commissioners voted to approve an amendment to the county's Personnel Policy Handbook regarding firearms and an acknowledgment/waiver form. They also approved a resolution allowing personnel from the Office of Emergency Management to carry personal firearms in county vehicles and on county property, where authorized.

Pittsburg County Office of Emergency Management Director Kevin Enloe said the measure allows himself, along with Deputy Directors Lois Lupardus and Hillary Steele, to carry weapons as long as they meet the state requirements for concealed or open carry of firearms. It also applies to the approximately 15 emergency management reserves or volunteers, Enloe said.

Sometimes Office of Emergency Management personnel are the first to arrive at the scenes of disasters, which can be late at night in secluded areas, Enloe noted. They also work long hours, as the situation requires.

Enloe said he's already cleared to carry a firearm because he is a reserve Pittsburg County Sheriff's Deputycertified through CLEET, the Council on Law Enforcement Education and Training. Now he's pleased the other emergency management personnel will now be able to carry firearms as well.

County commissioners said they wanted to give the emergency management personnel the opportunity to defend themselves, should it ever be necessary.

"They're put into dangerous situations on their job and after hours," said District 2 Commissioner Kevin Smith.

District 3 Commissioner Ross Selman agreed. "They're sometimes out by themselves in the middle of the night," said Selman.

District 1 Commissioner Gene Rogers made it unanimous. "It's for personal safety," Rogers said.

In emergencies, don't trust a robot too much

Source: http://www.homelandsecuritynewswire.com/dr20160301-in-emergencies-don-t-trust-a-robot-too-much

Mar 01 – **In emergencies, people may trust robots too much for their own safety, a new study suggests. In a mock building fire, test subjects followed instructions from an "Emergency Guide Robot" even after the machine had proven itself unreliable — and after some participants were told that robot had broken down.**

The research was designed to determine whether or not building occupants would trust a robot designed to help them evacuate a high-rise in case of fire or other emergency. Georgia Tech reports that the researchers were surprised to find that the test subjects followed the robot's instructions – even when the machine's behavior should not have inspired trust.

The research, believed to be the first to study human-robot trust in an emergency situation, is scheduled to be presented 9 March at the 2016 ACM/IEEE International Conference on Human-Robot Interaction (HRI 2016) in Christchurch, New Zealand.

"People seem to believe that these robotic systems know more about the world than they really do, and that they would never make mistakes or have any kind of fault," said Alan Wagner, a senior research engineer in the Georgia Tech Research Institute (GTRI). "In our studies, test subjects followed the robot's directions even to the point where it might have put them in danger had this been a real emergency."

In the study, sponsored in part by the Air Force Office of Scientific Research (AFOSR), the researchers recruited a group of forty-two volunteers, most of them college students, and asked them to follow a brightly colored robot that had the words "Emergency Guide Robot" on its side. The robot led the study subjects to a conference room, where they were asked to complete a survey about robots and read an unrelated magazine article. The subjects were not told the true nature of the research project.

In some cases, the robot — which was controlled by a hidden researcher — led the volunteers into the wrong room and traveled around in a circle twice before entering the conference room. For several test subjects, the robot stopped moving, and an experimenter told the subjects that the robot had broken down. Once the subjects were in the conference room with the door closed, the hallway through which the participants had entered the building was filled with artificial smoke, which set off a smoke alarm.

When the test subjects opened the conference room door, they saw the smoke – and the robot, which was then brightly-lit with red LEDs and white "arms" that served as pointers. The robot directed the subjects to an exit in the back of the building instead of toward the doorway – marked with exit signs – that had been used to enter the building.

"We expected that if the robot had proven itself untrustworthy in guiding them to the conference room, that people wouldn't follow it during the simulated emergency," said Paul Robinette, a GTRI research engineer who conducted the study as part of his doctoral dissertation. "Instead, all of the volunteers followed the robot's instructions, no matter how well it had performed previously. We absolutely didn't expect this."

The researchers surmise that in the scenario they studied, the robot may have become an "authority figure" that the test subjects were more likely to trust in the time pressure of an emergency. In simulation-based research done without a realistic emergency scenario, test subjects did not trust a robot that had previously made mistakes.

"These are just the type of human-robot experiments that we as roboticists should be investigating," said Ayanna Howard, professor and Linda J. and Mark C. Smith Chair in the Georgia Tech School of Electrical and Computer Engineering. "We need to ensure that our robots, when placed in situations that evoke trust, are also designed to mitigate that trust when trust is detrimental to the human."

Only when the robot made obvious errors during the emergency part of the experiment did the participants question its directions. In those cases, some subjects still followed the robot's instructions even when it directed them toward a darkened room that was blocked by furniture.

In future research, the scientists hope to learn more about why the test subjects trusted the robot, whether that response differs by education level or demographics, and how the robots themselves might indicate the level of trust that should be given to them.

Georgia Tech notes that the research is part of a long-term study of how humans trust robots, an important issue as robots play a greater role in society. The researchers envision using groups of robots stationed in high-rise buildings to point occupants toward exits and urge them to evacuate during

emergencies. Research has shown that people often do not leave buildings when fire alarms sound, and that they sometimes ignore nearby emergency exits in favor of more familiar building entrances.

But in light of these findings, the researchers are reconsidering the questions they should ask.

"We wanted to ask the question about whether people would be willing to trust these rescue robots," said Wagner. "A more important question now might be to ask how to prevent them from trusting these robots too much."

Beyond emergency situations, there are other issues of trust in human-robot relationships, said Robinette.

"Would people trust a hamburger-making robot to provide them with food?" he asked. "If a robot carried a sign saying it was a 'child-care robot,' would people leave their babies with it? Will people put their children into an autonomous vehicle and trust it to take them to grandma's house? We don't know why people trust or don't trust machines."

— Read more in Paul Robinette et al., "Overtrust of Robots in Emergency Evacuation Scenarios" (paper to be presented at the 2016 ACM/IEEE International Conference on Human-Robot Interaction, [HRI], New Zealand, 7-10 march 2016).

Are America's cities prepared for extreme weather events?

Source: http://www.homelandsecuritynewswire.com/dr20160308-are-americas-cities-prepared-for-extreme-weather-events

Mar 08 – From September 2012 until March 2013, Australia sweltered. And burned.

The worst heat wave recorded in the continent's history sent temperatures soaring well over 100°F for weeks. Fires spread along the coasts and across Tasmania. In the Outback, roads melted.

News reports called it the "angry summer." It was so bad that it literally changed the map: meteorologists had to add two new color bands to their maps on the evening weather reports, to go up to 130°.

So Australians turned on the air conditioning. The electric grid suffered in both Melbourne and Sydney. Urban railways were delayed as heat damaged the wiring. A report later that year found the heat wave was almost certainly beyond the bounds of natural climate variation.

Scientists agree that the future will bring higher temperatures for longer periods of time, higher sea levels, and both more droughts and more storms. "This means that our infrastructure, as it exists today, isn't going to be able to operate at the same level in the future," said Megan Clifford, deputy director of the Risk and Infrastructure Science Center at Argonne National Lab.

ANL reports that infrastructure is, by design, largely unnoticed until it breaks and service fails. It is the water supply, the gas lines, bridges and dams, phone lines and cell towers, roads and culverts, train lines and railways, and the electric grid; all of the complex systems that keep our society and economy running.

Engineers typically design systems to withstand reasonable worst-case conditions based on historical records; for example, an engineer builds a bridge strong enough to withstand floods based on historical rainfall and flooding. But what happens when the worst case is no longer bad enough?

"If we don't adapt the systems, they will break," said Duane Verner, an urban planner who works with Clifford.

"When you look at cities' long-term plans, which every city has — and they go out decades for planning major infrastructure — they rarely have local climate projections available for their planning assumptions or design criteria," Clifford said.

A major difficulty, she explained, is that it is difficult for city planners to look at a large-scale climate model and understand the impacts to their local area.

ANL says that this is where Argonne scientists and researchers are bridging the gap. Argonne's infrastructure experts are just a building over from climate scientists in the environmental science division and supercomputing resources at the Argonne Leadership Computing Facility. They can develop and interpret the complex global

climate models to predict the effects of climate change by region.

The Risk and Infrastructure Science Center can pull all of these forces together with other subject matter experts, including engineers and analysts with experience in various infrastructure industries. Combining these resources helps them develop practical and comprehensive analyses for planners. These tools not only help city planners analyze risks, but also prioritize them in light of tight budgets.

One type of analysis that Argonne frequently conducts is called an RRAP – the Regional Resiliency Assessment Program. Every year, the U.S. Department of Homeland Security funds several assessments that each look at a particular area's vulnerabilities.

Verner is part of a team working on an RRAP for the Casco Bay region of Maine. Like other regions they have studied, they are finding that floods, heat waves, and other changes predicted for Maine could cause trouble for its infrastructure.

For example, in general, power plants do not like heat — their output declines, some types more than others. The same is true for transmission lines; they lose some ability to carry electricity in the heat.

"This change is in the margins, but when you add that together with increased demand for power to run air conditioning, for example, you can cross the thresholds for brownouts," Verner said.

Then there's rain. "The climate models are showing that increases in extreme precipitation events are projected for the entire U.S., because there's more humidity in the atmosphere," Verner said, "and structures like culverts, that are built to standards for past historical rainfall events, won't be able to accommodate this rush of rain" (culverts are pipes that channel streams and water underneath roads).

Too much rain all at once causes floods, and floods are devastating to infrastructure. Water is extraordinarily destructive. Hurricane Sandy shut down New York City, one of the largest, most prosperous cities in the world, for days. Floods wash out roads and bridges, damage homes, schools, and buildings, and overwhelm sewer systems, causing sewage dumps into local waterways; the economic impact can be severe. Sandy caused $65 billion worth of damage.

At the same time, we have also seen record droughts in recent years. "Generally, planners are using historical records for droughts in their water resource planning processes, and our climate models show that, in many cases, historical records won't provide an adequate worst-case scenario to plan for," Verner said. "It will be much worse."

Droughts are financially ruinous for farmers and agriculture; that same year as Sandy, 2012, saw a Midwest/Plains drought that cost $35 billion.

That drought saw the mighty Mississippi River drop to such low levels that shipping on the river, which normally carries billions of dollars of cargo every month, was nearly halted. "I have never seen anything like it," Colonel Chris Hall, commander of the Corps of Engineers' St. Louis District, told the *Chicago Tribune*.

In response, Argonne researchers scrambled to analyze the potential economic impacts if water levels dipped below a certain point on the middle Mississippi River. Billions of dollars of cargo are shipped on the river every month; power plants pull cooling water; and local communities draw water, including drinking and irrigation water. The analysis quantified the thousands of jobs and billions in income that could be in jeopardy across six states for a worst-case scenario drought.

ANL notes that these kinds of analyses help federal, state, and local governments understand stakes and prioritize action. With the help of the Risk and Infrastructure Science Center, as well as resiliency efforts in multiple areas at Argonne, planners can find out the types of stresses their cities and regions will face in the future.

Infrastructure is generally an ounce-of-prevention game; smart changes now can save a region billions of dollars in damages and lost economic productivity in the future. Communities can ration water from aquifers, shore up electric grids, and build roads out of water's reach. New estimates of rainfall help engineers determine what kind of storms their bridges should withstand; power companies can estimate energy demand in upcoming heat waves. They just need to know what they're facing.

"Our goal is to help planners get the information they need to do their jobs, and to drive national efforts for future resilient

infrastructure design," Clifford said.
ANL says that with the ongoing involvement of Argonne and the scientific community, infrastructure can be adapted and designed to withstand the changes ahead — before it breaks.

Modern buildings have an alarming flaw when people need to escape quickly

By Achille Fonzone
Source: http://www.homelandsecuritynewswire.com/dr20160311-modern-buildings-have-an-alarming-flaw-when-people-need-to-escape-quickly

Mar 11 – The landscapes in which many of us live would have been unimaginable to previous generations. We now have skyscrapers so striking and tall they would make Icarus turn pale. Yet in emergency situations, our seemingly brilliant designs sometimes turn against us – and become death traps when disaster strikes.
Safety engineering is about designing buildings that reduce the negative effects of accidents and attacks. The basic concept is straightforward: it takes a while after an incident before a structure collapses. If you can design it so that the time for everyone to flee is shorter than the time it takes to collapse, you save lives. This is the standard approach for big or complex structures in many countries, including the UK, US, Japan, Sweden and Italy.
But how long does it take to evacuate a building? It depends on the building and the escape routes, but crucially also on how people behave. To estimate the time it would take for everyone to flee – the "egress time" as we call it – safety engineers use computer simulations in which people evacuate after an incident and react to whatever happens around them.
The problem is that the simulations aren't good enough – that's what we have learned from detailed behavioural studies based on recent fires and terrorist attacks including 9/11 and the Mont Blanc tunnel fire of 1999 in which 41 people died. So either we teach evacuees to behave like our models – or, more realistically, improve our models.
This is not easy because the evacuee will make a host of different decisions: whether and when to start moving, in which direction, whether to respond to other evacuees, and which exit to use. Each choice also depends on how various factors interact with one another. Is the decision maker bold or risk-averse? Is there smoke in the room? How far away are the exits? And of most interest for our research purposes, what are the other evacuees doing?

Seen and then herd
We have all seen what sometimes happens with pedestrians at a red traffic light. Everybody quietly waits for the green light until someone decides to cross early, and then suddenly the whole group copies them. We call this "herding behaviour" – and when it comes to evacuation, it can be dangerous. It can create excessive congestion at some exits, increasing the all-important amount of time it takes for everyone to flee.
Herding used to have a bad name among evacuation scholars. It is an irrational consequence of panic, we used to say – the more evacuees panic, the more they herd. And of course it is difficult to design structures that take account of irrationality. But we showed in a recent study that it can be perfectly rational to copy the behaviour of other evacuees. And if herding is actually what people do in an emergency, it is not something to fight but something to understand and possibly exploit. Panic was being made a scapegoat for tragedies that were partly avoidable.
The purpose of our study was to look at how common herding is in an emergency situation. To do this, we set up a choice experiment online. We created a few realistic videos with different emergency situations, in each case offering decision makers a series of choices between two doors. We invited people around the world to participate, and ended up with more than 1,500 participants. This was a big improvement on previous studies in which we have been involved, which offered far fewer choices and involved fewer than 200 respondents.
We found that in an emergency, if an evacuee is faced with two doors and no one else is around, they are as likely to choose one

door as the other. If you put a few other evacuees close to one of the doors, however, some of the other evacuees will follow them – instead of worrying that those people might slow down their escape. According to our analysis, the sight of ten people close to a door may be roughly as persuasive to these people as seeing an "exit" sign hanging on it.

The point is that if herding is the human norm, safety engineers need to start taking it into consideration. It is not as easy as saying that this or that disaster could have been avoided if we considered herding, but we need to build it into our simulators and then use the insight to make buildings that are safer in emergencies. One option might be to provide evacuees with real-time information, for instance, such as with dynamic signage systems of the kind that have been tested in Barcelona.

But first we have to understand what kind of people are more prone to trust the decisions of other evacuees, and also how herding affects other evacuation choices such as the decision to start evacuating. Suffice to say, for now there is a major problem with the way we evaluate the safety of the structures in which we live and work. Until we address it, our chances of survival are a little like those of the characters from Greek legend – in the lap of the gods.

Achille Fonzone is Lecturer in Transport Modelling, Edinburgh Napier University.

Increasing speed, accuracy of flood risk assessment

Source: http://www.homelandsecuritynewswire.com/dr20160321-increasing-speed-accuracy-of-flood-risk-assessment

Mar 21 – **Research from the University of Adelaide hopes to provide advances in the planning for flood risk, thanks to a new, faster method of assessing the highly complex factors that cause floods in a specific location.**

The results of the study, published in this month's issue of the *Journal of Hydrology*, have shown it is possible **to increase the speed of a highly accurate flood risk prediction by between 100-1,000 times** compared with techniques currently used by researchers to estimate flood risk under climate change.

"Engineering companies and local councils involved in flood risk assessment and infrastructure planning have a major challenge ahead for them, and that's driven by climate change," says Associate Professor Mark Thyer, from the University's School of Civil, Environmental, and Mining Engineering. He led the research team, which also included collaborators from the School of Mathematical Sciences at the University of Adelaide and the School of Engineering at the University of Newcastle.

"Approaches typically used by industry for flood risk assessment have been based on information about historical flood events. But climate change will eventually make that method obsolete, because with a change in climate those historical events start to become more irrelevant as predictors of future flood activity," he says.

"The other main contender for predicting flood events under climate change, called continuous simulation, can be incredibly slow, as it uses long-term rainfall sequences spanning hundreds of years, taking into account climate variability and its impact on the catchment processes that drive major flood events. This can take anywhere from weeks to months to generate an accurate prediction for a single catchment," he says.

U Adelaide reports that the new method tested by the research team is aimed at providing a highly accurate assessment at a much faster rate. **The method (known as hybrid causative events, or HCE) relies on an algorithm that knocks out all of the unnecessary information used by the slower, continuous simulation approach – such as long, dry periods without rainfall.**

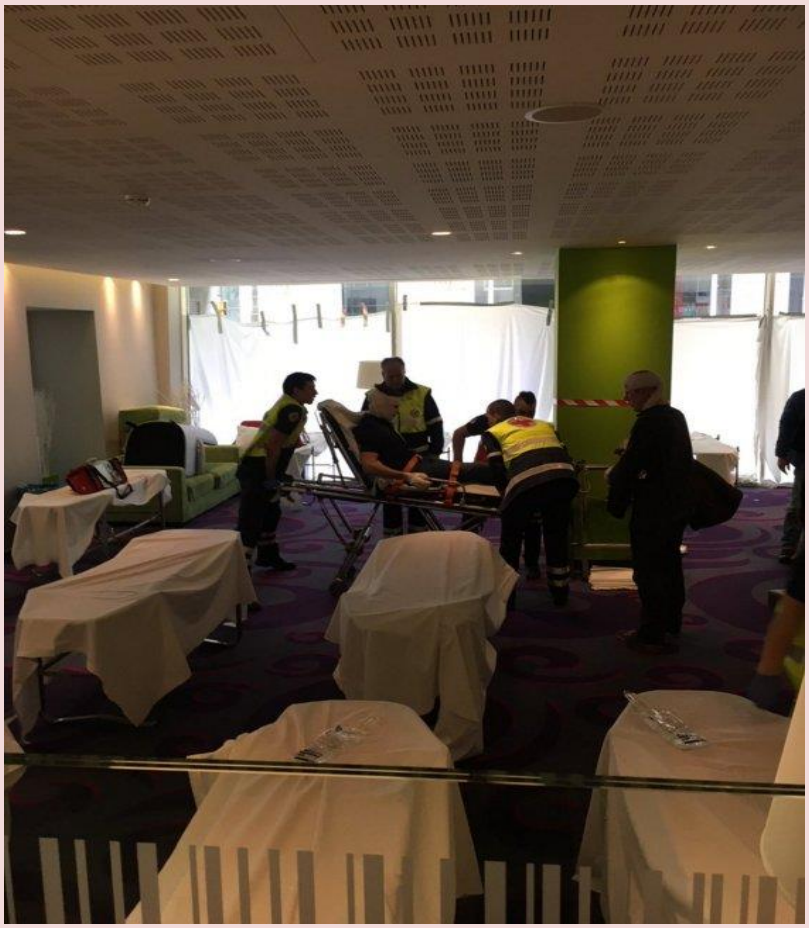
"Our new predictive method focuses on the key causative events that drive major floods such as high catchment saturation and extreme rainfall events. By extracting these key drivers, we realized we don't need to run the catchment model for all the long-term dry periods. This greatly reduces the time taken for our modelling, while also maintaining the high level of accuracy we're seeking," Thyer says.

"So far our method has been tested in a virtual laboratory on eight different sites in Australia, ranging from desert to Mediterranean, tropical and sub-tropical climate zones. We've found it to be highly accurate at each location, and increasing the speed of the flood prediction by between 100-1,000 times compared with continuous simulation."

While it might take another five years or so for this method to be available to industry, Thyer says the need for such predictions was highlighted during the 2012 flood at Wagga Wagga, NSW.

"An 11-metre levy had been built at Wagga based on historical flood data. In 2012, Wagga was hit with a flood that peaked at 10.8 metres, just 20 centimetres from the top of the levy. This narrowly averted disaster and was an excellent example of how flood prediction can help save properties and lives. We hope that our new, faster and more accurate predictive method will eventually have the same effect elsewhere in Australia and overseas," he says.

— Read more in Jing Li et al., "An efficient causative event-based approach for deriving the annual flood frequency distribution," Journal of Hydrology 510 (14 March 2014): 412–23 (doi:10.1016/j.jhydrol.2013.12.035); Mark Thyer et al., "A new approach for annual flood frequency estimation: Hybrid Causative Event Method: Conference Presentation" (paper presented at the :Engineers Australia, Hydrology and Water Resources Symposium, 2012, Sydney Australia); and Mark Thyer, "An efficient hybrid causative event-based approach for estimating flood frequency: Conference Poster" (Conference poster presented at European Geophysical Union Assembly 2015, Vienna, Austria).



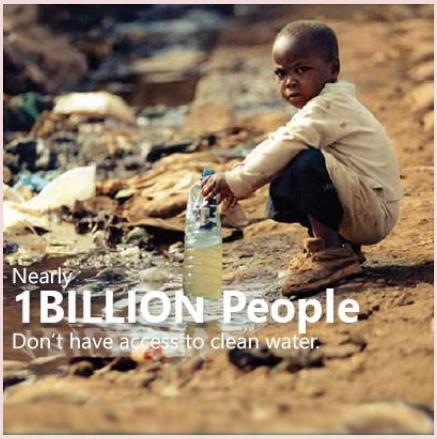
Improvisation in urban emergencies

Mar 22 – The lobby of the Thon Hotel in close proximity to the bombed Brussels metro station changed to initial triage and first aid station for victimized commuters.

Windows were covered with tablecloths providing isolation.

Water storage strategies in Sub-Sahara Africa

Source: http://www.homelandsecuritynewswire.com/dr20160302-water-storage-strategies-in-subsahara-africa



Mar 02 – Direct abstraction of water from rivers through ponds and pumping devices seems the most attractive water storage option in Ethiopia. However, the funding agencies that may be interested in investing in such a storage system have to consider that better access to credit, and clear abstraction policies should be ensured.

World Scientific reports that the current study proposes a multi-criteria decision aid framework to funding agencies for the integrated evaluation of water storage systems in Ethiopia and more broadly in Sub-Saharan Africa. Various water storage schemes within the country are assessed while the farmers are placed at the center of the analysis as the principal stakeholders. The approach is based on a multi-criteria outranking method for the avoidance of complete trade-offs between criteria.

Throughout Sub-Saharan Africa (SSA), past storage development has largely occurred in a piecemeal fashion, through local initiatives and with minimal planning. In some cases lack of information and planning has resulted in less than optimal investments. Population growth, in conjunction with climate change, will increase the importance of water storage but without greater understanding of which types of storage are best utilized under specific agro-ecological and social conditions it is likely that many water storage investments will fail to deliver the intended benefits.

To ensure sustainability, national policies are needed that promote much more rigorous and integrated planning of all water storage options. World Scientific notes that to this end, the current study suggests outranking assessment as a tool that facilitates the systematic inclusion of a wider range of criteria in planning processes. In combination with existing approaches it could contribute significantly to better planning of water storage throughout SSA.

The study presents an integrated assessment approach for funding agencies and organizations as a promising option to better evaluate the performance of water storage in Sub-Saharan Africa.

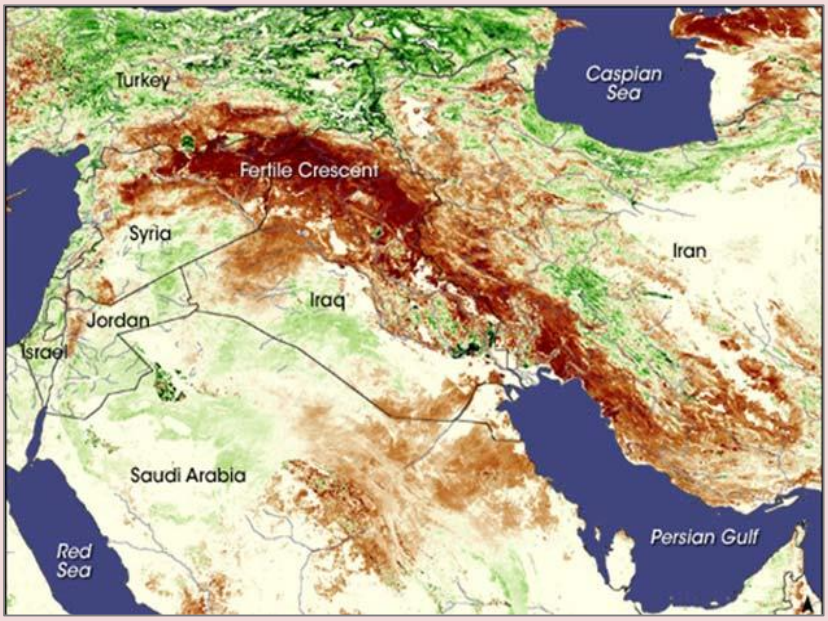
The study was carried out within the project "Rethinking Water Storage for Climate Change Adaptation in Sub-Saharan Africa". This multidisciplinary project (2008-2011) was funded by the German Federal Ministry for Economic Cooperation and Development.

— Read more in Stefanos Xenarios et al., "Developing a User-Based Decision-Aid Framework for Water Storage Systems in Sub-Saharan Africa: The Case of Blue Nile Basin in Ethiopia," Water Economics and Policy 1, no. 4 (December 2015).

Syria's 1998-2012 drought likely its most severe in more than 900 years

http://www.homelandsecuritynewswire.com/dr20160307-syria-s-19982012-drought-likely-its-most-severe-in-more-than-900-years

Mar 07 – **In the years before the Syrian conflict erupted, the region's worst drought on record set in across the Levant, destroying crops and restricting water supplies in the already water-stressed region. A new study shows that that drought, from 1998 to 2012, was not just the most severe in a century of record-keeping — it was the Levant's most severe drought in at least 500 years and likely more than 900 years.**



In the years before the Syrian conflict erupted, the region's worst drought on record set in across the Levant, destroying crops and restricting water supplies in the already water-stressed region. A new study shows that that drought, from 1998 to 2012, was not just the most severe in a century of record-keeping — it was the Levant's most severe drought in at least 500 years and likely more than 900 years.

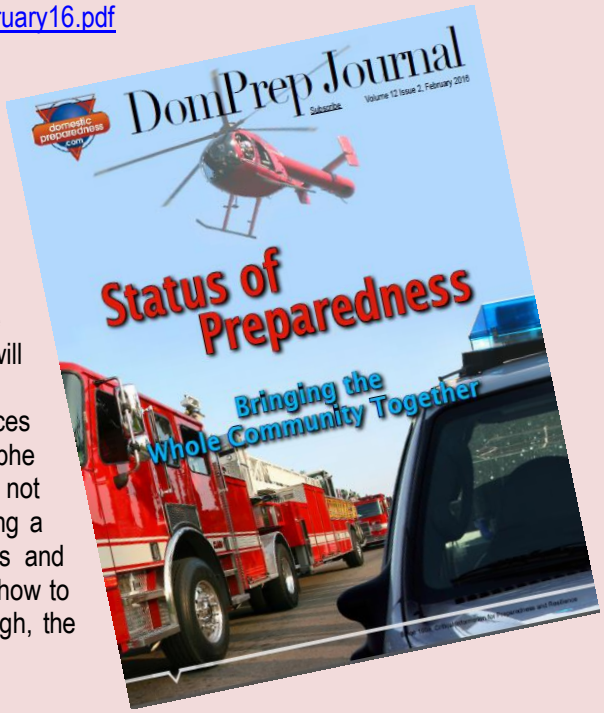
The study, published in the *Journal of Geophysical Research: Atmospheres,* is the first to quantitatively evaluate droughts across the Mediterranean region during the past 900 years at a high level of detail. It doesn't identify a cause of the recent Syrian drought, but it does provide independent support for studies that have suggested global warming may already be having an effect there, said lead author Benjamin Cook, a climate scientist at Columbia University's Lamont-Doherty Earth Observatory and NASA Goddard Institute for Space Studies.

"We can now say with some degree of confidence that what we're seeing in that part of the Mediterranean is likely separable from natural variability," Cook said. "If climate change is having an impact and is making droughts worse, then we should see this in the record over several centuries—and we do."

The Continuity Gap

By Vincent B. Davis

Source: http://www.domesticpreparedness.com/pub/docs/DPJFebruary16.pdf



Business continuity and emergency management, with various nuances, are not the same. In the years since Y2K – through the technology boom, the Internet, and the evolution of sophisticated cyber systems – corporations have spent billions of dollars in their efforts to ensure business resilience in the face of new threats, risks, and vulnerabilities. Often lost within the processes, procedures, and plans for redundancy of data systems and information is a subtle but powerful reality: if the event cannot be managed effectively, no long-term efforts to protect the business will succeed.

Many corporations have invested little time, effort, and resources toward preparing to "manage" the inevitable outcome of a catastrophe at its onset. That discipline is the core of emergency management, not business continuity. This type of failure can be equated to having a new, state-of-the-art computerized automobile with all the bells and whistles, but forgetting to include a tire jack, with instructions on how to use it. When the "wheels fall off" of costly planning efforts, though, the result is a disaster of disconnected response.

Fundamental Gaps & Models for Success

The following three fundamental realities create a phenomenon that can be best described as the "Continuity Gap":

- Most businesses do not employ a full-time emergency manager because they believe managing disasters can be handled by existing security or management staff.
- The heavy emphasis of business managers on data and information technology (IT) recovery has left a gap that does not account for prevention, protection, employee preparedness, and capabilities essential to response and recovery of the whole business.
- The assumption that managing emergencies is a "natural" consequence of managing the business has itself led to a deficiency of proper planning, training, and exercises to manage life safety and responses first for many businesses.

Contributing to the Continuity Gap is something that conspicuously seems to be absent in the business continuity planning cycle of many companies: the focus on employee and family preparedness. Adding to the mix is "corporate fear" among business managers, many of whom may feel intimidated and threatened by their lack of understanding of emergency management best practices such as the Incident Command Structure (ICS) and emergency operation center operations. Combined, the Continuity Gap, family preparedness levels, and corporate fear create the perfect storm for a failed response to major disasters, or even to minor emergencies.

Multiple models and hybrid subsets of emergency management and business continuity planning, most of which evolved independently, exist within wide-ranging corporate structures.

The result has been a mixed bag of programs that vary in emphasis and approach. Table 1 provides a matrix of program types. A fully mature program has no gaps that are unchecked either as part of individual or overall planning. This matrix is a first step in assessing where an organization is with regard to business continuity planning and emergency management.

Integrated programs work; however, they must be firmly anchored in true collaboration and understanding of what is needed, what is important, and what is effective. When it fails, the results can be catastrophic.

Lessons Learned – Failure to Plan

An example of such failure is ABC Manufacturing (company name changed for privacy). ABC spent hundreds of thousands of dollars establishing very detailed IT recovery plans

and strategies, but excluded (intentionally) all other departments and disciplines from the planning process. The "we're in charge and we know what's best" attitude of the company's lead planners was fully in play. However, a structural fire at a main data facility exposed the fact that, despite their planning, the company had not created a simple evacuation plan or conducted a drill for the employees at the facility. Although this may sound improbable, it actually happened, and thankfully nobody was killed or injured. The incident did, however, underscore the very weaknesses in many corporate plans, and led to changes in the company's planning policies.

The following four lessons learned may help corporate leaders address the Continuity Gap:

- ***Lesson 1:*** Do not allow business continuity, IT, risk, compliance, security, or other key business functions to plan in a vacuum. Although these organizations are typically specialists, they often lack a broader understanding of emergency planning. This means not merely expecting key stakeholders to "play nice" and collaborate on their own, because chances are it will not happen. To ensure accountability, consider Lessons 2-4.
- ***Lesson 2:*** Establish a planning team representative of the key players. If possible, retain an outside consultant to help establish regular planning meetings, goals, objectives, and outcomes. This will help prevent "turf wars" and ensure all voices are equally heard in the planning process.
- ***Lesson 3:*** If not already on staff, hire an experienced emergency manager. Although the business continuity and other teams may be staffed with quality people, they are not necessarily experienced in the nuances of emergency planning and operations.
- ***Lesson 4:*** Establish an inclusive and comprehensive guidance document that clearly sets forth the company's philosophy, culture, and methodology for handling emergencies. Do not leave planning to chance, and do not assume all key managers and departments are entering the discussion from the same vantage point. Collaborate at all costs, do not assume any function has all the answers.

Finally, a common company goal is to be resilient to support its stockholders, investors, and customers, and to continue to lead the long-term financial viability of the communities it serves. Often forgotten in that effort are the people who make it happen! Every business continuity or emergency management program plan should begin and end with the understanding that, regardless of the business, it cannot run by itself without employees. Part of every resilience plan, program, and activity should involve asking the question, "What have we done today to ensure our employees are equipped and capable of supporting the recovery?" Disaster planning should be anchored in employee and family preparedness. To accomplish this, human resources must be actively engaged on the planning team. If an employee's family is affected by the emergency, he or she will not be free to come to work or to play a critical part in company recovery.

Vincent B. Davis, CEM, *is senior preparedness manager for Sony Network Entertainment, where he is responsible for developing disaster plans and programs for the company's North America locations. Before joining Sony, he was program manager of emergency preparedness and response for Walgreens Co., where he designed emergency plans and coordinated emergency operations center operations for the company's 8,300 stores and facilities during major disasters. Following his career in the U.S. Air Force and Illinois National Guard, with 23 years in military public affairs, he served as: external affairs and community relations manager at the Federal Emergency Management Agency (FEMA); regional preparedness manager for the American Red Cross of Greater Chicago; and private sector consultant to the Illinois-Indiana-Wisconsin Regional Catastrophic Planning Team. He holds certifications as an Illinois Professional Emergency Manager and FEMA Professional Continuity Practitioner, and is a member of the International Association of Emergency Managers Children's Caucus and a lifetime member of the Black Emergency Managers Association. He authored, "Lost And Turned Out, A Guide To Preparing Underserved Communities For Disasters," and founded PreparednessMatters.org Consulting. He also is vice president of strategic alliances and community relations for PrepWorld LLC, creators of PrepBiz Video Gamification for Disaster Preparedness Education APP for children.*

DISASTER RECOVERY JOURNAL

White Papers
Source: http://www.drj.com/resources/white-papers.html?utm_medium=email&utm_source=3-16-16-Regus&utm_campaign=Regus#Clearview

DRJ's White Paper section is the one place to explore in-depth thoughts on today's most relevant issues. Discover insight into a variety of topics including cloud computing, industry standards, personnel management, risk analysis and much more. The subjects are constantly evolving, providing you a non-stop feed of up-to-date industry information.
White Papers are sponsored by our industry's leading service providers. This allows DRJ to bring you the most relevant information in a free, convenient format. Your contact information will be shared with White Paper sponsors.

▶ **Note: You must be logged into DRJ.com to download these free White Papers**

Employee Safety Critical Communication Best Practices

Sponsored by Everbridge
Keeping employees safe should be one of the main goals of any organization. Whether the threat is a severe storm on the way or a possible shooter employees should be informed about all things that could endanger them. In this white paper, Employee Safety: Critical Communication Best Practices, learn about key recommendations to consider when deploying a critical communication system to improve employee safety.
DOWNLOAD

Targeting Employees with Location-Based Notifications

Sponsored by Everbridge
Workplace mobility is on the rise, which means organizations likely have an increasing number of employees who travel or work from home creating unique communication challenges. During emergencies and other critical incidents one of the major worries for organizations is employee safety regardless if they are at the office or not. How can you ensure that employees get the right message at the right time when they could be in danger?
In this white paper Targeting Employees with Location-Based Notifications learn how to:

- Gather accurate employee data
- Use custom maps to send targeted notifications to employees
- Keep employees up-to-date about critical incidents and other threats that could endanger them

DOWNLOAD

Identifying and Responding to Threats

Sponsored by Everbridge
Hurricanes, bombings, power outages and infrastructure events remind us that all organizations are vulnerable to threats. How can effective incident monitoring processes help you better anticipate prepare for and respond to risks and improve corporate resiliency? In this paper global risk analysis experts from NC4 share best practices for incident monitoring tips for effectively managing the impact of incidents and guidance on how to incorporate incident notification into your critical communication strategy.
DOWNLOAD

Continuous Avaiability Mission Critical Apps

Sponsored by Artisan Infrastructure

When it comes to extending the benefits of server virtualization to their mission critical business applications, many organizations often struggle with how to re-architect their environment and strike the right balance between performance, scalability, manageability and most importantly, high availability and disaster recovery. This white paper outlines many of the common deployment scenarios that such organizations face and describes how Neverfail Business Continuity Management can be used to deliver a more complete, consistent and cost effective availability solution for mission-critical, business applications.

DOWNLOAD

Buyers Guide Choosing The Right BC Technology

Sponsored by Artisan Infrastructure

There are a myriad of technologies offering different approaches to data protection, application availability, high availability and disaster recovery. These technologies typically have at least one thing in common: they are IT-based solutions that are built to protect IT assets. When it comes to business continuity, it is imperative that choosing the right solution is a business decision based on the level of risk and disruption that can be tolerated by the different parts of the business. This paper explores some of the factors which will govern the selection of the right solutions to deliver an appropriate solution for business continuity.

DOWNLOAD

Common DR Plan Misconceptions

Sponsored by Artisan Infrastructure

Outages do not discriminate. Not having had an outage for a year (or even ten years) does not mean you are any less vulnerable than anyone else. An outage may be nothing more than a wrinkle in your day or it can end your business in one fell swoop. This paper discusses four primary misconceptions regarding a disaster recovery plan, and their corrective actions.

DOWNLOAD

A BCM Professional's Playbook on Converging Business Continuity & Risk Management

Strategic BCP

Discover a better way to address key business continuity standards and guidelines that are so important for compliance and better continuity plans. Harness the power of the original BCP Genome™ to strengthen your own planning and compliance practices—whether you adopt its framework as is, or adapt its logic to create your own framework. Also, compare eight leading industry standards—ISO22301, FFIEC, NFPA, NIST, HIPAA, and more—to identify their strengths and gaps relative to program organization, management, training, and audit vs. emergency facilities or business and IT recovery.

DOWNLOAD

Best Practices in Using a Notification System

Sponsored by MIR3, Inc.

When a crisis strikes, you need to alert your stakeholders. And if you want to control your message, you need to get that information out as fast as, or faster, than anyone else. With the growth of social media, that's not always easy. By preparing your message and using your notification system more effectively, your organization will stand the best chance of surviving a crisis. Regardless of how you use notification today, this paper will show you how get more from the system you already have.

DOWNLOAD

The BCM Professional's Playbook: Convergence of Business Continuity & Risk Management

Sponsored by Strategic BCP

The demands placed upon Business Continuity, Risk Management, and Disaster Recovery professionals increase every day. As a result, organizations need to reassess their approach Business Continuity Management. If they don't, they'll get left behind, affected by continued adherence to outdated methods. The convergence of these disciplines is ongoing. Emerging regulations, frameworks, and standards place greater emphasis on risk management. As decision makers accept this evolution, Business Continuity increasingly becomes a subset of Risk Management. How the process is implemented—the value it brings a risk-based model—determines whether or not the process is a sound.

DOWNLOAD

Exploring the Business Continuity Software Market

Sponsored by Clearview

ClearView Continuity is a UK based supplier of specialist business continuity software. Re-launched in 2010, it has seen rapid global growth with collaborators and clients in all parts of the world, from Australia to South Africa, South East Asia, Russia, the Middle East, Europe and the US. The global network of collaborators enables ClearView to provide 24/7 global support for its clients, who range from the largest global financials to more modest single-country organizations. Clearview does not place restrictions on user numbers or functionality which means that all clients benefit from the same powerful functionality.

DOWNLOAD

Is Business Continuity Certification Right For your Organization?

Sponsored by Avalution

This white paper analyzes the business case for pursuing organizational business continuity certification, including what it takes to complete the certification process and how best to begin preparing.

DOWNLOAD

Designing a Business Continuity Training Program to Maximize Value & Minimize Cost

Sponsored by Avalution

Business continuity is a key component of an organization's risk management program. However, employees (ranging from executives to the general employee population), partners and customers are often unaware of the existence of the program or their role within the business continuity effort. Can management rely on a business continuity program if key stakeholders are unaware of their response and recovery responsibilities? No. And, as a result, the time and resources invested in the planning effort are often wasted.

DOWNLOAD

Unitrends Backup & Recovery Solutions and Disaster Recovery Best Practices: Hurricane Preparedness

Sponsored by Unitrends

The ability of your business to respond to a disaster depends on how well your IT organization can address specific situations. While you can only plan for so much in the way of detail, you can understand and anticipate both the likelihood and ramifications of certain types of disasters, and use this knowledge to plan your response and thus expedite the disaster recovery process.

In this case, let's take a look at the threat of a hurricane…

DOWNLOAD