August 2015

CBRNE NEWSLETTERRORISM

E-Journal for CBRNE & CT First Responders

10 years

www.cbrne-terrorism-newsletter.com

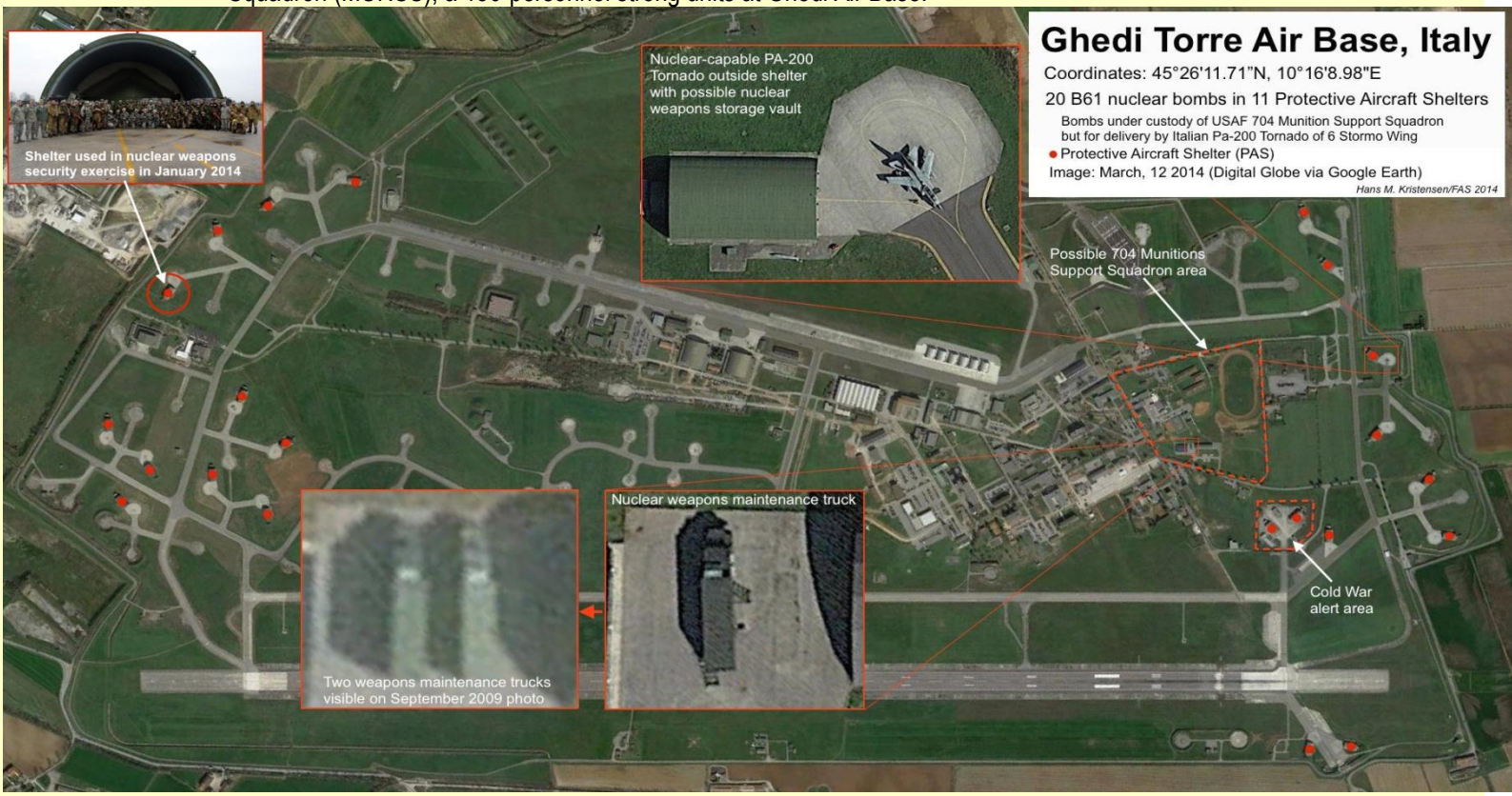
US Nuclear Weapons Base In Italy Eyed By Alleged Terrorists

Source: http://fas.org/blogs/security/2015/07/ghedi-terror/

July 22 – Two suspected terrorists arrested by the Italian police allegedly were planning an attack against the nuclear weapons base at Ghedi.

The base stores 20 US B61 nuclear bombs earmarked for delivery by Italian PA-200

Tornado fighter-bombers in war. Nuclear security and strike exercises were conducted at the base in 2014. During peacetime the bombs are under the custody of the US Air Force 704th Munitions Support Squadron (MUNSS), a 130-personnel strong units at Ghedi Air Base.



The Italian police said at a press conference today that the two men in their conversations "were referring to several targets, particularly the Ghedi military base" near Brescia in northern Italy.

Ghedi Air Base is one of several national air bases in Europe that a US Air Force investigation in 2008 concluded did not meet US security standards for nuclear weapons storage. Since then, the Pentagon and NATO have spent tens of millions of dollars and are planning to spend more to improve security at the nuclear weapons bases in Europe.

There are currently approximately 180 US B61 bombs deployed in Europe at six bases in five NATO countries: Belgium (Kleine Brogel AB), Germany (Buchel AB), Italy (Aviano AB and Ghedi AB), the Netherlands (Volkel AB), and Turkey (Incirlik AB).
Over the next decade, the B61s in Europe will be modernized and, when delivered by the new F-35A fighter-bomber, turned into a guided nuclear bomb (B61-12) with greater accuracy than the B61s currently deployed in Europe. Aircraft integration of the B61-12 has already started.

EDITOR'S COMMENT: If the mapping of an AF Base with nukes is so detailed on Internet why we wonder about possible future attacks.

NNSA repatriates radiological material from Mexico

Source: http://www.homelandsecuritynewswire.com/dr20150729-nnsa-repatriates-radiological-material-from-mexico

July 29 – Several U.S. government agencies — the Department of Energy's (DOE) National Nuclear Security Administration (NNSA), in partnership with the Defense Threat Reduction Agency (DTRA), the U.S. Air Force (USAF), the U.S. Department of Agriculture (USDA) — and the United Mexican States, have **successfully completed the repatriation of three irradiators containing U.S.-origin radioactive sources from Mexico**.

For thirty years, these irradiators played an important role in the eradication of a devastating livestock parasite, the screwworm. **The three irradiators contain more than 50,000 curies of cesium-137**, a high-activity radioisotope that could be used in radiological dispersal devices (RDD).

"This announcement marks a significant achievement in collaboration with our Mexican partners to improve global nuclear and radiological security," said NNSA Deputy Administrator for Defense Nuclear Nonproliferation Anne Harrington. "This work is a reflection of our shared threat reduction and nuclear security goals."
The irradiators were packaged and transported on a secure truck to an airport in Southern Mexico and then flown via USAF C-17 to an Air Force base in the United States. The shipment was then transported via truck to a permanent storage facility. Teams from Idaho National Laboratory, Los Alamos National Laboratory, Lawrence Livermore National Laboratory, and the Savanah

River Site supported this repatriation project for DOE/NNSA.

NNSA notes that DOE/NNSA's Office of Radiological Security (ORS) mission is to prevent radioactive materials from use in acts of terrorism. To achieve the mission, ORS protects radioactive sources used for medical, research, and commercial purposes, and removes and disposes of disused radioactive sources. The agency also aims to reduce the global reliance on radioactive sources by promoting non-isotopic alternative technologies.

NNSA was established by Congress in 2000 as a semi-autonomous agency within the U.S. Department of Energy responsible for enhancing national security through the military application of nuclear science. Among other tasks, NNSA maintains and enhances the safety, security, reliability and performance of the U.S. nuclear weapons stockpile without nuclear testing; works to reduce global danger from weapons of mass destruction; provides the U.S. Navy with safe and effective nuclear propulsion; and responds to nuclear and radiological emergencies in the U.S. and abroad.

Next stop Mars, with Israeli radiation protection

Source: http://www.timesofisrael.com/next-stop-mars-with-israeli-radiation-protection/#.VcDbqP_nEvo.linkedin

Israeli technology that can protect first responders from deadly gamma radiation – the kind of radiation emitted by nuclear bombs – may one day protect astronauts who explore deep space from the high levels of radiation they are likely to encounter.

Israel's StemRad is working with US defense giant Lockheed-Martin to develop a version of its gamma-ray shielding vest for use in deep-space missions, the companies announced this week.

"We're going to take our extensive knowledge of human spaceflight, apply our nano- materials engineering expertise, and working closely with StemRad, evaluate the viability for this type of radiation shielding in deep-space," said Randy Sweet, Lockheed Martin business development director for the civil space line of business. "The Lockheed Martin team believes this could result in an innovative solution to enhance crew safety on the journey to Mars."

Lockheed Martin is the prime contractor building Orion, NASA's next-generation spacecraft designed to transport humans to destinations beyond low Earth orbit and bring them safely home. Designed for the space missions of tomorrow, Orion will, among other things, provide technology against the effects of deep-space radiation, considered one of the biggest threats and roadblocks to human exploration of the solar system beyond the moon.

Key to the effort to protect against such radiation is the solution by StemRad, which has a product that protects first responders against gamma radiation generated by, among other things, nuclear explosions. Cleverly designed to allow freedom of movement, the **StemRad 360 Gamma belt** is not a full-body suit that makes it difficult to maneuver and freely explore – a key requirement for rescue workers.

Exposure to gamma radiation results in radiation sickness, the accelerated destruction of the blood cells and the inability of the body to replenish them, due to the damage sustained to bone marrow, which needed to generate new

cells. Fifty percent of the body's bone marrow is located in the groin and midsection areas of the body – and that is exactly the part of the body the StemRad belt protects, ensuring that rescue workers are protected against the effects of radiation sickness, but are able to maintain freedom of movement needed to assist others.

The company's technology got a tribute from the Japanese ambassador to Israel, who said that "StemRad has answered the challenge of the 2011 earthquake and tsunami." Ambassador H.E. Hideo Sato did not reveal the specifics of StemRad's activities in Japan in the wake of the Fukushima nuclear disaster, perhaps the worst, and long-lasting, effect of those events, but StemRad has received numerous awards and accolades ijn Japan for its work there.

Now that radiation on earth has been "conquered," it's time to move into outer space – and the new project with LM will do just that, officials in both companies said. The joint project won the support of a bilateral research committee and will be supported by grants from Space Florida, the aerospace economic development agency of Florida and MATIMOP, the executive agency of the Office of the Chief Scientist of the Economy Ministry of Israel.

"We are excited to be collaborating with Lockheed Martin on this important project," said Dr. Oren Milstein, co-founder and Chief Scientific Officer of StemRad. "Our team possesses advanced capabilities in the areas of radiation biology and innovative shielding strategies, and we will now be applying those skills to the unique challenges in human space exploration."

Hiroshima and Nagasaki: Lessons learned?

Source: http://thebulletin.org/hiroshima-and-nagasaki-lessons-learned8599

In August 1945, little more than three weeks after the Trinity test inaugurated the atomic age, the United States detonated "Little Boy" over Hiroshima, killing tens of thousands. Days later, the same fate was visited on Nagasaki with "Fat Man." Historians have debated whether the bombings were necessary or gratuitous; justified or criminal; responsible for Japan's surrender or largely irrelevant to it. Today, with the remaining survivors of Hiroshima and Nagasaki approaching the

end of life, to what extent has the world absorbed the lessons of the bombings—and can seven more decades elapse without the wartime detonation of a nuclear weapon?

In the lifetimes of the survivors

By Akira Kawasaki

The 70th anniversary of the Hiroshima and Nagasaki bombings is a highly symbolic one. Seventy years, after all, is roughly an average human lifespan—so time is running out for the relatively few individuals who have first-hand experience of a wartime nuclear detonation. Many survivors of Hiroshima and Nagasaki, known in Japanese as *Hibakusha*, have already passed away. Fewer than 200,000 are still living. The average *Hibakusha* is now more than 80 years old. What will their legacy be? Has the world absorbed the lessons that the *Hibakusha* have sought to teach? And how will Hiroshima and Nagasaki be remembered by generations to come?

For decades, *Hibakusha* have spoken tirelessly and courageously about their tragic experiences. They have warned the world about the cruel, inhumane, and immoral effects of nuclear weapons. They have repeatedly sent delegations to the UN General Assembly and to review conferences for the Nuclear Non-Proliferation Treaty (NPT). They have conducted letter-writing campaigns urging nuclear weapon states to accelerate disarmament. They have appealed to both policy makers and ordinary people to create a world free of nuclear weapons.

But outside Japan, their voices have often been ignored. Indeed, their message has sometimes been misinterpreted so badly that the horrific experiences they describe have been portrayed as an incentive for nations to develop nuclear weapons in the name of deterrence.

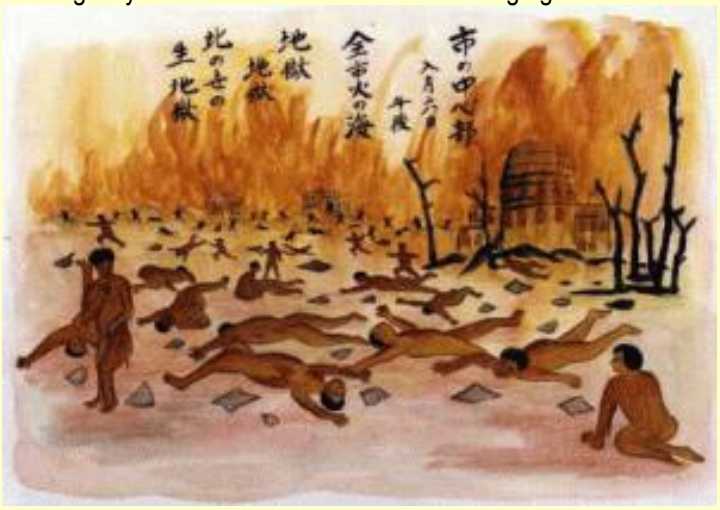
But deterrence doesn't explain why nuclear weapons have not been used in wartime over the last seven decades. The United States considered using nuclear weapons during both the Korean and Vietnam Wars—but did not use them. US leaders rejected the nuclear option not because they feared retaliation but because they understood the physical, humanitarian, and political consequences that the nuclear option would have entailed. In other words, it is not an adversary's readiness to use nuclear weapons, but rather recognition of these weapons' catastrophic impact, that has prevented wartime nuclear detonations for 70 years.

But as *Hibakusha* continue to age, and as their memories fade, the taboo surrounding the use of nuclear weapons may weaken in national policy debates. Even in Japan nowadays, the doctrine of nuclear deterrence is challenged less and less. This has provided space for a handful of ideologues to advocate that Japan become nuclear-armed itself.

Still, the *Hibakusha*, whose dream is to see a world without nuclear weapons within their lifetimes, have in recent years gained hope for disarmament. Their renewed hope is largely due to the international community's increased focus on the humanitarian consequences of using nuclear weapons.

A movement gets moving

The "humanitarian initiative" arguably began with a 2010 appeal by the president of the International Committee of the Red Cross that noted "the unspeakable human suffering" that nuclear weapons cause and called for their elimination "through a legally binding international treaty." The next year, the Council of Delegates of the Red Cross and Red Crescent issued a resolution that highlighted the "destructive power of nuclear weapons [and] the threat they pose to the environment and to future generations." The resolution appealed to all states to "ensure that nuclear weapons are never again used" and to work with urgency and determination toward a binding agreement that eliminates nuclear weapons.



Then, during a 2012 NPT meeting in Vienna, the nation of Switzerland issued a statement on behalf of 16 countries emphasizing the humanitarian dimensions of nuclear disarmament. The statement stopped short of calling for a ban on nuclear weapons. But the number of countries that support the statement has grown. By April of this year, 159 countries had signed on to a sixth version.

In the interim, a series of international conferences on the humanitarian impact of nuclear weapons was conducted. Featuring testimony from *Hibakusha*, these conferences built upon the lessons of Hiroshima and Nagasaki; there was also testimony from survivors of nuclear tests. Experts highlighted the catastrophic effects that would proceed from any nuclear detonation—whether intentional, accidental, or as a result of miscalculation. Tens of millions would be killed, injured, or displaced. The global climate would be disrupted, leading to famine. Communication infrastructures would be destroyed and the global economy would be impaired, rendering impossible any effective humanitarian response by governments or relief agencies.

In response to these appalling scenarios, the chair of the 2014 humanitarian conference in Nayarit, Mexico stated that the “time has come to initiate a diplomatic process” toward reaching “new international standards and norms, through a legally binding instrument.” He also stated that “in the past, weapons have been eliminated after they have been outlawed” and that “this is the path to achieve a world without nuclear weapons.” In other words, he called for an outright ban on nuclear weapons—something that would go far beyond the relatively weak disarmament requirements of the NPT. He identified the 70th anniversary of the Hiroshima and Nagasaki attacks as “the appropriate milestone to achieve our goal.”

Existing international law doesn't regulate nuclear weapons properly. Unlike other weapons of mass destruction, nuclear weapons are not banned in explicit terms. The NPT is the only multilateral treaty that contains a binding commitment to nuclear disarmament—but this treaty, while it prevents most states from acquiring nuclear weapons, effectively allows five states to possess them. What's needed, then, is a complete legal prohibition against all nuclear weapons.

In order to redress this fundamental deficit in the disarmament regime, the Austrian government at the 2014 humanitarian conference in Vienna initiated what has become known as the Humanitarian Pledge. In the pledge, Austria called on all parties to the NPT to "identify and pursue effective measures to fill the legal gap for the prohibition and elimination of nuclear weapons.” This statement, though rendered in rather bland diplomatic language, appears to identify the Nuclear Non-Proliferation Treaty as inadequate for achieving disarmament and pledges action to create an alternate, much stricter legal structure. A number of civil society groups have begun promoting the pledge—and it has now been endorsed by some 110 governments, a number that continues to grow.

A fitting legacy

For 70 years, *Hibakusha* have worked to communicate that nuclear weapons are inhumane and the consequences of using them are unacceptable. In Nayarit, the *Hibakusha* Setsuko Thurlow said that "Although we *Hibakusha* have spent our life energy to warn people about the hell that is nuclear war, in nearly 70 years there has been little progress in the field of nuclear disarmament. … It is our hope that this new movement to ban nuclear weapons will finally lead us to a nuclear weapon–free world."

Now, within the limited time left to those who have first-hand experience of wartime nuclear detonations, is the moment to establish an international treaty that stigmatizes nuclear weapons, criminalizes them, and provides for their total elimination. Such a treaty would honor the *Hibakusha*'s seven decades of work and provide them a fitting, lasting legacy.

Akira Kawasaki *is a member of the Executive Committee of the Tokyo-based nongovernmental organization Peace Boat. He also serves on the International Steering Group of the International Campaign to Abolish Nuclear Weapons. Since 2008, Kawasaki has coordinated "Global Voyage for a Nuclear-Free World: Peace Boat's* Hibakusha *Project," in which atomic bomb survivors travel the world to share their stories. In 2009 and 2010, he was an advisor to the cochairs of the International Commission on Nuclear Non-proliferation and Disarmament. He lectures at Rikkyo University in Tokyo and writes frequently for Japanese newspapers and for peace and disarmament journals.*

One photo a thousand words

Nagasaki, Japan: Atmic bomb survivor Sumiteru Tanigushi 70 yrs today

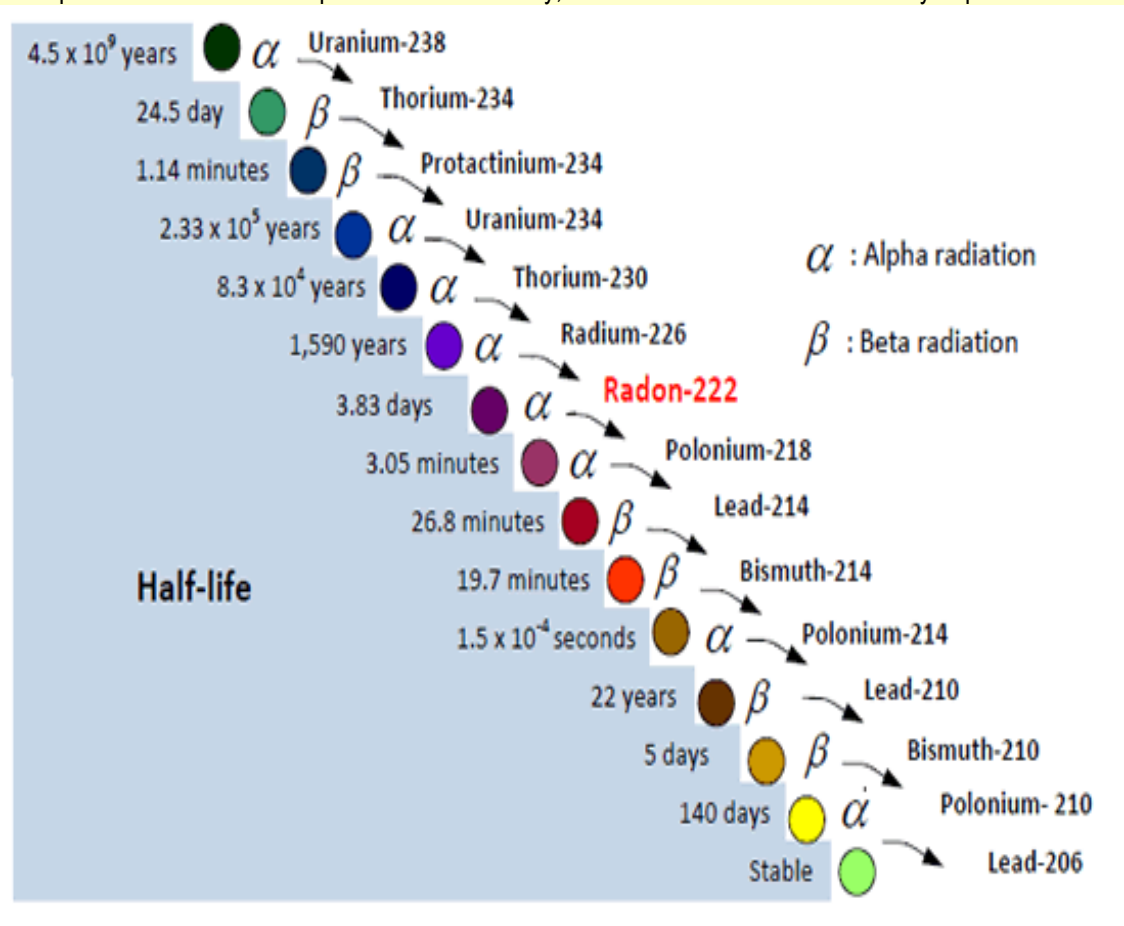
Ukrainian security services stop criminal gang from selling uranium

Source: http://www.homelandsecuritynewswire.com/dr20150806-ukrainian-security-services-stop-criminal-gang-from-selling-uranium

Aug 06 – The security services of Ukraine say they have seized a small quantity of ore-grade uranium from a criminal gang in the western part of the country.

The **State Security Service of Ukraine (SBU) said the group had been trying to sell the uranium-238 isotope to an unknown client** when they were arrested.

The police arrested the suspects on Wednesday, and the arrest was immediately reported to the



president, Petro Poroshenko. "Four members of a criminal group that was trying to sell the nuclear material were detained with the evidence in hand," Interfax quoted an SBU statement as saying. "According to preliminary information, the nuclear matter was uranium-238."

The U-238 isotope is the most commonly occurring in nature and. It is radioactive, but it is not fissile so it cannot be used directly to create a nuclear chain reaction or explosion.

The *Guardian* reports that Ukrainian media has recently reported of speculations about pro-Russian rebels' ability to develop a "dirty" bomb which would use conventional explosives to scatter lethal radioactive fallout.

When the Soviet Union collapsed in December 1991 and the Red Army hastily, and in a disorganized fashion, withdrew from Ukraine , Ukraine found itself in possession of a small nuclear arsenal which was left behind. After lengthy negotiations, Ukraine agreed to return the nuclear warheads to Russia in exchange for a generous economic aid package from the United States. Ukraine, however, still has nuclear materials storage facilities and disposal sites for nuclear waste from nuclear power reactors.

The Ukrainian authorities that the uranium was seized in a region in the heart of Ukraine's nationalistic west, which has been untouched by the 16-month separatist war to the east.

Israeli port evacuated after container emitting suspicious radioactive radiation detected

Source: http://www.homelandsecuritynewswire.com/dr20150806-israeli-port-evacuated-after-container-emitting-suspicious-radioactive-radiation-detected

Aug 06 – **Israeli authorities on Monday evacuated the Ashdod port in southern Israel after an Israeli shipping container which arrived on a Chinese ship was detected to emit irregular radioactive radiation. By mid-afternoon, the port went back to normal operation.**

Arutz Sheva reports that the container, which contained **industrial iron**, was immediately isolated for inspection, and large forces of police, bomb disposal crews, firefighters, and EMS personnel was dispatched to the scene.

Experts from the Israel Atomic Energy Commission (IAEC) were also sent to examine the suspicious container.

The Ministry of Environmental Protection, after instructing that the container be transferred to remote area at the port, announced that the public was in no danger from the radiation.

By late afternoon, the Ashdod port authority announced that the hazardous materials protocol was followed, and that the incident involved "minimal levels" of radioactive material.

The port authority said that at no time was there a danger from the radiation outside of the container's wall.

Arutz Sheva notes that Israeli ports have installed advanced radioactive radiation systems in an effort to detect "dirty bombs" which terrorists may try to smuggle into Israel.

Two years ago there was a similar incident, when a container was detected to be emitting radiation, but it was later discovered to be a false alarm.

New reference material to help monitor oceans' radioactive contamination

Source: http://www.homelandsecuritynewswire.com/dr20150806-new-reference-material-to-help-monitor-oceans-radioactive-contamination

Aug 06 – **A new reference material which will help laboratories accurately measure radioactive contamination in seawater is now available from the National Institute of Standards and Technology (NIST).**

NIST SRM 4358, Ocean Shellfish Radionuclide Standard

The new reference material, a mixture of freeze-dried, powdered shellfish, provides a benchmark for scientists analyzing the local ocean environment's level of contamination — for example, after an accident such as the 2011 nuclear plant disaster in Fukushima, Japan. The material, formally NIST Standard Reference Material (SRM) 4358, is made from shellfish that contain low but well-characterized amounts of several radioactive elements. NIST notes that reference materials which are certified by NIST to have certain known measurement values

help researchers calibrate measurement equipment and validate their own analysis methods with greater precision.

"In particular, this SRM will help laboratories measure radioactivity levels in seafood," says NIST's Svetlana Nour. "It will help them to screen more samples in a shorter period of time."

The reference material contains a powdered mixture of oysters and mussels collected from three locations: the Irish Sea, the White Sea, and the Sea of Japan before 2011. Each of these water bodies possesses some level of radioactive contamination.

"The radioactive contamination of the ocean is a concerning environmental problem," Nour says. "Shellfish are important indicators because of their capacity to accumulate radioactive elements from seawater."

Each reference bottle holds 150 grams of powder that contains specific amounts of radioactivity. More than 1,500 bottles were produced, which could supply the radiochemistry community with an anticipated 10-year supply of the SRM according to previous estimates.

NIST created this reference material with the assistance of eleven other laboratories from nine countries, including several other national metrology institutes. The labs involved used several different extractions and analysis methods to characterize the radioactive content of the shellfish. Nour says the reference material benefits from the support and experience of the other labs that participated in its development.

"Creating an SRM like this is costly and time-consuming work," she says, "but it's important to have them so we can make good measurements that would allow good and quick decisions when a specific contamination situation occurs."

SRM 4358, "Ocean Shellfish Radionuclide Standard," is available for purchase from NIST. A complete technical description of the SRM and the details of its development was published in 2013 in the *Journal of Radioanalytical Nuclear Chemistry*.

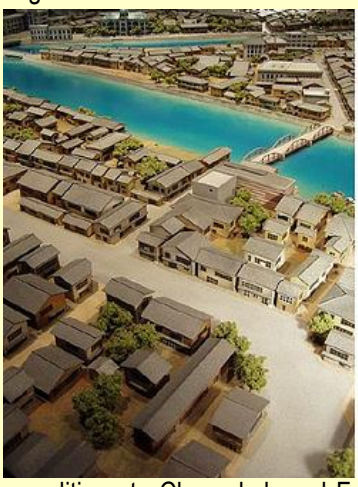
— Read more in S. Nour et al., "Characterization of the NIST shellfish Standard Reference Material 4358," Journal of Radioanalytical Nuclear Chemistry 296, no. 1 (April 2013): 301-7.

What if it happened again? What we need to do to prepare for a nuclear event

By Cham Dallas

Source: http://www.homelandsecuritynewswire.com/dr20150820-what-if-it-happened-again-what-we-need-to-do-to-prepare-for-a-nuclear-event

Aug 20 – As we observe the 70th anniversary of the bombings of Hiroshima and Nagasaki, it may seem like the threat from nuclear weapons has receded. But it hasn't; the threat is actually increasing steadily. This is difficult to face for many people, and this denial also means that we are not very well-prepared for nuclear and radiological events.



I've been studying the effects of nuclear events – from detonations to accidents – for over thirty years. I've been involved in research, teaching and humanitarian efforts in multiple expeditions to Chernobyl- and Fukushima-contaminated areas. Now I am involved in the proposal for the formation of the Nuclear Global Health Workforce.

Such a group could bring together nuclear and non-nuclear technical and health professionals for education and training, and help to meet the preparedness, coordination, collaboration and staffing requirements necessary to respond to a large-scale nuclear crisis.
Any nuclear weapon exchange or major nuclear plant meltdown will immediately lead to a global public health emergency. The Ebola outbreak taught the world that we should have resources in place to handle a major health emergency before it happens.
What would a Nuclear Global Health Workforce need to be prepared to manage? For that we can look back at the legacy of the atomic bombings of Hiroshima and Nagasaki, as well as the nuclear accidents like Chernobyl and Fukushima.

What happens when a nuclear device is detonated over a city?

Approximately 135,000 and 64,000 people died, respectively, in Hiroshima and Nagasaki. The great majority of deaths happened in the first days after the bombings, mainly from thermal burns, severe physical injuries and radiation.
Over 90 percent of the doctors in nurses in Hiroshima were killed and injured, and therefore unable to assist in the response. This was largely due to the concentration of medical personnel and facilities in inner urban areas. This exact concentration exists today in the majority of American cities, and is a chilling reminder of the difficulty in medically responding to nuclear events.
What if a nuclear device were detonated in an urban area today? I explored this issue in a 2007 study modeling a nuclear weapon attack on four American cities. As in Hiroshima and Nagasaki, the majority of deaths would happen soon after the detonation, and the local health care response capability would be largely eradicated.
Models show that such an event in an urban area in particular will not only destroy the existing public health protections but will, most likely, make it extremely difficult to respond, recover and rehabilitate them.
With medical facilities decimated after a detonation, treating the injured will be a tremendous challenge. We would need predicted casualty distributions and locations to figure out how to best allocate what resources and personnel remain.
Very few medical personnel today have the skills or knowledge to treat the kind and the quantity of injuries a nuclear blast can cause. Health care workers would have little to no familiarity with the treatment of radiation victims. Thermal burns would require enormous resources to treat even a single patient, and a large number of patients with these injuries will overwhelm any existing medical system. There would also be a massive number of laceration injuries from the breakage of virtually all glass in a wide area.
Currently, it has not been worked out how medical systems in affected areas are supposed to cope with the overwhelming numbers of patients from an urban nuclear detonation. This makes it that much more important to have an effort like the Nuclear Global Health Workforce to work to address and help nations prepare for these overwhelming events.

Getting people out of the blast and radiation contamination zones

A major nuclear event would leave large swaths of territory uninhabitable for decades, with catastrophic impacts on humans, the economy and the environment.
Decisions to evacuate at-risk populations must be made within hours, but plans for and criteria to evacuate are lacking. And the scale of these evacuations and potential resettlement is tremendous.
For instance, within a few weeks after the Chernobyl accident, more than 116,000 people were evacuated from the most contaminated areas of Ukraine and Belarus. Another 220,000 people were relocated in subsequent years. But thousands continue to live in areas classified by Ukrainian and Belarussian authorities as strictly controlled zones, where chronic radioactive cesium contamination remains a problem.
The day after the Fukushima earthquake and tsunami, over 200,000 people were evacuated from areas within 20 kilometers (12 miles) the nuclear plant because of the fear of the potential for radiation exposure.
On Day 3, people living in the 20-30 kilometer (12-18 mile) zone around the plant were asked to remain indoors, and eventually advised to self-evacuate.
The evacuation process was plagued by misinformation, inadequate and

confusing orders and delays in releasing information. There was also trouble evacuating everyone from the affected areas. Elderly and infirm residents were left in areas near the plant, and hospitalized patients were not always taken where they needed to go. All of these troubles lead to a loss of public trust in the government.

Chernobyl and Fukushima were both reactor meltdowns. A high-yield nuclear weapon – that is, a large device with a very large blast and radiation capability – would bring patient and evacuation numbers to incomprehensible levels.

However, the current Department of Homeland Security most-anticipated scenario for a nuclear attack in the United States is for smaller nuclear weapons – 10 kilotons – about the size of the weapons used to attack Hiroshima and Nagasaki.

And new evidence has altered previous dire predictions in relatively low-yield nuclear blasts such as Hiroshima and Nagasaki. Current U.S. nuclear war response protocols do not rely as much on large-scale evacuations from nearby areas.

For instance, in a hypothetical low-yield (10 kiloton) nuclear bomb over Washington, D.C., only limited evacuations are planned. Despite projections of 100,000 fatalities and about 150,000 casualties, the casualty-producing radiation plume would actually be expected to be confined to a relatively small area. People upwind would not need to take any action, and most of those downwind, in areas receiving relatively small radiation levels (from the point of view of being sufficient to cause radiation-related health issues), would need to seek only "moderate shelter."

A Nuclear Global Health Workforce could start to lay out plans for how to rapidly respond to such an attack and project whether and what sort of evacuation plans would be needed.

The long-term effects of radiation exposure

The Radiation Effects Research Foundation (RERF), which was established to study the effects of radiation on survivors of the Hiroshima and Nagasaki, has been tracking the health effects of radiation for decades.

According to RERF, about 1,900 excess cancer deaths can be attributed to the atomic bombs, with about 200 cases of leukemia and 1,700 solid cancers. Japan has constructed very detailed cancer screenings after Hiroshima, Nagasaki and Fukushima; Chernobyl research has also been extensive, but not to the extent as in ongoing in Japan.

But the data on many potential health effects from radiation exposure, such as birth defects, are less conclusive.

While it has been shown that intense medical X-ray exposure has accidentally produced birth defects in humans, there is considerable debate about whether there were birth defects in the descendants of Hiroshima and Nagasaki atomic bomb survivors.

For example, one study found more than a doubling of brain malformations in some children from Hiroshima and Nagasaki, while other respected long-term investigations have concluded there are no statistically significant increases in birth defects resulting in atomic bomb survivors.

Looking at data from Chernobyl, where the release of airborne radiation was 100 times as much as Hiroshima and Nagasaki combined, there is a similar lack of definitive data for radiation-induced birth defects.
A wide-ranging WHO study concluded that there were no differences in rates of mental retardation and emotional problems in Chernobyl radiation-exposed children compared to children in control groups.
A Harvard review on Chernobyl concluded that there was no substantive proof regarding radiation-induced effects on embryos or fetuses from the accident. Another study looked at the congenital abnormality registers for sixteen European regions that received fallout from Chernobyl, and concluded that the widespread fear in the population about the possible effects of radiation exposure on the unborn fetus was not justified.
Indeed, the most definitive Chernobyl health impact in terms of numbers was the dramatic increase of elective abortions near and at significant distances from the accident site. This was due to "nuclear phobia,", lack of information and inadequate official guidance. Not having been informed about the actual lack of risk, there was understandable anxiety regarding the possible effects of radiation on the fetus, and a panic among expectant mothers about giving birth to a child with a birth defect.
A Nuclear Global Health Workforce could help health care practitioners, policymakers, administrators and others understand myths and realities of radiation. In the critical time just after a nuclear crisis, this would help officials make evidence-based policy decisions and help people understand the actual risks they face.

What's the risk of another Hiroshima or Nagasaki?

Today, the risk for a nuclear exchange – and its devastating impact on medicine and public health worldwide – have only escalated. Nuclear weapons are spreading to more nations, and international relations are increasingly volatile. The developing technological sophistication among terrorist groups and the growing global availability and distribution of radioactive materials are also especially worrying.
Despite the gloomy prospects of health outcomes of any large scale nuclear event common in the minds of many, it is our mutually shared moral and ethical obligation to respond.

Cham Dallas *is Professor and Director, Institute for Disaster Management at University of Georgia.*

Thermo Fisher Scientific Launches Hands-Free Radiation Detection Technology

By: Judi Ritter Sutherland

Source: http://www.hstoday.us/single-article/thermo-fisher-scientific-launches-hands-free-radiation-detection-technology/2efa409c0a6215227c1234b8315504df.html

Aug 20 – With increasing fears that chemical, biological, radiological and nuclear materials or weapons will fall into terrorist hands, the need for innovative radiation detection technology has never been so pressing. In response, Thermo Fisher Scientific developed a new line of radiation area monitors that eliminates operational requirements for on-site safety and security personnel.
Security personnel, military teams and first responders can now utilize the Thermo Scientific RadHalo rapid deployment prove (RDP) and fixed monitor (FM) to address radiation threats. The highly-sensitive **Thermo Scientific RadHalo RDP and FM spectroscopic area monitors** offer the industry's first hands-free technology to monitor dose rate and identify radiation on location or from miles away via five different reachback options.
According to the Environmental Protection Agency, some of the early symptoms of radiation sickness are fairly nonspecific and include nausea, weakness, hair loss, skin burns or diminished organ function (especially bone marrow)—and can eventually cause death—attesting to the importance of testing and monitoring an area to mitigate health hazards and aid in recovery.

"Our line of radiation detection instruments now provides higher sensitivity and accuracy while adding remote-operation functionality, putting a premium on the safety of people whose job it is to be in harm's way," said Scott Masiella, Thermo Fisher Scientific spectroscopy product line manager. "We designed the RadHalo to provide fast, autonomous radiation measurement in hot zones, further protecting personnel from exposure risk."

The RadHalo lines gives security personnel, military and emergency response teams the ability to quickly and safety identify and address radiation threats. The instruments can be deployed as fixed area (permanent) or mobile (temporary) radiation monitoring devices, enabling real-time data collection in a number of scenarios, from security checkpoints to large public gatherings. In addition, RadHalo instruments can be networked wirelessly to expand reach across large areas, venues, or even across an entire city.

The RadHalo RDP and the RadHalo FM are designed to deliver high sensitivity and accuracy across a wide range of low to extremely high radiation dose rate levels. The instruments also feature a rugged design for uninterrupted usage in various environments, including certain extreme weather conditions. With multiple configurations available, the instrument can adapt to any situation, from special event monitoring to responding to a nuclear power accident.

Other notable features of the RadHalo instrument include a 72 hour battery, a full range of built-in reachback capabilities—including WiFi, satellite, radio, cellular and direct wire, and multiple ways to view data, including a mobile app, web interface and Thermo Scientific ViewPoint command and control software.

Why was the Sendai nuclear power plant restarted?

15

By Tadahiro Katsuta

Source: http://thebulletin.org/why-was-sendai-nuclear-power-plant-restarted8644

Two of Japan's reactors—Units 1 and 2 of the Kyushu Electric Power Company's Sendai nuclear power plant—have just restarted, and Unit 1 should begin generating electricity on August 14. Like all other Japanese nuclear power plants, Sendai was shut down after the events at Fukushima Daiichi in 2011, in which an earthquake, a tsunami, egregious design mistakes, and a poor safety culture combined to form "a cascade of stupid errors" that led to a triple meltdown.

This is the first restart of any of Japan's 43 operable commercial reactors since Fukushima, and it is happening despite many unresolved questions concerning nuclear safety regulations. When it comes to safety, the Sendai nuclear power plant is definitely not at the head of the class: The utility owning the power plant was given a pass despite a very problematic history. (At one point, a regulatory commissioner called the plan to restart Sendai "wishful thinking".)

There is certainly no nationwide re-emergence of nuclear power in Japan. Indeed, there have been vocal public protests against the Sendai restart. One of the protestors even included a former prime minister of Japan.

So, why is it happening? What are the ostensible reasons for a restart? Were they valid?

A three-pointed rationalization

The justification for a restart was based upon three key points: the type of reactors to be used at Sendai were considered inherently "safer;" the chance of a similar natural disaster(s) was considered to be minimal; and the concerns of the local communities were dismissed as inconsequential.

Let us look at each of these items in turn.

Pressurized water reactors are considered inherently safe. Because strict new standards for the regulation of nuclear power plants were imposed in July 2012—the result of the belated adoption of a tougher global standard—Japan's newly formed Nuclear Regulation Authority deemed that pressurized water reactors (PWRs) such as those used at Sendai were safer than the boiling water reactor technology used at the ill-fated Fukushima Daiichi nuclear plant. Consequently, facilities with PWRs were given a longer time span—five years—to introduce severe accident countermeasures when the new regulation standards come into force.

For example, a nuclear power plant using a pressurized water reactor is not required to immediately install a filtered containment venting system to prevent large-scale radioactive contamination to the environment if the containment vessel inside is damaged. The Nuclear Regulation Authority's reasoning is that the risk of containment vessel damage is low in a pressurized water reactor because it is so much larger than in a boiling water reactor, thus allowing considerably more time before any accident measures must be put into effect. Building on this logic, the agency then gave a temporary exemption to the requirement to install the venting system to any facility using PWRs. This relieved the plant operators of heavy burdens in terms of both finances and preparatory work. All 10 of the nuclear power plants (representing six different electric companies) that applied for the waiver use pressurized water reactors.

But PWRs are not inherently safe at all; for example, their steam generators are a serious concern. In 1991, the steam generator in the pressurized water reactor at Mihama Unit 2 of Kansai Electric Power in Japan was damaged, and the emergency core cooling system had to activated. Though caused by something as simple as the failure of the mount of a metal fitting, the resulting accident was rated at Level 3, or "serious incident," on the seven levels of the International Nuclear Event Scale. Similarly, in 2013, Unit 2 and Unit 3 of the San Onofre nuclear power plant in California had to be closed due to a radiation leak from the plant's virtually new steam generators; the two units subsequently had to be retired and the plant is now in the process of a costly decommissioning, predicted to cost $3 billion. And San Onofre used pressurized water reactor technology.

Natural disasters can be predicted. There are many glaring problems with this argument, not the least of which is the tendency of, say, volcanoes to behave in ways we don't foresee. This is of major concern in Japan, which sits on the Pacific Ring of Fire, where tectonic plates interact and a large chunk of the planet's volcanic eruptions and earthquakes takes place. Kyushu Electric Power claims that volcanic eruptions can be readily predicted, and the Nuclear Regulation Authority accepted this argument. But many volcanologists insist that it is scientifically impossible to predict the eruption of a volcano—and there are many volcanoes and calderas near the Sendai nuclear power plant. According to a survey conducted by Kyushu Electric Power, catastrophic eruptions have been occurring on a 90,000-year cycle at the Aira Caldera, located 53 kilometers, or about 33 miles, from the Sendai site, with the latest eruption about 30,000 years ago. (There have been many smaller, near-continuous eruptions in the caldera since 1955.) Furthermore, sediment from the pyroclastic flow of a volcano has been discovered only 5 kilometers, or roughly 3 miles, from the reactors at Sendai.

Another problem comes from trying to determine the maximum acceleration likely to occur at the time of an earthquake. This is an issue of tremendous concern, because there are about 1,500 earthquakes of varying sizes in Japan every year. In the words of the World Nuclear Association: "Because of the frequency and magnitude of earthquakes in Japan, extra attention is paid to seismic activity in the siting, design, and construction of nuclear power plants. The seismic design of such plants is based on criteria far more stringent than those applying to non-nuclear facilities."

Yet one of the reasons that the authority announced fast-track approval for Sendai was based upon a recalculation of the largest earthquake that could reasonably be expected to occur at the site of this nuclear power plant—which was found to be *larger and more devastating* than before, based upon the known seismicity of the area and local active faults. Known as "peak ground acceleration," this figure is expressed in the number of centimeters per second squared, also known as "Galileo units" or Gal. Setting the value of a specific region's peak ground acceleration is difficult scientifically; guessing just how bad an earthquake can get is the cause of many safety design revisions and much expense. In the case of the Kyushu Electric Power Company, however, the company not only said on its restart application that an earthquake was likely to be worse than previously expected (620 Gal rather than the earlier estimate of 540 Gal), it cavalierly said that its current reactor would be able to handle the higher figure. The NRA apparently considered this platitude about the resiliency of the company's Sendai plant to be a statement of scientific fact and sufficient in terms of safety.

And some seismologists insist that an earthquake at Sendai is likely to be even more severe—they say that the earth could shake much more than 620 centimeters (about 20 feet) per second squared. For example, Katsuhiko Ishibashi, a Kobe University professor and seismologist, has been warning about the problem of nuclear power plant accidents caused by earthquakes since his first book on the topic in 1994—17 years before what happened at Fukushima Daiichi. (Ishibashi even coined a term in the Japanese language to describe the problem: "gempatsu shinsai," or "nuclear earthquake disaster.") He insists that the intensity of a more severe earthquake is underestimated because the current value does not take into consideration other phenomena, such as an interplate earthquake.

And in any case, the 620 Gal figure comes from earthquake data collected from the north end of Japan, while the Sendai nuclear power plant is located at the south end, where conditions may be different. So, we don't precisely know just how severe the peak ground acceleration will be at Sendai.

There is no available scientific literature on the influence of a major earthquake on delicate devices such as the steam generators used in pressurized water reactors.

Concerns of the local communities were dismissed. After the Nuclear Regulation Authority granted its approval in regards to the safety requirements, the final hurdle was to secure approval from two of the local governments: Kagoshima prefecture and Satsumasendai city. If they agreed, then the Sendai facility could restart.

Other neighboring communities, including six cities and two towns, had asked that the prefecture and the city include them in the list of "local governments of the nuclear power plant site." They based their request on the fact that they would likely be affected by any radioactive contamination—after all, the plume caused by the Fukushima accident spread over 250 kilometers (155 miles) from the reactor site. But only those communities within 8 to 10 kilometers (about 5 to 6 miles) from the Sendai nuclear power plant were allowed to participate.

And even those within that radius were sometimes barred from having their concerns heard. A neighboring city, Ichikikushikino, is located just 5 kilometers (about 3 miles) from the Sendai plant, but that city's request to be heard was denied by the governor of Kagoshima prefecture governor, Yuichi Ito, and by the mayor of Satsumasendai city, Hideo Iwakiri. This refusal is assumed to be based on two reasons: In addition to the difficulty of summarizing the different opinions on the nuclear restart, prefecture and city officials were concerned about having to decrease their own constituents' share of the subsidy benefits that are to be provided by the plant to local governments. In the end, only Kagoshima prefecture and Satsumasendai city approved the restart in November 2014.

Other actions by the prefecture governor caused problems, as well. The prefecture's disaster prevention plan was supposed to include an evacuation program for people requiring special assistance in any medical or welfare facilities located within 30 kilometers (about 20 miles) from the Sendai nuclear power plant. The prefectural governor, however, declared that an area within 10 kilometers (roughly 6 miles) from the power plant was more than sufficient as the target area for this program. Therefore, the number of applicable facilities was reduced from 244 facilities to to only

17 facilities, or less than one-tenth the original number. Furthermore, an evacuation facility that had been constructed by repairing an old elementary school, Yorita Elementary, turned out to have insufficient protective measures against radiation, even though the total construction cost for the facility was the equivalent of $760,000.

The real reasons for the restart

The decision to restart the reactor at Sendai is probably based upon the "dismal science:" economics.

It seems that financial considerations and worries about the health of the national and local economies triumphed over safety concerns; an article in the *Japan Times* says that when Kyushu Electric tried to turn to other means of generating electricity—such as thermal power—its costs more than doubled. "The huge costs have weighed heavily on its earnings. The company is aiming to shore up its earnings by reactivating idled nuclear power reactors. Kyushu Electric expects that the restart of the Sendai Number 1 reactor will save the company about 7.5 billion yen (over $60 million) per month."

Kyushu Electric Power had previously tried raising the price of electricity after their nuclear power plant was stopped, but that still was not enough—their deficit continued. The best hope of profitability comes from restarting nuclear power plants.

This concern for their bottom line may be understandable, but it seems to come at the expense of public safety and open, democratic, rational decision-making. Kyushu Electric Power has used questionable means to promote its agenda. For example, at an informational meeting for local residents about nuclear power plant operation only three months after the Fukushima accident, Kyushu Electric Power sent in undercover employees pretending to be ordinary citizens, who then stood up and spoke in favor of nuclear power. The company also tried to manipulate public opinion by sending in "fake e-mails" in support of the restart of nuclear power plants to a television broadcaster. The president of Kyushu Electric Power resigned after the ruses were discovered.

Meanwhile, Kyushu Electric Power still refuses to hold talks with citizen groups and neighboring local governments, even after the plant has been cleared to restart. They also refused an offer from nearly 100 citizen groups this March to hold a discussion, and did not accept a petition containing more than 100,000 signatures. The company continues to refuse the requests of many local governments within the 30 kilometer (20 miles) radius of the Sendai site.

Economics also played a role in another way: The prefecture and the nearest city are financially dependent on nuclear energy. For a long time, the prefecture governor has been clearly stating that he endorses the restart. After the prefectural assembly election this April, he revealed that the reason the restart was approved in November 2014 was to avoid having it become an election issue.

Satsumasendai city receives more than $12 million in grants annually from the nuclear industry, which it uses to pay for its public and educational facilities, receiving about $270 million over the years. According to the Satsumasendai Chamber of Commerce and Industry, the overall economic benefit of the restart of the Sendai nuclear power plant is approximately $25 million to the local economy yearly.

There are also questions of transparency in the dealings of local government authorities with Kyushu Electric Power. According to an article published this January by the *Asahi Shimbun* newspaper, construction companies run by members of the Kagoshima prefectural assembly received 26 orders for construction work at Sendai, representing $2.5 million of work, in the three years since the Fukushima accident. Not surprisingly, these members of the prefectural assembly endorsed the restart of the Sendai nuclear power plant.

According to a survey conducted this May by a major local newspaper, *Minami-Nippon Shimbun*, 59.9 percent of those polled were against a restart of the Sendai nuclear power plant. But their opinions may not be regarded as important because they have no economic significance. In this way, strict regulations are not being applied to nuclear decisions, even after the Fukushima accident. Economics was considered more important than human life: That is why the Sendai nuclear power plant was able to restart.

Note: *In the time since this article was published, Japan's weather agency on Saturday told thousands of residents to prepare for a possible evacuation as it upgraded a volcanic eruption warning. Officials raised their alert to "extremely high"—its second-highest level—after picking up increasing seismic activity around the volcano Sakurajima, which sits just off the coast of Kagoshima, a city of more than 600,000 people. The volcano is about 50 kilometres (31 miles) from the Sendai nuclear reactor.*

Tadahiro Katsuta *has a doctorate in plasma physics from Hiroshima University (1997) and is an associate professor at Meiji University in Japan. He is a 2014-2015 visiting fellow at Princeton University's program on Science and Global Security. Katsuta's research focuses on the technical and political aspects of Japan's spent fuel management problems, with particular emphasis on the Fukushima Daiichi nuclear power plant accident and the resulting new regulatory standards for commercial nuclear power reactors, nuclear fuel facilities, research reactors, and nuclear waste storage and disposal facilities.*

EDITOR'S COMMENT: Notice how low the sea waves' barrier is (photo)???

Islamic State Chickens: Terror Groups Uses Fowl, Goats as Suicide Bombers; Online Pictures Show Hens Strapped With Improvised Explosives

Source: http://www.christianpost.com/news/islamic-state-chickens-terror-groups-uses-fowl-goats-as-suicide-bombers-online-pictures-show-hens-strapped-with-improvised-explosives-141845/

Photos have been posted online purporting to show the Islamic State's new attack strategy — using innocent chickens and hens as suicide bombers to kill their enemies.

The Daily Mail reports that both pro-IS and anti-IS tweeters have shared pictures of what appears to be chickens with improvised explosive devices strapped onto them.

According to the British news agency, claims have been made that IS is equipping chickens with explosives in the Iraqi city of Fallujah. The chickens are then encouraged by the militants to venture into the opposition's territory, where IS militants remotely detonate the explosives and kill opposition fighters that are within the striking distance of the birds.

The photos emerged after Kurdish forces claimed to have captured a bomb-strapped chicken in the Syrian city of Al-Hasakah, according to the International Business Times.

Although there's no verification as to whether or not IS has in fact taken up the practice of using chickens as suicide bombers to carry out militants' dirty work, an unnamed British man fighting for the Kurdish forces explained to the Daily Mail that IS is using any means necessary to bring about the demise of the opposition.

"IS will use whatever means they can to bring death and destruction," the British fighter said. "Using animals has little military value. It is just another example of how their twisted minds enjoy dreaming up bizarre ways to kill people."

As IS has recently suffered a few defeats along its supply lines in Syria, Nasser Kataw — an expert on Iraqi terror groups who lectures at the University of Baghdad — told British newspaper The Daily Star that IS' ammunition continues to become scarce and could be forcing the terror group to devise more creative ways to utilize the weapons it has.

"The regime has countless small arms like semi-automatic weapons and pistols and lots of field weapons like mortars, but the ammunition is running low and cannot easily be replaced," Kataw said. "The regime is now desperately trying to fashion its own weapons, but lacks the machine shops to make such precision items."

According to the Daily Mail, the emergence of the bomb-strapped chicken photos comes after reports surfaced alleging that IS strapped improvised explosives to a goat and sent the goat into a Kurdish base in the Syrian border town of Kobane.

IS has also used children as suicide bombers. In early July, militants forced a 14-year-old boy to carry out a suicide attack in northern Syria that killed over 50 members of the Kurdistan Workers' Party.

The Iranian AhlulBayt News Agency reports that at least 40 children, aged between 12 and 17, have died in suicide operations for IS in the last seven months.

If the fowl claims are true, it wouldn't be the first time that IS has massacred chickens. In April, the terror group destroyed two truck shipments of U.S.-produced chicken that were on their way to starving Syrians in the war-ravished nation because it supposedly violated the caliphate's dietary restrictions.

Bomb-proof lining contains explosion in aircraft's luggage hold

Source: http://www.homelandsecuritynewswire.com/dr20150727-bombproof-lining-contains-explosion-in-aircraft-s-luggage-hold

July 27 – A bomb-proof lining developed by an international team of scientists, including academics from the University of Sheffield, has successfully contained blasts in a series of controlled explosions in the luggage hold of a Boeing 747 and an Airbus 321.

A University of Sheffield release reports that the tests, using this technology, have demonstrated that a plane's luggage hold may be able to contain the force of an explosion should a device concealed within a passenger's luggage be detonated during a flight. This would mitigate damage to the plane a nd help keep passengers safe.

A controlled explosion without (left) and with (right) Fly-Bag in the hold

The Fly-Bag, which lines an aircraft's luggage hold with multiple layers of novel fabrics and composites, was tested under increasing explosive charges on disused planes at Cotswolds Airport, near Cirencester, last week.

After the tests, explosives were placed in the aircraft without the lining to show the damage that could be caused.

Disasters such as the Lockerbie bombing in 1988 drove the need for this kind of invention, as well as an incident in which a printer cartridge bomb was found on-board a cargo plane at East Midlands Airport in 2010.

Fundamental to the design of the bag is a combination of fabrics

which have high strength and impact and heat resistance. The fabrics include Aramid, which is used in ballistic body armor.

"Key to the concept is that the lining is flexible and this adds to its resilience when containing the explosive force and any fragments produced," said Andy Tyas, of the Department

of Civil and Structural Engineering, who is leading the research at the University of Sheffield. "This helps to ensure that the Fly-Bag acts as a membrane rather than as a rigid-walled container which might shatter on impact."

"We have extensively tested Fly-Bag prototypes at the University of Sheffield's blast-testing laboratory, but the purpose of these tests was to investigate how the concept works in the confines of a real aircraft and the results are extremely promising."

Hardened luggage containers (HULD) have been developed to deal with bombs hidden in passenger luggage, but these containers are heavier and more costly than conventional equivalents.

A European consortium working on the Fly Bag project includes Blastech, a spin out company from the University of Sheffield, as well as partners from Greece, Spain, Italy, Germany, Sweden, and the Netherlands.

The technology could either be something that becomes compulsory for all airlines to use if the law was changed or could be used by airlines responding to particular threats.

It has also been adapted for use in cabin holds within the plane if the airline crew spot something they think might be a threat and could be a risk to passengers.

The Road Ahead : The Constant Threat of the Roadside Bomb

By Frank G. Rando

Source: http://www.cbrneportal.com/the-road-ahead-the-constant-threat-of-the-roadside-bomb/

*"Don't step off the road-There might be another one!"- **James Garrity***

July 27 - Antipersonnel and territory-denial devices utilizing clandestine or improvised techniques have been utilized in asymmetric and guerilla warfare since the beginning of conflicts and war. During World War I, the systematic use of IEDs and booby traps to effect casualties during the retreat of German troops at the Somme region was a well-used tactic. Another early example of coordinated large-scale use of IEDs was the Belarusian Rail War, launched by Belarusian guerillas against the Germans in World War II. Both command-detonated and delayed-fuse IEDs were used to derail thousands of German trains during 1943-1944.

In the Vietnam War, booby traps consisting of well concealed fragmentation grenades, claymore mines, and even sharpened bamboo stakes, known as "punji stakes" were strung between trees, configured on trails and roads with trip wires and camouflaged cover. IEDs were commonly deployed by the Viet Cong against land-and river-borne vehicles, as well as personnel. These devices were commonly constructed using materials from unexploded American ordnance (UXO). 33% of U.S. casualties in Vietnam and 28% of deaths were officially attributed to mines; these figures include losses caused by both IEDs and commercially manufactured mines. The "grenade in a can" was a simple, field-expedient and effective booby trap. A hand grenade with the safety pin removed and safety lever compressed was placed into a container such as a tin can, with a length of string or tripwire attached to the grenade.

The Irish Republican Army (IRA) direct action teams had rapidly adopted guerilla and urban warfare -style tactics, and became expert in the construction and use of Improvised Explosive Devices (IEDs), while the anti-establishment subversives of 1960s, such as the Weathermen Underground, had developed expertise of their own. The Provisional IRA made extensive use of IEDs in their 1969-97 campaign. They used barrack buster mortars and remote controlled IEDs. IRA bombs became highly sophisticated, featuring anti-handling devices such as a mercury tilt switch or microswitches.

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

Frank G. Rando *possesses over 30 years of real world experience as a public safety professional,clinician, educator ,emergency and crisis manager ,author and consultant in the areas of tactical ,disaster and operational medicine, weapons and tactics, law enforcement /criminal investigations ,counterterrorism, hazardous materials management and emergency response ,toxicology, environmental safety and health,and health care and public health emergency management.*

US Military's Bomb Techs Fear Flying IEDs

Source: http://www.defensenews.com/story/defense/policy-budget/warfare/2015/07/28/us-militarys-bomb-techs-fear-flying-ieds/30747275/

July 28 – **The US military's explosive ordnance disposal community, bedeviled by roadside bombs in recent wars, is girding for a new threat: flying drones as IEDs.**

The crash landing of a hobbyist's quadcopter on the grounds of the White House in January has sparked fears that a low-tech enemy like the Islamic State could harness such a device to deliver a bomb — and that explosive ordnance disposal (EOD) techs would have to confront it.

"I personally believe that the unmanned platform is going to be one of the most important weapons of our age," Navy Capt. Vincent Martinez, commander of the Naval Surface Warfare Center (NSWC) EOD Technology Division, said. "I'm going to have to start thinking not only about how I defuse the payload but how I defuse the platform. When I walk up on that platform, is it watching me, is it sensing me, is it waiting for me?"

Though the quadcopter's crash landing was an accident, and no one was hurt, Martinez noted the drone's 6-pound payload could have been full of explosives.

"Imagine the media event if it lands on top of the White House and detonates, whether it kills anybody or not," Martinez said. "The signal is sent. Add C4 [plastic explosive] to that, and it's a pretty big bang."

Members of the military's EOD community said they are concerned enemies will harness technology quicker and in new ways, and that they must be vigilant and streamline acquisitions in order to keep pace. The National Defense Industrial Association on Tuesday and Wednesday held its annual EOD conference in Bethesda, Maryland, where officials discussed the issue.

A small, unmanned quadcopter crash landed at the White House in late January.(Photo: US Secret Service/AFP)

The Islamic State group has used drones in the past. US Central Command announced in March that it had bombed an IS remotely piloted aircraft, which a Defense Department spokesman later described as a "model plane," spotted as it was loaded into the trunk of a car.

Jerry Leverich, a senior analyst with Army Training and Doctrine Command's futures directorate, called fixed-wing scale models very difficult to track, and the quadcopter "a $100 device, currently being used for surveillance, that can be quickly adapted for lightweight explosives."

Leverich declined to detail specific methods used by the Islamic State, but the group is reportedly behind countless car

bombs and vehicle-borne suicide IEDs. The New York Times reported in May that mass quantities of fertilizer — a bomb ingredient — have been flowing into Islamic State territory.

In recent wars the US has often had a technological edge, but the streak may not last, Leverich said.

"One of the strengths of the United States is when we have one adversary, we can quickly reorient and bring our treasure and ability to focus on that adversary," Leverich said. "But right now we're in a period of tremendous uncertainty, and trying to determine what the singular threat is going to be is a significant challenge."

For the largely defense industry audience, Martinez outlined avenues for potential innovation: undersea explosives detectors that allow real-time analysis, social media aggregators that predict local IED trends, or a voice-operated archive of bombs and parts a tech could use, like Siri, while defusing a bomb.

A past success was a capability that detected nearby video camera emissions — bombers film their work — to predict attacks.

"How about suit innovations," Martinez said. "I'd like to be fully covered, if possible, I'd like to be stronger, I'd like to be faster. I'd like to be the bionic man, but I don't want to spend $6 million on the suit."

While potential adversaries work with "breakneck speed," Martinez said, the community and industry need to collaborate to goose the lumbering military's acquisition system. It was a sentiment echoed by others dissatisfied with the pace of military procurement.

Air Force Maj. Shane Frith, also with the NSWC, said the military has yet to field a portable X-ray for EOD techs, even though requirements were created in 2007. The military would have done better to field an imperfect version than encumber the program with needless specifications, he said.

"The requirements have been surpassed by technology and innovation coming out of the war zone, out of industry, so we're going to end up purchasing an item that is expired, irrelevant," Frith said. "Technology has advanced past the acquisition."

Turkish military builds 2.5 meter-high, rocket-proof wall on Syria border

Source: http://www.todayszaman.com/anasayfa_turkish-military-builds-25-meter-high-rocket-proof-wall-on-syria-border_395022.html

The Turkish Armed Forces (TSK) is building a 2.5 meter-high and 1 meter-wide, rocket-proof wall along the Syrian border to counter a growing threat by the Islamic State of Iraq and the Levant (ISIL).

The military has recently stepped up the construction work at the wall it began to build in May in the Yayladağı district of Hatay along the Syria border to prevent illegal crossings into Turkey from Syria in the wake of recently increasing terror attacks. The 2.5 kilometer-long part of the wall has already been built, the Doğan news agency reported on Wednesday. The military also dug ditches just behind the wall.

Doğan said wire fences will also be placed behind the wall, along with security lights and cameras.

Bomb making for Beginners: Inside Al-Qaeda E-Learning Course

Source: http://www.ffi.no/no/Forskningen/Avdeling-Analyse/Terra/Publikasjoner/Documents/Stenersen-Bomb-making-for-beginners.pdf

PERSPECTIVES ON TERRORISM Volume 7, Issue 1

'Bomb-Making for Beginners': Inside al Al-Qaeda E-Learning Course

by Anne Stenersen

Abstract

This study explores how terrorists utilise the Internet to learn bomb-making skills. Unlike previous studies, it does not focus on assessing the quality of online bomb recipes. Rather, it discusses the efforts being made by on-line jihadists to help others learn by providing so-called "e-learning courses." As of today, such courses have few active participants yet they tend to attract large interest – indicating that there is a demand among Al-Qaeda's online sympathisers for developing this concept further.

***Anne Stenersen** is a research fellow at FFI's Terrorism Research Group. With an academic background rooted in Middle Eastern studies, Arabic and Russian, she has conducted research on militant Islamism, with a focus on CBRN (chemical, biological, radiological and nuclear) terrorism, al-Qaeda's use of the Internet, and the Taliban insurgency. Ms. Stenersen has a B.A. in Cultural and Social Sciences from the University of Bergen, and an M.Phil in Asian and African Studies from the University of Oslo. She has recently finished a doctorate on The Taliban insurgency and al-Qaeda-Taliban relations. She has presented her research findings at various conferences in Norway as well as abroad, and to the media.*

Indra To Develop Forensic Analysis Lab For Counter-IEDs

Source:http://www.defenseworld.net/news/13696/Indra_To_Develop_Forensic_Analysis_Lab_For_Counter_IEDs#.VcwsR_k417t

Indra has won a €4 million contract to develop new forensic analysis laboratories for Counter-Improvised Explosive Devices (C-IED) used in terrorist attacks.

The European Defense Agency (EDA) awarded project initially contemplates the design and supply of a first laboratory for €2.2M and an option to buy a second, which would raise the global contract amount of up to €4M, Indra said in a statement Monday.

The ultimate goal of these labs is to gather information on techniques, tactics and procedures used in terrorist attacks. Improvised Explosive Devices are the leading cause of death in international military operations.

The laboratory is comprised of 13 modular containers that may be configured differently, depending on a mission's requirements. They are prepared for on-site collecting of samples from CBRNe (Chemical, Biological, Radiological, Nuclear, and Explosives) attacks, performing biometric and chemical forensic analyses of traces found, including those of electronic devices that may have been used for their control and activation.

1 Triage (DMAT Entrance)
2 Biometric Analysis
3 Detailed Visual Examination (DVE) & Electronic Analysis
4 Chemical Analysis
5 Secure Storage Area (SEA)
6 Command Area
7 Platform Management & Control
8 Sanitation Area

The laboratory is also capable of analyzing computer data and is equipped with an advanced data management system. This application will enable the comparison of an attack with previous incidents and will provide support for planning tasks, generating the corresponding reports and monitoring and traceability of the custody chain of evidence and samples.

Indra is awarded this new contract with the EDA after the Agency had already entrusted it the development of the first C-IED laboratory, with which ISAF forces were successfully supported in Afghanistan, between August 2011 and 2014. During this period, the laboratory completed over 300 analyses monthly of devices, artifacts, materials and traces associated with attacks.

Serial bomber demands BITCOIN ransom after planting explosives at supermarkets

Source: http://www.mirror.co.uk/news/technology-science/technology/serial-bomber-demands-bitcoin-ransom-6250202

Aug 15 – **A bomber in the Netherlands is demanding a ransom be paid in the bitcoin digital currency to stop a spree of attacks.**

Dutch police are currently hunting the "Bitcoin bomber" who has been planting home-made explosives at a supermarket chain called **Jumbo** since May.

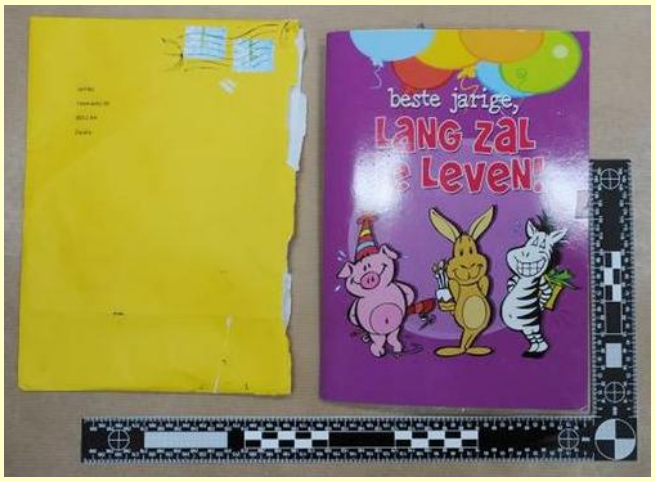
The police made the case known this week and have called for anyone to come forward with information that will help them catch the perpatrator.

Three bombs have been found at different Jumbo supermarkets in Groningen - a large city in the north of the country.

The first was discovered by a member of the public and diffused but the second, three weeks later, was detonated. There was damage to a window and door frame but no-one was hurt.
The owners of the supermarket chain then received a letter - written on the Notepad computer program - demanding the ransom.
"In the letter the offender requests a quantitiy of bitcoins, an electronic payment," said the Dutch police. "He writes that he will no sooner stop his activities until he receives the requested bitcoins."

One of the Jumbo supermarkets in Groningen, Netherlands where one of the bombs was planted

The day after the letter was received, an anonymous tip was submitted about another bomb. Police evacuated the store in question but weren't able to find a device.
Since then, a letter containing a musical birthday card was sent to the supermarket chain containing a small amount of explosive powder and another threat.

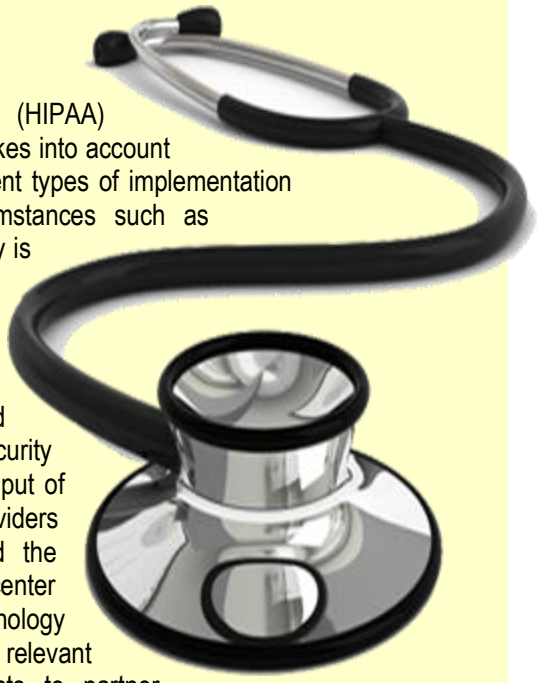


Bitcoin Bomber card that he sent

Bitcoin is a digital currency that doesn't have a central authority and is often used in transactions for illegal activities.
While users are not identified by name, transactions can be linked to individuals and companies, as they are all recorded into a public ledger, which are viewable by everyone.
However it is not difficult to maintain anonymity by using a different bitcoin address for each transaction.
There are also mixing services that allow users to trade the currency which links them to other coins with different transactions histories.

Comments Requested on Draft Guide for Keeping Medical Information Secure on Mobile Devices

Source: http://www.nist.gov/itl/20140723_nccoe_mobile_medical.cfm



July 24 – The National Cybersecurity Center of Excellence (NCCoE) has released a draft for public comment of the first guide in a new series of publications that will show businesses and other organizations how to improve their cybersecurity using standards-based, commercially available or open-source tools. The step-by-step guide released today demonstrates how health care providers can make mobile devices, such as smartphones and tablets, more secure, in order to better protect patient information and still take advantage of advances in communications technology.

The center was established in 2012 by the U.S. Commerce Department's National Institute of Standards and Technology (NIST), the state of Maryland, and Montgomery County, Md. Since that time, the center has been building partnerships with industry and academia to identify cybersecurity challenges and develop example solutions in industries such as health care, energy and financial services.

"The NCCoE was established specifically to help organizations solve real-world challenges, and this was one of particular concern to the health care community," says NCCoE Director Donna Dodson. "This guide can help providers protect critical patient information without getting in the way of delivering quality care."

Stolen personal information can have negative financial impacts, but stolen medical information cuts to the very core of personal privacy. Medical identity theft already costs billions of dollars each year, and altered medical information can put a person's health at risk through misdiagnosis, delayed treatment or incorrect prescriptions. Yet, the use of mobile devices to store, access and transmit electronic health care records is outpacing the privacy and security protections on those devices.

Securing Electronic Records on Mobile Devices provides IT implementers and security engineers with a detailed architecture so that they can copy, or recreate with different but similar technologies, the security characteristics of the guide. It also maps to standards and best practices from NIST and others, and to Health Insurance Portability and Accountability Act (HIPAA) rules. The guide takes into account the need for different types of implementation for different circumstances such as when cyber security is handled in-house or is outsourced.

The draft guide was developed by industry and academic cybersecurity experts, with the input of health care providers who first identified the challenge. The center then invited technology providers with relevant commercial products to partner with NIST through cooperative research and development agreements and collected public feedback at multiple steps along the way.

The team at the NCCoE built a virtual environment that simulates interaction among mobile devices and an electronic health record system supported by the IT infrastructure of a medical organization. They developed a scenario in which a hypothetical primary care physician uses her mobile device to perform recurring activities such as sending a referral containing clinical information to another physician or sending an electronic prescription to a pharmacy. Then, using commercially available technologies, they built a solution to improve privacy and security protections.

"We know from working with them that health care organizations want to protect their clients' personal information and themselves from the high costs associated with breaches," said Dodson. "This guide can be an important tool among the many they use to reduce risk."

The draft guide is the first in the newly established 1800 series of NIST special publications, designed to help companies protect their information systems.

As a non-regulatory agency of the U.S. Department of Commerce, NIST promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards and technology in ways

that enhance economic security and improve our quality of life.

▶ **To learn more about NIST, visit** www.nist.gov.

Spy-in-the-sky terror threat to William: Security alert over app that lets anyone track pilot Prince's air ambulance helicopter

Source: http://www.dailymail.co.uk/news/article-3174593/Spy-sky-terror-threat-William-Security-alert-app-lets-track-pilot-Prince-s-air-ambulance-helicopter.html

Prince William was at the centre of a major security alert last night after The Mail on Sunday discovered that terrorists could use a mobile phone to track his every movement in

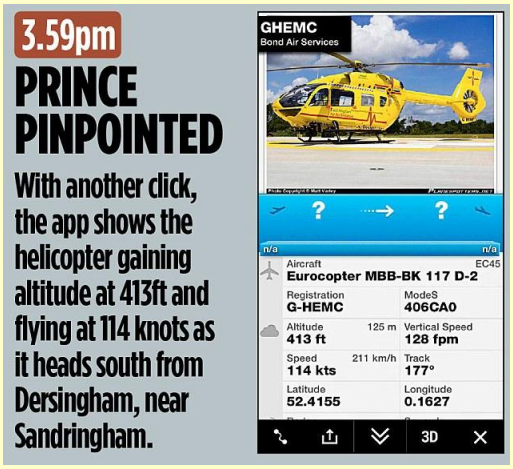
his new job as an air ambulance pilot.

Experts warned of the 'extraordinary risk' to the

future King presented by a £2.99 app, which gives away precise details of his helicopter's position, direction of travel, speed and altitude.

Former police officers said the information presented 'intelligence gold' for terrorists wishing to track the Prince's flightpath in an attempt to shoot him down.

Astonishingly, subscribers can even opt to receive alerts every time the Prince's East Anglian Air Ambulance takes off from its base at Cambridge Airport on a 999 rescue mission, relaying real-time flight data from the helicopter's on-board transponder.



The app also reveals where the air ambulance lands.

Although Prince William's presence on official visits is often publicised in advance, security experts stressed that when he arrives at the scene of an emergency the area will not have been screened in advance.

A Mail on Sunday team last week used the app, called flightradar24, to monitor Prince William's progress as he flew from North Norfolk after attending a road accident.

Using the detailed information on the screen, we were able to have a photographer waiting at the precise moment the helicopter came into land at the airport.

A terrorist armed with a rocket-propelled grenade, ground-to-air missile or even less sophisticated weaponry would have had little difficulty targeting William's aircraft as it

regularly flies below 1,500ft with a cruising speed of just 150mph.

Roy Ramm, a former Commander of Specialist Operations at Scotland Yard and an ex-head of the Flying Squad, called for immediate action to shut down the security loophole.

4.51pm

ROUTE TRACKED

After following the aircraft for more than an hour – giving us time to get into place – the app shows its approach to Cambridge Airport, crossing the A14.

He said: 'Knowing the precise movements, altitude and speed of an aircraft in flight is intelligence gold for any terrorist. The ability to track a high-profile target like this presents a really serious risk.

'Even without expensive and sophisticated weaponry, there is the real danger that an inexpensive drone could be used to put any aircraft flown by William at risk.

'There is also the risk that a terrorist might simply open fire on his aircraft at low altitude with the kind of automatic weapon readily available to gangs in London. After all, the Prince is flying an air ambulance, not an armoured gunship.'

4.51pm **RETURN TO BASE**

Knowing exactly which direction the helicopter will come from, our photographer takes a picture as it approaches.

Only last week the Civil Aviation Authority warned of the risks that readily available drones could cause if they collided with aircraft.

Buckingham Palace and the Metropolitan Police, who are tasked with Royal protection, declined to comment when The Mail on Sunday alerted them to the app.

5.00pm **PRINCE DISEMBARKS**

Safely landed, co-pilot William chats to colleagues wearing his blue flight suit. His pilot is in a high-vis jacket.

But it appeared last night that urgent efforts were being made to remove information relating to the Prince's air ambulance from flightradar24.

While most commercial and civilian aircraft can be tracked by the app, military and diplomatic flights and private jets do not normally appear for security reasons.

But until yesterday evening, detailed information of the Prince's missions in his air ambulance helicopter, codenamed 'Anglia Two', was available every time he took to the skies. The data is also available on the flightradar24 website for free as well as via the app.

Princess Diana's former personal protection officer Ken Wharfe added: 'It's madness to have his flight details displayed in this way on an open website, and it should have been addressed long before now.

'Prince William is a target whether he likes it or not, and it just takes one nutter with a gun to act on this information and take a potshot.

'More generally, I would question the security risks of Prince William doing this job at all. It would be far preferable, if he's determined to fly helicopters, to do so in the secure environment of an RAF base, where he could be an instructor, rather than attending road accidents on the streets of King's Lynn.'

Former head of the Met's Royalty Protection Squad, retired chief superintendent Dai Davies, said: 'This would give me cause for concern and solutions need to be found by those in charge of the Prince's security.

'You always have to be aware of the advance of technology – which this illustrates – and the ability of these terrorist groups to think outside the box. You always, always have to be one step ahead.'

Former Conservative Cabinet Minister Andrew Mitchell said: 'I congratulate The Mail on Sunday for exposing this significant flaw in Prince William's security. I urge

the authorities to take urgent and firm action to correct it.'

Unlike William's civilian helicopter, most military aircraft do not show up on the tracking website, and normally neither does the US President's airliner, Air Force One.

Just last year, the Japanese government made a successful request to flightradar24 have their own VIP aircraft details removed from the site.

Several flight tracking websites and mobile phone apps provide live tracking of hundreds of aircraft flying over Britain, including the Prince's helicopter. But the flightradar24 app is the market leader and offers the most sophisticated service, using information from more than 7,000 worldwide receivers which pick up aircraft transponder signals. The basic version of the app is available to any smartphone user and costs just £2.99.

Users can enter the registration number of the East Anglian Air Ambulance's Anglia Two helicopter which Prince William started flying earlier this month. If the Eurocopter is in the air, it can be seen flying across a map on the screen which can be enlarged to show greater detail.

Anyone can pay an extra £3.99 for a 'custom alert', creating a message on their phones every time the helicopter takes off.

The alert flashes up on screen and makes an audible sound like a text message. Users can then search for the helicopter to track it on a map. Another button can be clicked to reveal the helicopter's speed, direction of flight, and its precise latitude and longitude position as it changes.

The air ambulance's flight path is easy to predict as it generally flies in a straight line while heading to an emergency, taking patients to hospitals or returning to base.

A Mail on Sunday reporter took just seconds to find the registration number of the Prince's helicopter after searching on aviation websites. The reporter then bought the flightradar24 app and paid the extra £3.99 to get an alert every time it is tracked.

He got an alert when the Prince and his crewmates took off after attending a road crash in Dersingham, Norfolk, last Tuesday. The reporter watched on his phone as the app provided live tracking of William's 50-mile flight back to Cambridge Airport.

And two days later, we tracked chopper to an open field: Air ambulance landed in full view of our photographer who tracked its progress on flightradar24 on Thursday

A photographer was able to predict the Prince's arrival time and got into position by the airport fence just seconds before his helicopter appeared.

He was able to photograph it as it came in to land – but a terrorist using the same app might have been armed with more than a camera. The photographer took pictures of William after he left his helicopter a few minutes later and stood around chatting to his colleagues.

The Prince was on leave on Wednesday when he and wife Kate held a second birthday party for Prince George at their family home, Anmer Hall on the Sandringham estate.

He was not working again on Thursday when the MoS tracked Anglia Two on a 999 call to help a man who had been found unconscious in Culford, near Bury St Edmunds, Suffolk.

The helicopter flew to the scene at 100mph and landed in a field where it stayed for around 30 minutes, giving a MoS photographer time to get in position about quarter of a mile away.

He photographed the helicopter as it flew overhead at low altitude on its way back to Cambridge Airport after efforts to save the man failed and he was pronounced dead at the scene.

The MoS also tracked a second rescue mission carried out by a late-shift crew who helped a man found bleeding in St Albans, Hertfordshire, later on Thursday afternoon.

Once again a photographer was able to get in position and snap the helicopter on its return, although it is understood that Prince William was not on duty at the time.

Flightradar24's data mainly comes from 'automatic dependent surveillance-broadcast' (ADS-B) transponders , which are fitted to 70 per cent of commercial passenger aircraft. The transponders record an aircraft's position using GPS satellites in a similar way to sat nav systems, then broadcast the information to ground stations monitored by flightradar24.

The ADS-B transponders are not generally fitted to military aircraft and many older commercial aircraft.

A spokesman for the Bond Aviation Group, which operates the two East Anglian Air Ambulance helicopters, refused to say if the company was able to take any action to make Anglia Two invisible on tracking websites.

He added that the company was aware of the flightradar24 app. But he added: 'Bond cannot comment on the security arrangements'

Flightradar24 did not respond to requests for comment.

Hacking Critical Infrastructure: A How-To Guide

By Patrick Tucker

Source: http://www.defenseone.com/technology/2015/07/hack-critical-infrastructure/118756/

July 31 – How easy would it be to pull off a catastrophic cyber attack on, say, a nuclear power plant? At next week's Black Hat and

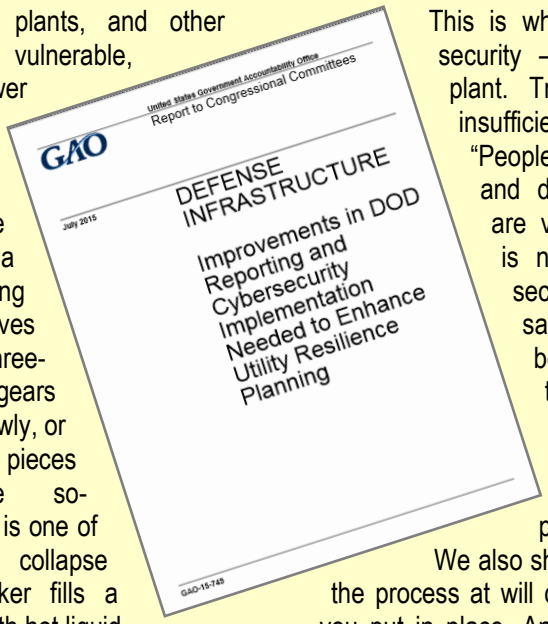
DEF CON cybersecurity conferences, two security consultants will describe how bits might be used to disrupt physical infrastructure. U.S. Cyber Command officials say this is the threat that most deeply concerns them, according to a recent Government Accountability Office report. "This is because a cyber-physical incident could result in a loss of utility service or the catastrophic destruction of utility infrastructure, such as an explosion," the report said. They've happened before. The most famous such attack is the 2010 Stuxnet worm, which damaged centrifuges at Iran's Natanz nuclear enrichment plant. (It's never been positively attributed to anyone, but common suspicion holds that it was the United States, possibly with Israel.)

Scheduled to speak at the Las Vegas conferences are Jason Larsen, a principal security consultant with the firm IOActive, and Marina Krotofil, a security consultant at the European Network for Cyber Security. Larsen and Krotofil didn't necessarily hack power plants to prove the exploits work; instead Krotofil has developed a model that can be used to simulate power plant attacks. It's so credible that NIST uses it to find weakness in systems.

The idea is to help cybersecurity professionals understand what to look for and design intrusion detection software to prevent attacks from taking place. You can't guard an asset until you know what weak spots your enemy will use to grab your prize. And when

it comes to online attack, the weak spots in U.S. infrastructure are many. But Larsen hopes he doesn't get "crucified" for his presentation.

When asked if there was a single error or issue that was common across the various installations accounted for in the model, perhaps a single unlocked back door that made power plants, chemical plants, and other pieces of infrastructure vulnerable, Larsen replied, "The answer to that is, which one?"



A hacker bent on destruction might try various methods. There are "water hammers," a method of destroying piping structures by closing valves too fast. There are three-phase attacks that cause gears to spin too quickly, too slowly, or out of sync with other vital pieces of equipment. (The so-called Aurora vulnerability is one of these.) And there are collapse attacks, where the hacker fills a round tube or container with hot liquid, rapidly closes the lid and waits for the liquid to cool to create a vacuum. "A lot of the round stuff we build doesn't hold up to vacuums very well. Whole valves that you can drive trucks through can collapse like a beer can," Larsen told *Defense One*.

Still, it remains far easier to get online access to a computer or network than it is to cause physical damage to infrastructure. Such attacks a very specific understanding of a physical event playing out — creating a vacuum, turning a valve, rotating a piston, etc. — and specific knowledge of a particular plant or facility.

"For instance, the attacker probably needs the point database because he needs to know that Point 16 operates the oil pump and Point 17 is the light in the bathroom…Without it, it's hard to launch an effective attack," said Larsen.

The attack on the Natanz enrichment plant is illustrative. "When Stuxnet came out, the very first version had a payload. It went over there and the effective process broke a whole bunch of stuff. But the actual creation of the payload…a lot of people had to work hard behind the scenes trying to figure out, 'Oh, there's a spinning apparatus. I can go damage the spinning apparatus. What information do I need to know to do that?'" asked Larsen. In general, he said, "We don't have the roadmap for an attacker once he gets in, where he gets to the final payload" that does the damage.

Still, it's time to start beefing up cyber defense, he said. Defenders need a comprehensive overview of plant cyber security, better sensors inside the facility, better control processes, and much better sensitivity to small abnormalities. This is what Krotofil calls process security — protecting the overall plant. Traditional IT security is insufficient, she said.

"People say, [supervisory control and data acquisition] systems are vulnerable because there is not enough traditional IT security put in place," she said. "Well, that's rubbish, because we just presented two attack possibilities where you can control the process at will even if it's password-protected and encrypted. We also show that you can exercise the process at will despite all the IT security you put in place. And we can spoof process states, to make the operator believe that everything is fine."

This sort of research can reveal the most likely vulnerabilities in a target — but turning keystrokes into physical damage requires more, says Larsen. "If you're hitting a nuclear reactor, you really have to know what the estimates they're using for flux and fluids are. That might not be really obvious. One of the ways to do that is tweak the process a little bit and see how it responds. If you can figure out how people would normally go about doing these little tweaks and responses to tune their cyber weapon, we can actually go look for those and develop signatures for them. We can say, 'Oh, someone might be tweaking a process' before someone launches a full-blown attack."

For policymakers, Larsen offers this advice: create a place for engineers to share data, and then butt out so they can do it. "There's been a lot of information-sharing things that have sprung up," including the Cybersecurity Framework the White House put out last year, he said. "What we need is information sharing between engineers at various facilities in order to improve. But sharing information is dangerous because

eventually you are going to share the information for how to attack somebody else. So the programs for information sharing have started off with lofty ideas and ended up with a very conservative, to the point of not being useful, implementation because no one wants to be the guy who leaked the information that somebody used to go attack something," he said. "On the policy decision, I would say that the government's role should be to mandate and facilitate the information sharing, but not be a member of the information sharing."

Of course, there also some vulnerabilities that are easy to fix. "Putting in a pressure relief valve in place is actually way cheaper than all the cyber work you have to do," he said.

Patrick Tucker *is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for* The Futurist *for nine years. Tucker has written about emerging technology in* Slate, The Sun, *MIT* Technology Review, Wilson Quarterly, The American Legion Magazine, *BBC* News Magazine, Utne Reader, *and elsewhere.*

FDA to hospitals: Infusion system vulnerable to hacks, should not be used

Source: http://www.homelandsecuritynewswire.com/dr20150803-fda-to-hospitals-infusion-system-vulnerable-to-hacks-should-not-be-used

Aug 03 – The Food and Drug Administration (FDA) issued a warning in which it "strongly encourages" hospitals to stop using Hospira's Symbiq Infusion System, because the device is vulnerable to attacks by hackers who could remotely control dosages delivered via the computerized pumps. The FDS said that tests have shown that an unauthorized third party – hackers – could access the Symbiq infusion system by breaching hospital networks.

The Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team. (ICS-CERT) reached similar conclusions after its own tests.

CERT reported the vulnerability on 21 July and the FDA released its own safety alert on Friday, 31 July. Thankfully, there are no reported incidences of the Symbiq system being hacked.

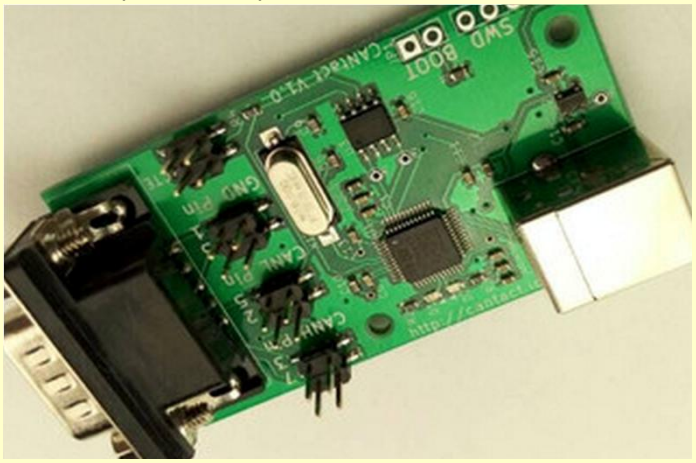
Endgadget reports that Hospira no longer sells the Symbiq system, but some third-party retailers are still selling it despite the FDA warning. The network vulnerability would "allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies," the FDA says.

This safety alert the FDA has issued about the infusion system is the first foray of the health monitoring agency into cybersecurity territory.

This Hacker's Tiny Device Unlocks Cars And Opens Garage

Source: http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages

The next time you press your wireless key fob to unlock your car, if you find that it doesn't



beep until the second try, the issue may not be a technical glitch. Instead, a hacker like Samy Kamkar may be using a clever radio hack to intercept and record your wireless key's command. And when that hacker walks up to your vehicle a few minutes, hours, or days later, it won't even take those two button presses to get inside.

At the hacker conference DefCon in Las Vegas tomorrow, **Samy Kamkar** plans to present the details of a gadget he's developed called "RollJam." The $32 radio device, smaller than a cell phone, is designed to defeat the "rolling codes" security used in not only most modern cars and trucks' keyless entry systems, but also in their alarm systems and in modern garage door openers. The technique, long understood but easier than ever to pull off with Kamkar's attack, lets an intruder break into cars without a trace, turn off their alarms and effortlessly access garages.

RollJam, as Kamkar describes it, is meant to be hidden on or near a target vehicle or garage, where it lies in wait for an unsuspecting victim to use his or her key fob within radio range. The victim will notice only that his or her key fob doesn't work on the first try. But after a second, successful button press locks or unlocks a car or garage door, the RollJam attacker can return at any time to retrieve the device, press a small button on it, and replay an intercepted code from the victim's fob to open that car or garage again at will. "Every garage that has a wireless remote, and virtually every car that has a wireless key can be broken into," says Kamkar.

Thieves have used "code grabber" devices for years to intercept and replay wireless codes for car and garage doors. But both industries have responded by moving the ISM radio signals their key fobs use to a system of rolling codes, in which the key fob's code changes with every use and any code is rejected if it's used a second time.

To circumvent that security measure, RollJam uses an uncannily devious technique: The first time the victim presses their key fob, RollJam "jams" the signal with a pair of cheap radios that send out noise on the two common frequencies used by cars and garage door openers. At the same time, the hacking device listens with a third radio—one that's more finely tuned to pick up the fob's signal than the actual intended receiver—and records the user's wireless code.

When that first signal is jammed and fails to unlock the door, the user naturally tries pressing the button again. On that second press, the RollJam is programmed to again jam the signal and record that second code, but also to simultaneously broadcast its first code. That replayed first code unlocks the door, and the user immediately forgets about the failed key press. But the RollJam has secretly stored away a second, still-usable code. "You think everything worked on the second time, and you drive home," says Kamkar. "But I now have a second code, and I can use that to unlock your car."

If the **RollJam** is attached to the car or hidden near a garage, it can repeat its jamming and interception indefinitely no matter how many times the car or garage door's owner presses the key fob, replaying one code and storing away the next one in the sequence for the attacker. Whenever the RollJam's owner

comes to retrieve the device, it's designed to have a fresh, unused code ready for intrusion. "It will always do the same thing, and always have the latest code," says Kamkar. "And then I can come at night or whenever and break in."

Kamkar says he's tested the proof-of-concept device with success on on Nissan, Cadillac, Ford, Toyota, Lotus, Volkswagen, and Chrysler vehicles, as well as Cobra and Viper alarm systems and Genie and Liftmaster garage door openers. He estimates that millions of vehicles and garage doors may be vulnerable. But he says he believes the problem is rooted in the chips used by many of those companies: the Keeloq system sold by the firm Microchip and the Hisec chips sold by Texas Instruments.

WIRED reached out one-by-one to each of those companies. All but a few have yet to respond. Liftmaster and Volkswagen declined to comment, and a Viper spokesperson said it's trying to learn more about Kamkar's findings. Cadillac spokesperson David Caldwell wrote in an email that Kamkar's intrusion method "is well-known to our cyber security experts," and he believes it works only with prior model year vehicles, "as recent/current Cadillac models have moved to a new system."

Kamkar isn't the first, as Cadillac implies, to invent the RollJam's method of jamming, interception and playback. Security researcher Spencer Whyte wrote in March of last year that he'd created a similar device. But Kamkar says his refined RollJam is designed to better automate the attack Whyte used, without the need to attach the device to a laptop. And while Whyte appears to have kept the code for his tool under wraps, Kamkar plans to release his on Github, timed to his DefCon talk Friday.

Kamkar also says that Cadillac may be correct that its newest vehicles aren't subject to the attack. The latest version of Keeloq's chips, which the company calls Dual Keeloq, use a system of codes that expire over short time periods and foil his attack. In fact, Kamkar says his goal with RollJam is to demonstrate to car and garage door companies that they need to make that upgrade to expiring codes, or leave their customers vulnerable to interception attacks like the one he's demonstrated.

After all, Kamkar points out, two factor authentication systems like Google Authenticator or RSA's SecurID use codes that expire in seconds, while millions of car owners still protect their vehicles with vulnerable systems whose codes never expire. With those precedents in traditional internet security, car makers should know that using rolling codes without an added code expiration measure no longer suffices to keep their products secure. RollJam is intended to definitively demonstrate that lesson.

"This is throwing the gauntlet down and saying, 'here's proof this is a problem,'" says Kamkar. "My own car is fully susceptible to this attack. I don't think that's right when we know this is solvable."

Cyber Hackers Can Now Shoot Others' Sniper Rifles

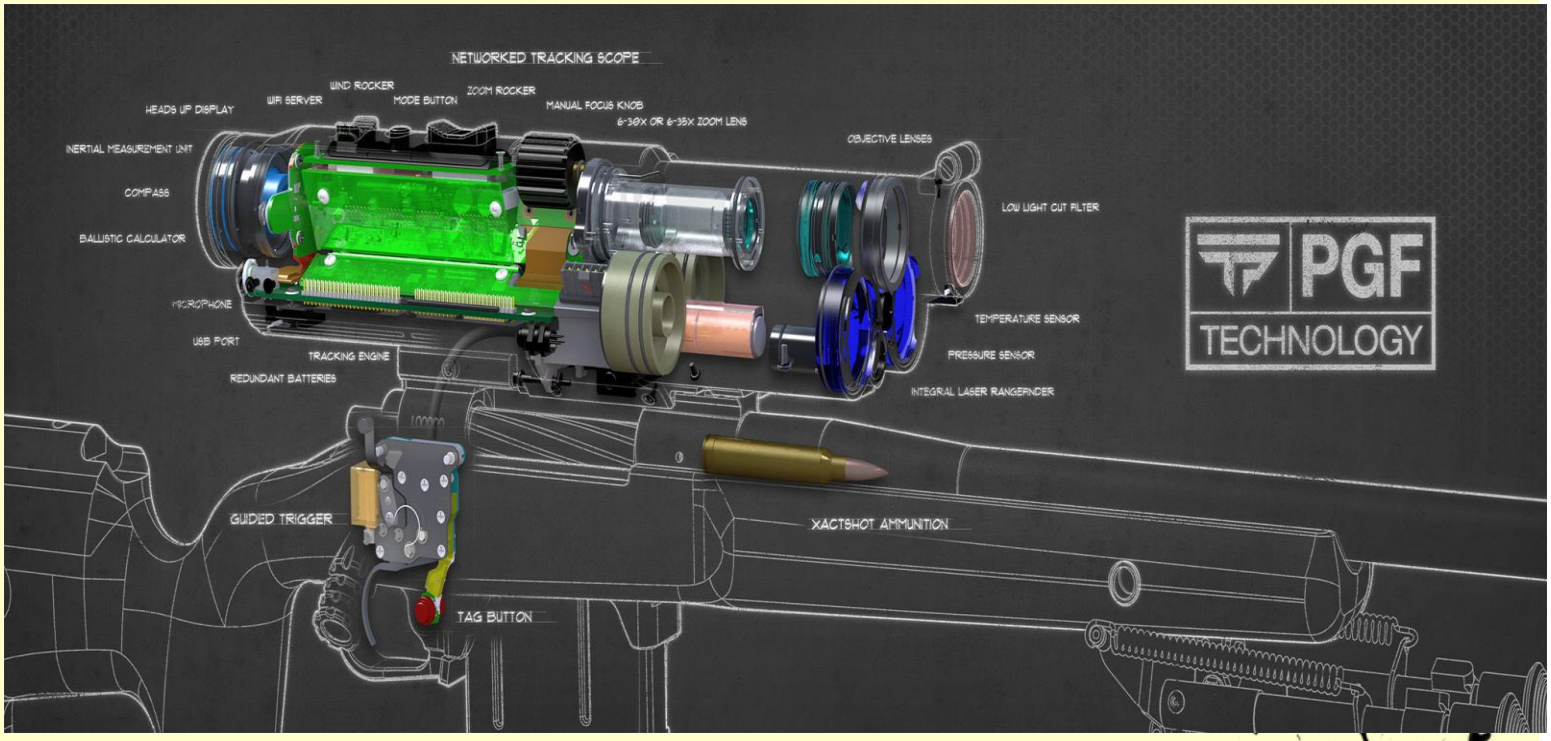
Source: http://i-hls.com/2015/08/cyber-hackers-can-now-shoot-others-sniper-rifles/

The modern military is heading step by step in a more tehcnological direction. With each day, as more experience is gained, technology is implemented into more aspects of battle. One recent innovation in the field of technology being frequently used in a wide variety of means is the smart weapons. These weapons make use of technological means in order to shoot more accurately and from a greater distance. One such example is the technological sniper rifle.

But then again, having weapons become more technological also holds many dangers, as technology make them vulnerable to different, perhaps greater, risks. There may come a time when an enemy exploits that vulnerability to cyber hack the weapon and disable it from a distance, or at least manipulate it into not working properly. The Black Hat Cyber and Security Information conference, which takes place every year in Las Vegas, has hosted this year the researchers Runa Sandvik and Michael Auger, who proved to everyone in real-time how they can **remote-control this sniper rifle – Tracking Point's TP750. The weapon is**

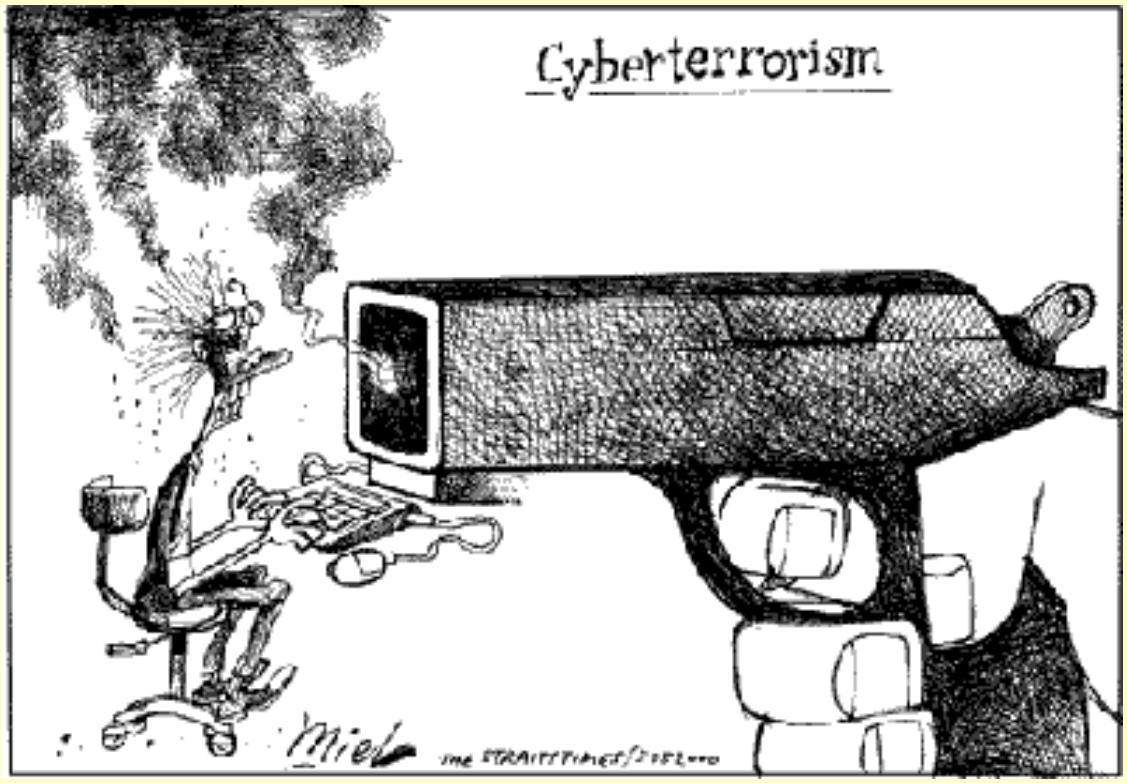
based on a WiFi connection and a Linux Operating System, which aided the two researchers in accomplishing their task. After breaking in the system, they can neutralize the weapon's shooting ability

completely, make it miss its target or even get it to hit a completely different one.
The two researchers, who lead a personal relationship beyond the work hours in the lab, have



presented to the viewers their discovery, step by step, to prove how much overly depending on technology can, well, backfire. In a world so full of technology, with more

devices which started out very low-tec now being highly technological, companies developing these products must make sure that they are fully secured should they happen to end up in the wrong hands.

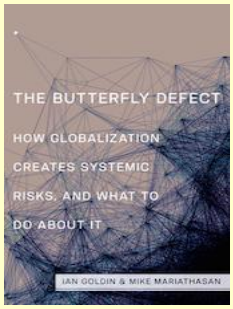


Crisis Management Books – Caroline Sapriel's Top 10 List

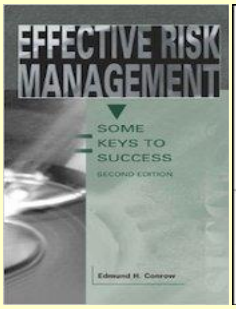
By Caroline Sapriel

Source: http://csa-crisis.com/csa-today/crisis-management-books-caroline-sapriels-top-10-list/

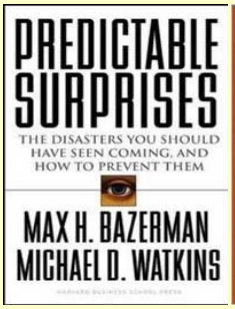
Recently a client asked me to recommend a few good books on crisis management. With over 25 years in risk and crisis management, I've had the pleasure of reading quite a few books on the subject.
There are many out there so how to weed the best from the lot. Crisis Management is not only about responding to crises, but also about detecting rising issues and looming crises, preventing and preparing for them, mitigating their impact and recovering from them. To build resilience companies must take an integrated approach to crisis management which includes risk management, crisis preparedness and response and business continuity. So a useful reading list on crisis management must include titles on risk management, scenario planning, crisis communication and crisis leadership. Here is my hit list!



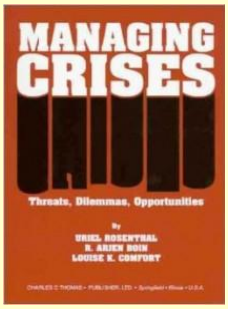
Wonderful read on understanding the systemic risks brought on by globalization and practical guidelines to be better prepared.



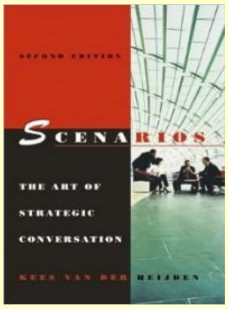
Quite academic, but necessary for anoyone wanting to understand and apply risk management in their organisation.



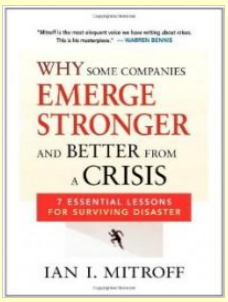
The Havard Business School Authors explain why predictable surprises are so common in business and society and provide a systematic framework that leaders can use to recognize and prioritize brewing disasters and mobilize their organizations to prevent them.



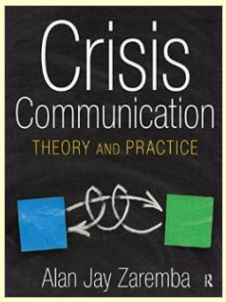
The Editors with 25 notable contributors expand the knowledge of crisis management, focusing on case studies of high profile events that have occurred in recent history.



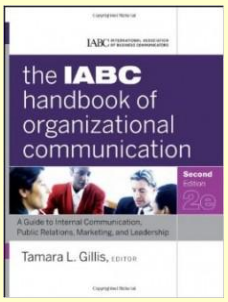
The art and power of scenario planning, articulated here by a Shell executive.



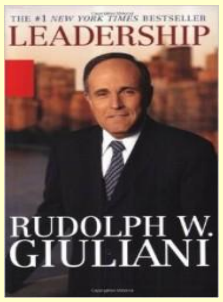
Self explanatory.



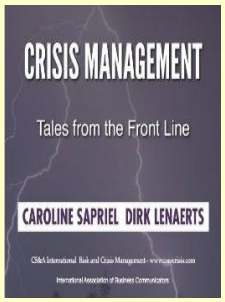
A well-structured book that examines the before, during and after of a crisis. Practical guidelines for the Communicator and his team.



A bible on organisational communication, including crisis communication.



Whether you agree with his politics or not, Guiliani was there and has much to share with anyone seeking to understand leadership under pressure.

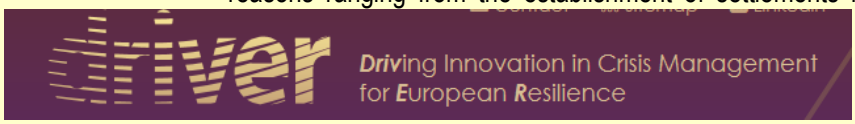


Get in touch to receive your own free copy

Driving Innovation in Crisis Management for European Resilience (DRIVER)

Source: http://driver-project.eu/

The DRIVER project implements the Crisis Management System-of-Systems Demonstration Programme funded under the 7th Framework Programme by the European Commission.
Crisis Management is an ever evolving challenge. **Hazards change**, both for natural and man-made reasons – climate change being a well-known example of the latter. **Vulnerabilities change**, for reasons ranging from the establishment of settlements in new areas to societal evolution affecting people's ability to cope with crises. **Interconnectedness changes** because of increased connectivity in the technical domain, for example the power transmission system, and in the socio-cultural domain as cross-border communities become increasingly important.



All these societal, technical and environmental changes interact to create new challenges for Crisis Management.
These evolving challenges are not compensated by traditional challenges becoming obsolete. Instead, as societies become more complex, both the increasing scope and unpredictability of potential crises, and the rapid dynamics of the incidents to be managed demand crisis management of an ever higher level of complexity. This does not necessarily mean that the frequency of crises increases, but unless innovation is up to the challenge of producing solutions, which fully exploit modularity, flexibility and adaptivity; then either the cost of capability development or the costs due to inadequate management of crises will grow. On the other hand it is a necessary starting point of Crisis Management innovation to realise that the European Crisis Management capabilities are already a mature and competent System of Systems – here interpreted as a federation of heterogeneous and loosely coupled local, regional and national systems able to collaborate in varying configurations and with varying levels of interoperability. Radical change to these capabilities would be very costly and likely incur unacceptable loss of Crisis Management capability during a long transition phase.

Proceedings of the Third UN World Conference on Disaster Risk Reduction

Source: http://www.preventionweb.net/english/professional/publications/v.php?id=45069

These proceedings highlight the five days of deliberations, discussions and presentations held at the Third United Nations World Conference on Disaster Risk Reduction (WCDRR) held at Sendai City, Japan in March 2015. The proceedings include the Sendai Declaration and the Sendai Framework for Disaster Risk Reduction 2015-2030, and a chart of the Framework. They also feature opening ceremony statements, brief summaries of ministerial tables, high level multi-stakeholder partnership dialogues, working sessions, special meetings and ceremonies, and study visits and excursions, and exhibitions and forums held at the WCDRR. The document also includes a list of all side events, exhibition booths, Ignite stage presentations, and collective affirmations made by several stakeholders (local and subnational governments, Private Sector Partnership, science and technology communities, children and youth, non-governmental organizations, members of parliament, media, and the United Nations System Chief Executives Board for Coordination).

▶ **View full document at:**
http://www.preventionweb.net/files/45069_proceedingsthirdunitednationsworldc.pdf

Are Disaster Infographics Still Cool? Useful?

By Brandon Greenberg

Source: http://www.disasternet.co/blog/2015/8/5/are-disaster-infographics-still-cool-useful

It seems like every week or month, I get "the latest" disaster infographic in my inbox. Inforgraphics have become popular in recent years to communicate complicated topics and data. There are infographics on social media, types of hazards, impact to businesses, emergency management careers, etc. I keep a Pinterest board for these types of graphics.

Many that I have seen, though, are actually marketing and recruiting tools for bachelors and masters emergency management programs. I am not opposed to this approach, but I am left wondering about the value of infographics these days.

Because I am largely a curator of this information, not a consumer, I am not clear how infographics have helped the industry. Are disaster infographics useful? How have they helped? Are they effective? Have you used any in your work? If so, how?

DHS S&T Licenses Groundbreaking Communications Technology

Source: http://www.firstresponder.gov/Pages/DHS-ST-Licenses-Groundbreaking-Communications-Technology.aspx

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) today announced that it has licensed the Radio Internet-Protocol Communications Module (RIC-M) to two commercial partners: Christine Wireless, Inc. and Avtec Inc.

This new interoperability solution developed by the First Responders Group (FRG) allows response agencies to easily upgrade and reconfigure legacy communications systems at a low cost, potentially extending the life of the technology for decades.

"FRG's mission is to work hand-in-hand with first responders—determining their needs, identifying solutions, testing progress and incorporating feedback, and then

making the technology available for their daily use," said DHS Under Secretary for Science and Technology Dr. Reginald Brothers.

"RIC-M is shining example of a collaborative effort that will further assist our partners in public safety communications." RIC-M, used by local, state and federal responders, is a low-cost, external, stand-alone, interface device that connects radio frequency (RF) system base stations, consoles and other RF equipment – regardless of brand – over the Internet or Private Internet Protocol (IP) network.

"Instead of having to replace an entire system – which can cost as much as $15,000 – when one component breaks or becomes obsolete, organizations can use any RIC-M compatible product to extend the system's life for another 10 to 20 years," said FRG Program Manager Christine Lee.

RIC-M converts from a commonly used V.24 serial communications protocol to an open-standard Voice-over-Internet-Protocol (VoIP). Both encrypted and unencrypted Project 25 (P25) digital communications are supported, and it can also operate with analog communication equipment.

"In the past, legacy systems were not interoperable," explained Lee. "If you bought one brand of base station, you had to buy the same brand for the all other components even if other brands offered more economical choices or better options. RIC-M allows first responder organizations to be free from dependence on expensive, single-vendor communication solutions, offering cost savings and wider variety."

Base stations are used by law enforcement, medical and other agency dispatchers to communicate with first responders and agents in the field. Using RIC-M, agencies can easily upgrade and reconfigure legacy systems at a low cost, Lee stressed.

Since its conception in 2011, RIC-M has been successfully field tested with various state and federal response agencies including Montgomery County, Maryland; U.S. Customs and Border Protection; Federal Protective Service; the Federal Bureau of Investigation; the U.S. Marshals Service; the Department of Justice and the Department of the Interior Office of Law Enforcement and Security.

The licenses to Christine Wireless Inc. (also RIC-M's inventor) and Avtec Inc. were awarded through a Cooperative Research and Development Agreement to manufacture and sell RIC-Ms in commercial markets. Interested agencies can order the devices from both vendors and will also soon be able to procure the devices via General Services Administration Schedules.

People living in wildfire-prone areas underestimate their risk

Source: http://www.homelandsecuritynewswire.com/dr20150814-people-living-in-wildfireprone-areas-underestimate-their-risk

Aug 14 – **The vast majority of people living in areas prone to wildfires know they face risk, but they tend to underestimate that risk compared with wildfire professionals.**

At the same time, they tend to over-estimate the importance of specific risk factors beyond their control — such as the composition of vegetation on their property — while giving less heed to those they can mitigate, such as replacing combustible siding with more fire-resistant materials.

Those are key findings of researchers from the University of Colorado Boulder, the U.S. Forest Service Rocky Mountain Research Station, the U.S. Bureau of Land Management, and the West Region Wildfire Council. UC Boulder reports that the team's findings, published in the journal *Risk Analysis* in June, are based on surveys of nearly 300 residents of Log Hill Village in southwestern Colorado's Ouray County in 2012.

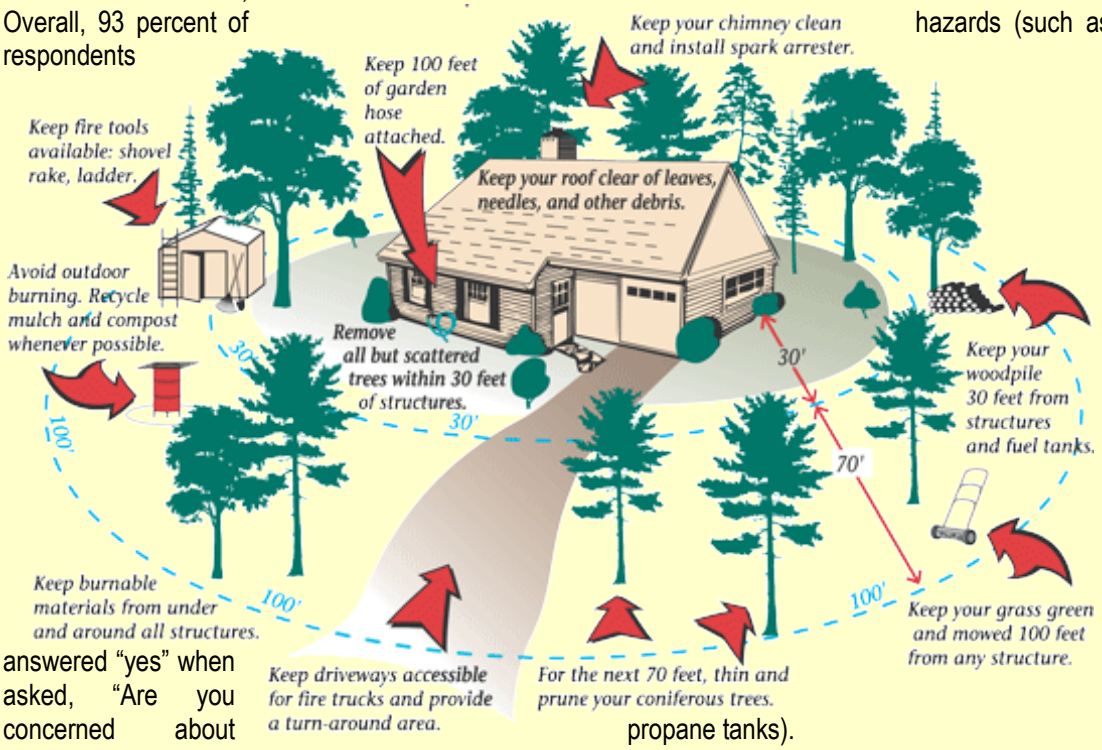
"A lot of natural hazards research finds that people tend to overweight things they have pretty limited control over. But they are downplaying the risk of things they can do something about, such as creating a 'defensible space' and what kind of siding they have," said James Meldrum, the study's lead author and a research associate in the environment and society program at the university's Institute of Behavioral Science.

But identifying such gaps in perception may be able to help wildfire professionals better communicate risks and design

incentives to get homeowners to better protect their properties.

"The reality is that there is not enough (wildfire) suppression to go around to protect every house that is out there," said Meldrum.

Overall, 93 percent of respondents answered "yes" when asked, "Are you concerned about wildfire risk affecting your current residence?"



But expert and residential opinion differed significantly.

While 50 percent of residents rated their properties as being at "moderate risk,"

professionals rated 65 percent as being at "high risk." Fifty-three percent underrated their wildfire risk relative to the professionals, and 18 percent overrated risk.

Digging deeper, researchers gauged residents' perception of specific risks in ten categories, including risk from vegetation type on the property, the type of materials used for roofing, and questions regarding accessibility to firefighting teams and equipment, such as the visibility of the address number.

Residents' perception of risk was less than that assessed by professionals for five attributes — address visibility, deck type, siding type, distance to hazardous vegetation, and distance to other combustible hazards (such as propane tanks).

The professionals and residents rated risk roughly the same for number of roads accessing a property and distance to problematic topography, such as a steep canyon or ridge, and roof type. In two categories, vegetation type and driveway width, residents reported higher risk perception than the professionals. Paradoxically, residents tended to fret more about things they could not change, such as the vegetation profile, than those they could, such as rebuilding a deck or cutting down trees near their homes.

"A lot of people do see the costs of being able to do the work themselves, and that stops them from doing it," Meldrum said. "They might want to, but when push comes to shove, they don't necessarily do it."

He said the good news is that financial incentives offered by communities or governments have been fairly effective at persuading people to take action to protect their properties.

"So we can recognize these gaps for what they are and put money toward programs to help push people into taking action," he said.

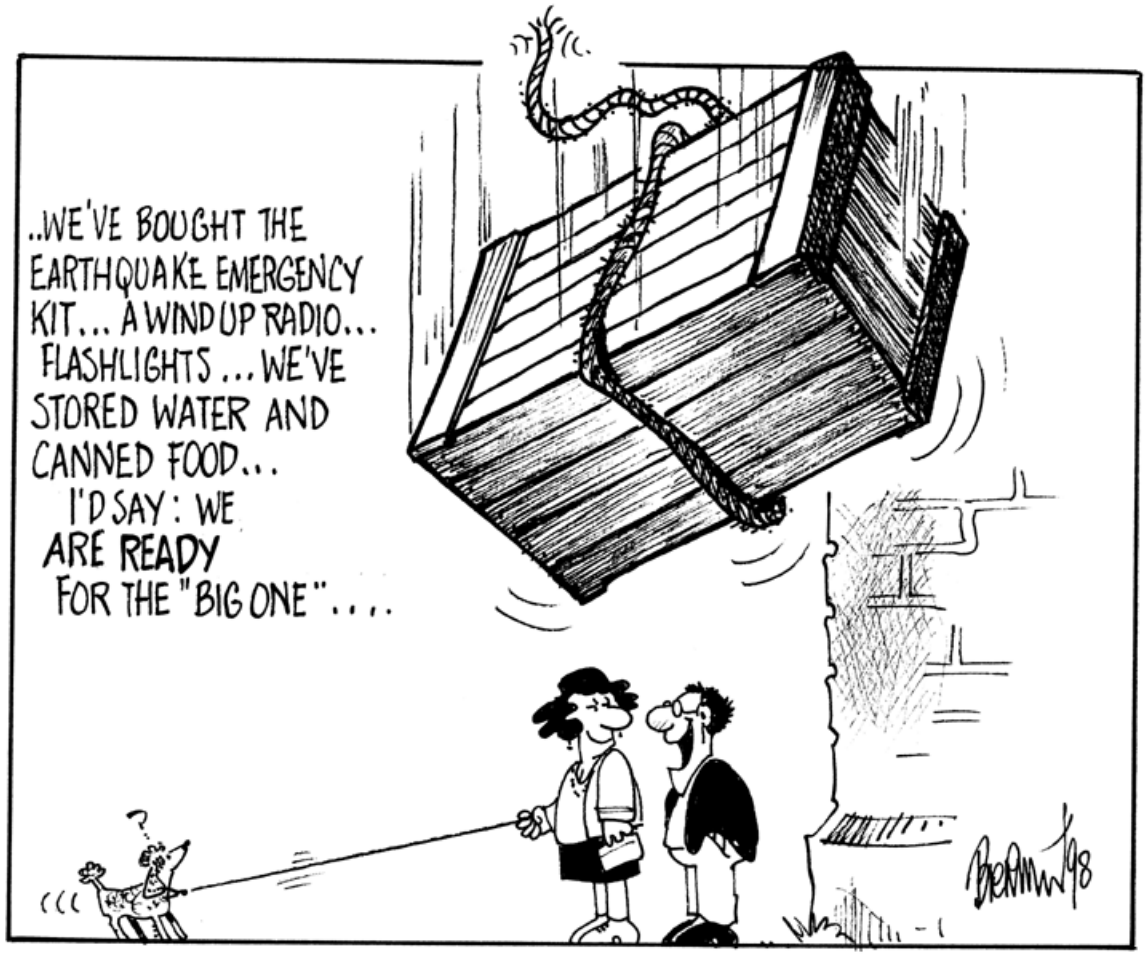
This is the idea behind Fire Adapted Communities, a coalition

of government, business, and nonprofit entities "committed to helping people and communities in the wildland-urban interface adapt to living with wildfire and reduce their risk for damage, without compromising firefighter or civilian safety."

That campaign recognizes that wildfire is a natural part of many landscapes, and that the emphasis on suppression that held sway for most of the 20th century in the United States unintentionally resulted in fuel buildups that led to more catastrophic fires.

"The idea that fire does belong on these landscapes is integral to the Fire Adapted Communities concept," Meldrum said. "This is a big, top-down effort to get communities to recognize this, to take responsibility for the fact that they live in these places, and not be dependent on suppression. We want you to be OK if suppression can't reach you."

— Read more in James R. Meldrum et al., "Understanding Gaps Between the Risk Perceptions of Wildland–Urban Interface (WUI) Residents and Wildfire Professionals," Risk Analysis (1 June 2015).



Pentagon: Climate change aggravates U.S. security risks

Source: http://www.homelandsecuritynewswire.com/dr20150805-pentagon-climate-change-aggravates-u-s-security-risks

Aug 05 – Global climate change will aggravate problems such as poverty, social tensions, environmental degradation, ineffectual leadership, and weak political institutions that threaten stability in a number of countries, according to a report the Defense Department sent to Congress last week.

The Senate Appropriations Committee requested the report in conjunction with the Defense Appropriations Act for Fiscal Year 2015, asking that the undersecretary of defense for policy provide a report which identifies the most serious and likely climate-related security risks for each combatant command and the ways those commands integrate risk mitigation into their planning processes.

Fragile states vulnerable to disruption

The report finds that climate change is a security risk, Pentagon officials said, because it degrades living conditions, human security, and the ability of governments to meet the basic needs of their populations. Communities and states that already are fragile and have limited resources are significantly more vulnerable to disruption and far less likely to respond effectively and be resilient to new challenges, they added.

"The Department of Defense's primary responsibility is to protect national security interests around the world," officials said in a news release announcing the report's submission. "This involves considering all aspects of the global security environment and planning appropriately for potential contingencies and the possibility of unexpected developments both in the near and the longer terms.

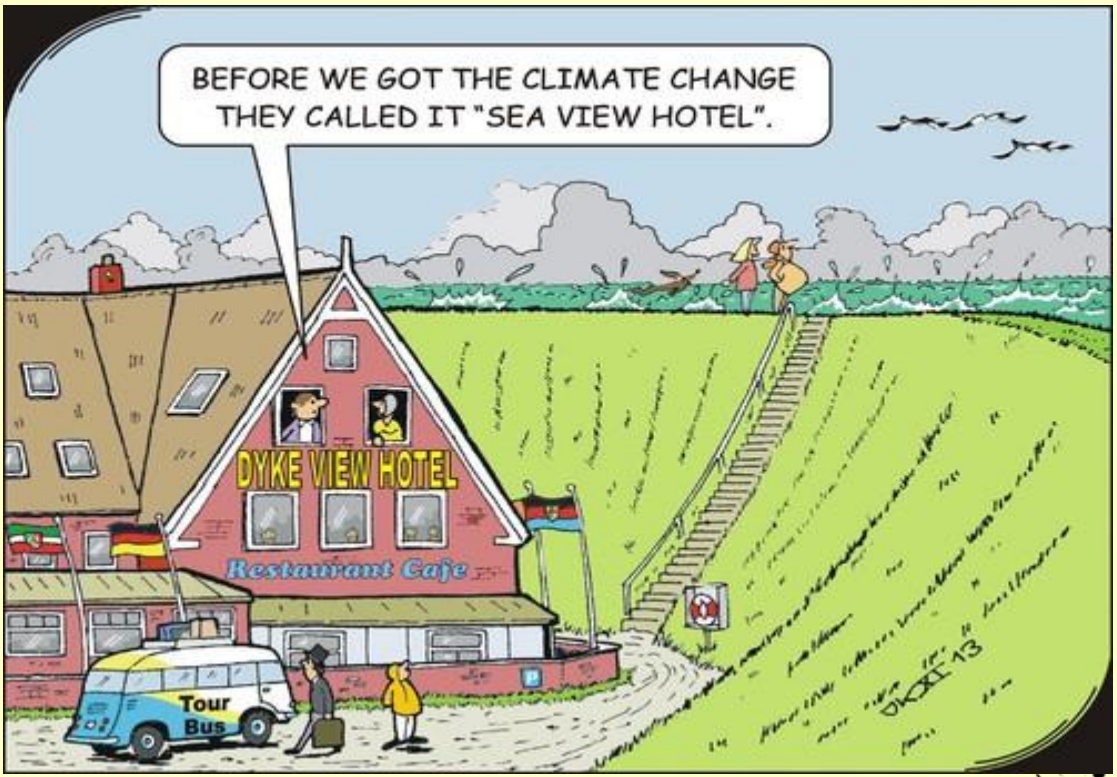
"It is in this context," they continued, "that the department must consider the effects of climate change — such as sea level rise, shifting climate zones and more frequent and intense severe weather events — and how these effects could impact national security."

Integrating climate-related impacts into planning

To reduce the national security implications of climate change, combatant commands are integrating climate-related impacts into their planning cycles, officials said. The ability of the United States and other countries to cope with the risks and implications of climate change requires monitoring, analysis and integration of those risks into existing overall risk management measures, as appropriate for each combatant command, they added.

The report concludes the Defense Department already is observing the impacts of climate change in shocks and stressors to vulnerable nations and communities, including in the United States, the Arctic, the Middle East, Africa, Asia and South America, officials said.

— Read more in National Security Implications of Climate-related Risks and a Changing Climate (U.S. Department of Defense, 23 July 2015)



BCI 20/20 Think Tank

Preparing the profession for a resilient future

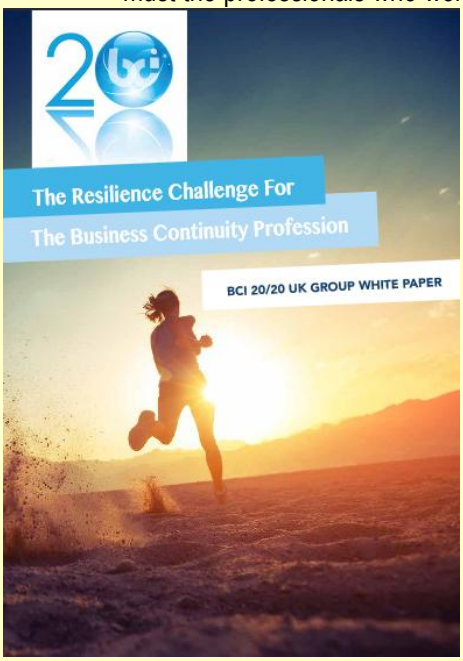
Source: http://www.thebci.org/index.php/home/bci-20-20-think-tank

Since its inception, the goal of the Business Continuity Institute has been to ***promote a more resilient world***, and with so much attention being placed on resiliency in recent years, never has this goal been more pertinent. When the Institute celebrated its 20th anniversary in 2014, the focus was not on our past achievements, it was on our vision of the future. From that vision emerged the 20/20 Think Tank, a group of Thought Leaders from across the discipline with a passion to drive it forward and fine tune it in order to meet the needs of the future. Taking a strategic view of the profession, the regional groups that make up the 20/20 Think Tank were created to support those working in the profession by performing two main functions:

Advisory
Use the vast wealth of **knowledge and experience** possessed by members of the 20/20 Think Tank to shape the direction of the profession, and so develop the career opportunities for those working in business continuity or resilience

Advocacy
Use the **resources and influence** of the 20/20 Think Tank to raise the profile of business continuity and resilience, demonstrate their value to business leaders and so get a seat at the top table with resilience embedded into organizational strategy

The role of the business continuity professional has evolved over the years. The challenges we have faced have changed, as have the technology and techniques used to combat these challenges. But the discipline is not only about changing threats or advancing technology, it is about the people within it. These are the people who strive to ensure that whatever disruptions our organizations face, we will be able to weather the storm and come out the other side. As the industry and organizations evolve, so must the professionals who work within them, so one of the key questions we need to consider is: what will the business continuity or resilience professional of the future look like? The 20/20 Think Tank will use its **knowledge and experience** to establish what skills will be required in order to meet the challenges we face now and in the future.



Of course it is not just the individuals who need to adapt to a changing environment, the professional associations that represent them must also play their part. The BCI has earned a reputation as the ***professional body of choice for resilience professionals*** by taking the lead role in discussions that help move the discipline forward. To advance the concept of resiliency further however, we and other disciplines in the resilience field must collaborate further. We must work together and combine our shared **resources and influence** to help bring about the reality of a resilient world.

In August 2015, the UK Group published its first White Paper - the resilience challenge for the business continuity profession - which positioned business continuity as an integral part of resilience, but also noting that building resilience goes beyond BC and requires substantial input from other protective disciplines. This represents a real opportunity for BCI members to advance professionally.

▶ **You can read the full white Paper at:** http://www.bcifiles.com/8thReport.pdf

Inspiring individuals | informing business | improving resilience

The 20/20 Think Tank is the umbrella name for a series of 20/20 Groups that have been set up worldwide. As a global organization, working in a global discipline, it is vital to get a global perspective. The three 20/20 Groups that exist so far are based in the United Kingdom, Australasia and the United States, but more are in the development phase.