Dedicated to Global First Responders

CBRNE NEWSLETTERRORISM

February 2017

www.cbne-terrorism-newsletter.com

It is now two and a half minutes to midnight

DOOMSDAY CLOCK MOVES AHEAD:

"Words Matter": Board Marks 70th Anniversary of Iconic Clock By Expressing Concern About "Unsettling" and "Ill-Considered" Statements of President Trump on Nuclear Weapons and Climate Change; Developments in North Korea, Russia, India and Pakistan Also Highlighted.

January 26, 2017 – It is now two and a half minutes to midnight. For the first time in the 70-year history of the Doomsday Clock, the *Bulletin of the Atomic Scientists*' Science and Security Board has moved the hands of the iconic clock 30 seconds closer to midnight. In another first, the Board has decided to act, in part, based on the words of a single person: Donald Trump, the new President of the United States.

The decision to move the hands of the Doomsday Clock is made by the Science and Security Board of the *Bulletin of the Atomic Scientists*in consultation with the *Bulletin*'s Board of Sponsors, which includes 15 Nobel Laureates. The Science and Security Board's full statement about the Clock is available online.

In January 2016, the Doomsday Clock's minute hand did not change, remaining at three minutes before midnight. The Clock was changed in 2015 from five to three minutes to midnight, the closest it had been since the arms race of the 1980s.

In the statement about the Doomsday Clock, the *Bulletin*'s Science and Security Board notes: "Over the course of 2016, the global security landscape darkened as the international community failed to come effectively to grips with humanity's most pressing existential threats, nuclear weapons and climate change … This already-threatening world situation was the backdrop for a rise in strident nationalism worldwide in 2016, including in a US presidential campaign during which the eventual victor, Donald Trump, made disturbing comments about the use and proliferation of nuclear weapons and expressed disbelief in the overwhelming scientific consensus on climate change …The board's decision to move the clock less than a full minute — something it has never before done — reflects a simple reality: As this statement is issued, Donald Trump has been the US president only a matter of days …"

The statement continues: "Just the same, words matter, and President Trump has had plenty to say over the last year. Both his statements and his actions as President-elect have broken with historical precedent in unsettling ways. He has made ill-considered comments about expanding the US nuclear arsenal. He has shown a troubling propensity to discount or outright reject expert advice related to international security, including the conclusions of intelligence experts. And his nominees to head the Energy Department, and the Environmental Protection Agency dispute the basics of climate science. In short, even though he has just now taken office, the president's intemperate statements, lack of openness to expert advice, and questionable cabinet nominations have already made a bad international security situation worse."

In addition to addressing the statements made by President Trump, the Board also expressed concern about the greater global context of nuclear and climate issues:

> *"On nuclear issues, the Board noted: "The United States and Russia—which together possess more than 90 percent of the world's nuclear weapons—remained at odds in a variety of theaters, from Syria to Ukraine to the borders of NATO; both countries continued wide-ranging modernizations of their nuclear forces, and serious arms control negotiations were nowhere to be seen.North Korea conducted its fourth and fifth underground nuclear tests and gave every indication it would continue to develop nuclear weapons delivery capabilities. Threats of nuclear warfare hung in the background as Pakistan and India faced each other warily across the Line of Control in Kashmir after militants attacked two Indian army bases."*
>
> *In surveying the status of climate matters, the Board concluded: "The climate change outlook was somewhat less dismal (in 2016) —but only somewhat. In the wake of the landmark Paris climate accord, the nations of the world have taken some actions to combat climate change, and global carbon dioxide emissions were*

essentially flat in 2016, compared to the previous year. Still, they have not yet started to decrease; the world continues to warm. Keeping future temperatures at less-than-catastrophic levels requires reductions in greenhouse gas emissions far beyond those agreed to in Paris—yet little appetite for additional cuts was in evidence at the November climate conference in Marrakech."

Rachel Bronson, executive director and publisher, *Bulletin of the Atomic Scientists*, said: "As we marked the 70th anniversary of the Doomsday Clock, this year's Clock deliberations felt more urgent than usual. In addition to the existential threats posed by nuclear weapons and climate change, new global realities emerged, as trusted sources of information came under attack, fake news was on the rise, and words were used by a President-elect of the United States in cavalier and often reckless ways to address the twin threats of nuclear weapons and climate change."

Lawrence Krauss, chair, *Bulletin* Board of Sponsors, director, Origins Project at Arizona State University, and foundation professor, School of Earth and Space Exploration and Physics Department, Arizona State University, said: "Wise men and women have said that public policy is never made in the absence of politics. But in this unusual political year, we offer a corollary: Good policy takes account of politics but is never made in the absence of expertise. Facts are indeed stubborn things, and they must be taken into account if the future of humanity is to be preserved, long term. Nuclear weapons and climate change are precisely the sort of complex existential threats that cannot be properly managed without access to and reliance on expert knowledge. In 2016, world leaders not only failed to deal adequately with those threats; they actually increased the risk of nuclear war and unchecked climate change through a variety of provocative statements and actions, including careless rhetoric about the use of nuclear weapons and the wanton defiance of scientific evidence. To step further back from the brink will require leaders of vision and restraint. President Trump and President Putin can choose to act together as statesmen, or as petulant children, risking our future. We call upon all people to speak out and send a loud message to your leaders so that they do not needlessly threaten your future, and the future of your children."

Retired Rear Admiral David Titley, *Bulletin* Science and Security Board; professor of practice, Pennsylvania State University Department of Meteorology, and founding director, Penn State's Center for Solutions to Weather and Climate Risk, said: "Climate change should not be a partisan issue. The well-established physics of Earth's carbon cycle is neither liberal nor conservative in character. The planet will continue to warm to ultimately dangerous levels so long as carbon dioxide continues to be pumped into the atmosphere— irrespective of political leadership. The current political situation in the United States is of particular concern. The Trump administration needs to state clearly and unequivocally that it accepts climate change, caused by human activity, as reality. No problem can be solved unless its existence is first recognized. There are no 'alternative facts' here".

A new kind of responder brings special expertise to disasters

Source: http://www.homelandsecuritynewswire.com/dr20170127-a-new-kind-of-responder-brings-special-expertise-to-disasters

Jan 27 – An emergency response incident commander should be well-versed on how to respond to all hazards, including the intricacies of radiological and nuclear incidents. Because the hazards associated with radiological or nuclear (rad/nuc) incidents are uniquely challenging to convey accurately to first responders, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has developed a solution in the form of the Radiological Operations Support Specialist (ROSS) Program. In the field, the ROSS makes recommendations, interprets models, and analyzes data for that incident commander.

DHS S&T says that the ROSS program helps radiation safety professionals integrate seamlessly with the incident command system so they can provide emergency-specific rad/nuc information to the incident commander, allowing emergency managers to make better decisions specific to the incident. S&T, in conjunction with the Federal Emergency Management Agency (FEMA) and the Department of Energy, designed the ROSS program to ensure radiation experts are

properly trained when mobilized as part of the incident command structure to help make the right recommendations, and to improvise if need be.

"By training radiation safety professionals on how incidents are managed and the types of radiological emergencies that local communities may face, these radiation protection experts, or ROSS, can provide necessary information, guidance and recommendations to incident commanders and decision-makers at the scene of a radiation incident to protect the public and responders," said Orly Amir, program analyst for DHS S&T's First Responder Group (FRG).

The ROSS training and certification program gives radiation health specialists emergency management knowledge. The training program developed by S&T, initially piloted in September 2016 and recently adopted by FEMA to manage and run – accomplishes this through a 40-hour training that establishes clear guidelines regarding their roles and responsibilities. Once certified, ROSS will be assigned a "type." Each type – administrators believe there will be three – signifies a varying level of capability. Those capabilities range from making recommendations on appropriate personal protective equipment for responders, to more advanced support, such as helping to coordinate a national radiological emergency response. The reason for these types is that different incidents may require different capabilities.

"The idea is that the ROSS training and certification will improve the level of rad capability within the incident command structure," said Amir.

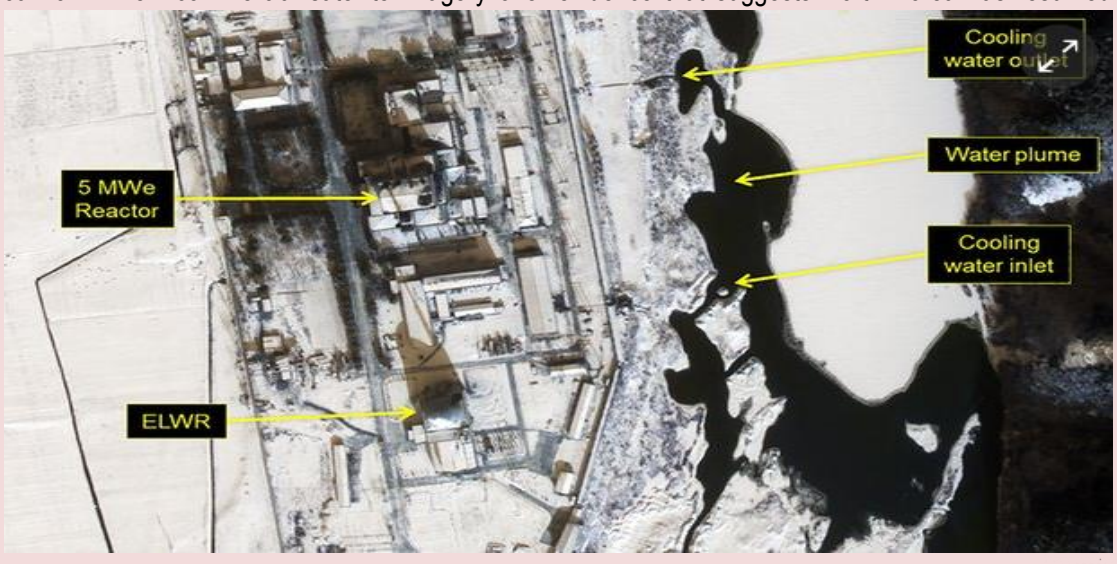
S&T notes that first responders and radiation experts both indicated the need for a specialist with these skills. With the input of first responders and radiological experts, FEMA, DOE, CRCPD, and S&T have already built training courses, onsite informational aides, and tools to train the first round of ROSS pilot participants. Now transitioned to FEMA, the in-person training will focus on radiological emergency response, terminology standardization, and analyzing the best responses for different types of hazards. For state and local radiological and health experts, the training is scheduled to be funded by FEMA's current training budget.

With the ROSS certification, health physicists and local and regional health and safety officials now have a vehicle to directly impact the outcome of an incident with their specialized knowledge. During a radiological incident, that knowledge would be critical to any incident commander.

North Korea has restarted reactor to make weapon-grade plutonium

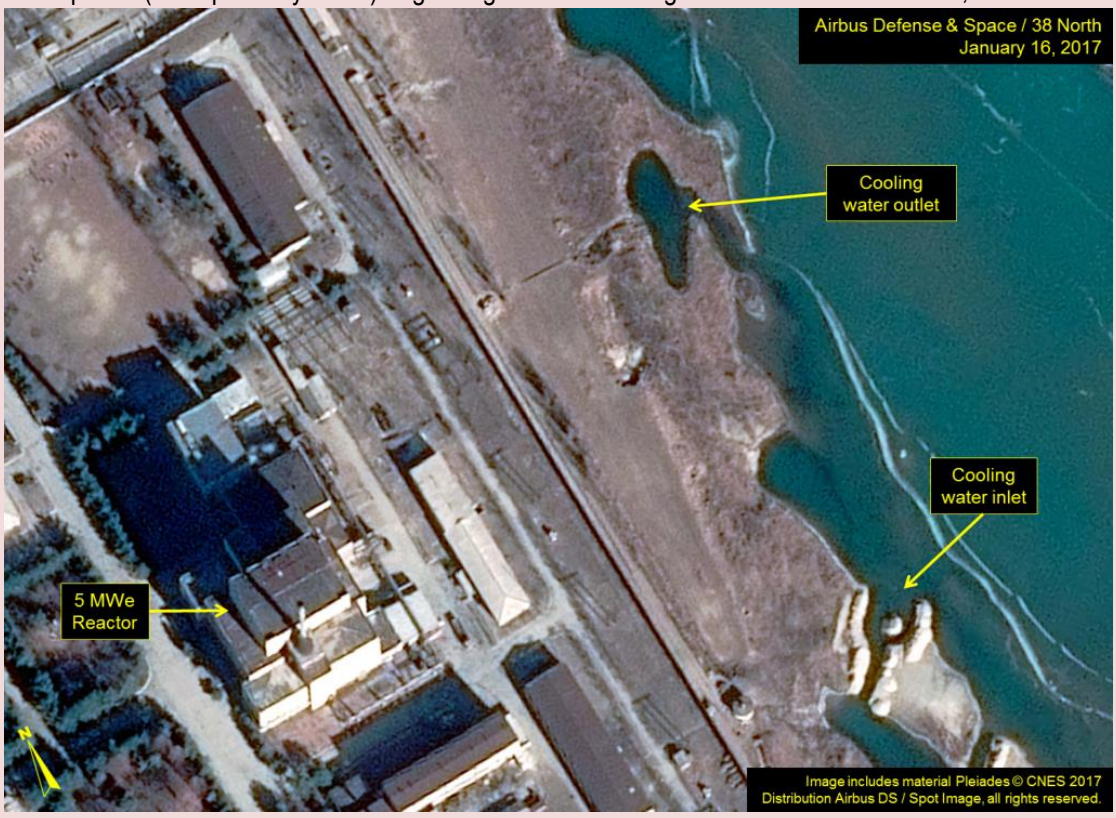
Source: https://www.theguardian.com/world/2017/jan/28/north-korea-has-restarted-reactor-to-make-plutonium-fresh-images-suggest

Jan 31 – New commercial satellite imagery offer evidence that suggests North Korea has resumed



operation of a reactor at its main nuclear site that is used to produce plutonium for its nuclear weapons program. A U.S. think tank, 38 North Project, which monitors North Korea, said on

Friday that analysis from 18 January showed signs that North Korea was preparing to restart the reactor at Yongbyon, after having unloaded spent fuel rods for reprocessing to produce additional plutonium for its nuclear weapons stockpile. It a report, the organization said that imagery from 22 January shows a water plume (most probably warm) originating from the cooling water outlet of the reactor, an indication



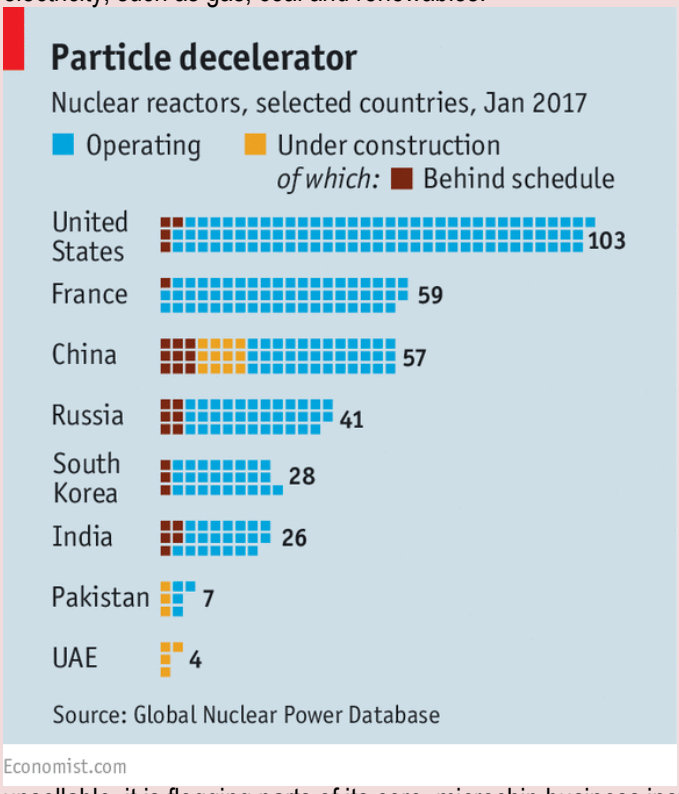
that the reactor is very likely operating. The think tank said it was impossible to estimate at what power level the reactor was running, "although it may be considerable."

How to build a nuclear-power plant

Source: http://www.economist.com/news/business/21715685-new-crop-developers-challenging-industry-leaders-how-build-nuclear-power-plant

Jan 28 – The Barakah nuclear-power plant under construction in Abu Dhabi will never attract the attention that the Burj Khalifa skyscraper in neighbouring Dubai does, but it is an engineering feat nonetheless. It is using three times as much concrete as the world's tallest building, and six times the amount of steel. Remarkably, its first reactor may start producing energy in the first half of this year—on schedule and (its South Korean developers insist) on budget. That would be a towering achievement.

In much of the world, building a nuclear-power plant looks like a terrible business prospect. Two recent additions to the world's nuclear fleet, in Argentina and America, took 33 and 44 years to erect. Of 55 plants under construction, the Global Nuclear Power database reckons almost two-thirds are behind schedule (see chart). The delays lift costs, and make nuclear less competitive with other sources of electricity, such as gas, coal and renewables.



Not one of the two technologies that were supposed to revolutionise the supply of nuclear energy—the European Pressurised Reactor, or EPR, and the AP1000 from America's Westinghouse—has yet been installed, despite being conceived early this century. In Finland, France and China, all the EPRs under construction are years behind schedule. The main hope for salvaging their reputation—and the nuclear business of EDF, the French utility that owns the technology—is the Hinkley Point C project in Britain, which by now looks a lot like a Hail Mary pass.

Meanwhile, delays with the Westinghouse AP1000 have caused mayhem at Toshiba, its owner. The Japanese firm may announce write-downs in February of up to $6bn on its American nuclear business. As nuclear assets are probably unsellable, it is flogging parts of its core, microchip business instead.

Yet relative upstarts in South Korea and China show that large reactors, such as the four 1,400-megawatt (MW) ones in Abu Dhabi, can be built. Moreover, the business case for a new breed of small reactors below 300MW is improving. This month, Oregon-based NuScale Power became the first American firm to apply for certification of a small modular reactor (SMR) design with America's nuclear regulators.

"Clearly the momentum seems to be shifting away from traditional suppliers," says William Magwood, director-general of the OECD's Nuclear Energy Agency. Both small and large reactors are required. In places like America and Europe, where electricity demand is growing slowly, there is rising interest in small, flexible ones. In fast-growing markets like China, large nuclear plants make more economic sense.

If the South Koreans succeed with their first foreign nuclear programme in Abu Dhabi, the reason is likely to be consistency. Nuclear accidents such as Three-Mile Island in 1979 and Chernobyl in 1986 caused a long hiatus in nuclear construction in America and Europe. But South Korea has invested in nuclear power for four decades, using its own technology since the 1990s, says Lee Jong-ho, an executive at Korea Electric Power (KEPCO), which leads the consortium building Barakah. It does not suffer from the skills shortages that bedevil nuclear construction in the West.

KEPCO always works with the same, familiar suppliers and construction firms hailing from Korea Inc. By contrast, both the EPR and AP1000, first-of-a-kind technologies with inevitable teething problems, have suffered from being contracted out to global engineering firms. Also, South Korea and China both keep nuclear building costs low through repetition and standardisation,

says the World Nuclear Association (WNA), an industry group. It estimates that South Korean capital costs have remained fairly stable in the past 20 years, while they have almost tripled in France and America.

The WNA also notes in a report this month a "revival" of interest in SMRs, partly because of rock-bottom sentiment toward large plants. Utilities are finding it tough to pay for big projects (Barakah, for instance costs a whopping $20bn), especially in deregulated power markets where prices have slumped because of an abundance of natural gas and renewable energy. Big investments can sink a firm's credit rating and jack up its cost of capital.

It is less onerous to pay for an SMR, which means that even though they produce less energy, they can be cost-competitive with larger plants once they are being mass produced, says the WNA. Other advantages are that SMRs will be factory-built, easy to scale up by stacking them together, and quick to install.

America's regulators expect to reach a decision on NuScale's application within 40 months. Safety will be the crucial issue; both the reactor and the facilities where it will be fabricated need to pass muster. It uses a well-established pressurised-water technology and claims not to be at risk from the problems that caused the Fukushima disaster in Japan in 2011; it has no pumps, and no need for external power or water. If approved, the success of the technology will not be known until many have been produced. Yet with the prospect of SMRs and the Abu Dhabi plant soon going into action, long-suffering backers of nuclear power at last have something to pin their hopes on.

Report: German intelligence believes Iran tested nuclear-capable cruise missile

Source: http://www.homelandsecuritynewswire.com/dr20170202-report-german-intelligence-believes-iran-tested-nuclearcapable-cruise-missile

Feb 02 – **In addition to a ballistic missile test that Iran itself revealed, Germany believes that Iran also test-fired a Sumar cruise missile, which could have a range of 2,000-3,000 kilometers (1,250-1,875 miles) and could reach Germany at its maximum capability. In its test, the Sumar successfully traveled 600 kilometers (375 miles), a little less than half the distance to Israel**.

Cruise missiles can travel at a lower altitude than ballistic missiles and also have radar-evading capabilities, making them harder to counter.

Iran may be pursuing this course because unlike with ballistic missiles, Iran is not explicitly banned by the United Nations Security Council from developing cruise missiles, a security expert explained to *Die Welt*.

However, if Iran is developing a nuclear-capable missile, it undercuts its claim, often made in defense of its ballistic missile program, that nuclear weapons have "no place" in Iran's defense doctrine.

The semi-official Tasnim news agency recently stated that "nuclear weapons have basically no place in the Islamic Republic's defense doctrine." A 2016 report from the Congressional

Research Service quoted a number of high-ranking Iranian officials, including Supreme Leader Ayatollah Ali Khamenei, making similar assertions.
The Sumar was unveiled in March 2015 and is based on the Russian Kh-55 missile.
German intelligence reports leaked in 2014 and 2015 showed that Iran sought to purchase technologies for nuclear, biological, and chemical weapons.
National Security Advisor Michael Flynn said Wednesday that in response to Iran's ballistic missile testing and support for the Houthi rebels in Yemen, the United States was putting Iran "on notice" and would not tolerate Iran's continued violations of international norms.

Should we really be so afraid of a nuclear North Korea?

By Markus Bell and Marco Milani
Source: http://www.homelandsecuritynewswire.com/dr20170206-should-we-really-be-so-afraid-of-a-nuclear-north-korea

Feb 06 – The common thinking is that North Korea's nuclear program poses a threat to global peace and diverts economic resources from an impoverished population. North Korean leaders are depicted in the Western media as a cabal of madmen who won't be satisfied until Washington, Seoul, or some other enemy city is turned into a "sea of fire."
Successive U.S. governments have used a range of carrots and sticks to entice or pressure the North Korean leadership to give up its nuclear program. The North's missile launches and nuclear tests in 2016 make plain that these efforts have failed; in short, the West has to accept that it is now a nuclear power and focus instead on limiting the risks a nuclear North Korea presents.
But it also pays to consider what sounds like a perverse question: could a North Korean bomb actually benefit both the country's people and the world at large?
First, a reality check: The North Korean nuclear program is less a madcap scheme than a clear and deliberate strategy. Its leaders have closely watched what's happened to other countries that have backed away from nuclear arsenals, and two in particular: Ukraine and Libya.
Ukraine gave up its massive Soviet-era nuclear arsenal in 1994 when it signed the Budapest Memorandum with Russia, the United States and the United Kingdom, on whose terms it traded nuclear weapons for a formal reassurance to respect its sovereignty; 20 years later, Moscow invaded and annexed the Crimean peninsula, and a pro-Russian insurgency in the east is still rumbling. As for Libya, Muammar Gaddafi renounced his weapons of mass destruction program as part of an opening to the West only to be forcibly removed from power by the same countries some eight years later.
Along with the Iraq War, these spectacles taught the North Korean regime that it's hard for a relatively small, isolated country to survive without the military hardware to guarantee it. Pyongyang has duly shown great diplomatic skill in drawing out nuclear negotiations, buying itself both time and financial aid as its program moves forward.
In 2016 alone, it tested two nuclear weapons, sent a satellite into orbit, and made advances in both submarine launched ballistic missiles (SLBM) and intercontinental ballistic missile (ICBM) technology. In his New Year's address at the start of 2017, Kim Jong-un emphasized that the country's nuclear forces are central to its self-defense capability: "We will defend peace and security of our state at all costs and by our own efforts, and make a positive contribution to safeguarding global peace and stability."

The long view

A nuclear North Korea obviously worries the international community for several reasons. Kim might in theory actually use nuclear weapons on his enemies, a threat he periodically makes. His country's admission into the "nuclear club" might spark a regional arms race. It could share or sell technologies of mass destruction to hostile states. And then there's the danger of a full-blown nuclear accident with all the attendant regional repercussions.

These risks aren't trivial, but they should be viewed with some perspective. For starters, a nuclear attack from Pyongyang appears highly unlikely. The government is fully aware that it would incur an overwhelmingly destructive military response from the United States and South Korea. It's also worth remembering that while the program has been underway for twenty-five years, there is still no sign of a regional nuclear arms race.

As for proliferation or accidents, these demand not isolation but co-operation and communication. Keeping Pyongyang cut off from the world will not help; if its nuclear facilities are to be kept safe and their products not used to bring in illicit foreign revenue, they must be properly monitored rather than kept hidden.

Meanwhile, a nuclear North Korea might well see fit to downsize its enormous and costly conventional military forces, which are among the world's largest. As it transitions away from what it calls a "Military First" policy to something more deterrent-centric, it makes sense to encourage it to reduce its conventional military forces. (Better still, if it did, heavily-armed South Korea might follow suit.)

With a smaller conventional military to maintain, Pyongyang might be able to channel scarce state funds away from defense and towards raising the standard of living for ordinary North Koreans. This point is in line with its stated strategy of growing the economy and developing the nuclear deterrent in parallel, a policy known as the Byungjin line, and with Kim's mooted five-year economic plan. His plans demand dramatic shifts in North Korean state policy, which could destabilize the regime. The calculation is that the security provided by nuclear capabilities would offset the shock of sudden domestic change.

Most paradoxically of all, North Korea's nuclear "arrival" might make for a positive turn in inter-Korean relations. International efforts to eliminate North Korea's nuclear program isolated the country, in turn greatly undermining the chances of a rapprochement with the South, whose efforts to defrost relations have lately come to nothing. The pace of the North's nuclear development meant that the now-impeached President Park's policy of reconciliation – "Trustpolitik" – was doomed before it began.

As far as Pyongyang is concerned, its militaristic strategy has worked: It has kept the Kim government internally stable, the population dependent on the government, and the country's enemies at bay. Accepting the country's nuclear status, rather than trying to head it off with sanctions and threats, could bring it back to the diplomatic bargaining table.

Markus Bell *is Anthropologist and Lecturer in Korean and Japanese studies, University of Sheffield.*
Marco Milani *is Postdoctoral Scholar, Korean Studies Institute, University of Southern California.*

Record high fatal radiation levels, hole in reactor detected at crippled Fukushima nuclear facility

Source: https://www.rt.com/news/376107-fukushima-record-radiation-level/

Feb 02 – Radiation levels of up to 530 Sieverts per hour were detected inside an inactive Reactor 2 at the Fukushima Daiichi nuclear complex damaged during the 2011 earthquake and tsunami catastrophe, Japanese media reported on Thursday citing the plant operator, Tokyo Electric Power Company (TEPCO).

A dose of about 8 Sieverts is considered incurable and fatal.

A hole of no less than one square meter in size has also been discovered beneath the reactor's pressure vessel, TEPCO said. According to researchers, the apparent opening in the metal grating of

one of three reactors that had melted down in 2011, is believed to be have been caused by melted nuclear fuel that fell through the vessel.

The iron scaffolding has a melting point of 1500 degrees, TEPCO said, explaining that there is a possibility the fuel debris has fallen onto it and burnt the hole. Such fuel debris have been discovered on equipment at the bottom of the pressure vessel just above the hole, it added.

The latest findings were released after a recent camera probe inside the reactor, TEPCO said. Using a remote-controlled camera fitted on a long pipe, scientists managed to get images of hard-to-reach places where residual nuclear material remained. The substance there is so toxic that even specially-made robots designed to probe the underwater depths beneath the power plant have previously crumbled and shut down.

However, TEPCO still plans to launch further more detailed assessments at the damaged nuclear facility with the help of self-propelled robots.

Speaking to RT, Yosuke Yamashiki, Doctor of Engineering from Kyoto University said the located leaking is *"a great discovery."*

"This is a kind of progress," Yamashiki said.

"There is a very small hole… and very small amount of the radiation is still leaking from the reactor. It's not the fatal level but it is going on."

"However, they haven't established a proper means of how to decompose the meltdown reactor yet. There not so many ways to decompose it," the expert noted, adding that he and his colleagues are providing a special technique using ice which, however, has not been approved yet.

Yamashiki warned that the complete reduction of the radiation will take hundreds of thousands of years.

However, looking on the bright side, he said, *"right now, the radiation level is much lower since the reactor hasn't been active for a while."*

Earlier this week, hopes for a more efficient cleanup at Fukushima were high, as the plant operator announced a portion of nuclear fuel debris responsible for a lot of the lingering contamination from six years ago may have finally been found.

First thyroid cancer case in Japan recognized as Fukushima-related & compensated by govt

Source: https://www.rt.com/news/370650-thyroid-cancer-fukushima-plant-radiation/

Dec 2016 – A man who worked at the Fukushima nuclear power plant in Japan during the disastrous 2011 meltdown has had his thyroid cancer recognized as work-related. The case prompted the government to finally determine its position on post-disaster compensation.

The unnamed man, said to be in his 40s, worked at several nuclear power plants between 1992 and 2012 as an employee of Tokyo Electric Power Company Holdings Inc. He was present at the Fukushima Daiichi nuclear power plant during the March 11, 2011 meltdown. Three years after the disaster, he was diagnosed with thyroid gland cancer, which the Japanese Ministry of Health, Labor and Welfare confirmed on Friday as stemming from exposure to radiation.

The man's body radiation exposure was totaled at 150 millisieverts, almost 140 of which were a result of the accident. Although this is not the first time that health authorities have linked cancer to radiation exposure for workers at the Fukushima plant, it is the first time a patient with thyroid cancer has won the right to work-related compensation.

There have been two cases previously, both of them involving leukemia.

The recent case prompted Japan's health and labor ministry to release for the first time its overall position on dealing with compensation issues for workers who were at the Fukushima plant at the time and after the accident. Workers who had been exposed to over 100 millisieverts and developed cancer five years or more after exposure were entitled to compensation, the ministry ruled this week. The dose level was not a strict standard but rather a yardstick, the officials added.

As of March, 174 people who worked at the plant had been exposed to over 100 millisieverts worth of radiation, according to a joint study by the UN and the Tokyo Electric Power Company. There is also an estimate that more than 2,000 workers have radiation doses exceeding 100

millisieverts just in their thyroid gland, reported. Japanese newspaper the Asahi Shimbun

Fukushima medical survey confirms 14 new child thyroid cancer cases

Source: https://www.rt.com/news/345641-fukushima-child-thyroid-cancer/

June 2016 – The number of child thyroid cancers discovered in the wake of the Fukushima nuclear disaster has reached 131, with the latest panel review adding 14 to the list of those suffering from the deadly disease, along with dozens of new suspected cases.

After the latest review of the ongoing second round of medical checkups conducted on almost 300,000 children who were aged 18 or younger at the time of the accident at the Fukushima Daiichi plant in March 2011, the prefecture-run program announced that a total 131 people have now been diagnosed with thyroid cancer.

Some 30 thyroid cancer cases were added to the radiation victims toll following the second round of checkups that began in April 2014. A further 27 people are suspected of having the disease. Previous numbers disclosed in February showed that 16 patients suffered from cancer.

In the latest announcement, scientists also say that a child who was less than five-years-old at the time of the tragedy had also been diagnosed with cancer. The new figures of those confirmed or suspected to have thyroid cancer have tumors ranging from 5.3 mm to 35.6 mm.

The first thyroid cancer detection round studying minors was conducted in Japan between 2011 to 2014 and discovered 101 people with thyroid cancer. With the latest numbers, the new toll stands at 131, while another 41 are suspected of suffering from radiation exposure, Japan Times reports.

"Concerns have been growing among Fukushima residents with the increase in the number of cancer patients. We'd like to further conduct an in-depth study," said Hokuto Hoshi, head of the panel and a senior member of the Fukushima Medical Association.

He however maintained the panel's earlier accession that it is *"unlikely"* that the disease cases was caused by radiation exposure, reiterating claims that there is no direct link between thyroid cancer and the nuclear disaster.

After the earthquake and tsunami in March 2011, radioactive elements were released from the Fukushima Daiichi Nuclear Power Plant. After the release, Fukushima Prefecture continued to conduct thyroid screening ultrasounds on all residents agds 18 years and younger. The first round of screening included 298,577 examinees, while the round that began in April 2014 focuses on 267,769 people.

Japan's Fukushima disaster costs double to almost $200bn

Source: https://www.rt.com/business/369789-japan-fukushima-costs-double/

Dec 2016 – The costs related to the Fukushima nuclear accident have significantly grown to $188 billion (21.5 trillion yen), according to the Japanese government. The costs were initially projected at about 11 trillion yen.

The rising estimated cost means a heavier burden on Tokyo Electric Power (TEPCO) and other utilities, which are being urged to conduct drastic restructuring and reforms. It could also result in higher power bills for consumers.

In 2011, a nine magnitude earthquake struck Japan, triggering a deadly tsunami. Flooding then caused a cooling system failure at TEPCO's Fukushima plant and a meltdown in three reactors.

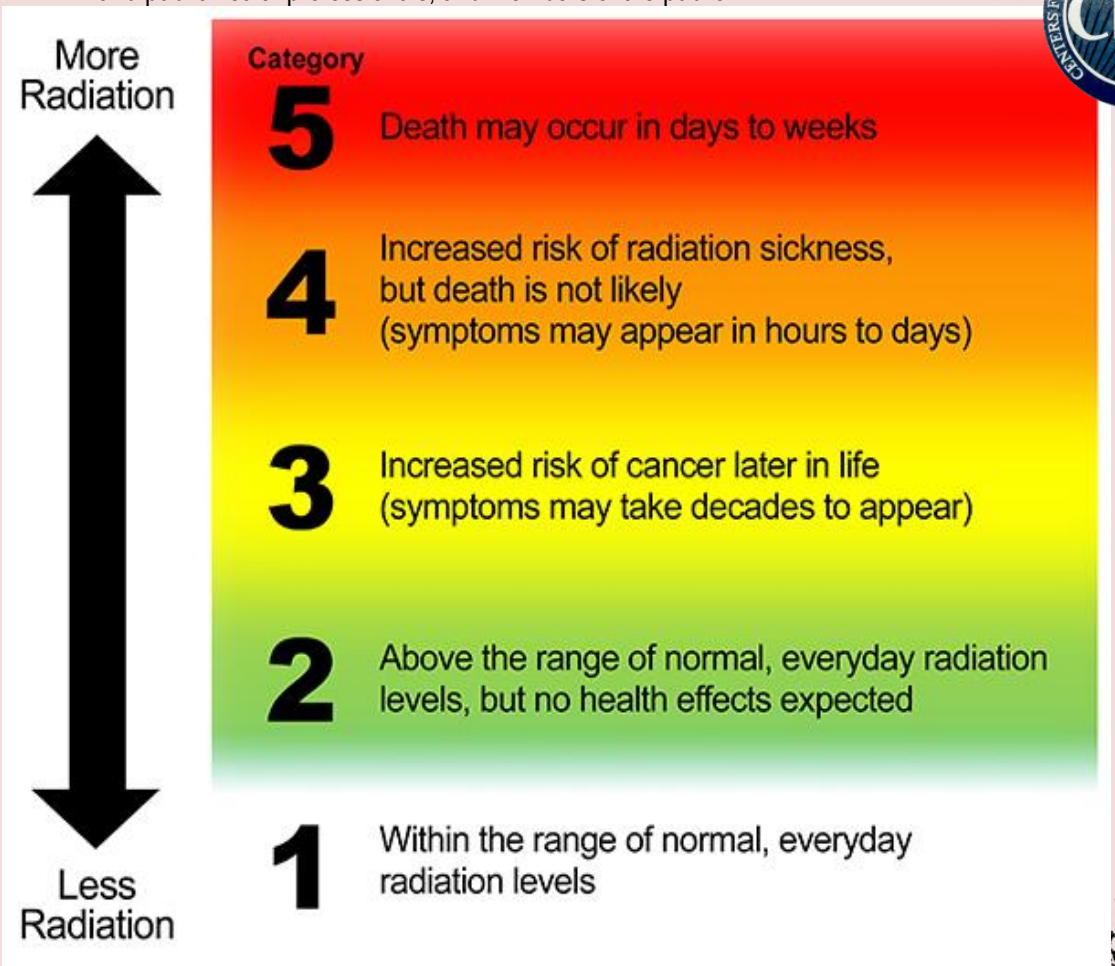
Officials say the decommissioning of the wrecked Fukushima reactors will take several decades. The cost is now estimated at $70 billion (8 trillion yen), quadruple an earlier projection of $17.5 billion (2 trillion yen).
TEPCO's portion of the bill has more than doubled to $138 billion (15.9 trillion yen) from $63 billion (7.2 trillion yen). The other leading utilities will need to pay $32 billion (3.7 trillion yen) while new electric companies will have to shoulder $2 billion (240 billion yen).
"For now, we don't expect the costs to increase further, but new developments and unforeseen factors mean there is a chance they could go higher," said Hiroshige Seko, Japan's Minister of Economy, Trade, and Industry.
"Decommissioning technological innovation and a speedier cleanup could help reduce costs and it is important that we put effort into that," he added.

Radiation Hazard Scale

A Tool for Communication in Nuclear and Radiological Emergencies
Source: https://emergency.cdc.gov/radiation/radiationhazardscale.asp

The Centers for Disease Control and Prevention has developed the Radiation Hazard Scale as a tool for communication in emergencies.
This tool:

- Provides a frame of reference for relative hazards of radiation.
- Conveys meaning without using radiation measurements or units that are unfamiliar to people.
- Is designed for use ***only*** in radiation emergencies and is applicable for short-term exposure durations, for example, over a period of several days.
- Is best used when accompanied with protective action recommendations or instructions.
- Has been audience tested with public information officers, emergency management and public health professionals, and members of the public.



Description of the Radiation Hazard Scale Categories

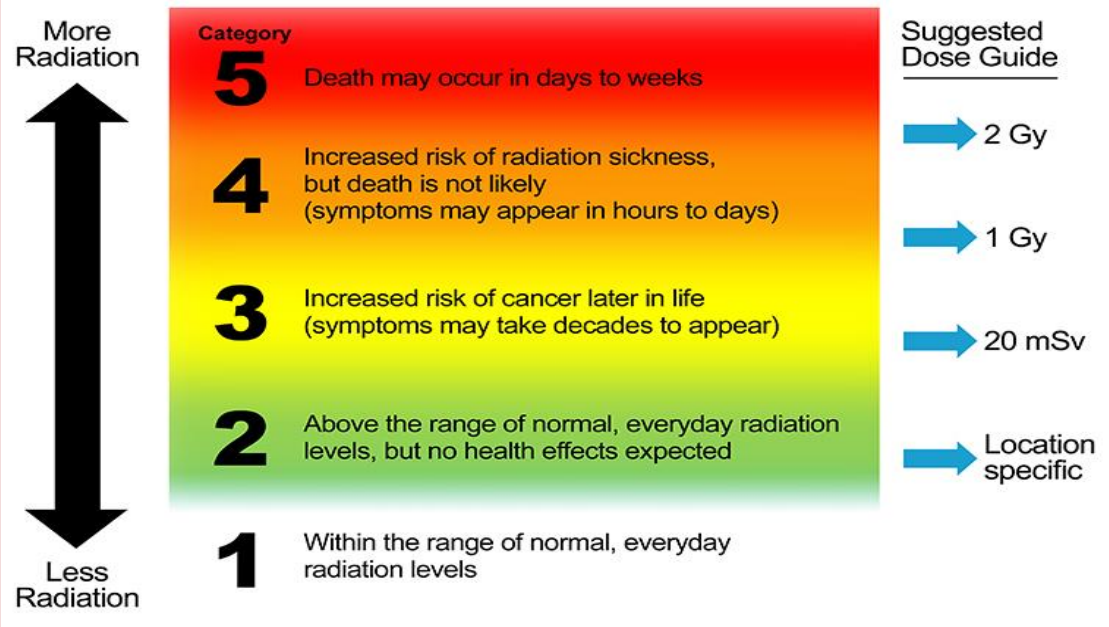
Category	Description
5	**Category 5** means that radiation doses are dangerously high and potentially lethal. High doses of radiation can cause massive damage to organs of the body and kill the person. The exposed person loses white blood cells and the ability to fight infections. Diarrhea and vomiting are likely. Medical treatment can help, but the condition may still be fatal in spite of treatment. At extremely high doses of radiation, the person may lose consciousness and die within hours. For more information, see https://www.remm.nlm.gov/ars_summary.htm
4	**Category 4** means that radiation doses are dangerously high and can make people seriously ill. Radiation doses are not high enough to cause death, but one or more symptoms of radiation sickness may appear. Radiation sickness, also known as Acute Radiation Syndrome (ARS), is caused by a high dose of radiation. The severity of illness depends on the amount (or dose) of radiation. The earliest symptoms may include nausea, fatigue, vomiting, and diarrhea. Symptoms such as hair loss or skin burns may appear in weeks. For more information about the health effects of radiation, see http://emergency.cdc.gov/radiation/healtheffects.asp For more information about medical treatment of radiation exposure, see http://emergency.cdc.gov/radiation/countermeasures.asp
3	**Category 3** means that radiation doses are becoming high enough where we may expect increased risk of cancer in the years ahead for people who are exposed. Leukemia and thyroid cancers can appear in as few as 5 years after exposure. Other types of cancer can take decades to develop. Studies have shown that radiation exposure can increase the risk of people developing cancer. This increased risk of cancer is typically a fraction of one percent. The lifetime risk of cancer for the population due to natural causes is approximately 40%. The increase in risk of cancer from radiation depends on the amount (or dose) of radiation, and it becomes vanishingly small and near zero at low doses of radiation. For more information, see http://emergency.cdc.gov/radiation/cancer.asp
2	**Category 2** means that radiation levels in the environment are higher than the natural background radiation for that geographic area. However, these radiation levels are still too low to observe any health effects. When radiation levels are higher than what we normally have in our natural environment, it does not necessarily mean that it will cause us harm. For more information about health effects of radiation, see http://www.cdc.gov/nceh/radiation/health.html
1	**Category 1** means that radiation levels in the environment are within the range of natural background radiation for that geographic area. Low amounts of radioactive materials exist naturally in our environment, food, air, water, and consequently in our bodies. We are also exposed to radiation from space that reaches the surface of the Earth. These conditions are natural, and this radiation is called the natural background radiation. For more information about radiation and radioactivity in everyday life and how it can vary by location, see http://www.cdc.gov/nceh/radiation/sources.html

Suggested Guide on How to Assign Radiation Hazard Categories

The Radiation Hazard Scale is intended to communicate relative hazards to populations under emergency conditions when exact radiation exposure parameters for specific individuals are not available. Note that:

- There are no sharp lines separating radiation hazard categories.
- Transition from Category 1 to Category 2 depends on the range of natural background radiation for a geographic area.
- The radiation dose values are whole-body doses and are suggested guides for radiation protection purposes. Dose values are meant to be used by radiation protection experts and emergency response or public health authorities. For a description of radiation units listed in the dose guide, see Primer on Radiation Measurements.
- Radiation dose values are not meant to be included in public messaging, especially during early phase of a radiation emergency.

This guide is applicable for short-term exposure durations, for example, over a period of several days during an emergency.



Example Uses of Radiation Hazard Scale in Emergency Communication Messages

Examples after a nuclear detonation:

- In areas where the Radiation Hazard Category is 5, sheltering in place can help maintain a Category 2 or 3 until instructed to evacuate. In contrast, self-directed evacuation in fallout areas can place a person at Category 4 or 5.
- If people are contaminated with nuclear fallout, self-decontamination can rapidly decrease radiation hazard from Category 5 to Category 2 or 1.

Example Uses of Radiation Hazard Scale in Displaying Environmental Data

Select a scenario:

- Detonation of an Improvised Nuclear Device (IND) – Download PDF
- Accidental release from a nuclear power plant (NPP) – Download PDF
- Explosion of a Radiological Dispersal Device (RDD) – Download PDF

Frequently Asked Questions

What is the difference between the International Nuclear Event Scale (INES) and the Radiation Hazard Scale?

These two scales have quite different applications in an emergency. The INES, developed by the International Atomic Energy Agency is a tool to grade the safety significance of a particular event associated with sources of ionizing radiation. The INES describes the accident itself. On the other hand, the Radiation Hazard Scale describes the immediate potential impact of the accident for people, and the hazard category depends on where people are located.

For example, the severity of the March 2011 accident at the Fukushima Daiichi nuclear power plant has been given the highest rating of 7 on the INES scale. Regardless of whether we live in the United States or Japan, the INES rating for the Fukushima Daiichi accident is 7. However, the Radiation Hazard Category would have been quite different for people depending on their location. For emergency responders working at the Fukushima Daiichi plant at the time of the accident, the Radiation Hazard Category was 4 or 5 depending on where they worked at the plant. At the same time, the Radiation Hazard Category for people living in Tokyo was 2 for a short period of time, and it was Category 1 for people in the United States.

Can the radiation hazard scale be used to describe medical exposures?

No. In its present form, this Scale is intended only for emergency exposure situations.

Would the public need pre-event education on interpreting the scale?

While pre-event education is always helpful, there is no requirement for pre-event public education for effective use of this Scale. Our audience testing with members of the public who

had at least a high school diploma indicated that the Scale is simple enough to understand, and it can be described briefly by a Public Information Officer or a news reporter.

Who would assign the radiation hazard categories in an emergency?

Environmental scientists and radiation safety experts can evaluate the data and assign the Radiation Hazard Categories in coordination with emergency management authorities, public health officials, and communication experts.

Meet the lake so polluted that spending an hour there would kill you

Source: http://grist.org/article/meet-the-lake-so-polluted-that-spending-an-hour-there-would-kill-you/

Welcome to beautiful Lake Karachay, a Russian lake so tainted by nearby nuclear facilities that it's

considered the most polluted place on the planet. In 1990, just standing on the shore for an hour would give you a radiation dose of 600 roentgen, more than enough to kill you. On the plus side, lakefront property is probably really, really cheap.

You can't really blame Lake Karachay for acting up — it comes from a really rough area. The lake is located within the Mayak Production Association, one of the largest — and leakiest —

nuclear facilities in Russia. The Russian government kept Mayak entirely secret until 1990, and it spent that period of invisibility mainly having nuclear meltdowns and dumping waste into the river. By the time Mayak's existence was officially acknowledged, there had been a 21 percent increase in cancer incidence, a 25 percent increase in birth defects, and a 41 percent increase in leukemia in the surrounding region of Chelyabinsk. The Techa river, which provided water to nearby villages, was so contaminated that up to 65 percent of locals fell ill with radiation sickness — which the doctors termed "special disease," because as long as the facility was secret, they weren't allowed to mention radiation in their diagnoses.

Filling in the lake with concrete.

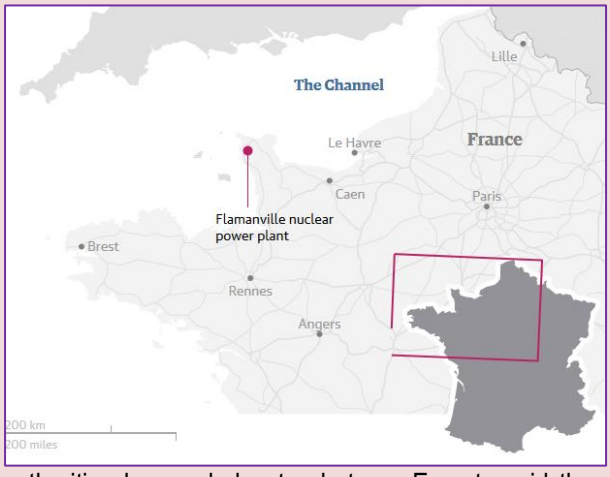
Perhaps unsurprisingly, this shady Siberian nuclear complex wasn't overly concerned with safety. Besides dumping nuclear material in the lakes and rivers, Mayak also suffered several serious accidents in the 1950s and '60s — including the time that Lake Karachay dried up and radioactive dust from the lakebed blew all over the nearby villages. But because Mayak and the city that serviced it (originally called Chelyabinsk-40 and then Chelyabinsk-65, both of which sound appropriately like radioactive materials) didn't even appear on maps, nobody heard about this, including affected locals. Some of the people living nearby were evacuated after these accidents, but many were just left to inhale contaminated dust and drink tainted water.

Lake Karachay is now full of concrete that's intended to keep radioactive sediment away from shore. Downstream water in the Techa river has almost no radioactive cesium, though you still can't drink the upstream stuff and the riverbanks will be dangerous for hundreds of years. The Mayak nuclear facility still sucks out loud — it had its operating license revoked in 2003 for dumping waste into open water, surprise surprise — but at least things like "operating licenses" now exist. And today, 20 years after Mayak started appearing on maps again, it's even possible that you could stand on the shores of Lake Karachay and not die. But we wouldn't risk it.

France nuclear plant explosion: no risk of contamination, say experts

Source: https://www.theguardian.com/environment/2017/feb/09/explosion-at-flamanville-nuclear-plant-in-western-france

Feb 09 – There is no risk of contamination after an explosion occurred at EDF's Flamanville nuclear plant in northern France, authorities have said.



EDF said the blast at 9.40am on Thursday was caused by a fire in the turbine hall, which is outside the nuclear zones of the power station, located 15 miles west of the port of Cherbourg. Five people were treated for smoke inhalation.

The nuclear operator said an on-site team brought the fire under control, and the incident was declared over by 11am. One of the plant's two water pressurised reactors, unit one, was shut down after the explosion and remains offline.

The cause of the fire is unknown, though authorities have ruled out sabotage. Experts said the explosion appeared to be a relatively minor event and did not pose a safety risk.

"Though any accident at a nuclear site must be taken seriously, I wouldn't call this a nuclear accident as there was no release of radioactive material and the reactor was not affected," said Prof Jim Smith, professor of environmental science at the University of Portsmouth. "There doesn't appear to be any risk to the general public."

Mycle Schneider, a Paris-based nuclear consultant, said that fires in a nuclear plant were always "bad news" because of side effects such as the smoke, which apparently intoxicated the five people.

"However, in this case, the fire had apparently been contained and rather quickly brought under control. I don't think this was a major event at all."

Other nuclear experts noted that because of the design of the plant's reactors, water passing through the turbine would not have gone through the reactor's core, so it was unlikely there was a radioactive release. "There were no consequences for safety at the plant or for environmental safety," EDF said in a statement.

A new third-generation reactor known as EPR is being built at Flamanville and it will be the world's largest when it goes into operation in late 2018. Construction of the new plant at the site began in 2007 and was initially scheduled for completion in 2012 but has been delayed several times and is over budget.

The design of the new reactor is the same as the one planned at Hinkley Point C, in Somerset, which will be the UK's first new nuclear power station in two decades.

Construction is underway at the site, where EDF has already moved two and a half million cubic metres of earth and begun work on a 500-metre long jetty to bring in the vast majority of material needed for the plant. There are currently 1,2000 people working on the project. EDF also hopes to build a second new plant at Sizewell on the Suffolk coast.

Nuclear power provides four-fifths of France's electricity generation, but many of the country's ageing power stations are expected to close in the 2030s. The reliance on the power stations led to warnings of a risk of power cuts this winter after safety checks forced several of 85% state-owned EDF's plants offline for tests.

Paul Dorfman, of the Energy Institute at University College London, said the Flamanville blast may be minor, but it nonetheless added to the pressure EDF had already come under with the inspections. "It's the cherry on the top of the horrendous time that French nuclear is having."

François Hollande's government passed an energy transition law, which came into effect last year, that encourages a switch to renewable energy sources such as wind and solar, and caps the amount of electricity produced by nuclear power.

The board of EDF recently voted to close the country's oldest atomic plant in order to stay under that cap and open a new one at Flamanville.

Animated map shows every nuclear-bomb explosion in history

Source: http://www.businessinsider.com/animated-map-shows-every-nuclear-bomb-explosion-history-2016-12

Where did the idea of an 'Islamic bomb' come from?

By Malcolm M. Craig

Source: http://www.homelandsecuritynewswire.com/dr20170210-where-did-the-idea-of-an-islamic-bomb-come-from

Feb 10 – The heavily freighted idea of an "Islamic bomb" has been around for some decades now. The notion behind it is that a nuclear weapon developed by an "Islamic" nation would

automatically become the Islamic world's shared property – and more than that, a "nuclear sword" with which to wage jihad. But as with many terms applied to the "Islamic world", it says more about Western attitudes than about why and how nuclear technology has spread.

The concept as we know it emerged from anxieties about proliferation, globalization, resurgent Islam, and conspiracies real and imagined, a fearful idea that could be applied to the atomic ambitions of any Muslim nation or non-state group. It looked at Pakistan's nuclear program and extrapolated it to encompass everything between the mountains of South Asia and the deserts of North Africa. And ever since it appeared it has retained its power to shock, eliding terrorism, jihadism, the perceived ambitions of "Islamic" states, and state-private proliferation networks into one fearsome term.

It has also made a useful avatar for all sorts of specific threats – Muammar Gaddafi's anti-Western "fanaticism", Saddam Hussein's socialist Ba'athism, the Iranian Mullahs' revolutionary Islamic ideology, contemporary fundamentalist terrorism, and Pakistan's military-Islamic thinking.

But of course, the Islamic bomb idea is part of a web of complex geopolitical ideas. International terrorism, the rise of modern political Islam, and Western interventions all muddle the issue. And oddly enough given the way it's used today, the term in fact began its strange life outside the West.

High hopes

The connection between religion and the bomb was in fact first explicitly made in 1970s Pakistan, where leaders Zulfikar Ali Bhutto and Muhammad Zia ul-Haq both saw nuclear weapons as a means to enhance the country's status within the so-called "Muslim world". Yet Pakistan's atomic program was at its heart a nationalistic security project, not a religious one.

The term "Islamic bomb" didn't appear in the Western news media until around 1979, when the Iranian Revolution set outsiders worrying about the potential intersections between nuclear weapons, proliferation and Islamic politics. At around the same time, India was mounting a campaign against Pakistan's nuclear ambitions; its government and media duly began deliberately stoking fears of a pan-Islamic nuclear threat originating with Islamabad. Israel's government, too, made it clear that it believed an Islamic bomb was imminent.

Media revelations about Pakistani metallurgist Abdul Qadeer Khan also helped to spur interest. In 1975, Khan had stolen uranium enrichment centrifuge blueprints from the URENCO plant in the Netherlands. These ended up providing the technical basis for Pakistan's bomb program.

Khan's theft – and the genuine conspiracy that was Pakistan's international nuclear purchasing project – led to conspiracy theories. Despite being a Pakistani nationalist, the Guardian newspaper stated that "Dr. Khan Stole the Bomb for Islam". His act was seen not as the actions of one man, but as part of a wider "Islamic" conspiracy.

In 1979, media institutions including West Germany's ZDF, the UK's BBC, and the US's CBS all popularized the concept. On little evidence, it became accepted that this was a project designed to benefit the entire Muslim world. But despite the genuine Pakistani-Libyan connections, there was simply never a unified Islamic nuclear quest.

Conspiracy theory

Through the 1980s and 1990s, countries as diverse and mutually antagonistic as Iran, Iraq, Libya, Niger and Pakistan were all tied together by the Western fear of an Islamic bomb. Prominent commentators such as Jack Anderson and William Safire consistently deployed the term; politicians as diverse as Tam Dalyell, Edward Kennedy, and Daniel Patrick Moynihan all talked about it in fearful terms. All were off-base.

After Khan's international proliferation network was exposed in 2004, there duly appeared a slew of books on the subject, more than a few of which posited that there was an international "Islamic" conspiracy to acquire "the bomb". Khan was portrayed as a "nuclear jihadist" bent on righting perceived wrongs inflicted by the West on the world's Muslims.

Again, a genuine conspiracy became tied up with conspiracy theory. Yes, Khan did proliferate centrifuge technology to Iran, Libya and North Korea – but he was motivated by money, power and prestige, not religion.

Today, the specter of the Islamic bomb haunts certain corners of the internet. From the Huffington Post to Breitbart and the Washington Times, the term crops up again and again,

always used to imply that nations such as Iran harbor ambitious ideological motives for their nuclear ambitions.

It's true that prominent Muslim figures from Bhutto to bin Laden spoke rhetorically about a "bomb for the ummah". But this was never more than rhetoric. Leaving aside all nuclear matters, internecine and sectarian differences and conflict mean that global Islamic political unity is unlikely in the extreme.

The Islamic bomb has always been a convenient device with which to elide complex problems of religion, politics, and nuclear weapons. And sadly, it still is. Those who still casually bandy the term about would do well to think about where it really comes from.

***Malcolm M. Craig** is Lecturer in History, Liverpool John Moores University.*

Source:https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/591619/170213_-_Civil_Nuclear_Cyber_Security_Strategy.pdf

The Mob Is Secretly Dumping Nuclear Waste Across Italy and Africa

Source: http://gizmodo.com/the-mob-is-secretly-dumping-nuclear-waste-across-italy-1513190243

Hezbollah Threatens to Hit Israel's Nuclear Facility If Confrontations Escalate

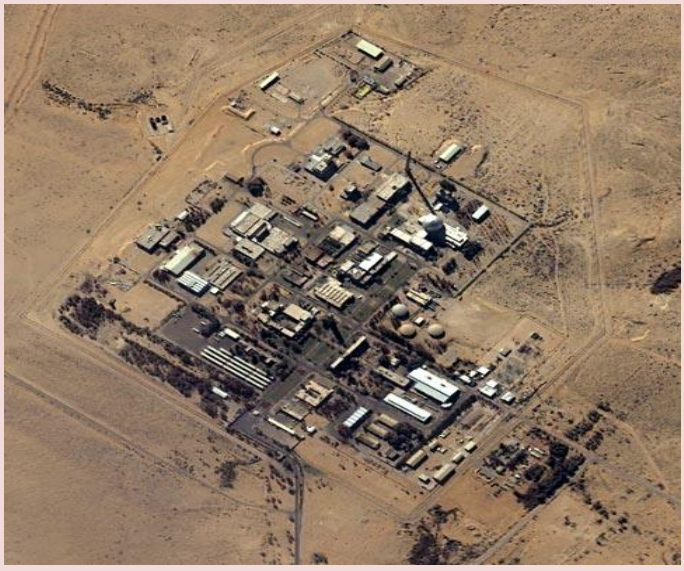
Source: https://sputniknews.com/middleeast/201702161050766177-hezbollah-israel-dimmona/

Feb 16 – **Lebanese Hezbollah movement threatened Thursday to strike the Dimona nuclear facility located in the south of Israel in case of further confrontations with the country.**

"We can make the Dimona facility, already threatening the region, a threat to Israel's existence," Hassan Nasrallah, Secretary General of Hezbollah, said as quoted by Al-Manar TV channel.

He also urged Israel to empty the ammonia tank in Haifa, which has been at the center of the recent bilateral confrontations, and to shut down the nuclear reactor in Dimona. Nasrallah characterized unloading of the ammonia reservoir as "a sign that the enemy [Israel] is aware of Lebanon's possibilities for resistance".

The leader of the Lebanese Shiites noted that Hezbollah fighters are combat-ready to disrupt Israel's attack against Lebanon.



The secretary general of Hezbollah also pointed out that Israel has been constructing defensive barriers around its settlements since 1948, when it started building a concrete wall on the Lebanese border.

On Sunday the Haifa Court for Local Affairs ruled that an ammonia tank menacing the lives of hundreds of thousands of people in the area must be emptied within 10 days. The ruling came after Hezbollah issued a statement threatening to strike Haifa.

The Dimona nuclear plant in the Negev desert has been seen as threatening the lives of people in Israel and neighboring Jordan since 2008.

Israel was in a month-long war with the Lebanese Shia Islamist militant group Hezbollah in 2006, and there has been no major direct confrontation between the parties since.

Stolen radioactive material found in Malaysian apartment building

Source: https://www.rt.com/news/377355-stolen-radioactive-material-malaysia/

Feb 15 – **Iridium-192, a substance which can potentially be used in a dirty bomb, has been found at a Malaysian apartment complex prompting fears that residents there may have been exposed to the hazardous material.**

South Klang district police said residents needed urgent health checks after two stolen radioactive canisters were found with their

seals broken, exposing people to the dangerous substance.
A team designated to finding the radioactive scanners traced the canisters to the apartment building after learning that they had been sold from a scrap metal shop in Kampung Jawa on Friday.
The canisters were from a radioactive scanning device found in a rubbish bin during a search of Seri Era Apartment complex, in the Klang district, on Saturday.
"They had disposed of the inner casings made of depleted uranium as well as the inner rods containing iridium-192 which emanates gamma ray," said the Atomic Energy Licensing Board's (ALEB) director Hasmadi Hassan.
Exposure to gamma rays can cause symptoms like dizziness, nausea, and vomiting.
Humans are capable of receiving 20 millisieverts of gamma rays a year, however, these canisters had the gamma ray capacity of up to 300 millisieverts per hour, according to the ALEB.
By Sunday, police had arrested a group of eight men in connection with the radioactive material, which was reportedly stolen from a car belonging to a business that maintains the pipes of an oil and gas company.
Among the eight detained suspects were four employees of the oil and gas service company, said Klang Selatan police chief Assistant Commissioner Alzafny Ahmad.

Serbia first in Europe by cancer mortality rate, main reason: NATO

Source: https://inserbia.info/today/2015/03/serbia-first-in-europe-by-cancer-mortality-rate-main-reason-nato/

March 2015 – **Serbia ranks as first in Europe by the cancer mortality rate, which grows an average 2.5 percent every year,** making the problem of malignant tumors in our country very serious, oncologist Slobodan Cikaric, President of the Serbian Society for the Fight Against Cancer, said Wednesday.
Speaking at a conference held as part of a cancer awareness month, Cikaric said that the main reason for the increase in the number of malignant tumor cases and deaths was the use of depleted uranium during the NATO bombing of the former Federal Republic of Yugoslavia in 1999.
According to a report for 2012 prepared by the Institute of Public Health of Serbia Dr Milan Jovanovic Batut, the total number of new cases was 36,408, and 21,269 people died from cancer.
The primary cancer site with the male population is the lungs, while in women, the most often the cause of death is breast cancer.
There are still no data for 2014, but the number of new cases is about 40,000 people, 2.8 times more than in the rest of the world, he said.
This is a real Serbian disaster, said Cikaric.

No One Can Figure Out What's Behind a Mysterious Radiation Spike Across Europe

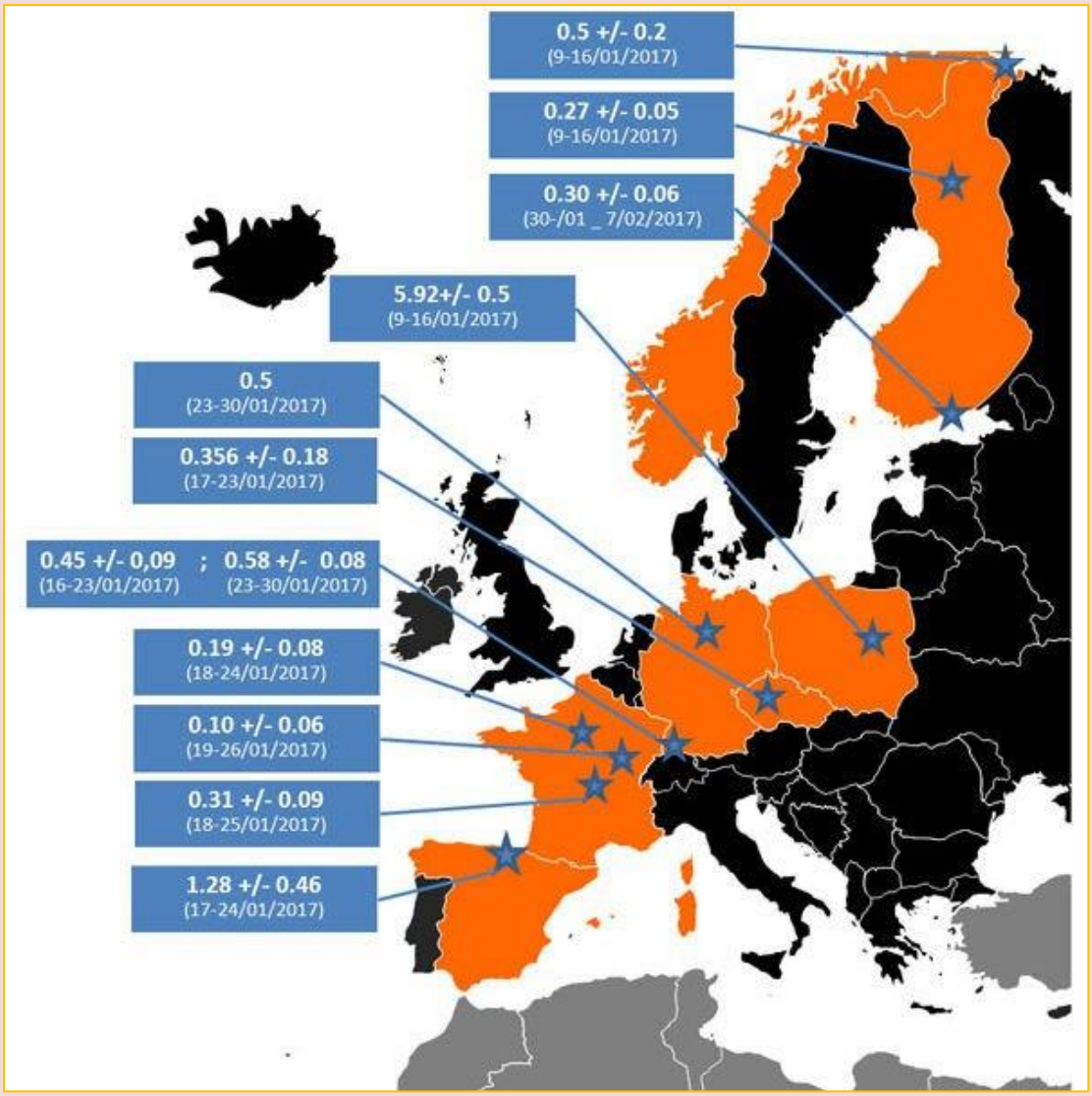
Source: http://www.sciencealert.com/no-one-can-figure-out-what-s-behind-a-mysterious-radiation-spike-across-europe

Feb 21 – Small amounts of nuclear radiation spread across Europe last month, and no one can figure out why.
First detected over the Norway-Russia border in January, the radioactive Iodine-131 bloom was then found over several European countries, and while unsubstantiated rumours of nuclear testing by Russia have been cropping up, officials say it's most likely linked to an unreported pharmaceutical mishap.
While the radiation spike happened in January, officials in Finland and France have only just gone public with information on the incident, announcing that after the spike was detected in Norway, it appeared in Finland, Poland, Czechia (Czech Republic), Germany, France and Spain, until the end of January.
When asked why Norway didn't inform the public last month, when it was the first to detect the radiation in its northernmost county, Finnmark, Astrid Liland from the Norwegian Radiation Protection Authority told the Barents Observer:

"The measurements at Svanhovd in January were very, very low. So were the measurements made in neighbouring countries, like Finland. The levels raise no concern for humans or the environment. Therefore, we believe this had no news value."

As France's nuclear safety authority, the IRSN, announced last week, the actual amount of radioactive Iodine-131 in Europe's ground-level atmosphere in January "raise no health concerns", and has since returned to normal.

But what's most disconcerting about the event isn't the level of radiation that spread through Europe - it's the fact that no one can say what actually happened.



Iodine-131 (value +/- uncertainty) in the atmosphere. Credit: IRSN

What we do know is that Iodine-131 has a half-life of just eight days, so detecting it in the atmosphere is proof of a recent release.

"The release was probably of recent origin. Further than this, it is impossible to speculate," Brian Gornall from Britain's Society for Radiological Protection told Ben Sullivan at Motherboard.

Right now, the best bet is that the origin of the radioactive Iodine-131 is somewhere in Eastern Europe - something that conspiracy theorists have latched onto as evidence that Russia performed a nuclear test in the Arctic.

But there is no evidence of this taking place, and the fact that only Iodine-131 - and no other radioactive substances - were detected strongly suggests this is not the answer.

"It was rough weather in the period when the measurements were made, so we can't trace the release back to a particular location. Measurements from several places in Europe might indicate it comes from Eastern Europe," Liland told the Barents Observer.

Based on the particular isotope, experts are saying it's far more likely that the radiation spike is the result of some kind of pharmaceutical factory leak, seeing as Iodine-131 is used widely in treating certain types of cancer.

"Since only Iodine-131 was measured, and no other radioactive substances, we think it originates from a pharmaceutical company producing radioactive drugs," Liland told Motherboard. "Iodine-131 is used for treatment of cancer."

And, oddly enough, the case for pharmaceuticals being behind the mess has a surprisingly similar parallel to back it up - an almost identical event occurred in 2011, when low levels of radioactive Iodine-131 were detected in several European countries for a few weeks.

At the time of the announcement, officials were also at a loss to explain the spike in Iodine-131, but quickly ruled out a link to nuclear power plants.

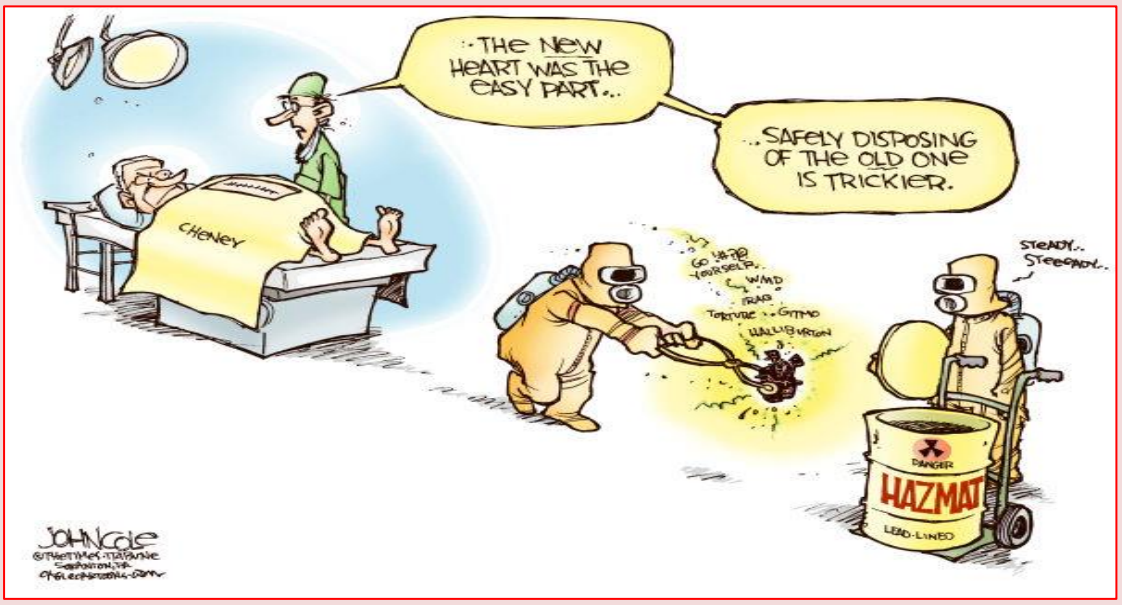
"If it came from a reactor we would find other elements in the air," Didier Champion, then head of environment and intervention at the IRSN, told Reuters in 2011.

Interestingly, a paper came out just last week confirming that the source of the 2011 Iodine-131 leak was a faulty filter system at the Institute of Isotopes Ltd in Budapest, Hungary, which produces a wide variety of radioactive isotopes for medical treatment and research.

The investigation is still ongoing for the 2017 leak, with the US Air Force deploying its WC-135 nuclear explosion 'sniffer' aircraft to the UK last week to help narrow down the source.

Hopefully researchers can nail down what exactly happened here, so factory owners - if they are to blame this time around - can ensure these kinds of leaks don't continue.

Because while both events posed no health risk to humans, it's really not something any manufacturer should be risking.



Resolve Handheld Through-Barrier Hazmat, Explosives and Narcotics ID

Source: https://www.cobaltlight.com/products/resolve/

Providing a revolutionary new capability in handheld detection, Cobalt's Resolve™ enables rapid detection and identification of explosives, narcotics and hazardous materials *through* sealed, opaque containers

A New Capability for Hazmat, EOD and Law Enforcement

Enabling Faster, Safer Critical Decision-Making

- Detect through coloured and opaque plastic, dark glass, paper, cardboard, sacks and fabrics
- Keep hazards contained - No need to open or disturb objects
- Fast - Accurate ID of chemicals and mixtures in ~1 minute (or less in some modes of operation), with no sample preparation or consumables
- Unique technology significantly reduces the risk of igniting sensitive explosives
- Rugged - Built to withstand tough user environments
- User-friendly - Large buttons, simple interface, designed for use in protective gear

Resolve identifies hazardous chemicals, explosives and narcotics through opaque barriers, including coloured plastics

Handheld Through-Barrier ID

Resolve is the world's only handheld Raman system for true *through-barrier* identification of hazardous or contraband materials. Resolve rapidly detects and identifies materials from comprehensive libraries, with Cobalt's unique handheld SORS™ technology enabling positive identification *through* a wide range of sealed non-metallic containers, barriers and packaging.

A New Capability in CBRNE Detection

Resolve differs from conventional handheld Raman ID systems, which are typically limited to line-of-sight measurements. Resolve operates in three principal modes:

- **Through-barrier** – Detects through non-metallic, sealed containers such as coloured and opaque plastics, glass, paper, wrapping, sacks and fabrics
- **Surface scan** – Line-of-sight measurements, similar to conventional Raman ID systems
- **Vial holder** – Quickly identifies materials contained within glass vials in a custom holder

A 'non-contact' mode is also available for both surface scan and *through-barrier* measurements.

Flexible On-board Libraries

Configure your own libraries:

- Explosives and precursors

- Hazardous and toxic materials
- Chemical agents
- Narcotics & new psychoactive substances
- Household products and less commonly-used chemicals
- Create and deploy your own libraries

True Through-Barrier Detection & Identification

Resolve's *through-barrier* capability removes the need to open containers - hazards remain contained & evidence is preserved - enabling response teams to identify container contents early in an operation, prior to escalation. This allows information about the situation to be gathered quickly and efficiently enabling better critical decision making.

Taliban suffer heavy casualties as 2 major IED factories destroyed in Nimroz

Source: http://www.khaama.com/taliban-suffer-heavy-casualties-as-2-major-ied-factories-destroyed-in-nimroz-02663

Jan 13 – The Taliban militants suffered heavy casualties during an operation of the Afghan security forces in western Nimroz province of Afghanistan, the Ministry of Interior (MoI) said Thursday.

According to a statement by MoI, at least 80 Taliban insurgents were killed and two large Improvised Explosive Device (IED) factories were destroyed during the operation.

The statement further added that the militants suffered casualties during the operations which were launched ten days ago in Khashrud district.

According to MoI, a compound used by the shadow district governor of the Taliban was also destroyed during the operations and at least 20 foreign insurgents were killed.

The anti-government armed militant groups including the Taliban insurgents have not commented regarding the report so far.

Taliban militants and insurgents belonging to other militant groups are frequently using Improvised Explosive Device (IED) as the weapon of their choice to target the security forces and government officials.

However, in majority of such attacks, the ordinary civilians are targeted as the anti-government armed militants are accused of incurring the most casualties to the civilians.

The United Nations Assistance Mission in Afghanistan (UNAMA) said late in October that the mission has documented 8,397 conflict-related civilian casualties (2,562 deaths and 5,835 injured) between 1 January and 30 September, representing a one per cent decrease compared to the same period in 2015.

Ground engagements remained the leading cause of civilian casualties, followed by suicide and complex attacks, and improvised explosive devices (IEDs).

Smiths Detection's HI-SCAN 6040aTiX X-Ray System Achieves Industry First EDS Cabin Baggage Screening Certification

Source:http://www.smithsdetection.com/index.php?option=com_k2&view=item&layout=item&id=585&Itemid=2912#.WJBdHfIgHCt

Jan 25 – Random searches of air travellers' cabin luggage will soon be a thing of the past for airports using Smiths Detection's industry leading cabin baggage X-ray system, the HI-SCAN 6040aTiX.

The advanced checkpoint screening solution is the first in the industry to be awarded the new European Explosive Detection Systems (EDS) certification EDS CB C1 for its automated explosives detection capability.

Airports using the system can dispense with random searches using additional explosive trace detectors or dogs, thanks to its advanced detection system, which significantly enhances airport security while also speeding up the inspection process and boosting throughput.

Additional benefits for airports include cost savings for administration and maintenance, as there is no need to use threat image projection to review operator performance. The system helps maintain high levels of operator performance as the complexity of X-ray images remain consistently the same, helping facilitate threat detection.

Cameron Mann, Global Market Director for Aviation at Smiths Detection, said: "We are delighted to be the first in the industry to receive EDS CB C1 certification. Regulators are looking to next-generation detection technology to handle ever evolving threats and we are proud that they have recognized our ability to keep passengers safe. We're continuously working to meet the highest industry standards with our security solutions, ensuring passengers can travel safely and securely, while also helping lighten the load for airport operators."

ECAC is focused on moving towards automatic detection of explosives in cabin baggage through the latest standards. EDS CB C2 systems will take automation a step further, meaning that electronic devices such as laptops can remain in bags. By introducing the new EDS standards, ECAC is both increasing the security level at aviation checkpoints whilst also facilitating operational improvements. Further, any system which meets EDS CB C1, C2 or C3 is automatically considered to have achieved EDS HBS (Hold Baggage Screening) Standard 3.

Algeria completes decades-long landmine removal along its borders

Source: https://africatimes.com/2017/01/27/algeria-completes-decades-long-landmine-removal-along-its-borders/

Jan 27 – Algeria says it has completed the removal of border landmines, **destroying nearly 9 million mines** that date to the colonial era.

"The completion of the mine clearance operation crowns over 50 years of constant work on the ground, for the final eradication of mines in our country," said General Boualem Madi, speaking on behalf of Algeria's defense ministry at a press conference earlier this week in Algiers.

Madi said the **cleared land amounts to more than 62,000 hectares**, now returned to productive use and available for development. The decades of mine removal were completed in extremely difficult conditions, notably "weather conditions, remote and hard-to-reach regions, dense forests and disappeared marks of the mines," he said, according to an English translation provided by Algeria News Service.

The use of land mines is banned under the 1997 Ottawa (Mine Ban) Treaty, although a few countries – Libya among them – have used them in recent years, according to the Landmines in Africa organization. Others have never signed the treaty, although most African nations have.

Yet decades of work has been focused on mines placed during wars in a previous era. The African continent has extensive minefields, with Angola and Chad among the most heavily mined countries.

The latest data from the International Campaign to Ban Landmines (ICBL) notes that Algeria, along with Eritrea, South Sudan and Zimbabwe, were heavily contaminated by landmine placement. Algeria will meet a target deadline for removal that the ICBL said is in April 2017.

In 2015, the ICBL reports, there were 18 people each day who were killed or injured by mines placed across the globe.

Greece: 72,000 people to be evacuated from western Thessaloniki to remove WWII bomb

Source: http://www.amna.gr/english/article/17093/72-000-people-to-be-evacuated-from-western-Thessaloniki-to-remove-WWII-bomb

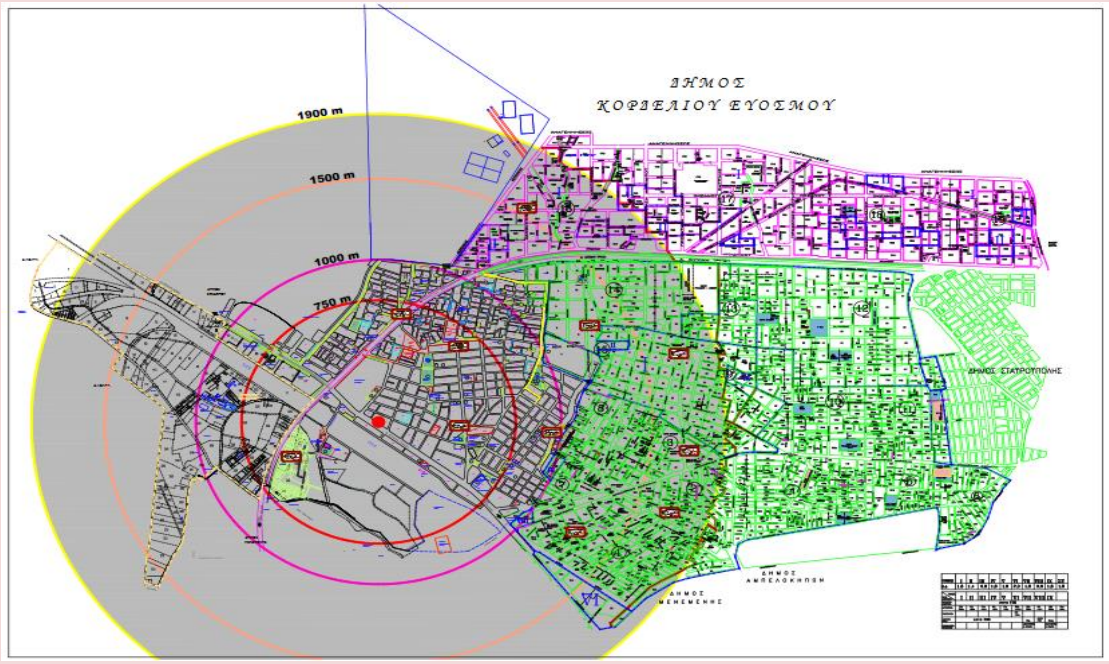
Feb 07 – **Authorities finalized on Tuesday a major plan to evacuate 72,000 residents from western Thessaloniki to allow bomb disposal units to safely defuse and remove an unexploded bomb dating from World War II.**

An initial evacuation plan of 250-300 people which started last Friday was deemed insufficient by local authorities and the process was halted to come up with a different procedure. **The bomb, containing 153 kilos of explosive material,** was found by the crew of a gas company digging to expand a gas station's underground tanks last week.

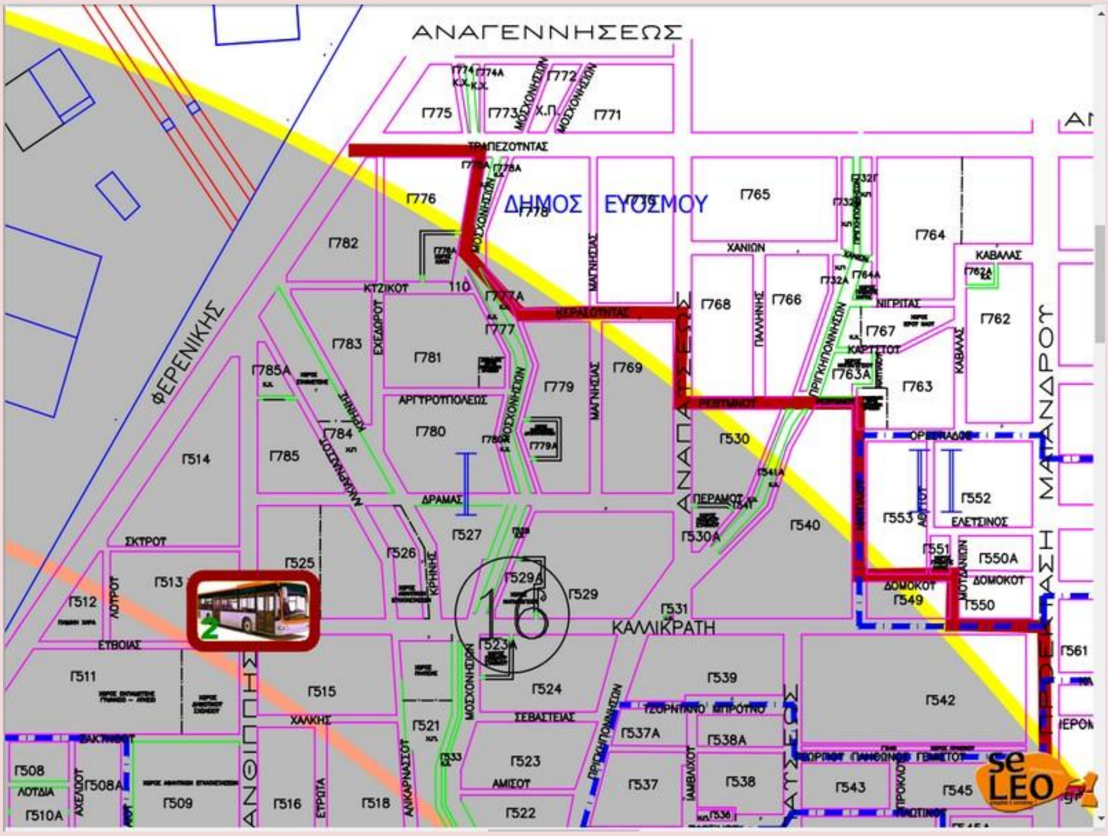
According to police information, the bomb is considered "ordinary" and the unit set to defuse it has deactivated dozens of similar bombs found at Thessaloniki's "Macedonia" international airport, along the TAP pipeline route and other areas.

Western Macedonia's deputy prefect Voula Patoulidou and representatives from the police, the army and local government decided in a meeting that 62,000 residents will be evacuated from the area of Kordelio-Evosmos and another 10,000 from Ambelokipi –Menemeni. Residents in the areas of Delta and Aghia Sofia will not have to move.

The evacuation is set to start early on Sunday so that by 10:00, the **two-kilometer evacuation area** will



be empty. Patoulidou said residents who can, will use their own means of transportation, while the rest will be transferred by 100 busses and municipal vans which will be made available. People with disabilities and older residents will be assisted by municipal officers and rented cars, while volunteers and municipal employees will distribute maps with information on how to evacuate safely.



Authorities said the assembly points will be announced on Wednesday and evacuees will have to stay there until the bomb has been removed. On Wednesday, the municipality will publish a map of the city so that residents can see if they are included in the evacuation order. A call center will also be set up to brief people on the process, while the entire area will be declared in a state of emergency by the General Secretariat of Citizen Protection.

All gas stations in the area will have to empty their tanks from fuel and gas supply installations will be closed down, while any business activity within the evacuation zone will be halted.

EDITOR'S COMMENT: Huge operation! Thanks God that the diffing machine did not penetrate the bomb (by just 4cm!!!), being under a petrol station. The Military EOD Battalion will neutralize the bomb (112 EOD Unit). Evacuation zones: (1) Red: 750m; (2) Purple: 1000m; (3) Orange: 1500m; and (4) Yellow: 1900m. Hope everything will go according to plan! ➔ Operation was successful!




HSS Development Releases Their New Remote RDS500 Suicide Bomb Detector

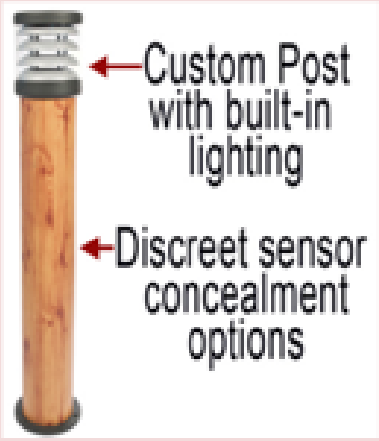
Source: http://www.secintel.com/ecom-prodshow/bomb_detector.html

Feb 07 – HSS Development, A New York based counter terrorist and defense manufacturing firm, released their highly anticipated upgrade of their bomb detection line, the RDS500. The RDS500 is a covert remote controlled and monitored 'walk-by' bomb and weapons detection system which can be installed into any type of custom casing or discreet enclosure for clandestine operation.

It is a sensor based bomb detector used by police, EOD teams and counter terrorist forces who deal with terror attacks by suicide bombers and criminal terrorist groups. Concealed person borne IED

threats and other weapons are also detectable in range of the RDS500 sensor technology. The RDS500 main operating principle is it's ability to remotely and safely scan people in range, enabling the operator to discriminate between a person carrying metallic objects such as shrapnel and who is not. It may also be operated in a remote manner and the graphic user interface can be hardwired or wireless, reducing the exposure of the operator to each person scanned.

The system can be placed covertly into discreet enclosure options or built into drywall, hallway wall board, pylon or bollard cones, other passive housings or overtly built into free-standing units and



powered by either AC or DC battery; the end user has the freedom to increase or decrease sensitivity based on their unique environment. HSS Development states they are ideal for any important entrance, be it an approach to an airport, the entry way of an embassy or consulate or even as basic as the doors to public theaters, stadiums for even shopping malls.

"Every week a criminal or terrorist sets off an explosion looking to maximize death and destruction. What if there was something you could do about it? Now there is. This is a terrorist trap to keep civilians, soft targets, armed forces and public and private institutions safe from suicide bombers, criminals and terrorists carrying bombs and concealed weapons looking to detonate in a crowded area or targeted building of importance, such as a consulate or embassy," states Joe Porter, VP of Counter Terrorist Solutions.

Blitz Raid in Tirana, 45 Kg of Explosives Seized

http://www.albaniannews.com/index.php?idm=11261&mod=2

Albanian Daily News

Albanian Daily News

Published February 16, 2017

A successful raid coded "The Power", conducted on Thursday by Tirana police officers, led to the sequestration of 45 kg of explosives and other military materials.

Ylli Done, 38, was arrested in flagrance while in possession of the explosives quantity. His arrest was carried on by disguised police officers close to a shopping center situated in Tirana suburbs.

45 kg of explosives, 5 pieces of plastic explosive (C4), 5 boxes with aluminum detonators, 10 defensive grenades, 720 bullets, 10 grenades igniters, a plastic bag filled with homemade explosive powder and a mobile were seized in quality of material proofs.

Police opened an inquiry aiming to identify the origin and destination of the explosive and military materials sequestrated during this blitz raid.

Discern® HME Detection Kit

Source: http://www.homelanddefsec.com/discerne/

The NEW **Discern® HME Detection Kit** from Serim Research rapidly identifies multiple compounds commonly used in homemade explosives with a simple point of use testing system. This detection kit combines the simplicity of a single test with a sophisticated colorimetric detection process that easily distinguishes between various fertilizer compounds, Peroxide, Chlorate, or Perchlorate based HME's. Mixing, spraying and using hazardous liquids commonly required for other chemistry kit detection systems are not necessary with this unique system. The Discern HME Detection Kit can be easily used by all EOD and First

Responders without the need for specialized training.

- **No hazardous/corrosive liquids**
- **Safer handling** through desensitized samples
- Use with **solid** or **liquid** samples
- **18-month shelf life**
- **Cost effective**
- **Portable**, single-use and bulk kits available

The Discern HME detection kit provides a quick and convenient test method that detects and distinguishes between various Nitrate fertilizers, Chlorate, Perchlorate, and Peroxide based HME's (Home-made Explosives). The test device is based on Serim's colorimetric test strip technology, widely applied in industrial, medical and scientific fields to detect any number of substances.

5 of the most powerful non-nuclear explosives ever

Source: http://www.businessinsider.com/most-powerful-explosives-2017-2

A chemistry department at a British university was recently evacuated after a student made the known explosive, TATP.

The chemical, tri-cyclic acetone peroxide, or TATP, was made by accident as the product of a chemistry experiment. But although the TATP in question came as an unwelcome surprise – the Ministry of Defence was forced to carry out a controlled disposal – there are many labs around the world which do design and make explosives for interest and application. Here are five of these non-nuclear chemicals which all explode via the rapid release of gas.

TNT

One of the most commonly known explosive chemicals is trinitrotoluene, or TNT, which has featured extensively in video games and films. It is often mistaken as dynamite, perhaps fueled by examples of confusion in popular culture, such as AC/DC's song TNT with lyrics such as "I'm TNT. I'm dynamite".

TNT is a yellow solid and was first produced as a dye in 1863. It doesn't explode spontaneously and is very easy and convenient to handle, so its explosive properties were only discovered some 30 years later by German chemist Carl Häussermann in 1891.

TNT can even be melted and poured into vessels without so much as a flicker of excitement but it will explode with the help of a detonator – and with a great deal of force, since the nitro groups in the molecule rapidly turn into nitrogen gas. This makes it ideal for use in controlled demolitions, where the explosive can be planted and detonated when planned (for example by miners), making it a relatively "safe" explosive. It's also used as a "standard measure" for bombs, so the "explosiveness" of other chemicals is often measured relative to TNT.

TATP

The chemical TATP belongs to a group of molecules named peroxides, which contain weak and unstable oxygen-oxygen bonds, and that are not found in TNT. This means that TATP is a lot less stable and more prone to

spontaneously exploding.

TATP Spatula Tzar/commonswiki

TATP is also known as the "mother of Satan" and with good reason – its explosions are known to be about 80% as strong as TNT, but the substance is much harder to handle. A firm shock or knock is enough to trigger an explosion, which means it's quite easy to accidentally blow yourself up in the process of making it – and good reason to evacuate your chemistry department if it is accidentally made.

TATP has also received a lot of media attention because it is easy to make and has been regularly used in improvised explosive devices (IEDs) associated with terror attacks such as the London 7/7 bombings in 2005.

RDX

RDX is a "nitrogen explosive", meaning that its explosive properties are due to the presence of many nitrogen-nitrogen bonds, rather than oxygen. These bonds are extremely unstable, since nitrogen atoms always want to come together to produce nitrogen gas because the triple bond in nitrogen gas. And the more nitrogen-nitrogen bonds a molecules has, like RDX, typically the more explosive it is.

Since TNT doesn't contain any unstable nitrogen-nitrogen bonds, RDX packs more power – but it is often mixed with other chemicals to produce different effects, such as making it less sensitive and less likely to explode unexpectedly. It is also commonly used in controlled demolition of buildings.

PETN

One of the most powerful explosive chemicals known to us is PETN, which contains nitro groups which are similar to that in TNT and the nitroglycerin in dynamite. But the presence of more of these nitro groups means it explodes with more power. However, despite its powerful explosions, it's quite difficult to get this chemical to detonate alone, and so it is usually used in combination with TNT or RDX.

PETN was used regularly in World War II, to create exploding-bridgewire detonators that use electric currents for detonation. It is now also used in the exploding-bridgewire detonators in nuclear weapons.

Its relatively low toxicity and medicinal properties as a vasodilator (it can widen blood vessels) also mean that it is used to treat angina – but don't worry, you won't explode.

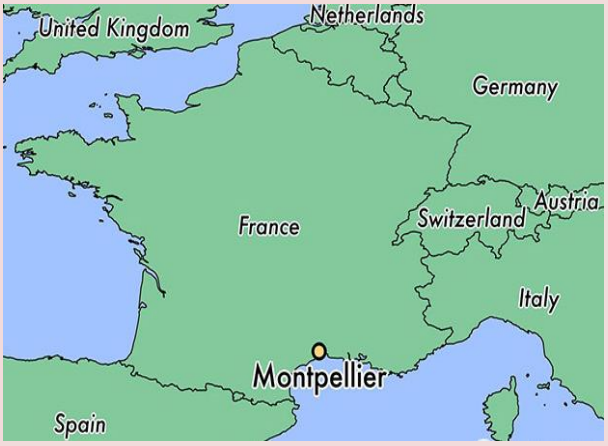
Aziroazide azide

Among the least stable nitrogen-explosives is aziroazide azide which has 14 nitrogen atoms, with most of them bonded to each other in successive, unstable nitrogen-nitrogen bonds – making them prone to explosion. You would never see these kinds of

molecules in nature due to their incredible instability, but they were made in a German research lab by Thomas Klapötke's group as recently as 2011.
Many explosives have been designed for military and other specific uses. Shutterstock
Attempts to touch or handle this chemical (and some may say so much as even look at) can cause it to detonate, breaking those bonds and turning them into multiple molecules of rapidly expanding nitrogen gas. The reaction creates a huge amount of heat and so only tiny amounts of this chemical have ever been synthesized for testing – which have blown up inside expensive pieces of analysis equipment on many occasions. You'd have to be pretty crazy to create large amounts and explains why it hasn't yet found any use.
This list is by no means comprehensive – there are plenty of other explosive chemicals at the disposal of chemists and industrialists. But these are among the most famous and dangerous non-nuclear chemicals to date. You'll be glad to know that many of them would be more difficult to make by accident than TATP – and we can usually predict and avoid the reactions that can produce them.

Bomb plot foiled in Montpellier

Source: http://www.bbc.co.uk/news/world-europe-38930201



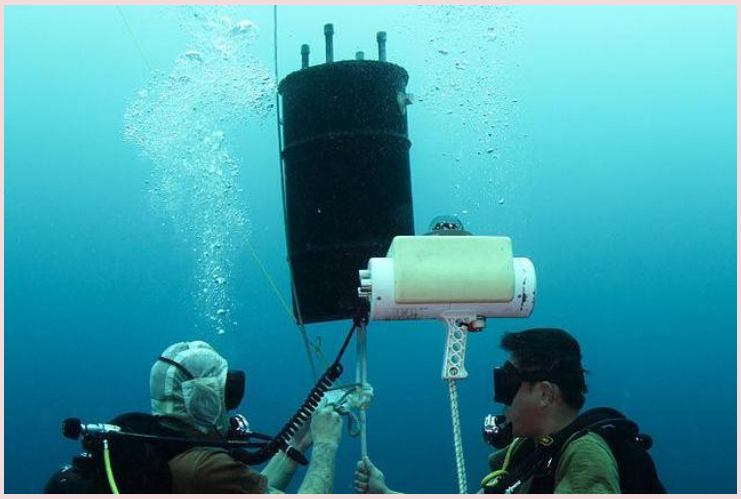
Feb 10 – **Three men and a girl of 16 have been arrested with bomb making materials by anti terrorist police in the southern French city of Montpellier.**
Home made explosives similar to those used in the Paris attacks of November 2015 were discovered, police and judicial sources said.
Reports suggest the girl had made jihadist declarations online.
Since the beginning of 2015, at least 230 people have been killed in jihadist attacks in France.
Last month, a soldier received minor injuries when a machete wielding man tried to enter the Louvre museum in Paris. The man, a 29 yearold Egyptian named as Abdullah Hamamy, was shot and critically injured.
Early reports suggested that one of the Montpellier detainees was a **wouldbe suicide attacker.**
The four arrested are suspected of plotting an imminent attack, Reuters news agency quoted the interior ministry as saying.
A local news site, M6 Info, said they were **planning to attack a tourist site in Paris**. They were arrested after buying acetone, a police source told AFP news agency. Acetone is an ingredient used in the making of triacetone triperoxide ,a high explosive. **TATP, the same explosive used in bomb vests worn by militants in the Paris attacks, was found in the city along with the acetone,** a judicial source said.
According to AFP, the female suspect had been spotted on social networks saying she wanted to leave for the SyriaIraq conflict zone or mount an attack in France instead.
She recorded a video in which she pledged allegiance to so-called Islamic State , M6 Info reports. Meanwhile, the countrys top constitutional court struck down a law which penalised those who consult jihadist websites.
The Constitutional Council found that the law infringed on peoples freedom of communication unnecessarily.

Robotic System Developed for Use in Underwater EOD Disposal

Source: http://i-hls.com/2017/02/robotic-system-developed-use-underwater-eod-disposal/

Feb 10 – RE2 Robotics, a developer of robotic manipulator arms, has received a Phase II Small Business Innovation Research (SBIR) award to develop an inflatable Underwater Dual Manipulator system for the US Navy's Office of Naval Research (ONR).

Explosive Ordnance Disposal (EOD) divers are often placed in harm's way while performing underwater location and identification of Improvised Explosive Devices (IEDs) on vessels, bridges, and underwater structures such as piers. The integration of a cost-effective and reliable manipulation system onto an Unmanned Underwater Vehicle (UUV) promises to bring the stand-off capabilities that robotic systems have brought to EOD technicians operating on land to those operating underwater.



According to the company's statement on its website, during Phase I, RE2 engineers designed an inflatable underwater dual manipulation system. This development effort produced a novel design concept for underwater dexterous manipulation that is light-weight, low-cost, and easily deployable in the field as a payload for UUVs. A prototype will be developed and tested during Phase II. Ultimately, the manipulator arms will be used as a collaborative robotic system to assist EOD divers in dismantling IEDs and other hazards.

"Developing robotic technologies that keep individuals out of harm's way is paramount to the mission of RE2 Robotics," stated Jorgen Pedersen, president and CEO of RE2. "Historically, we have developed manipulation systems for EOD ground robots. Over the past year, we have worked closely with the Navy to transition our expertise to underwater systems. By extending our manipulation capabilities into the submersible space, we are able to enter new markets, such as Offshore Oil and Gas, which rely on the safe inspection, maintenance and repair of underwater structures."

CDC Releases Blast Injury Mobile Application NEW

The Centers for Disease Control and Prevention (CDC) recently announced the release of a new Blast Injury mobile application to assist in the response and clinical management of injuries resulting from terrorist bombings and other mass casualty explosive events. The application provides clear, concise, up-to-date medical and healthcare systems information to assist healthcare providers and public health professionals in the preparation, response, and management of injuries resulting from terrorist bombing events.

Download the mobile application for free for your smart phone by searching for 'CDC Blast Injury.'

Read also: **Bombings: Injury Patterns and Care Pocket Guide** - free pocket guide available for download. This guide can be printed on 8 1/2" x 14" paper.

Manchester City 'to install anti-shatter glass' at the Etihad in bid to make ground bombproof

Source: http://www.mirror.co.uk/sport/football/news/manchester-city-install-anti-shatter-9838178

Feb 17 – **Manchester City are installing anti-shatter glass at the Etihad in an effort to strengthen their defence against a potential terrorist attack.**

The 55,000-seat stadium will have anti-shatter film wrapped around glass panes at the main entrance as they look to boost security.

They have also banned driving directly around the stadium, report the Mail , as the Premier League side looks to minimise the threat of an attack.

This comes after local rivals United increased security at the start of the season following a letter that the Premier League sent to all their clubs advising them to be extra vigilant.

A bomb attack outside Besiktas' stadium killed 44 people in December, while the Stade de France was targeted in the Paris attacks of 2015.

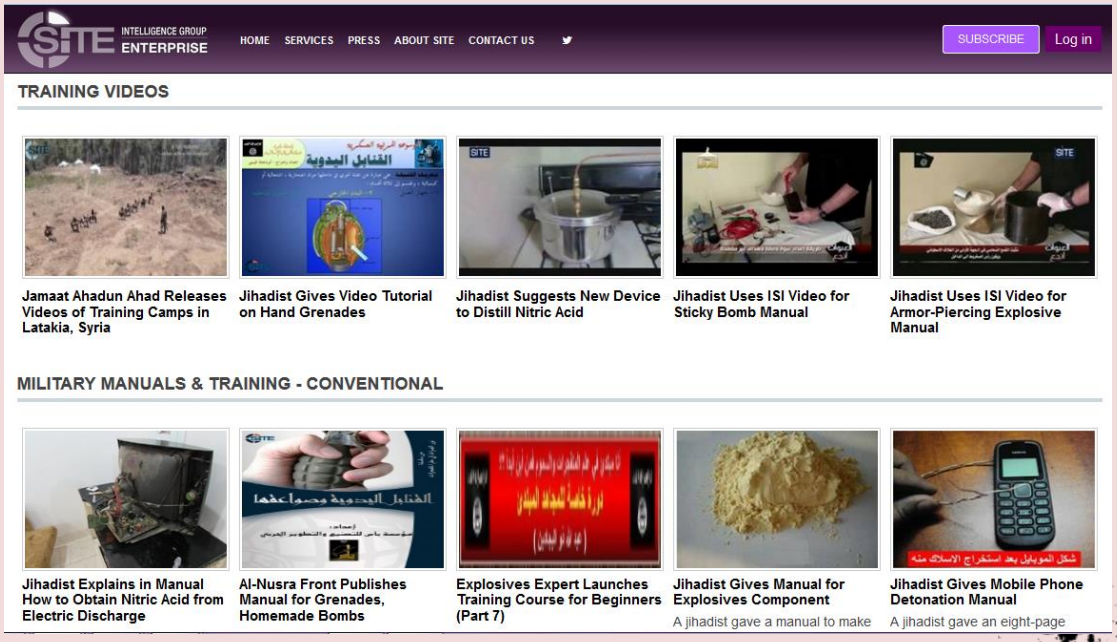
Football stadiums are though to be particularly attractive targets to terrorists owing to the huge crowds that flock to games.

United installed similar anti-shatter glass at Old Trafford in January and were also the first Premier League side to employ a counter-terrorism officer.

On matchdays all cars in club car parks are searched for bombs and every staff member is frisked when they enter the stadium.

A must visit website

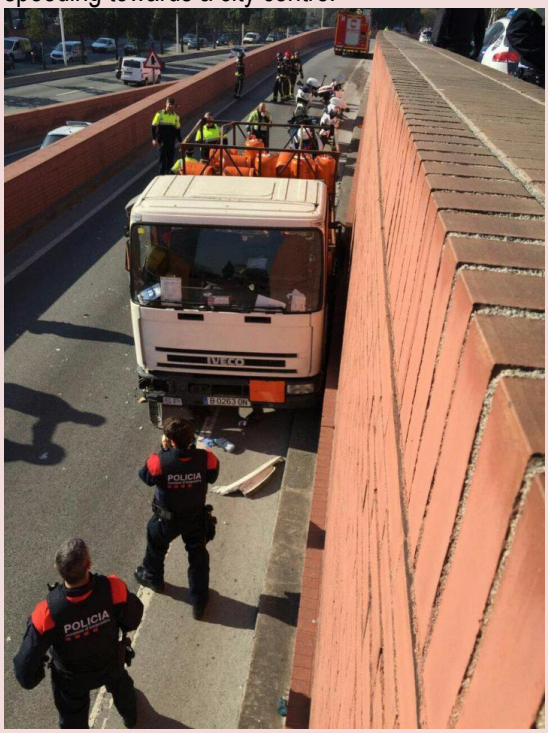
Source: https://ent.siteintelgroup.com/Table/Military-Manuals-and-Training/Conventional/Page-8.html



Barcelona cops 'shoot at and arrest truck driver in vehicle packed with gas cylinders speeding towards city centre'

Source: https://www.thesun.co.uk/news/2915325/barcelona-truck-shooting-butane/

Feb 21 – BARCELONA cops have shot at the driver of a truck reportedly packed with gas cylinders and speeding towards a city centre.

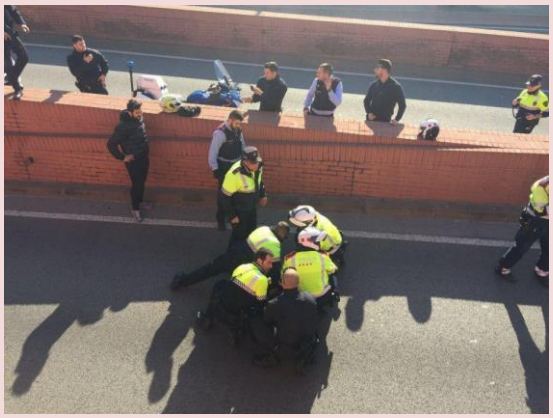


The butane carrying truck reportedly rammed several cars as it sped towards the city.

It is believed that no one was injured in the shooting and the driver, whose motivations are unknown, has been arrested.

A passer-by is reported to have been injured by a butane bottle falling from the truck, reports lavanguardia.

Local media elperiodico reported that the truck was



stolen from a shipyard and driven the wrong way down a road, ramming several vehicles before it was pulled over by police.

Details of the shooting on a busy route into the city are being shared by local journalists through social media.

Lavanguardia says an officer shot at the vehicle's rear window, causing it to stop.

On Twitter journalist Juan Antonio Tirado said: "A detainee for stealing a butane truck and driving against the Barcelona round."

El Espanol reported that the driver is Swedish and said police believe he may be suffering from mental health problems.

Lavanguardia cites sources who claim the driver could have acted under the influence of "psychotropic drugs".

Several local news outlets including Lavanguardia and elperiodico report that the man arrested is 33-year-old Joakim Robin Berggren, a Swedish citizen.

Pictures from the scene show a stationary truck loaded with gas cylinders at the side of a road surrounded by police.

Some media outlets have reported that the driver was killed, but police have said this is not the case.

Get ready for the cyber war in 2017: know your enemy

Source: http://www.information-age.com/get-ready-cyber-war-123464202/

Feb 02 – The current state of the cyber security industry is troubling to say the least, with 2016 experiencing a greater number of successful, more vicious cyber attacks than ever before.

The past few months have summed up the current state of the cyber security industry.

In a matter of days at the end of November the European Commission was brought offline by a distributed denial-of-service (DDoS) attack, San Francisco's Municipal Railway was held to ransom by ransomware in a system-wide attack and it was revealed that in September the Japanese Defence Ministry and Self-Defence Forces were hacked, which may have compromised Japan's internal military network.

It seems almost farcical, and from these recent examples it is evident that critical infrastructure is totally unprepared for an attack and will continue to be severely vulnerable at the beginning of 2017.

It is not just the public sector that is suffering, with private organisations facing daily hacking attacks despite serious investment in cyber security strategies.

The problem is inherently twofold. The first is that cyber criminals and their tactics are constantly evolving, becoming more overwhelming and hard to detect by the day, it seems.

The ferocity of cyber attacks was illustrated last year by the Mirai botnet n(or Dyn) attacks that overran a number of systems using corrupted Internet of Things (IoT) devices.

When the malicious code was first published online in October, it gave a suspected group of teenagers the ability to shut down the likes of Twitter and Spotify.

In the preceding month, Liberia's internet was taken offline using the same code. Improving the security of IoT devices will be crucial during 2017. This is where the most devastating cyber attacks will originate.

The second problem lies in the boardroom. Whether it is a result of attitude or ignorance, cyber security has not, until recently, been given the priority it warrants.

Cyber security is not an IT issue, it is a business-critical issue. The C-suite is starting to take note, however, and must begin preparing – if they are not doing so already – advanced prevention, detection and response systems.

This will be all the more crucial once the European General Data Protection Regulation (EU GDPR) comes into effect in May 2018. After this date, not only will reputation be on the line, but so will an organisation's financial stability.

'The nuts and bolts of cyber security are either still not understood or, in most cases, simply ignored by many boardrooms,' confirms Jacob Ginsberg, senior director at Echoworx.

'The clear majority of enterprises remain completely reactive to cyber security, waiting until their reputation is in question or legislation forces them to act. Boards are run by committees, and security still doesn't have a chair at the table – until it does, security will never get the attention it warrants.'

Looking ahead to the 2017 cyber security predictions, it could get tumultuous to say the least. There is no doubt that the issue of cyber security was thrust into the public spotlight last year, which was highlighted throughout the controversial US presidential election campaign and the high-profile hacks of Yahoo! and LinkedIn.

The point is, in 2017 cyber attacks will continue to dominate headlines, and any proof of state-sponsored hacking could be, as BeyondTrust (an information security software company) suggests, acknowledged as an act of war. The age of cyber warfare could begin, where hacking techniques are regarded in the same breath as heavy weaponry.

This is not an exaggeration, and is why the White House's Commission on Enhancing National Cybersecurity ordered a nine-month, 100-page study of America's cyber security problems, which was published last December.

Escalating threats

'The sky's the limit,' says Mike Ahmadi, global director – critical systems security at Synopsys. 'Accessing a water treatment plant and diverting sewage to municipal water systems can cause disease and death. Shutting down all power during a heat wave can cause death. Hacking combat

drones can create devastating weapons. Let your imagination run wild here.'

Nathan Dornbrook, CTO at IT consultancy ECS, shares this cyber warfare prediction and suggests that 'there will be a sharp increase in politically motivated and protest cyber crime, driven by increasing social inequality, the rise of far-right populism, Brexit, US-China-Taiwan relations and looming changes in international trade relationships'.

Cyber war may be the most extreme 2017 prediction in this feature, but it's not beyond the realms of possibility. Moving on, what are the other, less apocalyptic, 2017 cyber security trends that we can expect?

Securing the Internet of Things

First and foremost, the Internet of Things must be secured. If Gartner is to be believed, there will be 20 billion connected devices by 2020, but 'the current playbook for IoT development is still immature', suggests Paul Curran, content specialist for Checkmarx.

Curran tells Information Age there is not enough attention being paid to securing IoT devices, and this is certainly evident from the already mentioned spate of DDoS attacks that originated from insecure IoT devices towards the end of 2016.

'There is a palpable fear that a major category of IoT products embedded within a life-critical application such as health, CNI or automotive is vulnerable to a major attack through negligence in software security,' notes Curran.

An enhancing of IoT security will therefore be a top trend during 2017. At the moment, the factory-grade security setting is not sufficient. This increased level of protection should be implemented within industry groups and by regulatory framework, similar to the GDPR but for IoT devices.

'Organisations, and especially device vendors, need to plan for this change and start considering how to build a secure software development cycle,' says Curran.'

The threat to the cloud

The number of organisations using the cloud – in all its forms – has surged over the past five years, and this adoption will continue to increase into 2017 as businesses look to make the best use of big data, or the 'data revolution'.

Inevitably, this will come under threat. 'There will be continued growth in cloud breaches,' says Ian Kilpatrick, chairman of security specialist Wick Hill Group and EVP cyber security for Nuvias Group. 'It's an attack vector that contains significant vulnerabilities around identity management and mobility or off-site access.'

Indeed, there has been a sharp rise in the number of cyber attacks going through cloud service providers. Consequently, Kilpatrick suggests, 'Cloud access security broking will experience significant growth, and there will be more interest in identity- as-a-service (IDaaS).'

Gartner's prediction that 40% of identity and access management (IAM) purchases will use the IDaaS delivery model by 2020 (up from just 20% in 2016) confirms this.

The rise and evolution of ransomware

In December last year, a new kind of ransomware began targeting individuals. This latest malicious code was called Popcorn Time and it offered its victims a free decryption key (unlocking their device), as long as the person targeted spread it to others and those victims pay the standard one bitcoin ransom.

This is unlikely to affect large organisations, although certainly employees will be at risk, but it demonstrates the constantly evolving and sinister nature of the cyber threat. Ransomworm is the suspected next evolutionary state of ransomware moving into 2017. It will move from 'a company's one-time issue to a network infiltration problem', says Nir Polak, CEO of Exabeam. These ransomworms will guarantee repeat business for the cybercriminals.

'They not only encrypt your files until you pay up, they leave behind a little present to make sure that their malicious ways live on,' warns Polak.

'Microsoft,' he goes on, 'warned of a ransomworm earlier this year called ZCryptor that propagated onto removable drives.' By placing a little code on every USB drive, a company's employees would bring more than their presentations to meetings. Expect to see nmore of this in 2017.

Other 2017 trends

There is, of course, a plethora of cyber security trends that are expected or will be uncovered in 2017. It is difficult to identify the most significant threat, and indeed prevention tools,

simply because there are so many.
The death of the password may be a feature that dominates this year, as its insecurity has taken centre stage for a number of high-profile data breaches, such as Yahoo! and FriendFinder Networks.
This, in turn, will give rise to an increase in advanced biometric software that will protect devices, individuals and organisations from cybercriminals. Going further, as BeyondTrust suggests, adaptive and behaviour-based authentication will grow in importance.
Mobility, cloud deployments and increased regulation will drive innovation in identity verification.
Finally, it is evident that known vulnerabilities will continue to be exploited in 2017. The security threat born from BYOD will remain prevalent, as will phishing scams that target those who are ignorant to the security threat.

Education is key

Boardroom strategy will have to change during 2017. This should take the shape of actually coming up with a strategy and making cyber security a boardroom priority.
As part of this revised strategy, employee education should be high on the agenda. This will entail making the workforce aware of the threats, how to avoid them and what to do in the likely event that a breach does occur.
Ultimately, breaches will occur in 2017 just as regularly as they did in 2016. In order to mitigate the damage caused, the boardroom strategy needs to change with an investment in new, combative philosophies and technologies.

A new hope?

Artificial intelligence (AI) offers a chance for organisations to fight back. Not only will AI be able to automatically detect a cyber breach, but it will also be able to heal the attack almost immediately.
Unfortunately, this capability is not yet available to organisations, but John Bruce, CEO of Resilient, says that it is not far off: 'This is the future of cyber security, and it's not a million miles out. We're not talking about this coming in the distant future; it is a conceivable time frame. You can expect to see some exciting developments in the foreseeable future.'
Of course, as Alex Mathews, lead security evangelist at Positive Technologies, points out, the bad guys can also use AI to their advantage. This can take the form of smart malware, which can 'analyse the environment when it lands on a network to determine if it's in a sandbox or honeypot, and then conceal its true intentions or delay its actual behaviour to evade detection'.
Dave Palmer, director of technology at Darktrace, also refers to 'polymorphic malware, which changes its attributes mid-attack to evade detection'. This, he suggests, 'has reinforced the obsoleteness of signature-based detection methods'. In the wrong hands it is evident that this technology has severe implications.
However, AI used in the right way, in a form of behaviour analyses, can help restore some form of balance to the cyber battleground. 'Instead of old-fashioned signature analysis, which is actually useless against unknown malware and zero-day attacks,' suggests Mathews, 'we'll see the rise of smart security apps that analyse the behaviour of a protected system by building statistical models of normal working processes (machine learning) and looking for anomalies.' This form of protection will become increasingly popular in 2017.

A heterodox conclusion on intelligence failures in the age of cyberwarfare

Source: https://warontherocks.com/2017/01/a-heterodox-conclusion-on-intelligence-failures-in-the-age-of-cyberwarfare/

Feb 02 – **Former CIA acting director Michael Morell defined the Russian hacking attack of the Democratic National Committee as "the political equivalent of 9/11."** The event constitutes a classic example of a warning failure. Such failures, as attested to by the rich literature on Pearl Harbor, Barbarossa, the Korean War, the 1973 Arab-Israeli War, and the 9/11 terrorist attacks, are not the product of insufficient information about the looming threat. Rather, they are the result of mistaken interpretation of available information. *The New York Times* investigation of the Russian intervention concluded that the American response to the

attack was shaped by "a series of missed signals, slow responses and a continuing underestimation of the seriousness of the cyberattack." This conclusion fits very well with the classic causes of major warning failures of the past. While the means of surprise attacks has shifted from airplanes and tanks to email accounts and computer networks, the dynamics between the initiator of the attack and its victim have remained very much the same.

Information about the Russian hacking is still relatively scant, but we know enough to hazard some initial observations and one main conclusion.

The first observation involves the identity of the enemy. In the era of conventional warfare, intelligence agencies were tasked with answering concerning the "if," "how," "where," and "when" of the attack — but the potential attacker's identity was known. However, while much has been written about the difficulties involved in attributing specific attacks to specific states in the age of cyberwarfare, this was not a problem in the present case. By September 2015, the FBI already knew that the Russian cyberespionage group known as "the Dukes" was hacking the computers of the Democratic National Committee, and the record of "the Dukes" as a tool of the Federal Security Service (FSB) was in the public domain.

This raises the issue of how Moscow viewed risk and the effectiveness of such an attack. The Russians have a long tradition of psychological warfare — "active measures" in the KGB terminology. Under Putin, they turned "information warfare" into a dominant component of their "new generation warfare." We might have expected Russian policymakers, including Putin, an experienced KGB officer, to be more concerned about keeping its responsibility in the dark. Yet, Putin approved the operation despite knowing that the gun had been "smoking" for a long time, so he was very likely to be caught red-handed. A fear of American retaliation apparently did not play a significant role in the Kremlin's strategic calculations. This attitude is different from the more risk-averse tendency of the Soviets during the Cold War. The KGB, just like the CIA, used various means of subversion to influence the political processes in third world countries as well as in Western Europe. However its disinformation campaigns in the United States were largely limited to smearing the CIA and the FBI or flaming conspiracy theories about the Kennedy assassination. The KGB had never interfered with the presidential elections.

When the hacking started in July 2015, no one could have predicted that the American public response to a Russian intervention in the presidential elections would be so feeble. But the American response to the attack clearly resembles past responses to warnings of an incoming attack. Specifically, three well-known common factors can already be identified.

First, standard operating procedures allow organizations to function effectively under routine situations, but may be disastrous at times of emergency. This was evident in 1941 when standard compartmentation procedures led to the information about a possible Japanese attack arriving in Pearl Harbor partial and unprioritized. Close to 75 years later, the FBI acted according to its own stand operating procedures in repeatedly sending routine warnings to the relevant official in the Democratic National Committee without even trying to meet and alert him personally. We do not know yet when the intelligence community started to realize the scope of the threat, but we do know that it did not bubble up to the top until far too late in the game. Situation Room meetings started only in July 2016, and intelligence assessments of the Russian role in the attack "took forever," according to one unnamed senior administration official.

Second, much as with Pearl Harbor and 9/11, intelligence analysts did not imagine that the enemy would strike in the way it did. In 1941, Japanese attack on Pearl Harbor was considered impossible. In 2001, the destruction of the symbols of American might by passenger planes was unimaginable to most. Similarly, despite what Western intelligence agencies observed of Russian information warfare in Estonia, Georgia, and the Ukraine, David Sanger claims "American officials did not imagine that the Russians would dare try those techniques inside the United States." The result was the underestimation of two threats: that Russia would leak the information it hacked in order to disrupt the electoral process and that the documents would be used to effectively attack Clinton's candidacy.

Third, President Obama's low-key response to the threat, which deterrence theory would suggest incentivized more Russian aggressiveness, resembles both the Munich crisis of 1938 and Stalin's thinking on the eve of the German attack on the Soviet Union in June 1941. Both cases were dominated by fear of escalation. In 1938, Chamberlain and Daladier accepted Hitler's territorial demands in Czechoslovakia in exchange for "peace in our time." In 1941, caught in his own distorted logic, Stalin refrained from taking defensive measures that could have triggered a German attack. Obama's refusal to publicly accuse the Russians for interfering with the American democratic process before the elections was largely motivated by fear of Russian retaliation. Some officials were concerned over escalation into a larger cyber-conflict, while others worried a U.S. response would compromise diplomatic efforts over Syria. Still others thought that an official attribution to Russia would only feed Donald Trump's narrative of a "rigged" election.

We may never know whether Obama made the right decision. The administration ultimately decided on a delayed half-measure: a warning delivered to the Kremlin a week before the election over the so-called "red phone" meant for nuclear crises. Administration officials claimed Obama's warning to Putin included a remark that the "law of armed conflict" applied to cyberspace and that Russia would be held to that standard. This warning might have prevented Russian interference on election day itself, but does not seem to have accomplished anything else. If there is a single important lesson to be drawn from comparing past warning failures to the present one, it involves intelligence collection.

The common wisdom at the age of cyberwarfare is that "Stuxnet worms," "Trojan horses," and "firewalls" are the weapons by which the next war will be won.

Given these assumptions, the actual lessons that history has to teach may be counterintuitive. They would show that while the United States had always relied on strategic warning obtained through technical means of collection, this form of intelligence-gathering was repeatedly revealed as futile. In 1941, the breaking of the Japanese diplomatic code ("Magic"), which allowed American intelligence to read Japanese diplomatic cables, gave no indication that Japan's target would be Pearl Harbor. The Japanese were aware that no code was uncrackable and thus kept all mention of Pearl Harbor outside their diplomatic traffic. Their fleet sailed to Hawaii under complete radio silence. Similarly, in fall 1950, U.S. signals intelligence assets and aerial photography failed to locate a 260,000-soldier Chinese army in Korea. The Chinese lacked radio equipment and moved into the battlefield at night using side roads. In October 1962, the United States was surprised by the positioning of Soviet attack missiles in Cuba. The surprise resulted partly from the fact that the ships that carried them took strict deception measures. In August 1990, U.S. spy satellites could observe every Iraqi tank on the borders of Kuwait. Nevertheless, the United States was surprised when they moved in. And prior to 9/11, the monitoring of warning indicators by sophisticated means of surveillance did not suffice to generate to the necessary action that would save America from the greatest terrorist attack in history.

At the same time, history also shows that human intelligence, the oldest form of espionage, provided the best warnings. The Soviet Union received numerous warnings from its spy networks all over the world that Germany planned to attack in June 1941. It sufficed to convince the Red Army generals, but not Stalin, who preferred to trust Hitler rather than his spies. A few months later, he did better. He was informed that Japan would not attack Siberia by his agents in Japan: Richard Sorge, who was the German ambassador's confidant in Tokyo, and Hotsumi Ozaki, who worked as an advisor the Japanese prime minister. On the basis of this information, he rushed the Siberian divisions to the west and was able to win the Battle for Moscow. In 1962, Col. Oleg Penkovsky of Soviet Military Intelligence provided the CIA with the information that ultimately allowed the United States to identify the nuclear missiles in Cuba. This was more proof that a single spy can be more valuable than a massive technical surveillance apparatus. And in 1973, only a last-minute warning from Ashraf Marwan, the most valuable spy Israel had ever had, saved the country from being completely surprised by sudden Arab attack and prevented the fall of the entire Golan Heights to Syria.

This short history does not aim to discredit value of collection by technological means. But in this sphere, the opponent is usually

aware of the fact that its secrets might be compromised and can act accordingly. The British code-breaking of the German strategic code in World War II ("Ultra") was a major achievement that helped the allies to win the war. But when the German navy added a fourth rotor to its Enigma cypher machine, the British failed to read its traffic for ten months, a failure that "threatened disaster" to the allies' chance to win the battle for the Atlantic. Today's technology changes far faster, and in the ongoing race between offensive and defensive cyber-espionage, any offensive advantage is likely to be short-lived. This is not true in the realm of human spies, where no counter-measures can assure capture.

The American intelligence community is known for its outstanding technical collection capabilities, but remains far weaker in human intelligence. It had no valuable spy in Tokyo in 1941, in Moscow and Beijing in 1950, in Baghdad in 1990, or in al Qaeda in 2001. Penkovsky, who played a crucial role in the 1962 crisis, was brought to the CIA by the British. **This sad record shows that despite being technologically superior to every other nation, the United States might be ill-equipped for war in the cyber age for the counterintuitive reason that its human intelligence capabilities are not robust enough.**

The rise of the age of cyber conflict does not obviate the imperative for well-placed human sources. Perhaps the United States should direct more of its efforts in that direction.

Worldwide Cyberattacks Caused Up to $1 Trillion Losses in 2016 - FSB

Source: https://sputniknews.com/military/201702021050265384-cyberattacks-losses-2016/

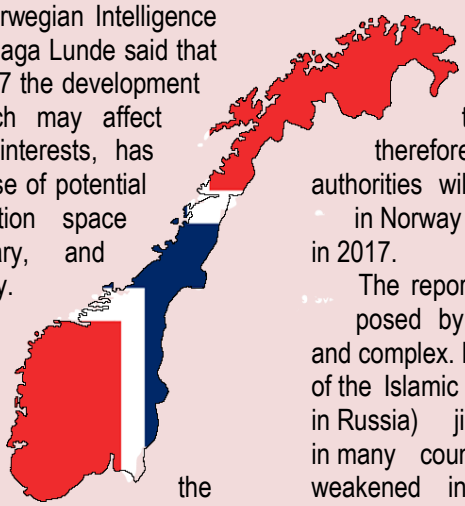
Feb 02 – FSB Center deputy chief Nikolai Murashov made the assessment at the "Inforforum" annual IT security event in Moscow.

"According to data for the last few years, on the basis of different assessment methods, the damage from malicious programs amounted from $300 billion to $1 trillion," Murashov said.

Cyberattacks, Terrorism May Pose Threat to Norway in 2017

Source: https://sputniknews.com/europe/201702061050396517-norway-threats-terrorism-cyber/

Feb 06 – Head of the Norwegian Intelligence Service, Lt. Gen. Morten Haga Lunde said that since the beginning of 2017 the development in three directions, which may affect Norway and Norwegian interests, has been noted, namely the rise of potential threats in the information space against political, military, and economic targets in Norway.



"Since the beginning of 2017 the development in three directions, which may affect Norway and Norwegian interests, has been noted, namely the rise of potential threats in the information space against political, military, and economic targets in Norway," the head of the Norwegian Intelligence Service, Lt. Gen. Morten Haga Lunde, said in the preface to the report, published on the official website of the Norwegian Armed Forces.

According to Lunde, "Russia has carried out large-scale digital operations in order to influence US election," therefore, it is possible that foreign authorities will have an impact on elections in Norway and in other countries of Europe in 2017.

The report stated that the terrorist threat, posed by Islamist militants, was serious and complex. Despite the fact that the positions of the Islamic State (ISIL or Daesh, outlawed in Russia) jihadist organization, banned in many countries including Russia, have weakened in Syria and Iraq, the threat of terrorist attacks in Europe still stands.

The report also highlighted the geopolitical contradictions between the West and Russia, saying that tensions have dramatically increased as a result of the conflicts in Ukraine and Syria, which may lead

to consequences that are undesirable for both sides.
Russia has repeatedly denied all allegations about any cyberattacks and influencing US presidential election, calling them absurd and characterizing them as an attempt to divert public opinion from revelations of corruption as well as other pressing domestic issues in the United States, and has stressed that Russia will never attack any NATO country.

How to Collect Open Source Intelligence

By Kim Miller
Source: http://www.hstoday.us/single-article/how-to-collect-open-source-intelligence/205468afb3e5fef4eed34854a76c99a3.html

Dec 2016 – Open source intelligence (OSINT) is information that comes from publicly available sources.

This type of information can be exploited, collected and disseminated to any audience.
For investigators or other individuals who need to collect background material on an individual, OSINT is highly useful. According to Michael Bazzell, a former FBI computer crime investigator and the author of several books on security, OSINT can be used to locate people or to conduct background checks or any online investigation.
Many names and addresses are publicly available online.
Websites such as **Spoke.com, Radaris.com and Intelius.com** allow users to search an individual's name and address for free. These sites allow investigators to more easily use the information found on these sites to conduct background checks on potential employees, but are also used by criminals to find information for identity theft.

Use of OSINT to track down criminals
Although OSINT has its hazards in regard to personal privacy, it can also have crime-fighting implications. For example, some Reddit users have asked others to help them solve theft problems. Victims sought help identifying phone numbers, license plate numbers or other information that could be used to track down thieves.

Dr. Kim Miller *is an adjunct professor of criminal justice in the School of Security and Global Studies at AMU. Her academic credentials include a B.S. in Criminal Justice and an M.S. in Criminal Justice from Kaplan University, as well as a Ph.D. in Public Safety-Criminal Justice from Capella University. She is also a Certified Fraud Examiner, a New Jersey Licensed Private Detective and an investigative analyst.*

Child from Pittsburgh admits to hack attempt of Brussels Airport after ISIS attacks

Source: http://www.homelandsecuritynewswire.com/dr20170209-child-from-pittsburgh-admits-to-hack-attempt-of-brussels-airport-after-isis-attacks

Feb 09 – A Pittsburgh child has admitted to launching a cyberattack against Brussels Airport in the aftermath of the 22 Mach 2016 suicide bombing by Belgian ISIS followers, which killed more than thirty people. The Belgian federal public prosecutor's office said the suspect aimed to take down the website of the airport operator – the Brussels Airport Company — and "infiltrate the computer system," but was unsuccessful.

Cyberattacks increase stress hormone levels, perceptions of vulnerability

Source: http://www.homelandsecuritynewswire.com/dr20170209-cyberattacks-increase-stress-hormone-levels-perceptions-of-vulnerability

Feb 09 – **A new study shows that individuals exposed to a simulated cyberterror attack had significantly increased levels of the stress hormone cortisol in their saliva compared to a control group.** Following the cyberattack, study participants were more likely to fear an imminent cyberthreat and to express feelings of personal insecurity, according to results published in *Cyberpsychology, Behavior, and Social Networking*.

Liebert Publishers says that ateam of Israeli researchers designed a study to investigate the psychological effects of cyber terror. The researchers examine the potential damaging effects of cyber terror, even though its victims suffer no direct bodily harm.

"Cyberattacks can increase both psychological and physiological stress in individuals. Teaching disaster preparedness for cyber events, as is done for real world events, may help mitigate some of this fear and anxiety," says Editor-in-Chief Brenda K. Wiederhold of the Interactive Media Institute in, San Diego and the Virtual Reality Medical Institute, Brussels, Belgium.

— Read more in Canetti Daphna et al., "How Cyberattacks Terrorize: Cortisol and Personal Insecurity Jump in the Wake of Cyberattacks," Cyberpsychology, Behavior, and Social Networking 20, no. 2 (January 2017): 72-77.

SPECIAL ANALYSIS: Cyber Ridicule - A New Weapon in the Global War on Terror?

Source: http://www.hstoday.us/single-article/special-analysis-cyber-ridicule-a-new-weapon-in-the-global-war-on-terror/753ad89bf8b47f2a68a42c4a6be131f0.html

Suicide Bomb At Market In Somali Capital Kills 39, Injures Around 50

Source: http://www.huffingtonpost.com/entry/suicide-bomb-at-market-in-somali-capital-kills-18-wounds-25_us_58a9a2a8e4b037d17d28cfe7

Feb 19 – **A car bomb ripped through a market in Mogadishu on Sunday, killing 39 people and injuring around 50,** a local official said, days after Somalia elected a new president.

The car was driven by a suicide bomber, said Ahmed Abdulle Afrax, the mayor of Wadajir district where the bombing happened.

"We carried 39 dead bodies and there were many others injured," Dr Abdikadir Abdirahman, director of the Aamin Ambulance Service, told Reuters.

Madina hospital took in 47 injured people, Dr Mohamed Yusuf, the manager, said.

Witness Abdulle Omar said the market was destroyed.

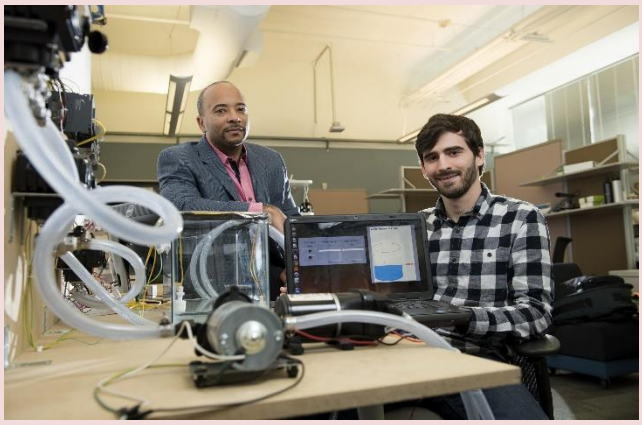
"I was staying in my shop when a car came in into the market and exploded. I saw more than 20 people lying on the ground. Most of them were dead," he said.

Al Shabaab, the Islamist insurgent group that is fighting the U.N.-backed Somali government, did not immediately claim responsibility.
Al Shabaab has been able to carry out increasingly deadly bombings despite losing most of its territory to African Union peacekeepers supporting the Somali government.
This month Somalia elected a new president, Mohamed Abdullahi Mohamed, a dual U.S.-Somali citizen and former prime minister.
Civil war has riven Somalia since 1991. Aid agencies warn that a severe drought has placed large swathes of the country at risk of famine.

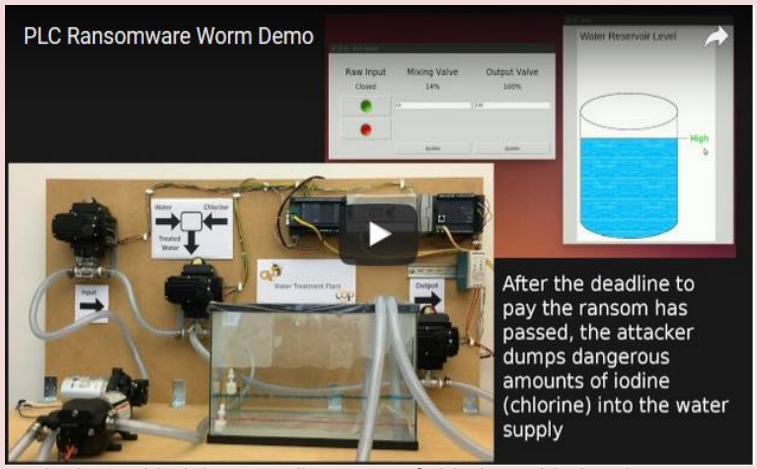
A simulation shows how a ransomware could hack PLCs in a water treatment plant

Source: http://securityaffairs.co/wordpress/56266/hacking/plcs-ransomware-attack.html

Feb 14 – The security researchers at the Georgia Institute of Technology have conducted an interesting research on the potential impact of ransomware on industrial control systems (ICS).
The researchers David Formby, a Ph.D. student in the Georgia Tech School of Electrical and Computer Engineering, and his faculty advisor, Raheem Beyah, have simulated a ransomware-based attack on a water treatment plant.



The team of researchers has developed a new strain of ransomware that was able to take over control of a simulated water treatment plant, then it allowed the attackers to command programmable logic controllers (PLCs) with serious consequences.
"The simulated attack was designed to highlight vulnerabilities in the control systems used to operate industrial facilities such as manufacturing plants, water *and wastewater treatment facilities, and building management systems for controlling escalators, elevators and HVAC systems. Believed to be the first to demonstrate ransomware compromise of real PLCs" reads the blog post published by the Georgia Tech.*
The experts have tested a number of commonly used programmable logic controllers (PLCs) trying to hack them.
The expert simulated a water treatment facility hosting the tested PLCs that also included pumps, tubes, and tanks.



Watch the vide at source's URL

The researchers simulated an attack on the PLCs, they interacted with valves and exploited the access to the logic controllers to display false information to the operator. As a result, they added the overall amount of chlorine added to the water.
"We were able to simulate a hacker who had gained access to this part of the system and is holding it hostage by threatening to dump large amounts of chlorine into the water unless the operator pays a ransom," Formby said. "In the right amount, chlorine disinfects the water and makes it safe to drink. But too much chlorine can create a bad reaction that would make the water unsafe."

The second phase of the research if the analysis of publicly exposed PLC that could open the doors to similar attacks. The security duo discovered 1,400 instances of a single PLC type exposed on the Internet and easily hackable. The experts highlighted the false sense of security of the organizations that are housing the control devices, they also explained that ransomware could represent a serious threat to every industry.

"But most such devices are located behind business systems that provide some level of protection – until they are compromised. Once attackers get into a business system, they could pivot to enter control systems if they are not properly walled off." Formby said.

"Many control systems assume that once you have access to the network, that you are authorized to make changes to the control systems," "They may have very weak password policies and security policies that could let intruders take control of pumps, valves and other key components of the industrial control system."

The extortion practice could look with increasing interest to compromise control systems.

"We are expecting ransomware to go one step farther, beyond the customer data to compromise the control systems themselves," said David Formby, a Ph.D. student in the Georgia Tech School of Electrical and Computer Engineering. "That could allow attackers to hold hostage critical systems such as water treatment plants and manufacturing facilities. Compromising the programmable logic controllers (PLCs) in these systems is a next logical step for these attackers."

Critical infrastructure is exposed to such category of malware as demonstrated by the researchers.

In April 2016, the Lansing Board of Water and Light (BWL) utility has had to shut down systems, phone lines in response to a ransomware-based attack.

Formby and Beyah have no doubts, profit-driven cybercriminals will target also poorly protected PLCs.cybercriminals will target also poorly protected PLCs.

Belgian Ministry of Home Affairs Incident & Crisis Management System

By Neil Cohen
Senior Consultant at Dynamis, Inc.
Source: http://dynamis.com/belgium-to-use-cobra-as-nationwide-crisis-management-system-in-2017/

Jan 26 – The Belgian Ministry of Home Affairs is developing a national crisis portal for emergency planning and crisis management called the **Incident & Crisis Management System (**ICMS**).**
Capable of supporting up to 4000 users from the local to the federal level, Belgian emergency services will use ICMS across the entire crisis cycle, from planning to exercises, incident management, and evaluation.
Dynamis' COBRA ™ software technology provides the possibility to make this a reality while offering the opportunity for further integrations with other applications, greatly improving critical interoperability in incident and crisis management. The excellent collaboration with the **Dynamis-CEMAC** team has provided comprehensive software life-cycle services, including standardization, development, hosting, testing, training, and support, and made it possible to deploy ICMS in the short development period of one year.
Thanks to ICMS using the COBRA-software, the Belgian authorities can collaborate for their missions in the field of safety and security, and have a common situational awareness which is critical during emergencies.

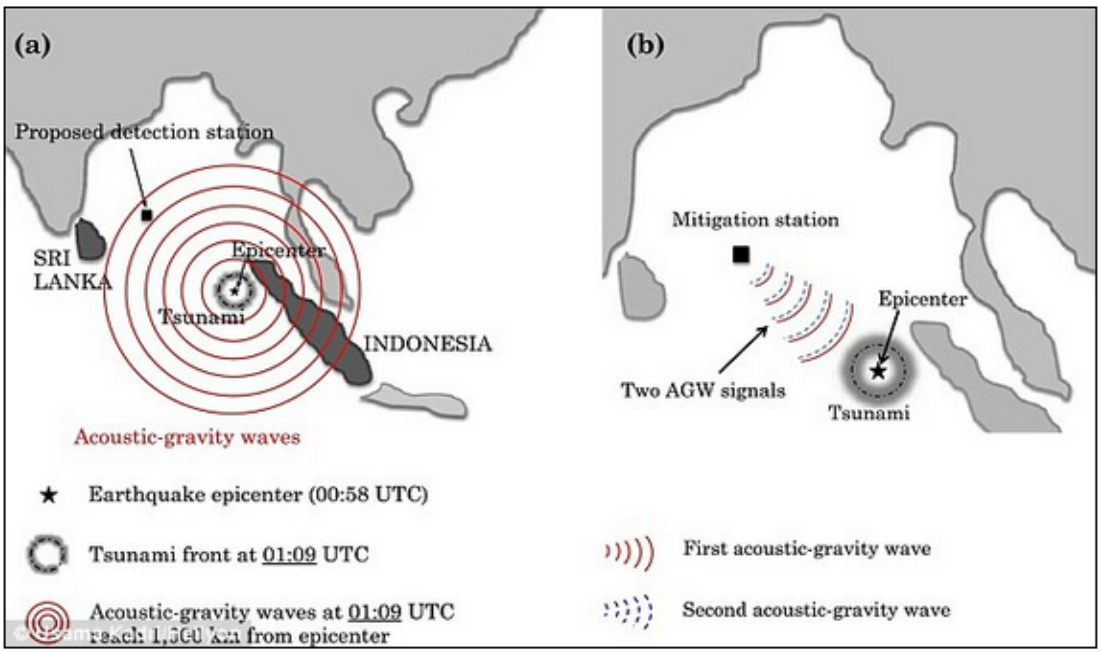
Sound-waves could prevent tsunamis from hitting shoreline

Source: http://www.homelandsecuritynewswire.com/dr20170127-soundwaves-could-prevent-tsunamis-from-hitting-shoreline

Jan 27 – **Devastating tsunamis could be halted before hitting the Earth's shoreline by firing deep-ocean sound waves at the oncoming mass of water, new research has proposed.**

Dr. Usama Kadri, from Cardiff University's School of Mathematics, believes that lives could ultimately be saved by using acoustic-gravity waves (AGWs) against tsunamis that are triggered by earthquakes, landslides and other violent geological events.
AGWs are naturally occurring sounds waves that move through the deep ocean at the speed of sound and can travel thousands of meters below the surface.

AGWs can measure tens or even hundreds of kilometers in length and it is thought that certain lifeforms such as plankton, that are unable to swim against a current, rely on the waves to aid their movement, enhancing their ability to find food.



The illustration (a) shows the tsunami and acoustic-gravity waves generated in the 2004 Indian Ocean earthquake, revealing how AGWs travel much faster to the proposed detection station. An Illustration of the proposed mitigation system is shown as well (b)

Cardiff University says that in a paper published today in the journal *Heliyon*, Dr. Kadri proposes that if we can find a way to engineer these waves, they can be fired at an incoming tsunami and will react with the wave in such a way that reduces its amplitude, or height, and causes its energy to be dissipated over a large area.

By the time the tsunami reaches the shoreline, Dr. Kadri writes, the reduced height of the tsunami would minimize the damage caused to both civilians and the environment.

Dr. Kadri also believes that this process of firing AGWs at a tsunami could be repeated continuously until the tsunami is completely dispersed.

"Within the last two decades, tsunamis have been responsible for the loss of almost half a million lives, widespread long-lasting destruction, profound environmental effects and global financial crisis," Dr. Kadri said.

The devastating tsunami that was generated in the Indian Ocean in 2004 after a magnitude 9 earthquake has been recorded as one of the deadliest natural disasters in recent history after it caused over 230,000 deaths in 14 countries.

The energy released on the Earth's surface by the earthquake and subsequent tsunami was estimated to be the equivalent of over 1,500 times that of the Hiroshima atomic bomb.

In order to use AGWs in tsunami mitigation, engineers will firstly need to devise highly accurate AGW frequency transmitters or modulators, which Dr. Kadri concedes would be challenging.

It may also be possible to utilize the AGWs that are naturally generated in the ocean when a violent geological event, such as an earthquake, occurs – essentially using nature's natural processes against itself.

Indeed, Dr. Kadri has already shown that naturally occurring AGWs could be utilized in an early tsunami detection system by placing detection systems in the deep ocean.

Dr. Kadri continued: "In practice, generating the appropriate acoustic-gravity waves introduces serious challenges due to the high energy required for an effective interaction with a tsunami…"

— Read more in Usama Kadri. "Tsunami mitigation by resonant triad interaction with acoustic–gravity waves," Heliyon 3, no. 1 (23 January 2017).

PREPAREDNESS

The Ongoing Quest to Assess & Measure Preparedness

Source: https://www.domesticpreparedness.com/preparedness/the-ongoing-quest-to-assess-measure-preparedness/

Feb 01 – Since 9/11, billions of dollars and an enormous amount of effort have been directed at enhancing national preparedness efforts as they relate to human-caused and natural disasters, yet many jurisdictions and organizations still struggle to determine how prepared they are and how prepared they need to be.

Despite the advent of the national preparedness system and associated assessment efforts, the emergency management community is still challenged to measure and articulate local, state, and national preparedness. One of the biggest challenges to measuring preparedness stems from the fact that preparedness means different things to different people. Additionally, how communities and organizations prepare greatly depends on what they are preparing for. Following is an examination of the ongoing quest to assess and measure preparedness with the goal of identifying good practices, ideas, and recommendations for the Federal Emergency Management Agency (FEMA) and other whole community stakeholders – including public sector, private sector, and nonprofit organizations – to consider.

Progress Has Been Made

Assessing and measuring preparedness are not new ideas and, over the years, FEMA and others have made progress. For example, FEMA's capability-based model that started with Homeland Security Presidential Directive 8 (HSPD-8) and has continued with Presidential Policy Directive 8 (PPD-8) provides a common framework, to include a series of capabilities that can be assessed and measured over time. The creation of standards such as National Fire Protection Association 1600 (NFPA-1600) and Emergency Management Accreditation Program (EMAP) standards have also proven to be helpful benchmarks for agencies to measure themselves against. Technology is aiding the effort as well, as the American Red Cross and others have developed intuitive web-based tools to help organizations assess their preparedness levels. Websites like the National Health Security Preparedness Index are also helping to promote the importance of preparedness assessments and the need to track progress over time.

In addition to the NFPA 1600, which has become a common framework used to guide private sector preparedness efforts, the creation of a voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep), has been an important advancement. Although more narrowly focused, the cybersecurity framework created by the National Institute for Standards and Technology is another good example of a mechanism that can be used to assess preparedness levels (related to cybersecurity) and has become an industry standard for both public and private sector organizations.

Room For Improvement

Despite progress, there is still a great deal of room for improvement, especially concerning the use of the Threat and Hazard Identification and Risk Assessment (THIRA) and associated State Preparedness Report (SPR) process to assess local, state, and national preparedness. Although the assessments are done differently across the country, FEMA "rolls up" the various data points to help produce the National Preparedness Report (NPR), which can lead to some potentially misleading data and conclusions. Although the SPR assessment process may be too subjective, a criticism echoed by the Government Accountability Office (GAO), the SPR's use of the planning, organization, equipment, training, and exercises (POETE) framework to examine the capabilities is intuitive.

Other methods and tools being used to assess preparedness include: after action reports from exercises and real-world events, surveys, subject matter experts, risk assessments, strategic plans, performance indicators, and standards such as EMAP. Despite the various

approaches, however, many do not have comprehensive programs in place to analyze the various data and information sources.

When it comes to preparedness, it is important to ensure the various preparedness efforts (including assessments) are grounded in risk. The various threats and hazards are simply too dynamic and it is impossible to prepare for everything equally. People, processes, and technology are constantly changing as well. Preparing for disasters is an enduring mission that requires ongoing and focused commitment, as well as some degree of ongoing financial support from the federal government to state and local governments for homeland security/emergency management purposes, particularly if there is a desire to be able to develop, sustain, and deploy specialized response capabilities (e.g., Incident Management Teams). However, no amount of money will guarantee preparedness, so risk-informed investments are important as is accountability for how the funds are used.

More effort is also needed to educate elected leaders and oversight agencies so that they better understand the ongoing nature of preparedness and appreciate that the nation will never be "done" preparing. Although it is unlikely that any one system will adequately measure national preparedness, the use of common tools and frameworks can certainly help the various stakeholders examine preparedness in a more consistent way.

Measuring What Matters

The emergency management community has struggled to develop metrics to measure preparedness. FEMA is working to develop a series of objective measures for the core capabilities, and some jurisdictions have made a lot of progress in developing their own measures for the core capabilities. Following are some examples of good practices:

- The New York State Division of Homeland Security and Emergency Services (DHSES) developed a County Emergency Preparedness Assessment (CEPA) Program that includes workshops in each county (and New York City) to assess local risk and capabilities using a POETE-based model.
- The Florida Division of Emergency Management has several innovative initiatives, including a program to assist counties with obtaining EMAP accreditation.
- The Bay Area Urban Area Security Initiative (UASI) partners worked with a consultant and their local stakeholders to develop a series of preparedness-related performance measures and associated tools to capture information from the jurisdictions within the UASI region.
- The National Preparedness Leadership Initiative (NPLI) at Harvard's Kennedy School of Government is an example of an innovative effort to educate leaders and to better understand executive decisions and attributes that can contribute to improved levels of preparedness.
- FEMA's National Preparedness Assessment Division (NPAD) has recently created an Evaluations and Decision Support Unit that is actively looking to identify and leverage various data and information sources to better understand preparedness.
- The American Red Cross has created the Ready Rating Program to help organizations assess their readiness and understand what steps they can take to improve preparedness.
- Of the other countries examined, New Zealand appears to have the most robust system in place to assess and measure preparedness. Like New York's CEPA program, New Zealand's National Capability Assessment is highly collaborative and captures data through a series of regional workshops.

Recommendations

Following are recommendations related to assessing and measuring preparedness that FEMA (and perhaps others) should consider:

- ***Promote POETE***: FEMA should focus more on promoting its definition of preparedness and the associated POETE methodology, which is intuitive and can likely be used by other public and private sector organizations.
- ***Streamline and improve the THIRA/SPR process***: FEMA should work with state and local stakeholders to improve the THIRA/SPR process by making it more intuitive and user-friendly.
- ***Trust but verify***: FEMA should trust the state and local data but develop mechanisms to verify the process used to capture the data and consider becoming a more active

participant in the process, rather than simply ensuring the appropriate boxes are checked.

- ***Invest in preparedness analysts***: FEMA, states, and others should consider the use of preparedness analysts to help analyze and assess preparedness.
- ***Participate in executive education initiatives***: Public, private sector, and nonprofit organizations should make a concerted effort to educate their leaders through programs like those offered at FEMA's Emergency Management Institute, Center for Homeland Defense and Security (CHDS), and Harvard's Kennedy School of Government.
- ***Create an Incident Command System (ICS) improvement officer position***: FEMA should consider the establishment of an improvement officer position and function within the ICS command staff structure.
- ***Establish a community of Practice***: FEMA should engage stakeholders by creating a preparedness assessment work group or community of practice.
- ***Consider a deliverables-based grant model***: The grant guidance is currently very broad and the funds can be used to support a wide variety of activities, which is a good thing, but FEMA should consider requiring some specific deliverables as well.
- ***Explore new assessment frameworks***: Much of the focus to date has been on assessing capabilities (ability and capacity), but other components such as competency (leadership and experience), collaboration (communication and coordination), and community (economics and demographics) warrant much further examination, to include the identification of relevant metrics and indicators for the various components (see Fig. 1).

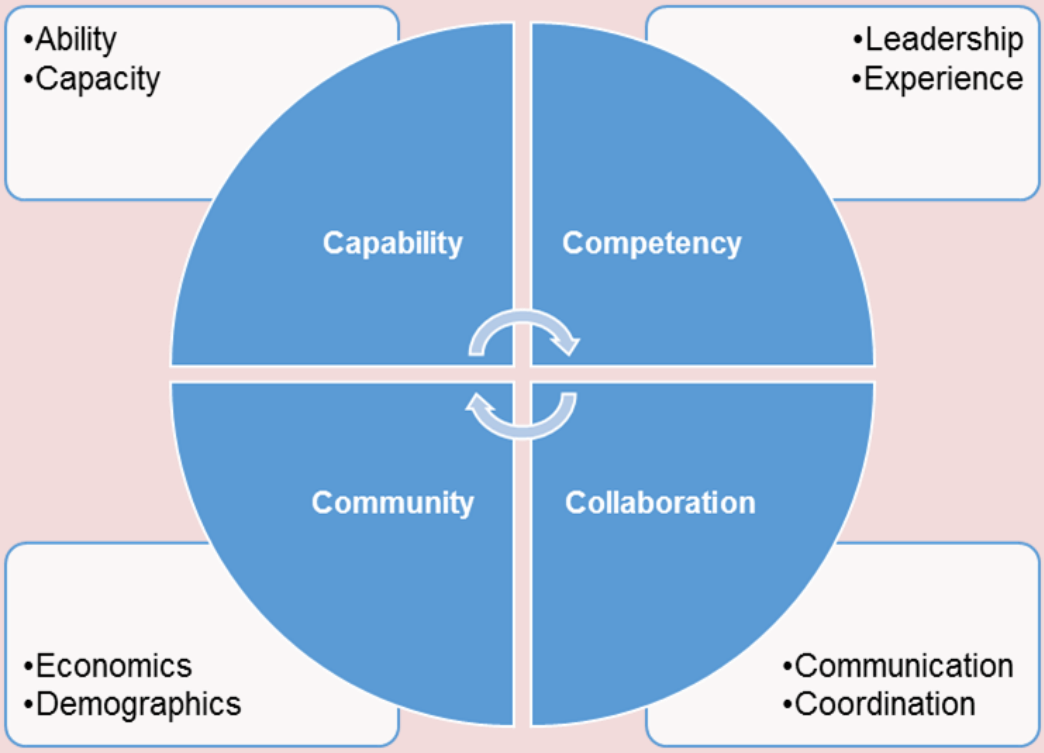


Fig. 1. "Four C" Assessment Framework. This new "Four C" Assessment Framework could serve as the basis of a broader assessment framework. Capability, competency, and collaboration are relevant for all organizations, but community factors should also be included in jurisdictional level assessments (*Source:* Authors).

Further Exploration

This is not the first effort to examine how the emergency management community can better assess and measure preparedness. Ideally, others will take this research even further and delve deeper into the issues identified. Much of the work to date has focused on assessing capability, but without sound leadership and effective relationships even the most capable organizations may struggle during a crisis. As such, the "Four C" framework warrants much

further examination. Preparedness is a never-ending process that requires a broader and more holistic analytical perspective to be truly understood. Progress has been made, but no single system or approach will suffice. To address an enduring challenge facing the emergency management community, it is time to think differently and determine how to assess and measure preparedness.

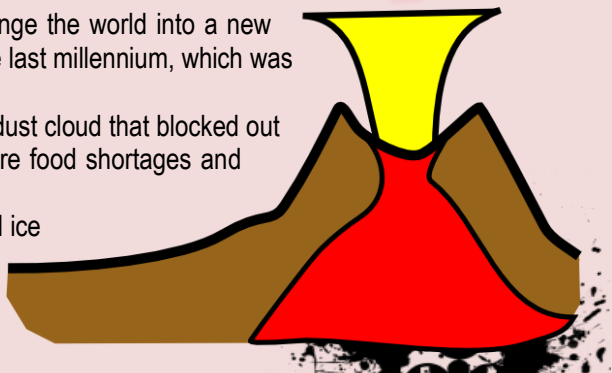
This article is based on a research project conducted as part of the Emergency Management Executive Academy at the FEMA's Emergency Management Institute. The project team for this effort included emergency management professionals from federal, state, local, and nongovernment agencies. Click here to read the full report and see below for more information on the team members.

***Terry Hastings** is the senior policy advisor for the New York Division of Homeland Security and Emergency Services, where he is responsible for the development and maintenance of New York State's Homeland Security Strategy and other statewide initiatives. He is also an adjunct instructor for the College of Emergency Preparedness, Homeland Security and Cybersecurity, at the State University of New York at Albany.*
***Chris Hennen** is the emergency manager for the United States Military Academy at West Point, where he oversees their all hazards emergency management program. He has been affiliated with West Point for more than 30 years, and is a retired U.S. Army Military Intelligence officer.*
***Gerald Manley** is the director of the headquarters, Department of the Army Directorate of Mission Assurance. He is responsible for the integration of the Headquarters Protection Program (which includes emergency management), the Safety and Occupational Health Program, Communications Security Program, Personnel Security Program, and the global Central United States North Atlantic Treaty Organization (NATO) Registry. He served in the active duty Army for over 25 years, and is also a local Community Emergency Response Team volunteer.*
***John Penido** is the disaster management area coordinator for Area C of Los Angeles County, California. He coordinates emergency preparedness, response, and recovery efforts in 10 cities with a combined population of 721,000 residents. His experience includes positions as a fire chief, paramedic, deputy sheriff, and Army officer. He is an instructor for the Emergency Services Training Institute of the Texas A&M Engineering Extension Service and the Paramedic Program at Mt. San Antonio College.*
***Art Samaras** most recently worked for the American Red Cross, where he was responsible for introducing and implementing the concepts of continuous improvement. He has more than 20 years of experience working as a consultant to industry and is currently a medevac flight paramedic.*
***Joe Sastre** is the emergency management director for the Town of Groton, Connecticut. He has 40 years of public safety experience, and currently serves as the chairman of the Connecticut Division of Emergency Management and Homeland Security Region 4 Emergency Planning Team Steering Committee.*
***Kevin Sligh** is the technical advisor to the chief, Marine Environmental Response Office at Coast Guard headquarters, where he serves as the principal advisor on a myriad of policy and response issues such as the National Contingency Plan and the Coast Guard's support to FEMA under ESF-10 (oil and hazardous substance response). He has served the military in active duty and reserve capacities for more than 24 years.*

Is the world prepared for another massive volcanic eruption?

Source: http://www.homelandsecuritynewswire.com/dr20170201-is-the-world-prepared-for-another-massive-volcanic-eruption

Feb 01 – An enormous volcanic eruption would not necessarily plunge the world into a new societal crisis, according to a new study of the biggest eruption of the last millennium, which was published in *Nature Geoscience*.
The 1257 eruption of the Samalas volcano in Indonesia produced a dust cloud that blocked out the sun around the world, and has been blamed for triggering severe food shortages and turmoil worldwide.
Analysis of nearly 200 medieval manuscripts, as well as tree-ring and ice core data spanning more than a thousand years, has revealed Samalas may not be the ultimate cause of the crises, states Dr.

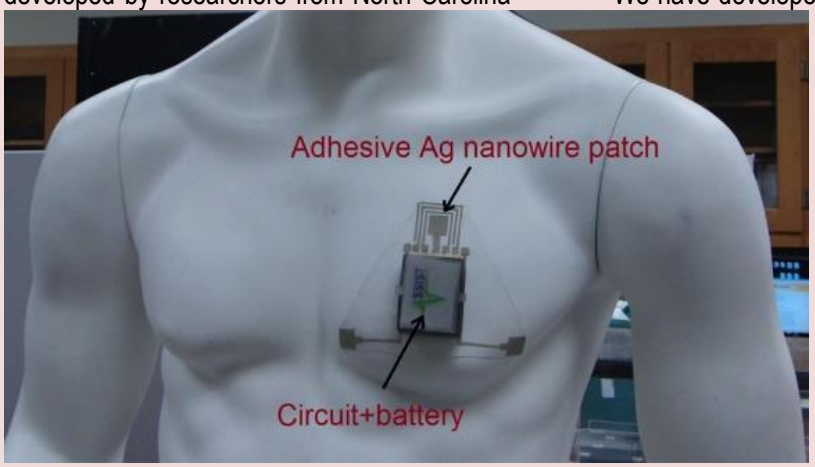


Sébastien Guillet, lead author of the study at the Faculty of Science, University of Geneva.
Dr. Pablo Ortega, a climate scientist at the University of Reading, who was involved in the research, said: "There are numerous indications of extreme weather conditions with serious societal consequences following the eruption, but also show that climatic conditions were back to normal by 1259 over most of Europe.
"While these extreme weather conditions originate at the Samalas eruption, our research shows it only played an aggravating role on the subsequent crises."
Reading notes that evidence showed famines in England and Japan had already begun before the eruption occurred. The scientists therefore argue that volcanic cooling might be less likely to lead to global crises than previously thought.
Documents from the years after the Samalas eruption describe the dimming of the sun, leading to cold temperatures, incessant rain and increased cloudiness, with one source from 1258 stating "There was no summer during summer". Descriptions of crop harvests following the eruption reveal they suffered badly, with wine production in Europe destroyed by "rock hard" grapes.
In addition, chronicles suggest a normal climate had resumed within four years of the eruption, contradicting previous model results suggesting temperature drops of as much as 1°C until 1264.
The scientists found the magnitude of the cooling by the Samalas eruption was very similar to smaller later eruptions, highlighting that the amount of sulphuric ash thrown into the air does not appear to directly correlate with the cooling effect on Earth.
Dr. Ortega said: "**Should a massive volcanic eruption occur in the next few years, its consequences for society might still be still difficult to predict, as the world in which we live in is more vulnerable and more exposed."**

Wearable Sensor to Alert on Soldiers and Firefighters Dehydration

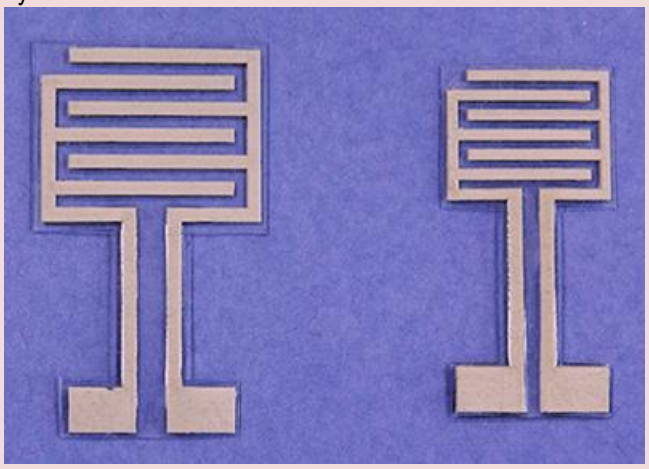
Source: http://i-hls.com/2017/02/wearable-sensor-alert-soldiers-firefighters-dehydration/

Feb 02 – **A wearable sensor that can monitor a person's skin hydration for use in applications that need to detect dehydration before it poses a health problem** was developed by researchers from North Carolina State University. The wireless device is lightweight, flexible and stretchable and has already been incorporated into prototype devices that can be worn on the wrist or as a chest patch.



"It's difficult to measure a person's hydration quantitatively, which is relevant for everyone from military personnel to athletes to firefighters, who are at risk of health problems related to heat stress when training or in the field," says John Muth, a professor of electrical and computer engineering at NC State.
"We have developed technology that allows us to track an individual's skin hydration in real time," says Yong Zhu, an associate professor of mechanical and aerospace engineering at NC State. "Our sensor could be used to protect the health of people working in hot conditions, improve athletic performance and safety, and to track hydration in older adults or in medical patients suffering from various conditions. It can even be used to tell how effective skin moisturizers are for cosmetics."
According to the university's website, the sensor consists of two electrodes made of an elastic polymer composite that contains conductive silver nanowires.

These electrodes monitor the electrical properties of the skin. Because the skin's electric properties change in a predictable way based on an individual's hydration, the readings from the electrodes can tell how hydrated the skin is.



The hydration sensors consist of two electrodes made of an elastic polymer composite that contains conductive silver nanowires.

In lab testing using custom-made artificial skins with a broad range of hydration levels, the researchers found that the performance of the wearable sensor was not affected by ambient humidity. And the wearable sensors were just as accurate as a large, expensive, commercially available hydration monitor that operates on similar principles, but utilizes rigid wand-like probes.

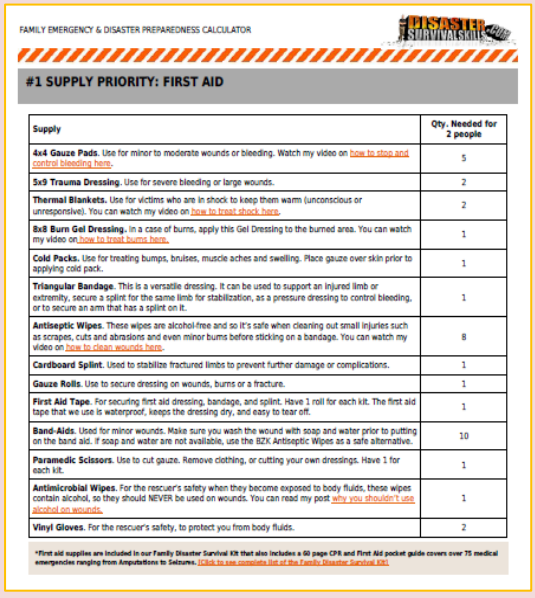
The researchers also incorporated the sensors into two different wearable systems: a wristwatch and an adhesive patch that can be worn on the chest. Both the watch and the patch wirelessly transmit sensor data to a program that can run on a laptop, tablet or smartphone. This means the data can be monitored by the user or by a designated third party – such as a doctor in a hospital setting, or an officer in a military setting.

What's more, the sensor is relatively inexpensive. "The commercially available monitor we tested our system against costs more than $8,000," says Shanshan Yao, a Ph.D. student at NC State. "**Our sensor costs about one dollar,** and the overall manufacturing cost of the wearable systems we developed would be no more than a common wearable device, such as a Fitbit."

EDITOR'S COMMENT: A good product for CBRN First Responders (especially Level-A people) as well!

Disaster Survival Skills launches new disaster preparedness calculator

Source: http://www.homelandsecuritynewswire.com/dr20170206-disaster-survival-skills-launches-new-disaster-preparedness-calculator



FAMILY EMERGENCY & DISASTER PREPAREDNESS CALCULATOR

DISASTER SURVIVAL SKILLS

#1 SUPPLY PRIORITY: FIRST AID

Supply	Qty. Needed for 2 people
4x4 Gauze Pads. Use for minor to moderate wounds or bleeding. Watch my video on how to stop and control bleeding here.	5
5x9 Trauma Dressing. Use for severe bleeding or large wounds.	2
Thermal Blankets. Use for victims who are in shock to keep them warm (unconscious or unresponsive). You can watch my video on how to treat shock here.	2
8x8 Burn Gel Dressing. In a case of burns, apply this Gel Dressing to the burned area. You can watch my video on how to treat burns here.	1
Cold Packs. Use for treating bumps, bruises, muscle aches and swelling. Place gauze over skin prior to applying cold pack.	1
Triangular Bandage. This is a versatile dressing. It can be used to support an injured limb or extremity, secure a splint for the same limb for stabilization, as a pressure dressing to control bleeding, or to secure an arm that has a splint on it.	1
Antiseptic Wipes. These wipes are alcohol-free and so it's safe when cleaning out small injuries such as scrapes, cuts and abrasions and even minor burns before sticking on a bandage. You can watch my video on how to clean wounds here.	8
Cardboard Splint. Used to stabilize fractured limbs to prevent further damage or complications.	1
Gauze Rolls. Use to secure dressing on wounds, burns or a fracture.	1
First Aid Tape. For securing first aid dressing, bandage, and splint. Have 1 roll for each kit. The first aid tape that we use is waterproof, keeps the dressing dry, and easy to tear off.	1
Band-Aids. Used for minor wounds. Make sure you wash the wound with soap and water prior to putting on the band aid. If soap and water are not available, use the BZK Antiseptic Wipes as a safe alternative.	10
Paramedic Scissors. Use to cut gauze. Remove clothing, or cutting your own dressings. Have 1 for each kit.	1
Antimicrobial Wipes. For the rescuer's safety when they become exposed to body fluids, these wipes contain alcohol, so they should NEVER be used on wounds. You can read my post why you shouldn't use alcohol on wounds.	1
Vinyl Gloves. For the rescuer's safety, to protect you from body fluids.	2

*First aid supplies are included in our Family Disaster Survival Kit that also includes a 60 page CPR and First Aid pocket guide covers over 75 medical emergencies ranging from Amputations to Seizures. [Click to see complete list of the Family Disaster Survival Kit]

Feb 06 – Disaster Survival Skills, LLC, launched its brand-new online Family disaster preparedness calculator. After inputting a few simple pieces of information, Disaster Survival Skills site visitors will receive a customized list of disaster supplies and advice that can be used to prepare for earthquakes, floods, and other emergencies. Disaster Survival Skills says that as a leading providers of disaster supplies and emergency response training services, the company help others can make sure that they are prepared for emergencies of any kind. The new calculator is free to use and is one of a number of free resources at the Disaster Survival Skills Web site.

"Preparing for a disaster is the kind of thing that many families put off until it's too late, but the fact is that it's also

often a lot easier than most would expect," said Wayne Bennett, founder of Disaster Survival Skills. "Over my thirty-three years as a professional firefighter and disaster response professional, I came to truly appreciate how even a bit of strategic preparation could make a real difference. Our new calculator makes it easier than ever before to get started and will also highlight how far even a little bit of preparation can go. We all owe it to ourselves and our families to be prepared for the worst, and we think our new calculator is going to be a big help."

Seismologists have warned for years about the danger of a so-called "megaquake" devastating the Pacific Northwest upon the rupture of the region's Cascadian Subduction Zone. Even given a 7 to 15 percent 50-year likelihood of an earthquake measuring 9.0 or higher on the Richter scale, though, many remain unprepared. A 2015 survey by Oregon Public Broadcasting of that state's residents, for example, found that only 12 percent characterized themselves as "very prepared," with over half believing their local communities were conspicuously lacking in preparedness.

The new Disaster Survival Skills preparedness calculator is designed to make it as simple as possible to figure out what could be needed in the aftermath of such a disaster or others. After being provided with a bit of information, the calculator creates a detailed report customized for each user. In addition to listing quantities of supplies that should be stockpiled and precautions to be taken, the new calculator also provides links to informative resources covering topics relevant to each.

Disaster Survival Skills notes that with the company's full range of supplies, it can also help make it easier to follow up on the calculator's recommendations. The new calculator is online now at the Disaster Survival Skills Web site and takes only seconds to use.

Civilian/Military Collaboration for Domestic Response

By Dr. Jeffrey Driskill Sr.

Source: https://www.domesticpreparedness.com/resilience/civilian-military-collaboration-for-domestic-response/

Feb 08 – The focus of PATRIOT's tactical level domestic response has matured to increase understanding of interagency and multidisciplinary coordination, policies, and doctrine, and to develop procedures and processes that could be adopted elsewhere. The best practices and lessons learned are relevant to any local and state emergency managers, and strengthen knowledge about how the military can provide support to civilian authorities.

The PATRIOT Exercise Program has evolved beyond being just a premier biannual domestic operations (DOMOPS) training exercise sponsored by the National Guard Bureau and accredited by the Joint National Training Capability Program. It is an excellent forum for military partners to coordinate with local, state, tribal, and federal civilian organizations, as well as nongovernment and private sector organizations in Federal Emergency Management Agency (FEMA) Regions IV and V. FEMA Region IV encompasses the states of Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee; whereas FEMA Region V consists of Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin.

Evolution of a Turnkey, Full-Scale Exercise

The biannual PATRIOT Exercise held at Volk Field, Wisconsin, and Gulfport/Camp Shelby, Mississippi, provides a vast array of training venues and support services that allow participants to step into a "turnkey" full-scale exercise. The venues include remote areas suitable for wide-area searches, ground-to-air operations, search and rescue, collapsed structure response, debris removal operations, and more; supplemented with a wide range of role-play support, modeling, and simulation, and subject matter experts to provide further realism.

PATRIOT planners provide a backdrop that realistically aligns military capabilities against projected civilian shortfalls. The host military facilities provide low-cost feeding and lodging for civilian organizations to support the exercise development through the three major planning meetings. This support continues into exercise conduct for participants, culminating in a rewarding exercise experience that has included more than 1,000 people annually.

The successfully collaborative practices of the PATRIOT Exercise Program, which is supported by and compliant with the National Incident Management System (NIMS) and

Homeland Security Exercise and Evaluation Program, leverage existing processes that institutionalize NIMS concepts and principles such as the Incident Command System, interoperable communications, and resource management. For example, the program provides a venue for Type 3 All-Hazards Incident Management Teams (AHIMT) to train and complete position task books while managing a complex response to a realistic disaster scenario. Type 3 AHIMTs are local, regional, state, or tribal level multiagency/multijurisdictional teams used to manage incidents spanning multiple operational periods. These teams are typically deployed with 10-20 trained personnel, and are capable of managing major and/or complex incidents requiring a significant number of local, state, or tribal resources. The complexity of incidents require a written incident action plan, that can later transition and transfer to a national level AHIMT.

Lessons learned from Hurricane Katrina in 2005 and other events provided the impetus for embedding military liaison officers into the branch, division, and incident management team levels. This practice improves coordination for patient treatment and information tracking between the United States Transportation Command (TRANSCOM) Regulating and Command and Control Evacuation System (TRAC2ES) and civilian systems, de-conflicts real-world and exercise logistics, and establishes a process for data collection and dissemination. The development of position descriptions and job aids for liaison officers are proving invaluable for the military/civilian interface at both the incident command and operations center levels.

In 2015, PATRIOT was the first exercise to integrate military rotary, fixed-wing, and remote-piloted aircraft in support of domestic operations by successfully executing the request for proper use memorandum, signed off by the secretary of defense to comply with real-world intelligence oversight expectations. The military fills resource shortfalls in supplementing civilian air operations, including the Civil Air Patrol, hospital medical flights, and more.

Building Mutual Military-Civilian Understanding

Military partners are required to meld into civilian processes to learn key lessons in resource management, operational planning, and accountability. Emergency managers should be aware that PATRIOT uses the Civil Support Task List for military units to explain which DOMOPS capabilities they will implement. The Civil Support Task List is a resource-typing list, a directory of capabilities that could be used as a crosswalk back to the core capabilities to which civilian organizations are accustomed to referring. This is a realm worthy of continued familiarization and further development.

PATRIOT Exercise scenarios test select core capabilities such as situational assessment, operational communications, mass care, and mass search and rescue operations. In addition, the military provides assets and resources to fill local shortfalls. An important lesson learned was that “planning” and “operations” in the conventional incident command sense meant different things to civilians and military personnel. The civilian world typically sees persons providing situational awareness, data display, and collection management within the planning section as a function. The military looks at this through an operational lens rather than the planning paradigm.

For example, the planning staff functioning within the Incident Command System is responsible for collecting, evaluating, and disseminating the tactical information related to the incident, and for preparing and documenting incident action plans. The planning section develops “action plans” that are implemented through operations, where the tactical resources exist. The traditional military paradigm views the development of plans from the wartime top-down joint operational planning perspective, where deliberate planning such as operational (OPLAN), communications (CONPLAN), functional and crisis-action planning like the Campaign Plan, and Operational Order (OPORD) are developed. The military’s Joint Staff system provides structuring that state-level planners recognize such as the J3 rating for operations and J5 for planning.

The “J” refers to Joint Staff in military lexicon, and is the staff of specified command, joint task force, or subordinate functional component that employs forces from more than one military department, and will include members from the several services comprising the force. These members should be assigned in such a manner as to ensure that the commander understands the tactics, techniques, capabilities, needs, and limitations of the component parts of the force. Positions on the staff should be divided so that service representation and influence generally reflect the service composition of the force. The J5 develops higher-level strategic plans, which are then handed off to the J3 to write future plans, or plans to be executed.

For this reason, military liaison officers in air operations coordinated information awareness and assessment in concert with the operations section, rather than planning section within the Incident Command System construct. The visual and data products were shared with the requesting consumer once developed – for example, maps for wide-area searches shared between search and rescue (SAR) task force, combat controllers establishing communications in remote areas, and command to coordinate SAR operations.

The planning "P" process is used to develop the incident action plan that drives the exercise. The discussion-based exercise enables participants to discuss legal, statutory, regulatory, and procedural challenges such as use of force and airspace, as well as information collection and sharing. PATRIOT North 16 in Wisconsin led to best practices in developing operating procedures for task force/strike team operations integrating military security forces, civilian law enforcement, military Religious Support Teams, and Salvation Army Spiritual Care Teams during a holistic response to aid an isolated community. Active shooter and civil disturbance vignettes created realistic levels for close coordination between these entities.

Military emergency managers found it helpful to learn tradecraft from their civilian counterparts when staffing various planning and logistic section units within the Incident Management Team. Emerging technology was explored, such as the no-cost DOMOPS Awareness and Assessment Response Tool (DAART), which is available to civilian organizations. The DAART provides: a flexible, scalable, and safe portal to share documents; processes such as flight scheduling to support incident assessment missions; resource ordering; and static and video data imaging to improve situational assessment and aid in establishing a common operating picture. The DAART can also be used for everyday events and incidents such as the 2016 and 2017 Super Bowls.

A Growing Number of Partnerships

Examples of growing PATRIOT partnerships include Team Rubicon, Salvation Army, American Red Cross, Civil Air Patrol, local law enforcement, fire departments and rescue companies, local hospitals and medical centers, Occupational Safety and Health Administration, and others. Although the exercise venues are limited to the two certified training areas of Hattiesburg, Mississippi, and Volk Field, Wisconsin, this does not preclude civilian organizations or entities from coming from outside the two FEMA regions. Self-nominations are reviewed and vetted by the planning team during the appropriate time, and the past participants are testimony to the enduring benefits derived at the PATRIOT Exercise.

Team Rubicon, members of the National Guard Bureau and debris removal teams attend operational briefing at PATRIOT North 16' (*Source:* SMSgt. David Lipp, ND National Guard Public Affairs, 17 July 2016).

These mutually beneficial partnerships are growing, with almost every state being represented by National Guard units at one time or another. Although all exercises and trainings have their inherent value, the PATRIOT Exercise Program offers a unique opportunity to advance and enhance national capabilities across National Guard units and among a vast civilian audience. At the PATRIOT Exercise, military and civilian participants are moving past mere NIMS compliance to becoming competent in the perishable skills needed to sustain an effective disaster response. More information, pictures, and videos of past PATRIOT exercises can be found on the National Guard PATRIOT Exercise Facebook page.

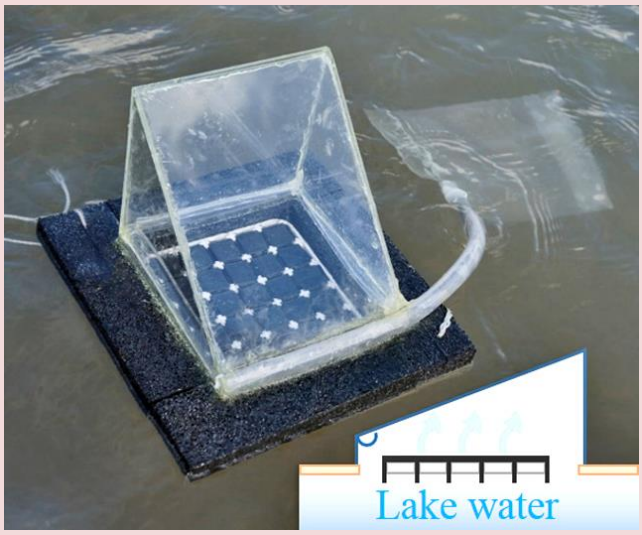
Dr. Jeffrey Driskill Sr. is currently a government contractor working as an exercise planner with the National Guard Bureau in Arlington, Virginia. Before his current position, he served as deputy emergency management coordinator with the City of Alexandria, Virginia, and is a retired chief of police, Certified Emergency Manager (CEM), and Master Exercise Practitioner Program (MEP) graduate. He holds a Doctor of Business Administration in Homeland Security Policy and Leadership from Northcentral University and is a subject matter expert in the NIMS doctrine.

"Solar vapor" device purifies dirty drinking water

Source: http://www.homelandsecuritynewswire.com/dr20170207-solar-vapor-device-purifies-dirty-drinking-water

Feb 07 – **A new way to make nasty or salty water drinkable features carbon-dipped paper. It could be a cheap and efficient option for addressing global drinking water shortages, particularly in developing areas and regions affected by natural disasters.**

"Using extremely low-cost materials, we have been able to create a system that makes near maximum use of the solar energy during evaporation. At the same time, we are minimizing the amount of heat loss during this process," says lead researcher Qiaoqiang Gan, associate professor of electrical engineering in the University at Buffalo School of Engineering and Applied Sciences.



As reported in the journal *Global Challenges*, the team built a small-scale solar still. The device, which they call a "solar vapor generator," cleans or desalinates water by using the heat converted from sunlight. Here's how it works: The sun evaporates the water. During this process, salt, bacteria, or other unwanted elements are left behind as the liquid moves into a gaseous state. The water vapor then cools and returns to a liquid state, where it is collected in a separate container without the salt or contaminants.

"People lacking adequate drinking water have employed solar stills for years, however, these devices are inefficient," says Haomin Song, PhD candidate and one of the study's leading coauthors. "For example, many devices lose valuable heat energy due to heating the bulk liquid during the evaporation process. Meanwhile, systems that require optical concentrators, such as mirrors and lenses, to concentrate the sunlight are costly."

The University at Buffalo says that the research team addressed these issues by creating a solar still about the size of mini-refrigerator. It's made of expanded polystyrene foam (a common plastic that acts as a thermal insulator and, if needed, a flotation device) and porous paper coated in carbon black. Like a napkin, the paper absorbs water, while the carbon black absorbs sunlight and transforms the solar energy into heat used during evaporation.

The solar still coverts water to vapor very efficiently. For example, only 12 percent of the available energy was lost during the evaporation process, a rate the research team believes is unprecedented. The accomplishment is made possible, in part, because the device converts only surface water, which evaporated at 44 degrees Celsius.

Based upon test results, researchers believe the still is capable of producing 3 to 10 liters of water per day, which is an improvement over most commercial solar stills of similar size that produce 1 to 5 liters per day.

Materials for the new solar still cost roughly $1.60 per square meter—a number that could decline if the materials were purchased in bulk. (By contrast, systems that use optical

concentrators can retail for more than $200 per square meter.) **If commercialized, the device's retail price could ultimately reduce a huge projected funding gap — $26 trillion worldwide between 2010 and 2030, according to the World Economic Forum — needed for water infrastructure upgrades.**

"The solar still we are developing would be ideal for small communities, allowing people to generate their own drinking water much like they generate their own power via solar panels on their house roof," says coauthor Zhejun Liu, a visiting scholar at the University at Buffalo and a Ph.D. candidate at Fudan University in China.

— Read more in Zhejun :iu et al., "Extremely Cost-Effective and Efficient Solar Vapor Generation under Nonconcentrated Illumination Using Thermally Isolated Black Paper," Global Challenges (30 January 2017).

Chaplain is 'First Responders' First Responder'

Source: http://www.govtech.com/em/disaster/Chaplain-is-first-responders-first-responder.html

Feb 08 – Once area first responders have ministered at the scene of fires, accidents and other traumatic events, who attends to them?

One of those folks wearing the emergency services ministering mantle is Chaplain Cole Massey of College Place. Because he runs a window cleaning operation and computer service, his time is flexible enough to attend to area firefighters, deputies, police officers, paramedics and state troopers as needed.

"I'm a first responder to the first responders," he emailed in reply to my inquiries. "I absorb the emotional trauma that is present on most scenes."

Either local dispatch calls him when police or fire agencies request him or he self-dispatches to structure fires, fatal accidents and pedestrian-versus-vehicles.

Neither a pastor nor a priest, rather he said he guides the responders to the next step in traumatic processing.

"Our community has great spiritual leaders and I'm not here to take that from the local church. I'm purposed for people's worst and best day of their lives and then I get them to the next stepping stone on their journey, which could be physical, emotional or spiritual rehab. I'm not a counselor like Father Steve Woolley, I'm 'peer support' and the best cheerleader outside of their spouses," Cole said.

He said such constant calls can wear on responders' thoughts and perspectives.

"Firefighters and police officers are my greatest heroes because they are constantly tested with their ethics, compassion and endurance yet usually are wrapped up in political policies that make their day-to-day jobs harder. I guess I'm a CHO (Chief Heart Officer) but the College Place Fire and Police department calls me "Chappy."

"Dispatchers (the FIRST First Responders) call me out on the radio by my call sign 'Chaplain 551.'"

He's also helped the Kennewick Fire and Police, Richland, Pasco and Benton County personnel.

Acquaintance Dixie Ferguson of Walla Walla said the fire department has been unusually busy of late, along with the inclement weather.

"Their skills, hard work and dedication have been a real eye opener for me. As first responders, I suppose I have certain expectations and natural assumptions that they are just out there doing their job," she said.

"I've been learning much more about the role of the volunteer fire/police chaplain Cole Massey. His support role is amazing, the long hours, compassion and commitment to serve in many difficult circumstances: e.g., suicides, car wrecks, ER crises, issues with first responders in their personal stresses, etc. Cole never knows what he is going to be called to do but volunteers willingly," Dixie said.

Cole, who lives in College Place with wife Lacey and their two dogs, has served as a chaplain here since 2013 after completing a national certification program at the Washington State Patrol headquarters. Also a certified firefighter chaplain, he has understudied outgoing County Chaplain Steve Woolley, who remains an active mentor.

Cole became an ordained minister in McCall, Idaho, in 2008, led youth ministry teams and served young people in the local church setting for about 10 years.

His life experiences range from running an award-winning restaurant in Phoenix, Ariz., and four years as a sponsored snowboarder for Volcom, Burton and Dragon. And he ran a large event-planning business for high-end clubs in Scottsdale and Tempe, Ariz.

But after his snowboard clothing company failed he sold his businesses and moved to McCall in 2005 for a change in lifestyle. He and Lacey met in 2006.

"We loved our little tourist town; I worked a seasonal job as a snowmobile guide for Tamarack Resort and spent time growing our church's youth group," he said.

When the economy tumbled in 2008, the Masseys looked for opportunities beyond their ski town that took them to Denver in 2010 and to Richland in January 2011 for job possibilities that didn't pan out.

While searching fruitlessly for work, he started soliciting window washing services, "a trade I had picked up years before," door-to-door, also to no avail.

Then the Masseys visited friends in Walla Walla one day and he struck up a conversation with the owner of a window-cleaning company who offered him a job.

They moved to Walla Walla in June 2011, found full-time jobs, a church to call home and served as youth leaders for four years.

During that time, he completed the Walla Walla County Fire District 4 training academy and pursued a fire science degree at Walla Walla Community College, secured his commercial driver's license endorsement and branched out on his own by starting Professional Window Services with a ladder donated by Walla Walla city firefighter/paramedic friend Jay Jones.

Cole started Eclat Creative Group, a social media management company, and Jont, a pedicab taxi service.

"I have found the economy in Walla Walla and surrounding areas to be as fertile as the soil this community was established on and I have been blessed in my business dealings with many wonderful Walla Walla residents," he said.

He teaches social media classes at WWCC and for Junior Achievement at College Place High School.

"I have a heart for entrepreneurs, which I guess is my current identity."

"Self-employment has given me the opportunity/flexibility to serve as a volunteer firefighter and fire and police chaplain.

"Our First Responders see parts of our community that most people don't see," he said.
The Incident Management Team brought Cole out the day after firefighters Tom Zbyszewki, 20, Andrew Zajac, 26, and Richard Wheeler, 31, died in the Twisp (Wash.) River Fire on Aug. 19, 2015. Cole stayed at the camp with remaining wildland firefighters for two weeks.
"I then was able to visit many other camps as a chaplain to 'take the temperature' of the morale and just encourage our heroes. I've never encountered a First Responder that didn't miss their family."
Certified in critical stress incident management, Cole can gauge the situation of a room, scene or the aftermath of a traumatic event.
He's a member of the Walla Walla School District Crisis Team,and Walla Walla Emergency Management ensures he's "constantly getting training to stay relevant in crisis management."
"We all have times of crisis, but it's how we respond to the blunt force of it that dictates our emotional success and perspective in life. I have not done this well at times in my own life so I have a great chaplain in Father Woolley and a great pastor and church that supports me in Kennewick called New Vintage Church."
"I am making a difference by being approachable, accountable and obedient to my chiefs, captains and lieutenants."
Once he arrives at a scene, Cole checks in with the incident commander as to where they want him and what he can help with.
"Sometimes that includes putting on my fire gear and going in or getting coffee for the crew when it's 2 a.m. and minus 10 degrees out. Other times, I put on my chaplain hat and help do death notifications or find lodging and dry clothes for those who lost their homes or loved ones by suicide, homicide or other forms of death. I'm not a coroner. I don't have the grace for that like Richard Greenwood does. I'm a 'do what I'm told to' chaplain for our First Responders."
He feels called by the Lord to do the work.
"He gives me the grace to spread His love to any race, sex, religion or age. I'm not here to convert people to my church. I'm here to hold their hand until we get them to their shepherd or their faith-based community. This calling has reminded me that ... we are all on a spiritual journey of some sort and other people's journeys remind me that I can finish my race if I have a good community around me."

Recovering from disasters: Social networks matter more than bottled water and batteries

By Daniel P. Aldrich
Source: http://www.homelandsecuritynewswire.com/dr20170214-recovering-from-disasters-social-networks-matter-more-than-bottled-water-and-batteries

Feb 14 – Standard advice about preparing for disasters focuses on building shelters and stockpiling things like food, water and batteries. But resilience — the ability to recover from shocks, including natural disasters —- comes from our connections to others, and not from physical infrastructure or disaster kits.
Almost six years ago, Japan faced a paralyzing triple disaster: a massive earthquake, tsunami, and nuclear meltdowns that forced 470,000 people to evacuate from more than 80 towns, villages and cities. My colleagues and I investigated how communities in the hardest-hit areas reacted to these shocks, and found that social networks - the horizontal and vertical ties that connect us to others - are our most important defense against disasters.

The 2011 catastrophe
At 2:46 pm on Friday, March 11, 2011, a massive 9.0 earthquake struck off Japan's northeastern coast. The quake was bigger and lasted longer than the hundreds of quakes which rattle the nation annually, but did little damage to homes and businesses. Unfortunately, however, the danger was far from over.
Within 40 minutes massive waves of water, some as high as six stories, smashed down on coastal communities in the Tohoku region in northeastern Japan. Some 18,500 lives were lost, primarily to the tsunami.
Damage from the earthquake and tsunami shut down the cooling systems at the Fukushima Daiichi nuclear power plants 1 through 3, which experienced nuclear fuel

meltdowns. Over 160,000 people were forced to evacuate from Fukushima prefecture. The radiation exclusion zone initially covered more than 5,400 square miles, but has slowly decreased as decontamination efforts have progressed.

In total, more than 470,000 people evacuated during the disaster. The nuclear accident paralyzed national politics, made many survivors anxious and depressed, and changed the landscape of energy policy in Japan by pushing local residents to pursue non-nuclear options. Many communities have started electricity cooperatives where they use geothermal, solar and wind to produce their power.

What saved lives during the tsunami?

A Japanese colleague and I hoped to learn why the mortality rate from the tsunami varied tremendously. In some cities along the coast, no one was killed by waves which reached up to 60 feet; in others, up to ten percent of the population lost their lives.

We studied more than 130 cities, towns and villages in Tohoku, looking at factors such as exposure to the ocean, seawall height, tsunami height, voting patterns, demographics, and social capital. We found that municipalities which had higher levels of trust and interaction had lower mortality levels after we controlled for all of those confounding factors.

The kind of social tie that mattered here was horizontal, between town residents. It was a surprising finding given that Japan has spent a tremendous amount of money on physical infrastructure such as seawalls, but invested very little in building social ties and cohesion.

Based on interviews with survivors and a review of the data, we believe that communities with more ties, interaction and shared norms worked effectively to provide help to kin, family and neighbors. In many cases only 40 minutes separated the earthquake and the arrival of the tsunami. During that time, residents literally picked up and carried many elderly people out of vulnerable, low-lying areas. In high-trust neighborhoods, people knocked on doors of those who needed help and escorted them out of harm's way.

What helped cities bounce back?

In another study I worked to understand why some 40 cities, towns and villages across the Tohoku region had rebuilt, put children back into schools and restarted businesses at very different rates over a two-year period. Two years after the disasters some communities seemed trapped in amber, struggling to restore even half of their utility service, operating businesses and clean streets. Other cities had managed to rebound completely, placing evacuees in temporary homes, restoring gas and water lines, and clearing debris.

To understand why some cities were struggling, I looked into explanations including the impact of the disaster, the size of the city, financial independence, horizontal ties between cities, and vertical ties from the community to power brokers in Tokyo. In this phase of the recovery, vertical ties were the best predictor of strong recoveries.

Communities that had sent more powerful senior representatives to Tokyo in the years before the disaster did the best. These politicians and local ambassadors helped to push the bureaucracy to send aid, reach out to foreign governments for assistance, and smooth the complex zoning and bureaucratic impediments to recovery.

While it is difficult for communities to simply decide to place more senior representatives in Tokyo, they can take the initiative to make connections with decision makers. Further, they can seek to make sure that they speak with a unified voice about their community's needs and vision.

Social ties, not just sandbags

The Tohoku disasters reinforce past evidence about the importance of social networks and social capital in disaster recovery around the world. While climate change is making some disasters more devastating over time, there is good news from our findings. Governments, NGOs and private citizens have many tools available to foster horizontal and vertical connections.

Nonprofits like the Australian Red Cross, BoCo Strong in Boulder, Colorado, and New Zealand's Wellington Regional Emergency Management Organization now take social capital seriously as they work to build resilience. In these programs local residents work alongside civil society organizations to help strengthen connections, build networks of

reciprocity, and think about the needs of the area. Rather than waiting for assistance from the government, these areas are creating their own plans for mitigating future crises.

How to build resilience

Communities can build cohesion and trust in a variety of ways. First, residents can emulate Mr. Fred Rogers and learn about their neighbors, who will serve as first responders during any crisis. Next, whole communities can seek to deepen interactions and trust by organizing sports days, parties, religious festivals and other community events that build trust and reciprocity.

For example, San Francisco provides funds to local residents to hold NeighborFest, a block party open to all. City planners and urban visionaries can learn to think like Jane Jacobs, an advocate for living cities and third spaces - that is, places beyond work and home where we can socialize. By designing what advocates call "placemaking public spaces," such as pedestrian-friendly streets and public markets, they can reshape cities to enhance social interaction.

Finally, communities can increase volunteerism rates by rewarding people who volunteer their time and providing concrete benefits for their service. One way to do this is by developing community currencies — local scrip which is only accepted at local businesses. Another strategy is time banking, in which participants earn credits for their volunteer hours and redeem them later for services from others.

After 3/11, one organization in Tohoku has sought to bring these kinds of programs - social capital creation and design - together by providing a communal space run by elderly evacuees where neighbors can connect.

As communities around the world face disasters more and more frequently, I hope that my research on Japan after 3/11 can provide guidance to residents facing challenges. While physical infrastructure is important for mitigating disaster, communities should also invest time and effort in building social ties.

***Daniel P. Aldrich** is Professor of Political Science, Public Policy and Urban Affairs and Director, Security and Resilience Program, Northeastern University.*

Alarms Raised Years Ago About Risks of Oroville Dam's Spillways

By Peter Fimrite, Cynthia Dizikes and Joaquin Palomino (staff writers @ San Francisco Chronicle)
Source: http://www.govtech.com/em/disaster/Alarms-raised-years-ago-about-risks-of-Oroville-Dams-spillways.html

Water flows through break in the wall of the Oroville Dam spillway, Thursday, Feb. 9, 2017, in Oroville, Calif. The torrent chewed up trees and soil alongside the concrete spillway before rejoining the main channel below. Engineers don't know what caused what state Department of Water Resources spokesman Eric See called a "massive" cave-in that is expected to keep growing until it reaches bedrock. AP/Rich Pedroncelli

Feb 14 – Potentially catastrophic problems with both the primary and emergency spillways at the Oroville Dam in Northern California appear to have been caused by flaws that either had shown up in inspections or were flagged to state and

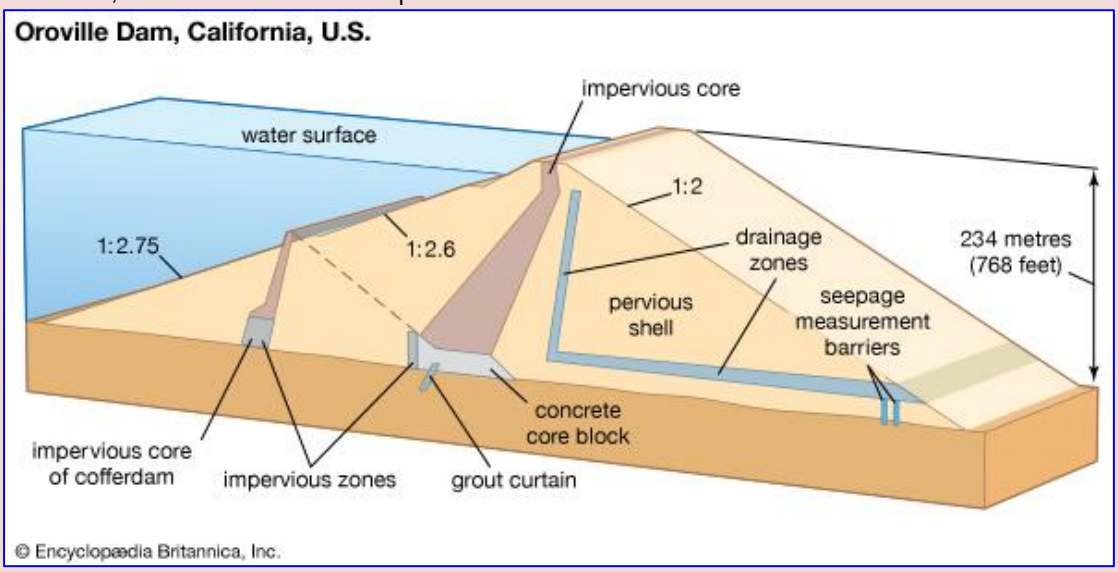
federal officials going back more than a decade, an expert in infrastructure failures said Monday.

The cratering of the main spillway — which spiraled into the current crisis in Butte County — occurred in a spot where cracks and other defects had been found repeatedly since 2009, said Robert Bea, a professor emeritus and engineering expert at UC Berkeley.

But the defects do not appear to have been adequately repaired or resolved by the state Department of Water Resources, which runs the dam, and the faulty work probably resulted in the fissure that opened up last week on the 1,730-foot-long spillway, Bea said.

"My God, we had evidence that there was trouble going back to 2008, 2009," said Bea, who at The Chronicle's request reviewed 14 dam inspections from 2008 to 2016 conducted by the Division of Safety of Dams, which is part of the Department of Water Resources.

"Yes, they had detected the defects (in the main spillway) and yes, they had put into gear remedial measures," Bea said. "Were those repairs sufficient? No. The result was a breach."



The cause of the fissure in the main spillway has not been identified. The Department of Water Resources, which runs the dam, has defended its management of the main spillway — saying it was inspected routinely — and its handling of the situation.

Bill Croyle, the agency's acting director, said Monday, "This was a new, never-happened-before event."

The disintegration of a section of the main spillway forced the state on Saturday to use the dam's emergency spillway, which sends water over a bare hillside and had not been used since the dam's completion in 1968.

Within 24 hours, erosion was threatening to burrow through the hillside and cause the emergency spillway to fail, prompting the evacuation of more than 180,000 people from downstream communities.

Critics said the state should have avoided this predicament, but chose years ago not to improve the emergency spillway by lining it with concrete.

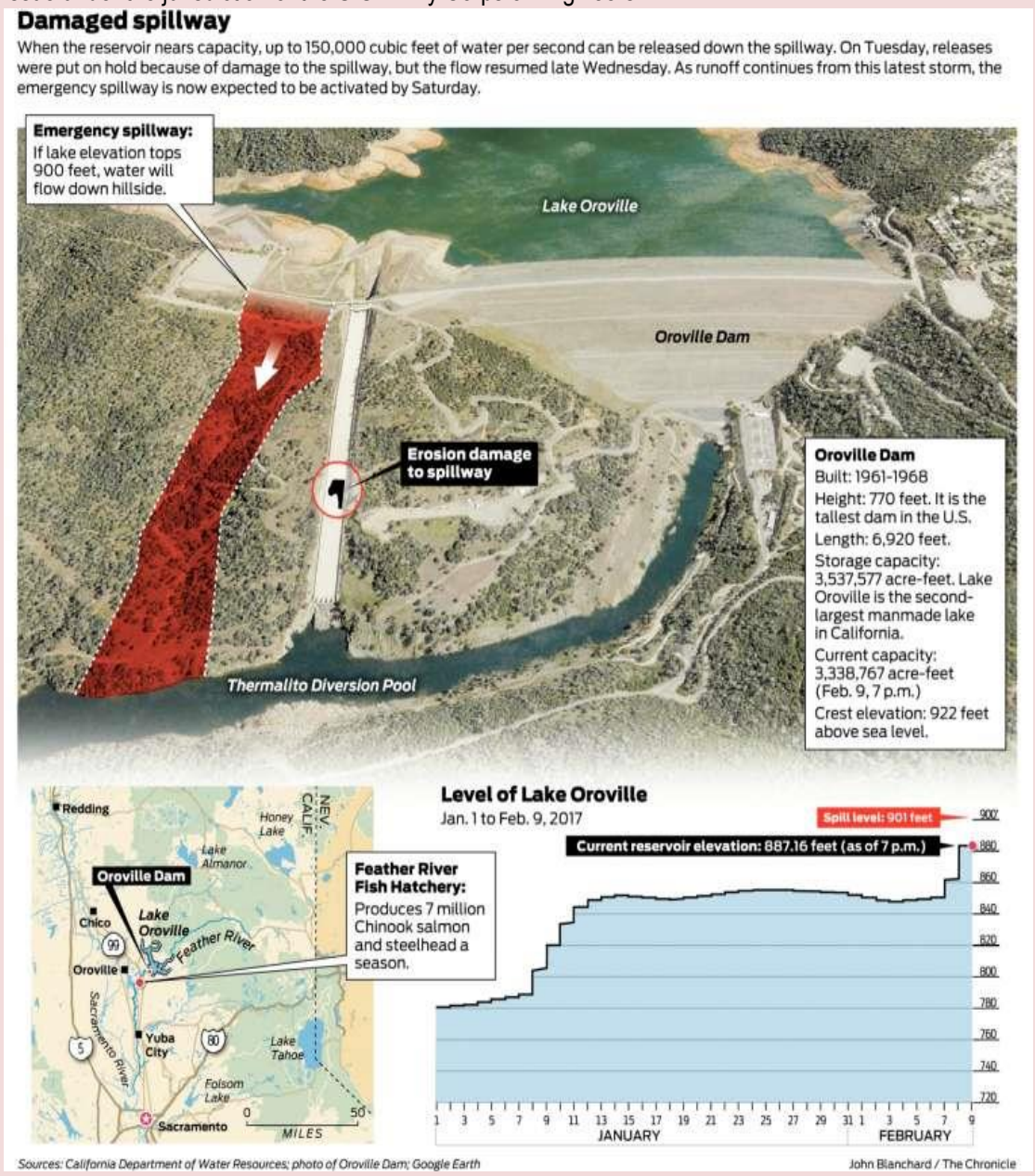
In 2005, three environmental groups — Friends of the River, the Sierra Club and the South Yuba River Citizens League — warned state and federal water regulators about the emergency spillway in a 31-page motion filed with the Federal Energy Regulatory Commission. The dam was going through a periodic relicensing review by the commission.

The groups were concerned that use of the unpaved auxiliary spillway would cause extreme erosion, endanger fish and damage downstream structures, including a fish hatchery where millions of fish had to be rescued and moved last week.

But the more than two dozen state water contractors that receive supplies from Lake Oroville, including the mammoth Metropolitan Water District in Southern California, refused to pay the estimated $100 million cost of "armoring" the spillway.

The threatened failure "was entirely predicted and warned about, and DWR refused to even do a study," said Deirdre Des Jardins, principal with California Water Research, which collaborates with environmental, fishing and local groups on water research projects. "If Metropolitan's headquarters were down from the dam, you can bet they would have" agreed to pay.

Jeff Kightlinger, Metropolitan's general manager, said the contractors had spent as much as $90 million to extend the dam's federal license and believed paving the emergency spillway was a flood-control issue under the jurisdiction of the U.S. Army Corps of Engineers.



In the end, the Federal Energy Regulatory Commission dismissed the concerns about the emergency spillway, declaring in a 2006 memorandum that "during a rare event with the emergency spillway flowing at its design capacity, spillway operations would not affect reservoir control or endanger the dam."

"We took no position on whether it should be paved or not," Kightlinger said, "and then FERC looked at it and said it was not an issue because it would rarely if ever be used."

As recently as 2014, the danger was spelled out in a flood management plan commission by the Department of Water Resources.

"The unlined emergency spillway for Oroville Dam would likely suffer heavy damage in the event it must be used in a major flood event," the state report said.

Croyle said he could not comment on the complaints about the emergency spillway, because he was unfamiliar with them. Gov. Jerry Brown, asked at a news conference Monday about the decades-old warnings by environmental groups, said, "Glad we found out about it."

The emergency spillway was briefly mentioned in the latest state inspection of the dam last August. The concrete weir or rim "remains stable appearing and in good condition," inspectors noted, but they made no mention of the integrity of the hillside below.

Another engineering expert who reviewed the Oroville Dam's inspection records said he did not find anything negligent in the state's management.

Art Schmidt, president of New York-based Underwater Consultants International Inc., said inspection records show that state and federal agencies were regularly testing and evaluating the dam, including addressing cracks and other potential problems.

"I don't see anything grossly negligent here, by any means," said Schmidt, whose company has been conducting dam inspections for more than 20 years. "Unfortunately, structures fail. But it looks like they were doing everything that normally should be done. They were inspecting on a regular basis and monitoring defects. Obviously, something failed before they thought it was going to."

Bea, who has analyzed disasters including the deadly 2010 pipeline explosion in San Bruno, said the first indication of trouble in the main spillway was in 2009, when defects in the base slabs, which form the concrete chute, were detected.

The situation got worse, and repairs were made in 2013, said Bea, who obtained photographs showing construction in the same spot as this month's rupture. More repairs were made in that area in 2014 and then in 2015, he said, when cracks were detected in the spillway.

Bea said inspectors noticed trees growing on the right side of the spillway in their 2015 report. The inspectors recommended removing the trees, but the damage may have already occurred.

"Those trees are there because they like water, and the question is, where are they getting the water from?" Bea said. "The answer is that we've got seepage in that spillway."

Inspectors noted in the two latest inspection reports, in 2015 and 2016, that they did not walk the main spillway, but instead viewed it from a distance — and found no problems.

In response to the crisis, the Federal Energy Regulatory Commission on Monday ordered the Department of Water Resources to perform a "forensic analysis aimed at determining the cause of the chute failure."

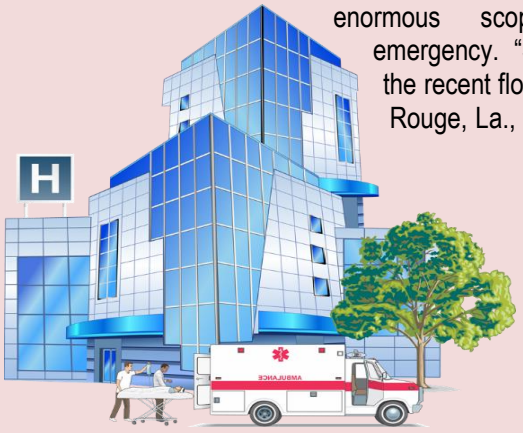
Big Changes Coming for Hospital Emergency Managers

Source: http://www.govtech.com/em/health/Big-Changes-Coming-for-Hospital-Emergency-Managers.html

Feb 10 – Emergency management leaders at hospitals and medical centers are grappling with a major rule change from the Centers for Medicare and Medicaid Services (CMS).

CMS finalized a rule it says is intended to establish consistent emergency preparedness requirements for health-care providers participating in Medicare and Medicaid.

In announcing the rule, CMS specifically mentioned this summer's flooding in Louisiana, where hospitals struggled to cope with the enormous scope of the emergency. "Situations like the recent flooding in Baton Rouge, La., remind us that in the event of an emergency, the first priority of health-care providers and suppliers is to protect the health and safety of their patients," CMS Deputy Administrator and Chief Medical Officer Dr. Patrick Conway said in a news release. "Preparation, planning and one comprehensive approach for emergency preparedness is key. One life lost is one too many."



Officially titled "Emergency Preparedness Requirements for Medicare and Medicaid Participating Providers and Suppliers," the new regulations must be implemented by November 2017. While CMS has yet to release specific guidelines around many of the new requirements, some in the hospital world believe big changes are coming.

"We have always had emergency plans, but now they are asking for really specific policies and procedures," said Ruth Ragusa, senior vice president for quality and care management at the 455-bed South Nassau Communities Hospital in Long Island, N.Y.

"Plans in the past were fairly detailed, but we expect that even further detail will be required. There will be more depth in the communications area and also in training and testing," she said.

The new rule applies not just to hospitals but also to long-term care facilities as well as to outpatient providers such as ambulatory surgical centers (ASCs) and end-stage renal disease facilities.

While that may seem like painting with a broad brush, some commend CMS for differentiating in the requirements for different types of facilities. For example, the communications component of the rule tasks hospitals with having very specific procedures in place to track patients during a crisis, whereas ASCs carry less of a burden in this area.

"We can cancel appointments or send patients home, and CMS acknowledged that, very appropriately. They recognized that ASCs would not need to keep track of patients in the same way as hospitals," said David Shapiro, a board member with the Accreditation Association for Ambulatory Health Care (AAAHC) and an anesthesiologist at Red Hills Surgical Center in Tallahassee, Fla.

CMS officials tailored a number of requirements to reflect the diverse types of providers covered under the rule. Outpatient providers don't have to have policies and procedures for provision of subsistence needs, for example, while hospitals and long-term care facilities do need to install emergency and standby power systems.

Nonetheless, providers of all stripes will likely feel the impact of the new rules. Even in the absence of specific guidance from CMS, the revised regulations "do seem to go a little further, a little deeper," Shapiro said. While AMCs have long coordinated their emergency plans with state and local authorities, for example, "now they are asking us to step up our game in terms of making sure that we specifically document those efforts."

For emergency managers outside the medical community, meanwhile, the new requirements could be a boon. "State and local emergency managers are always happy when the people who are their customers in a crisis have got a good plan," said Michael Anderson, a director at public safety consulting and managed services IXP Corp. in Princeton, N.J.

"This is an opportunity for emergency managers to be a resource to the medical community, to evaluate their plans and help make them stronger," he said. "Knowing who your counterpart is in that hospital, knowing how to get hold of people in a crisis, those are going to be key benefits for emergency management."

What's required

CMS lays out four areas that medical providers need to address as part of their overall preparedness efforts:

Emergency plan: Perform a risk assessment and build a plan using an all-hazards approach to address the full spectrum of location-specific emergencies or disasters.

- **Policies and procedures:** Develop and implement policies and procedures based on the plan.
- **Communication plan:** In a plan based on state and federal law, ensure patient care is coordinated within the facility, across health-care providers and with other emergency entities.
- **Training and testing program:** Develop and maintain training and testing programs, including initial and annual trainings, and conduct drills and exercises or participate in an actual incident that tests the plan.

This is the tip of the iceberg: The full rule runs to almost 190 pages, and CMS still is expected to issue a range of more detailed documents laying out its expectations for exactly how providers will fulfill the new requirements. CMS offers a number of pointers to help emergency planners begin to address the new requirements. It identifies FEMA documents for risk assessment, communication and training as potentially helpful tools.

The intention, overall, seems to be to turn up the heat on emergency planners. While most medical facilities have emergency plans in place, CMS insists a more rigorous, comprehensive approach is needed. Upon reviewing providers' present readiness efforts, "we concluded that the current requirements are not comprehensive enough to address the complexities of actual emergencies," the rule states. In the event of a disaster, "health-care facilities across the nation will not have the necessary emergency planning and preparation in place to adequately protect the health and safety of their patients."

It's not the lack of planning per se, so much as it is the fragmented

nature of the rules that has CMS most concerned. "[T]he current regulatory patchwork of federal, state and local laws and guidelines, combined with various accrediting organizations' emergency preparedness standards, falls far short" of what is needed, CMS writes.

To ensure facilities get up to speed, CMS is calling for a higher degree of practical exercise. In addition to training and testing, "you also need to drill your staff," noted Andrew Randazzo, CEO of Prime Medical Training in Knoxville, Tenn. Among other things, the new rules call for hospitals to participate in a community mock disaster drill at least annually, along with tabletop exercises.

This will likely require some financial investment. At South Nassau Communities Hospital, Ragusa voiced a common concern: that the new requirements may come with a steep price tag. "It may mean additional supplies, resources, systems," she said. "We are going to have to revisit communications and training, all these areas. Will it require 10 percent or 20 percent more? Without the specifics it's hard to say."

Psychological "vaccine" could immunize public against fake news on climate change

Source: http://www.homelandsecuritynewswire.com/dr20170203-psychological-vaccine-could-immunize-public-against-fake-news-on-climate-change

Feb 03 – **In medicine, vaccinating against a virus involves exposing a body to a weakened version of the threat, enough to build a tolerance. Social psychologists believe that a similar logic can be applied to help "inoculate" the public against misinformation, including the damaging influence of "fake news" Web sites propagating myths about climate change.**

The University of Cambridge says that a new study compared reactions to a well-known climate change fact with those to a popular misinformation campaign. When presented consecutively, the false material completely cancelled out the accurate statement in people's minds – opinions ended up back where they started.

Researchers then added a small dose of misinformation to delivery of the climate change fact, by briefly introducing people to distortion tactics used by certain groups. This "inoculation" helped shift and hold opinions closer to the truth, despite the follow-up exposure to fake news.

The study on U.S. attitudes found the inoculation technique shifted the climate change opinions of Republicans, Independents, and Democrats alike.

Published in the journal *Global Challenges*, the study was conducted by researchers from the universities of Cambridge, Yale, and George Mason. It is one of the first on inoculation theory to try and replicate a real world scenario of conflicting information on a highly politicized subject.

"Misinformation can be sticky, spreading and replicating like a virus," says lead author Dr. Sander van der Linden, a social psychologist from the University of Cambridge and director of the Cambridge Social Decision-Making Lab.

"We wanted to see if we could find a 'vaccine' by pre-emptively exposing people to a small amount of the type of misinformation they might experience. A warning that helps preserve the facts.

"The idea is to provide a cognitive repertoire that helps build up resistance to misinformation, so the next time people come across it they are less susceptible."

Fact vs. Falsehood

To find the most compelling climate change falsehood currently influencing public opinion, van der Linden and colleagues tested popular statements from corners of the

internet on a nationally representative sample of U.S. citizens, with each one rated for familiarity and persuasiveness.

The winner: the assertion that there is no consensus among scientists, apparently supported by the Oregon Global Warming Petition Project. This Web site claims to hold a petition signed by "over 31,000 American scientists" stating there is no evidence that human CO2 release will cause climate change.

The study also used the accurate statement that "97 percent of scientists agree on manmade climate change." Prior work by van der Linden has shown this fact about scientific consensus is an effective gateway for public acceptance of climate change.

In a disguised experiment, researchers tested the opposing statements on over 2,000 participants across the U.S. spectrum of age, education, gender, and politics using the online platform Amazon Mechanical Turk.

In order to gauge shifts in opinion, each participant was asked to estimate current levels of scientific agreement on climate change throughout the study.

Those shown only the fact about climate change consensus (in pie chart form) reported a large increase in perceived scientific agreement – an average of 20 percentage points. Those shown only misinformation (a screenshot of the Oregon petition website) dropped their belief in a scientific consensus by 9 percentage points.

Some participants were shown the accurate pie chart followed by the erroneous Oregon petition. The researchers were surprised to find the two neutralized each other (a tiny difference of 0.5 percentage points).

"It's uncomfortable to think that misinformation is so potent in our society," says van der Linden. "A lot of people's attitudes toward climate change aren't very firm. They are aware there is a debate going on, but aren't necessarily sure what to believe. Conflicting messages can leave them feeling back at square one."

Psychological "inoculation"

Alongside the consensus fact, two groups in the study were randomly given "vaccines":

- A *general inoculation*, consisting of a warning that "some politically-motivated groups use misleading tactics to try and convince the public that there is a lot of disagreement among scientists."
- A *detailed inoculation* that picks apart the Oregon petition specifically. For example, by highlighting some of the signatories are fraudulent, such as Charles Darwin and members of the Spice Girls, and less than 1 percent of signatories have backgrounds in climate science.

For those inoculated with this extra data, the misinformation that followed did not cancel out the accurate message.

The general inoculation saw an average opinion shift of 6.5 percentage points towards acceptance of the climate science consensus, despite exposure to fake news.

When the detailed inoculation was added to the general, it was almost 13 percentage points – two-thirds of the effect seen when participants were just given the consensus fact.

Cambridge notes that the research team point out that tobacco and fossil fuel companies have used psychological inoculation in the past to sow seeds of doubt, and to undermine scientific consensus in the public consciousness.

They say the latest study demonstrates that such techniques can be partially "reversed" to promote scientific consensus, and work in favor of the public good.

The researchers also analyzed the results in terms of political parties. Before inoculation, the fake negated the factual for both Democrats and Independents. For Republicans, the fake actually overrode the facts by 9 percentage points.

However, following inoculation, the positive effects of the accurate information were preserved across all parties to match the average findings (around a third with just general inoculation; two-thirds with detailed).

"We found that inoculation messages were equally effective in shifting the opinions of Republicans, Independents and Democrats in a direction consistent with the conclusions of climate science," says van der Linden.

"What's striking is that, on average, we found no backfire effect to inoculation messages among groups predisposed to reject climate science, they didn't seem to retreat into conspiracy theories.

"There will always be people completely resistant to change, but we tend to find there is room

for most people to change their minds, even just a little."

— Read more in Sander van der Linden et al., "Inoculating the Public against Misinformation about Climate Change," Global Challenges (23 January 2017).

Extreme fires will increasingly be part of our global landscape

Source: http://www.homelandsecuritynewswire.com/dr20170207-extreme-fires-will-increasingly-be-part-of-our-global-landscape

Feb 07 – **Increasingly dangerous fire weather is forecast as the global footprint of extreme fires expands, according to the latest research.**

University of Tasmania Professor of Environmental Change Biology David Bowman led an international collaboration — including researchers from the University of Idaho and South Dakota State University — to compile a global satellite database of the intensity of 23 million landscape fires between 2002 and 2013. Of the 23 million fires, researchers honed in on 478 of the most extreme wildfire events.

"Extreme fire events are a global and natural phenomenon, particularly in forested areas that have pronounced dry seasons," Professor Bowman said.

"With the exception of land clearance, the research found that extremely intense fires are associated with anomalous weather - such as droughts, winds, or in desert regions, following particularly wet seasons.

"Of the top 478 events we identified 144 economically and socially disastrous extreme fire events that were concentrated in regions where humans have built into flammable forested landscapes, such as areas surrounding cities in southern Australia and western North America."

The University of Tasmania says that the researchers, using climate change model projections to investigate the likely consequences of climate change, found more extreme fires are predicted in the future for Australia's east coast, including Brisbane, and the whole of the Mediterranean region - Portugal, Spain, France, Greece and Turkey.

"The projections suggest an increase in the days conducive to extreme wildfire events by 20 to 50 percent in these disaster-prone landscapes, with sharper increases in the subtropical Southern Hemisphere, and the European Mediterranean Basin," Professor Bowman said.

University of Idaho Assistant Professor Crystal Kolden said the United States had a much higher proportion of fire events become disasters than any other country in the study. Wildfire burned more than 10 million acres in the United States in 2015, and cost over $2 billion to suppress.

"What is really novel about this study is that in the United States, we tend to make the assumption that all large and intense fires are disasters, and that there is nothing we can do about it," Assistant Professor Kolden said.

"But that is not the case at all. What makes a fire event a disaster in the United States is when key factors combine - low density housing amidst dense forests, the right climatic conditions, and a lack of fire preparedness on the part of humans.

"We can't stop big, intense fires from happening here, and they are increasing under climate change. However, in the western United States, we can reduce the potential for fire disasters by both reducing forest density and improving mitigation and preparedness through the development of fire-resilient communities."

U Tasmania notes that the research was released on the day that Professor Bowman's home state remembers the impact of 1967 bushfires which claimed the lives of 62 people, left 900 injured, and more than 7,000 homeless. The research resulting from these fires built the foundations of a globally relevant research effort in the field for Tasmania.

— Read more in David M. J. S. Bowman et al., "Human exposure and sensitivity to globally extreme wildfire events," Nature Ecology & Evolution 1, Article number: 0058 (2017) (6 February 2017).

Humans now affect Earth system more than natural forces

Source: http://www.homelandsecuritynewswire.com/dr20170215-humans-now-affect-earth-system-more-than-natural-forces

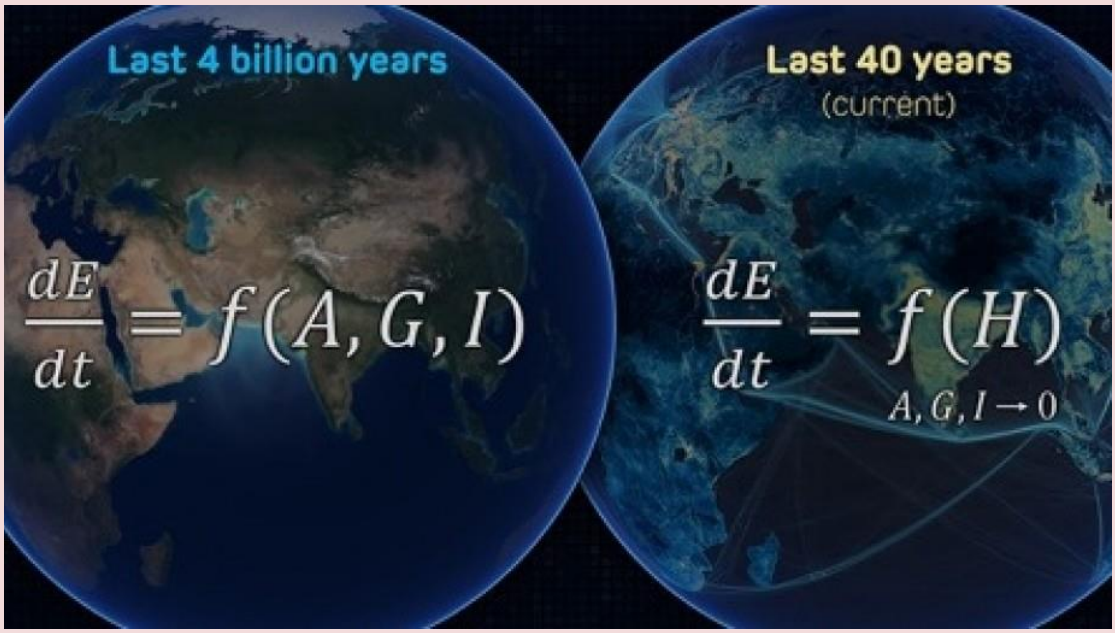
Feb 15 – Humans are causing the climate to change 170 times faster than natural forces, new research co-led by the Australian National University (ANU) has found.

Co-researcher Professor Will Steffen from ANU said the study for the first time came up with a mathematical equation to describe the impact of human activity on the Earth system, known as the Anthropocene equation.

"Over the past 7,000 years the primary forces driving change have been astronomical — changes in solar intensity and subtle changes in orbital parameters, along with a few volcanoes. They have driven a rate of change of 0.01 degrees Celsius per century," said Professor Steffen, from the Fenner School of Environment and Society and the Climate Change Institute at ANU.

"Human-caused greenhouse gas emissions over the past forty-five years have increased the rate of temperature rise to 1.7 degrees Celsius per century, dwarfing the natural background rate."

ANU notes that the paper published in *The Anthropocene Review* examines the Earth system as a single complex system and assesses the impact of human activities on the system's trajectory.



The Anthropocene equation: E is the Earth system; A is astronomical forces; G is geophysical forces; I is internal dynamics; and H is industrialised societies.

"We are not saying the astronomical forces of our solar system or geological processes have disappeared, but in terms of their impact in such a short period of time they are now negligible compared with our own influence," Professor Steffen said.

"Crystallising this evidence in the form of a simple equation gives the current situation a clarity that the wealth of data often dilutes.

"It also places the contemporary human impact in the context of the great forces of nature that have driven Earth system dynamics over billions of years."
Professor Steffen said humanity still had a chance to prevent catastrophic climate change, but time was rapidly running out.
"The global economy can function equally well with zero emissions. Research shows we can feed nine billion people - the projected world population by 2050 - and reduce greenhouse gas emissions at the same time," he said.

— Read more in Owen Gaffney et al., "The Anthropocene equation," Anthropocene Review *(10 February 2017).*

Improving climate change modeling by including variables such as inequality, consumption, and population

Source: http://www.homelandsecuritynewswire.com/dr20170221-improving-climate-change-modeling-by-including-variables-such-as-inequality-consumption-and-population

Feb 21 – **A new scientific paper by a University of Maryland-led international team of distinguished scientists, including five members of the National Academies, argues that there are critical two-way feedbacks missing from current climate models that are used to inform environmental, climate, and economic policies. The most important inadequately modeled variables are inequality, consumption, and population.**

In this research, the authors present extensive evidence of the need for a new paradigm of modeling that incorporates the feedbacks that the Earth System has on humans, and propose a framework for future modeling that would serve as a more realistic guide for policymaking and sustainable development.
UMD says that twelve of the interdisciplinary team of 20 coauthors are from the University of Maryland, with multiple other universities (Northeastern University, Columbia University, George Mason University, Johns Hopkins University, and Brown University) and other institutions (Joint Global Change Research Institute, University Corporation for Atmospheric Research, the Institute for Global Environment and Society, Japan's RIKEN research institute, and NASA's Goddard Space Flight Center) also represented.
The study explains that the Earth System (e.g., atmosphere, ocean, land, and biosphere) provides the Human System (e.g., humans and their production, distribution, and consumption) not only the sources of its inputs (e.g., water, energy, biomass, and materials) but also the sinks (e.g., atmosphere, oceans, rivers, lakes, and lands) that absorb and process its outputs (e.g., emissions, pollution, and other wastes).
Titled **"Modeling Sustainability: Population, Inequality, Consumption, and Bidirectional Coupling of the Earth and Human Systems,"** the paper describes how the rapid growth in resource use, land-use change, emissions, and pollution has made humanity the dominant driver of change in most of the Earth's natural systems, and how these changes, in turn, have critical feedback effects on humans with costly and serious consequences, including on human health and well-being, economic growth and development, and even human migration and societal conflict. However, the paper argues that these two-way interactions ("bidirectional coupling") are not included in the current models.
The Oxford University Press's multidisciplinary journal *National Science Review*, which published the paper, has highlighted the work in its current issue, pointing out that "the rate of change of atmospheric concentrations of CO2, CH4, and N2O [the primary greenhouse gases] increased by over 700, 1000, and 300 times (respectively) in the period after the Green Revolution when compared to pre-industrial rates."

"Many datasets, for example, the data for the total concentration of atmospheric greenhouse gases, show that human population has been a strong driver of the total impact of humans on our planet Earth. This is seen particularly after the two major accelerating regime shifts: Industrial Revolution (~1750) and Green Revolution (~1950)," said Safa Motesharrei, UMD systems scientist and lead author of the paper. "For the most recent time, we show that the total impact has grown on average ~4 percent between 1950 and 2010, with almost equal contributions from population growth (~1.7 percent) and GDP per capita growth (~2.2 percent). This corresponds to a doubling of the total impact every ~17 years. This doubling of the impact is shockingly rapid."

"However, these human impacts can only truly be understood within the context of economic inequality," pointed out political scientist and co-author Jorge Rivas of the Institute for Global Environment and Society. "The average per capita resource use in wealthy countries is 5 to 10 times higher than in developing countries, and the developed countries are responsible for over three quarters of cumulative greenhouse gas emissions from 1850 to 2000."

University of Maryland geographer and co-author Klaus Hubacek added: "The disparity is even greater when inequality within countries is included. For example, about 50 percent of the world's people live on less than $3 per day, 75 percent on less than $8.50, and 90 percent on less than $23. One effect of this inequality is that the top 10 percent produce almost as much total carbon emissions as the bottom 90 percent combined."

The study explains that increases in economic inequality, consumption per capita, and total population are all driving this rapid growth in human impact, but that the major scientific models of Earth-Human System interaction do not bidirectionally (interactively) couple Earth System Models with the primary Human System drivers of change such as demographics, inequality, economic growth, and migration.

The researchers argue that current models instead generally use independent, external *projections* of those drivers. "This lack of two-way coupling makes current models likely to miss critical feedbacks in the combined Earth-Human system," said National Academy of Engineering member and co-author Eugenia Kalnay, a Distinguished University Professor of Atmospheric and Oceanic Science at the University of Maryland.

"It would be like trying to predict El Niño with a sophisticated atmospheric model, but with the Sea Surface Temperatures taken from external, independent projections by, for example, the United Nations," said Kalnay. "Without including the real feedbacks, predictions for coupled systems cannot work; the model will get away from reality very quickly."

"Ignoring this bidirectional coupling of the Earth and Human Systems can lead to missing something important, even decisive, for the fate of our planet and our species," said co-author Mark Cane, G. Unger Vetlesen Professor of Earth and Climate Sciences at Columbia University's Lamont-Doherty Earth Observatory, who recently won the Vetlesen Prize for creating the first coupled ocean–atmosphere model with feedbacks that successfully predicted El Niño.

"The result of not dynamically modeling these critical Human-Earth System feedbacks would be that the environmental challenges humanity faces may be significantly underestimated. Moreover, there's no explicit role given to policies and investments to actively shape the course in which the dynamics unfold. Rather, as the models are designed now, any intervention — almost by definition — comes from the outside and is perceived as a cost," said co-author Matthias Ruth, Director and Professor at the School of Public Policy and Urban Affairs, Northeastern University. "Such modeling, and the mindset that goes with it, leaves no room for creativity in solving some of the most pressing challenges."

"The paper correctly highlights that other human stressors, not only the climate ones, are very important for long-term sustainability, including the need to reduce inequality", said Carlos Nobre (not a co-author), one of the world's leading Earth System scientists, who recently won the prestigious Volvo Environment Prize in Sustainability for his role in understanding and protecting the Amazon. "Social and economic equality empowers societies to engage in sustainable pathways, which includes, by the way, not only the sustainable use of natural resources but also slowing down population growth, to actively diminish the human footprint on the environment."

Michael Mann, Distinguished Professor and Director of the Earth System Science Center at Penn State University, who was not a co-author of the paper, commented: "We cannot separate the issues of population growth, resource consumption, the burning of fossil fuels, and climate risk. They are part of a coupled dynamical system, and, as the authors show,

this has dire potential consequences for societal collapse. The implications couldn't be more profound."

— Read more in Safa Motesharrei et al., "Modeling Sustainability: Population, Inequality, Consumption, and Bidirectional Coupling of the Earth and Human Systems," National Science Review *3, no. 4 (11 December 2016): 470-94.*