****

## http://r54.cooltext.com/rendered/cooltext1333426312.pngCost of plutonium disposal facility skyrockets

Source: http://www.homelandsecuritynewswire.com/dr20140225-cost-of-plutonium-disposal-facility-skyrockets

**A Department of Energy (DOE) classified report says that completing the Mixed Oxide (MOX) nuclear fuel factory at the Savannah River Site in South Carolina may cost billions of dollars more than previously estimated. Completing and operating the factory to help dispose of cold war-era plutonium as part of the nonproliferation arrangement with Russia would cost up to $30 billion in addition to the $4 billion spent on construction so far.**

Government officials and industry sources familiar with the study say that the Obama administration is contemplating other options to eliminate the thirty-four tons of weapons-grade plutonium the factory was expected to help eliminate.

The Center for Public Integrity reports that with no clear alternative in site, the administration may propose to fund the plant’s construction in fiscal 2015, but for less than the $343 million appropriated in 2014. The plant’s builder, Shaw Areva MOX Services, a French-Dutch-owned consortium, seeks roughly $700 million a year to keep construction on schedule, but senior administration officials have insisted on a reduction in construction costs in order to support the completion and operation of the MOX factory.

**The DOE report estimates that construction costs alone could reach $10 billion, or ten times the initial estimate.** To reduce costs, DOE wants Shaw Areva MOX Services to revise the contract to limit the company’s profits and expand the firm’s responsibility for cost overruns. “Areva should know that if it makes mistakes, it should suffer the consequences,” one government critic of the program said, noting past construction problems that have boosted the project’s costs. Shaw Areva’s refusal of DOE demands have led the administration to explore other options to dispose of the plutonium.

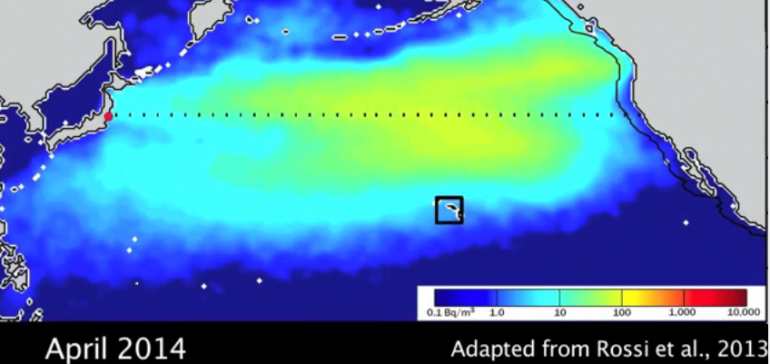
**A government official involved with discussions about plutonium disposal said that Russia has, surprisingly, indicated that it might support a U.S. decision to dispose of the plutonium by transforming the plutonium metal into a less explosive powder, then bury it deep underground in concrete containers. This option is the cheapest alternative — it would cost only $6 billion and would take five years.** The original plan to transform plutonium into a Mixed Oxide fuel which would be burned in commercial reactors has yet to secure a commercial reactor operator who would be willing to use the material. One reason for the MOX factory’s high cost is that DOE would have to pay commercial reactor operators a fee to burn the MOX fuel.

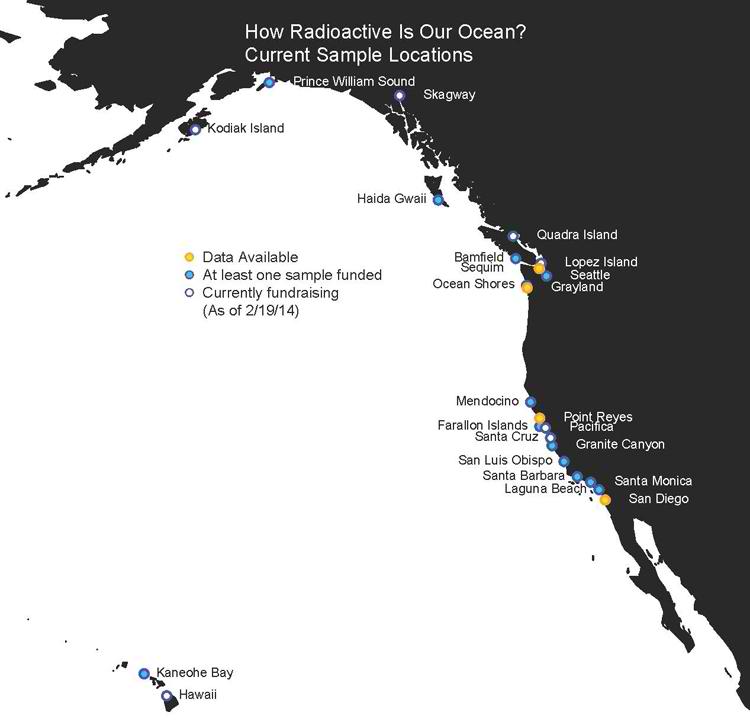
Matthew Bunn, a former Clinton White House official who helped develop the plutonium disposal program, agrees that the cost of the MOX factory is excessive. “The things we’re trying to accomplish aren’t worth that amount of money,” he said. “To me, in an environment of extreme budget constraints and sequesters, there has got to be a better way.”

John MacWilliams, who conducted the DOE study, has proposed disposing of the plutonium in three-mile deep “boreholes” drilled deep into the bedrock. Another option is to mix the plutonium with high-level radioactive waste and store it in a future long-term storage facility. Burying oxidized plutonium would likely take place at DOE’s Waste Isolation Pilot Plant (WIPP) near Carlsbad, New Mexico, a network of underground salt-lined caves. Such an option would demand the site’s expansion, which will require local permission and political will.

# Fukushima Radiation Reaches Waters Off the Coast Of Canada, Expected To Reach U.S. In April

Source: http://www.ibtimes.com/fukushima-radiation-reaches-waters-coast-canada-expected-reach-us-april-1557857

Fukushima may have reached North American shores. Water samples collected off the coast of Vancouver, British Columbia, had trace amounts of radionuclides associated with the disastrous 2011 radiation leak at the Japanese nuclear plant, according to research presented at the Ocean Sciences Meeting on Feb. 24.

The levels of radioactive cesium isotopes are well below safe limits and researchers from the Woods Hole Oceanographic Institution will monitor the shores of Canada and the United States throughout 2014 as Fukushima fallout is expected to arrive in the coming months. Ken Buesseler, senior scientist at WHOI, has been performing tests and collecting samples from 24 different costal locations and presented the research at the Ocean Sciences Meeting Monday.

WHOI scientists detected cesium-134 and cesium-137, radioactive isotopes that have more neutrons, reports LiveScience, but the levels are below safe limits in drinking water. Radioactive isotopes leaked from **Fukushima include cesium-134, cesium-137 and iodine-131. Cesium-137 has a longer half-life than cesium-134 and can be found in the ocean as the result of past nuclear tests.**

The scientists are looking to find cesium-134 as it has a half-life of only two years and would be definitive proof of Fukushima radiation reaching North American shores. Cesium-137 has been found in eight testing locations but no evidence of cesium-134, reports LiveScience.

Sample locations being monitored by Woods Hole Oceanographic Institution scientists.  Woods Hole Oceanographic Institution

According to the WHOI plume prediction, Fukushima radionuclides will reach Alaska and British Columbia in early 2014, traveling south along the coast over the course of two years with trace amounts arriving in Hawaii. **WHOI says the levels will be below the safety limit set by the U.S. Environmental Protection Agency.** **The EPA limit for cesium-137 in drinking water is 7,400 Becquerels, the radioactive decay per second, per cubic meter.**

Buesseler said in a statement, "We expect over the rest of 2014, levels will become detectable starting first along the northern coastline. But the complex behavior of coastal currents will likely result in varying intensities and changes that cannot be predicted from models alone."

The radioactive plume has not reached the United States coast yet and experts believe the radiation levels will not pose a threat to humans or to marine life. **The San Francisco Chronicle reports that, based on ocean circulation patterns, the first traces of the Fukushima radiation plume will be seen in April.**

|  |
| --- |
| EDITOR’S COMMENT: Canadian and U.S. citizens are starting to worry about possible adverse implications of contaminated waters. On the other hand, citizens from Mediterranean countries are worrying about possible implications of the destraction of Syria’s chemical weapons into their sea. I only hope that mother Nature is not yet pissed enough with human activities… |



Is it nuclear winter?

**No it is urban pollution in China – 2014…**

# 13 workers contaminated by radiation

Source: http://www.koat.com/news/new-mexico/wipp-13-workers-contaminated-by-radiation/24719308

WIPP officials said that around 5 a.m. Wednesday (Feb 27), they informed 13 workers who tested positive for radiation contamination. Since then, more workers have come forward asking to be tested.  
"We have identified additional employees who were on-site the morning of Feb. 15," said WIPP project manager Farok Sharif. "And we are requesting biological samples from them to determine if they are also affected."

**The 13 workers who tested positive were performing above-ground duties at the WIPP facility on Feb. 14, the day the radiation leak was detected.**

Sharif said in a few days, an attempt will be made to get back into the mine for testing. They will send two probes down the salt-handling shaft to get airborne radiation readings and air quality readings.

From there, officials will attempt to safely fix the leak and bring the facility back to full operation. This could take months.

The U.S. Department of Energy said it will hold the contractor accountable for the leak.

WIPP officials said Thursday it's premature to say what effect the radiation will have on the workers' health and what course of treatment is necessary. Officials said these results are preliminary, and more tests need to be done.

There are about 300 employees on the physical property each day, according to the Department of Energy. About 200 are classified as essential, and they have kept the plant running since the leak.

WIPP opened in 1999. This is the first reported radiation leak at the facility.

WIPP officials reiterated their previous statement that residents of nearby communities are not at risk. Officials said the radiation levels detected were very low. They said the source of the leak could be a container.

The plant is 26 miles east of Carlsbad.

## Islanders’ radiation worries 60 years after Bikini Atoll atomic test

Source: http://www.homelandsecuritynewswire.com/dr20140303-islanders-radiation-worries-60-years-after-bikini-atoll-atomic-test

Sixty years ago, On 1 March 1954 the United States tested a 15-megaton hydrogen bomb – a thousand times more powerful than the bomb dropped on Hsroshima —- at Bikini Atoll, part of the Marshall Islands. The explosion vaporized one island, and exposed inhabitants on neighboring islands to radioactive fallout. **The United States relocated many of the islanders and spent years – and more than $45 million – to clean up and decontaminate the islands, before allowing the relocated inhabitants to return. Many were forced to leave again, however, after they were found to be exposed to residual radiation. From 30 June 1946 to 18 August 1958, the United States conducted 67 atmospheric nuclear tests in the Marshall Islands.**

On 1 March 1954 the United States tested a 15-megaton hydrogen bomb – a thousand times more powerful than the bomb dropped on Hsroshima —- at Bikini Atoll, part of the Marshall Islands. The explosion vaporized one island, and exposed inhabitants on neighboring islands to radioactive fallout. The United States relocated thousands of them to temporary shelters farther away from the test site, and for the following three years, at a cost of $45 million, cleaned up and decontaminated those atolls exposed to radiation.

In 1957 the relocated inhabitant were allowed to return to their homes.

**Thirty years later, in 1985, scientists found out that the cleanup had not been as effective as initially thought, and that many of the inhabitants who returned were exposed to residual radiation.**

Yahoo News reports that Bikini islanders have lived in exile since they were moved for the first weapons tests in 1946. In the early 1970s U.S. government scientists declared Bikini safe for resettlement, and some residents were allowed to return. They were removed again in 1978, however, after ingesting high levels of radiation from eating local foods grown on the former nuclear test site.

The United States has expressed regret about islanders’ exposure to high doses of radiation during the series of nuclear tests.

“While international scientists did study the effects of that accident on the human population unintentionally affected, the United States never intended for Marshallese to be hurt by the tests,” the U.S. embassy in Majuro says on its Web site.

**During the period from 30 June 1946 to 18 August 1958, the United States conducted 67 atmospheric nuclear tests in the Marshall Islands: 43 at Enewetak Atoll, 23 at Bikini Atoll, and one approximately eighty-five miles from Enewetak. The most powerful of those tests was the 1 March 1954 “Bravo” shot, a 15-megaton device detonated at Bikini atoll.**

**From 1945 to 1988, the United States conducted a total of 930 nuclear tests with a combined yield estimated to be 174 megatons. Approximately 137 megatons of that total was detonated in the atmosphere. This means that while the number of tests conducted in the Marshall Islands represents about 14 percent of all U.S. tests, the yield of the tests in the Marshalls comprised nearly 80 percent of the atmospheric total detonated by the United States.**

Despite the cleanup efforts, a 2012 UN report said the effects of those tests were long-lasting.

Special Rapporteur Calin Georgescu, in his report to the UN Human Rights Council, said that “near-irreversible environmental contamination” had led to the loss of livelihoods and many people continued to experience “indefinite displacement.”

**The report called for the United States to provide extra compensation to settle claims by nuclear-affected Marshall Islanders and end a “legacy of distrust.”**

Yahoo News notes that the Nuclear Claims Tribunal awarded more than $2 billion in personal injury and land damage claims arising from the nuclear tests, but stopped paying after a U.S.-provided $150 million compensation fund was exhausted.

# Ukraine says stepping up protection of nuclear plants

Source: http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-iaea-idUSBREA231V820140304

**Ukraine is reinforcing the protection of its nuclear power plants, it told the U.N. atomic watchdog on Tuesday, because of "a grave threat to the security" of the country posed by the Russian military.**

**Ukraine has 15 nuclear power reactors in operation, accounting for nearly 44 percent of its electricity production in 2013**, according to the International Atomic Energy Agency's (IAEA's) website.

Ukraine's envoy to the IAEA said in a letter to IAEA Director General Yukiya Amano: "Illegal actions of the Russian armed forces on Ukrainian territory and the threat of use of force amount to a grave threat to security of Ukraine with its potential consequences for its nuclear power infrastructure."

Ambassador Ihor Prokopchuk's letter, dated March 4, was circulated among delegations attending a week-long meeting of the IAEA's 35-nation governing board in Vienna. It was given to Reuters by a diplomat from another country.

President Vladimir Putin delivered a robust defense of Russia's military intervention in Crimea on Tuesday and reserved the right to use all options to protect compatriots after the overthrow of Ukraine's Russian-backed President Victor Yanukovich, but he said the use of force would be a last resort.

Prokopchuk's letter to Amano, apparently written before Putin's comments, said: "Under these circumstances, the competent authorities of Ukraine make every effort to ensure physical security, including reinforced physical protection of 15 power units in operation at four sites of Ukrainian NPPs (nuclear power plants).

"However, consequences of the use of military force by the Russian federation against Ukraine will be unpredictable."

On Sunday, Ukraine's parliament called for international monitors to help protect its nuclear power plants, as tension mounted with its neighbor.

Prokopchuk urged Amano to "join international efforts in de-escalating the crisis around Ukraine and to urgently raise the issue of nuclear security" with Russia.

Amano said on Monday there were 31 nuclear-related facilities in Ukraine that were being monitored by the IAEA to make sure there was no diversion of material for military purposes, as it does in other countries with nuclear plants.

He said it was the responsibility of individual countries to ensure the security of nuclear power plants.

# B61-12: First Pictures Show New Military Capability

Source: http://blogs.fas.org/security/2014/02/b61-12pictures/#more-6219

The guided tail kit of the B61-12 will create the first U.S. guided nuclear bomb.

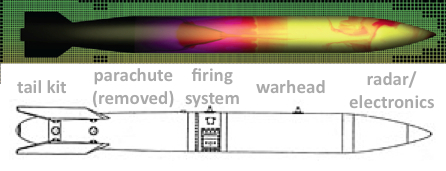
  
The U.S. government has published the first images of the Air Force’s new B61-12 nuclear bomb. The images for the first time show the new guided tail kit that will provide new military capabilities in violation of the Nuclear Posture Review.

The tail kit will increase the accuracy of the bomb and enable it to be used against targets that today require bombs with higher yields.

The guided tail kit is also capable of supporting new military missions and will, according to the former USAF Chief of Staff, affect the way strike planners think about how to use the weapon in a war.

**The new guided weapon will be deployed to Europe, replacing nearly 200 non-guided nuclear B61 bombs currently deployed in Belgium, Germany, Italy, the Netherlands, and Turkey.**

**Military Characteristics**

The images show significant changes to the rear end of the bomb where the tail wing section has been completely replaced and the internal parachute removed. The length of the B61-12 appears to be very similar to the existing B61 (except B61-11 which is longer) although possibly a little bit shorter (see below).

The guided tail kit on the B61-12 (top) is replacing the fixed tail section on the existing B61 (bottom) and the parachute inside.

The new guided tail kit will not use GPS (global positioning system) but is thought to use an Internal Guidance System (INS). **The precise accuracy is not known, but conventional bombs using INS can achieve an accuracy of 30 meters or less.** Even if it were a little less for the B61-12, it is still a significant improvement of the 110-180 meters accuracy that nuclear gravity bombs normally achieve in test drops.

The tail kit will also provide the B61 with a “modest standoff capability” by enabling it to glide toward its target, another military capability the B61 doesn’t have today.

Inside the bomb, non-nuclear components will be refurbished or replaced. In the nuclear explosives package the B61-4 primary (pit) will be reused and the secondary remanufactured. Detonators will be replaced with a design used in the W88 warhead, conventional Insensitive High Explosives will be remanufactured, and a new Gas Transfer System will be installed to increase the performance margin of the primary.

The B61-4 warhead used in the B61-12 has four selectable yields of 0.3, 5, 10, and 50 kilotons. LEPs are not allowed to increase the yield of warheads but GAO disclosed in 2011 that STRATCOM “expressed a requirement for a different yield [and that] U.S. European Command and SHAPE [Supreme Headquarters Allied Powers Europe] agreed to the proposal.” It is unknown if the different yield is a modification of one of the three lower yield options or an increase of the maximum yield. During another upgrade of the B61-7 bomb to the B61-11 earth-penetrator, the yield was increased from 360 kilotons to 400 kilotons.

Although increasing safety and security were prominent justifications for securing Congressional funding for the B61-12, enhancements to the safety and security of the new bomb are apparently modest. More exotic technologies such as multi-point safety and optical detonators were rejected.

The complex upgrades add up to the most expensive U.S. nuclear bomb project ever – currently estimated at approximately $10 billion for 400-500 bombs.

**Political Implications**

Enhancing military capabilities of nuclear weapons (accuracy and yield) is controversial and Government officials in the United States and European capitals are trying to dodge the issue. The 2010 Nuclear Posture Review Report explicitly promised  that “Life Extension Programs…will not support new military missions or provide for new military capability capabilities.” But the guided tail kit is a new military capability and so is a different explosive yield.

Military and government officials will privately admit to the change but the public line is that this is a simple life-extension of the existing B61 with no new military capabilities.

During a recent visit to Europe where I briefed the Dutch and Belgian parliaments on the status and implications of the B61 modernization, parliamentarians were concerned that this kind of clandestine nuclear modernization under the guise of life-extension is unacceptable at the national level and counterproductive at the international level. They said they had not been informed about the upcoming deployment of improved nuclear capabilities in their countries. Their governments’ position is that there is no improvement and therefore no need to inform anyone. But one Dutch government official told me in so many words that they haven’t actually checked but trust the United States would not introduce improved nuclear bombs in Europe without telling the allies. A Dutch parliamentarian said he knew for sure that the improved capability is known within the ministry of defense.

The parliamentarians were also concerned that improving the military capabilities sends the wrong message about NATO’s nuclear policy, in particular its promise to reduce nuclear weapons in Europe and seeking to create the conditions for a world without nuclear weapons. Deploying a new guided nuclear bomb on a new stealthy F-35 fighter-bomber in Europe will make it hard for NATO to argue that Russia should reduce and not improve its non-strategic nuclear posture.

Many NATO countries quietly favor a withdrawal of the U.S. nuclear weapons from Europe but feel hamstrung by NATO policy, which mistakenly confuses generic security concerns of some eastern European allies with a need for nuclear weapons in Europe. The security concerns obviously must be addressed but not with fake assurance by tactical nuclear bombs that are the least likely to ever be used in response to the kinds of security challenges that face Europe today.

**NATO decided in 2012 “that the Alliance’s nuclear force posture currently meets the criteria for an effective deterrence and defense posture.” If so, why enhance it with guided B61-12 nuclear bombs and F-35 stealth fighter-bombers?**

# Greenpeace protests Europe's aging nuclear plants

Source: http://www.ndtv.com/article/world/greenpeace-protests-europe-s-aging-nuclear-plants-491831

Greenpeace activists broke into the grounds of nuclear plants in six European countries on Wednesday, urging governments to close down aging reactors on safety grounds.

Protesters dressed in orange jumpsuits scaled boundary fences at plants in France, Belgium, the Netherlands, Switzerland, Sweden and Spain and hoisted large banners with images of cracking reactors and projected the words "The End" onto walls.

Some 240 activists took part, said Greenpeace, urging governments in a statement to "invest instead in clean and safe energy".

**Of the 151 reactors in Europe, 66 are older than 30 years, 25 older than 35, and seven over 40, the environmental group said.**

This handout picture released by environmental organisation Greenpeace shows activists holding a banner reading "the end" at the Beznau nuclear power plant on March 5, 2015 in Doettingen, northern Switzerland.

The lives of many had already been stretched beyond their initially-intended span, it added.

"The majority is threatening to overshoot their technical design life-time," said Greenpeace nuclear energy spokesman Jan Haverkamp, pointing to the March 2011 disaster at Japan's Fukushima plant, which started operating in 1971.

"The increasing age of the reactors also increases the risks for a nuclear incident and significant economic and environmental damage," Mr. Haverkamp said.

In northern France, 18 protesters entered the Gravelines power plant, which will turn 40 in 2020, at dawn, said Greenpeace.

They claimed to have crossed three security barriers and were approaching reactor No. 6 when they were apprehended.

France's interior ministry insisted the group was arrested within eight minutes of setting foot on the premises, and said their movements were followed from the start.

In Belgium, some 60 activists entered the grounds of the Tihange reactor 80 kilometres (50 miles) southeast of Brussels, and projected the words "The End" onto one of the chimneys, Greenpeace claimed.

Protesters in Borssele in the southern Netherlands also used a film projector to display the message onto a reactor which was built to last 40 years but has been given another 20-year lease on life.  
Twenty-odd protesters in southern Sweden climbed over the fence around the Oskarshamn reactor and erected a banner stating "Time for retirement".

Police told the local news agency TT that 13 activists were arrested for trespassing at the reactor, built in 1972 and initially due to last for 40 years.

Several safety scares had forced its temporary closure in recent years.

Banners announcing "The End" of nuclear power were also erected at the 45-year-old Beznau nuclear plant in northern Sweden, while in Spain, about 30 activists with construction vehicles reenacted the dismantling of the Garona plant erected in 1971.

A dozen protesters used trucks to block the entrance to the Bugey nuclear station in eastern France, which will turn 40 in 2018.

|  |
| --- |
| EDITOR’S COMMENT: I am not sure anymore about what scares me most: Old over-aged nuclear reactos or placid security around top targets? |

# A primer: Military nuclear wastes in the United States

**By Robert Alvarez**

Source: http://thebulletin.org/primer-military-nuclear-wastes-united-states

Research, development, testing, and production of US nuclear weapons occurred at thousands of sites in nearly every state, as well as Puerto Rico, the Marshall Islands, Johnston Atoll, and Christmas Island in the Pacific. Between 1940 and 1996, the United States spent approximately $5.8 trillion dollars to develop and deploy nuclear weapons. As a result, the nuclear weapons program created one of the largest radioactive waste legacies in the world—rivaling the former Soviet Union's.

US nuclear weapons sites—many of them under the aegis of the Energy Department—constitute some of the most contaminated zones in the Western hemisphere, and attempts to remediate those sites are now approaching their fifth decade. It is the most costly, complex, and risky environmental cleanup effort ever undertaken, dwarfing the cleanup of Defense Department sites and the Environmental Protection Agency’s Superfund program. **Long-term liability estimates range from approximately $300 billion to $1 trillion.** Site remediation and disposition of radioactive detritus are expected to continue well into this century. After that, long-term stewardship of profoundly contaminated areas will pose a challenge spanning hundreds of centuries.

**Research, development, testing and production of nuclear weapons by the United States created:**

* More than 3 billion metric tons of uranium mining and milling wastes.
* More than 1 million cubic meters of transuranic radioactive wastes.
* Approximately 6 million cubic meters of low-level radioactive wastes.
* Approximately 4.7 billion cubic meters of contaminated soil and groundwater (according to an Energy Department document unavailable online).
* More than 10,000 radiation-contaminated structures such as uranium processing and enrichment plants, radiochemical processing and storage facilities and laboratories.
* About 100 million gallons of high-level radioactive wastes, considered among the most dangerous, left in aging tanks larger that most state capitol domes. More than a third of some 200 tanks have leaked and threaten groundwater and waterways such as the Columbia River.
* Areas contaminated by more than 1,054 nuclear weapons tests, 219 of which involved aboveground detonations. As of 1992, underground shots released about 300 million curies of radioactive materials at the Nevada Test Site—making it the most radioactively contaminated area in the United States. Areas in the Republic of the Marshall Islands remain uninhabitable from US aboveground tests in the 1940s and 1950s.
* More than 700,000 metric tons of excess nuclear weapons production materials, in addition to hundreds of tons of weapons-usable plutonium and highly enriched uranium.

The human health legacy of the US nuclear weapons program is also quite significant. As of February 2014, more than 100,000 sick nuclear weapons workers have received more than $10 billion in compensation following exposure to ionizing radiation and other hazardous materials.

**Even today, the radioactive waste from the dawn of the nuclear age remains a significant challenge to public health in highly populated areas.** **For instance,** in 1973 a large amount of uranium processing wastes, generated to make the first nuclear weapons at the Mallinckrodt Chemical Works in St. Louis, was illegally dumped in a municipal landfill in a nearby suburb.  The landfill is experiencing the latest of at least two subsurface fires over the past 21 years and lies on a floodplain approximately 1.2 miles from the Missouri River.

The dump contains the largest single amount of thorium 230 in the country and possibly the world. With a half-life of more than 75,000 years, it is comparable in toxicity to plutonium. Even though these concerns were repeatedly raised with the US Environmental Protection Agency, the agency issued a Record of Decision in 2008 that allows for “in place disposal” of these wastes, subject to institutional controls and with a cap over radiologically contaminated areas. Lost in this process is an important warning by a panel of the National Academy of Sciences in 2000 that "engineered barriers and institutional controls—are inherently failure prone.”

The radiological legacy of nuclear weapons will be with us for a very long time.

*A senior scholar at the Institute for Policy Studies,* ***Robert Alvarez*** *served as senior policy adviser to the Energy Department's secretary and deputy assistant secretary for national security and the environment from 1993 to 1999. During this tenure, he led teams in North Korea to establish control of nuclear weapons materials. He also coordinated the Energy Department's nuclear material strategic planning and established the department's first asset management program. Before joining the Energy Department, Alvarez served for five years as a senior investigator for the US Senate Committee on Governmental Affairs, chaired by Sen. John Glenn, and as one of the Senate’s primary staff experts on the US nuclear weapons program. In 1975, Alvarez helped found and direct the Environmental Policy Institute, a respected national public interest organization. He also helped organize a successful lawsuit on behalf of the family of Karen Silkwood, a nuclear worker and active union member who was killed under mysterious circumstances in 1974. Alvarez has published articles in* Science*, the* Bulletin of Atomic Scientists*,* Technology Review*, and* The Washington Post*. He has been featured in television programs such as* NOVA *and* 60 Minutes*.*

# Ukraine crisis sends a terrible message about nuclear weapons

Source: http://www.heraldscotland.com/comment/letters/ukraine-crisis-sends-a-terrible-message-about-nuclear-weapons.23633111

The US, UK and Russia guaranteed the territorial integrity of Ukraine as part of the "deal" in which Ukraine, then possessing one of the world's largest nuclear arsenals, agreed to give up its weapons of mass destruction.

**Can anyone believe that the current situation would exist were Ukraine still to possess even some of those nuclear weapons?** Surely the sad result of the current situation is that any nation with - or about to get - nuclear weapons will learn the lesson and refuse to believe the promises of the "big powers" when it comes to nuclear weapons and national security. The agreement appears to be as meaningless (because Russia doesn't honour it and the US/UK are unwilling/unable to sustain it) as Franco-British guarantees to Poland or Czechoslovakia in the 1930s.

Nations around the world will conclude that the only sure way to protect themselves from Big Power aggression would be to possess WMDs. What an appalling outcome for which we've no-one to blame but ourselves.

**Professor William G Naphy,**

1 Calsayseat Road,

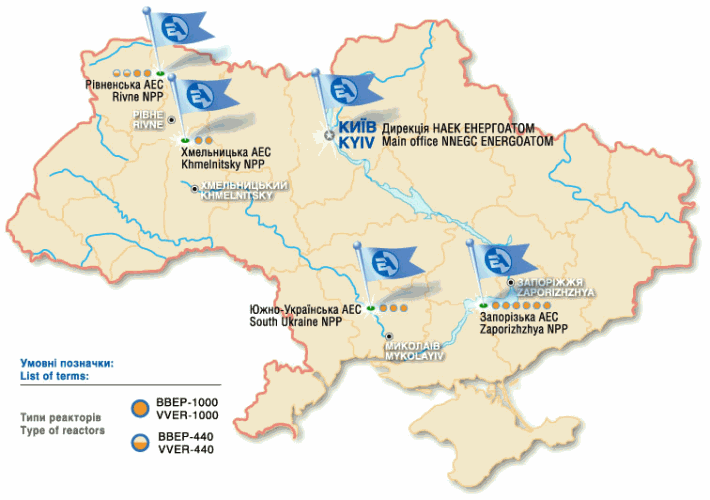
Aberdeen.

# Nuclear Power in Ukraine

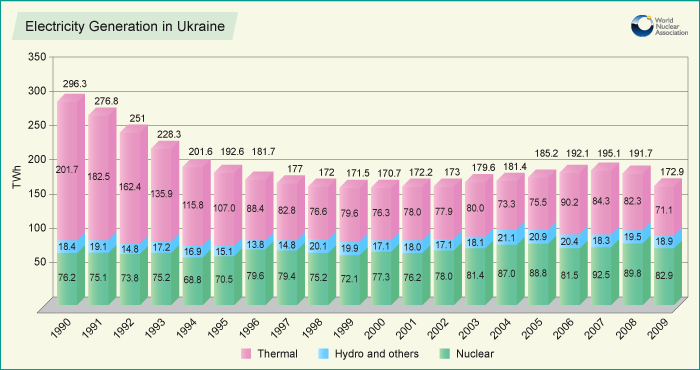
(Updated January 2014)

Source: http://www.world-nuclear.org/info/Country-Profiles/Countries-T-Z/Ukraine/

A large share of primary energy supply in Ukraine comes from the country's uranium and substantial coal resources. The remainder is oil and gas, mostly imported from Russia. In 1991, due to breakdown of the Soviet Union, the country's economy collapsed and its electricity consumption declined dramatically from 296 billion kWh in 1990 to 170 in 2000, all the decrease being from coal and gas plants. Today Ukraine is developing shale gas deposits and hoping to export this to western Europe by 2020 through the established pipeline infrastructure crossing its territory from the east.

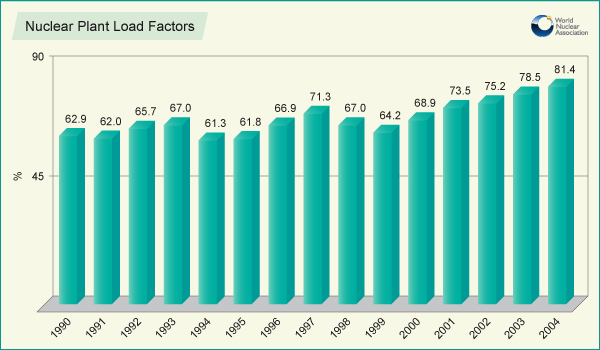
Total **electricity production** in 2009 amounted to 173 billion kWh, with 4 billion kWh net exports, and total capacity is over 52 GWe. In 2009, 41% of power came from coal and gas (approx 20% gas), 48% from nuclear (82.9 TWh) and 7% from hydro, according to the Ministry of Fuel and Energy. In 2009, 77.9 billion kWh net came from nuclear, according to IAEA. Nuclear plant comprises 26.6% of capacity, hydro 9.3%.

A major increase in electricity demand to 307 billion kWh per year by 2020 and 420 billion kWh by 2030 is envisaged, and government policy was to continue supplying half of this from nuclear power. This would have required 29.5 GWe of nuclear capacity in 2030, up from 13.9 GWe (13.2 GWe net) now.

In mid 2011 the Ukraine energy strategy to 2030 was updated, and in the electricity sector nuclear power's role was emphasized, with improved safety and increased domestic fuel fabrication. In mid-2012 the policy was gain updated, and 5000 to 7000 MWe of new nuclear capacity was proposed by 2030, costing some $25 billion.

## Nuclear industry development

Nuclear energy development started in 1970 with construction of the Chernobyl power plant, the first unit being commissioned in 1977.

Though the Ukrainian nuclear industry was closely involved with Russia for many years, it remained relatively stable during the changes that occurred when the country became independent of the former Soviet Union. In fact, during that period and since, there have been continuing improvements in the operational safety and output levels of Ukraine's nuclear reactors.

Ukraine's 15 nuclear power units at four nuclear power plants are operated by Energoatom, the country's nuclear power utility. Following the addition of two new VVER-1000 reactors in 2005, capacity increased to 13,168 which was 26.3% of the country’s total installed capacity. Energoatom expects nuclear to retain its contribution of 50-52% of Ukraine's electricity in 2020.

All are Russian VVER types, two being 440 MWe V-312 models and the rest the larger 1000 MWe units – two early models and the rest V-320s.

Power reactors have operated in Ukraine since 1977, and over 300 reactor years of operating experience have been accumulated. Load factors have increased steadily and reached 81.4% in 2004. A decrease of the country's load factor after 2005 is related to restrictions imposed by the national electricity grid. Early in 2010 it was at 73%. "Operational disturbances" at nuclear plants dropped from 71 in 1999 to 21 in 2009.

At the end of 1995 Zaporozhe unit 6 was connected to the grid making Zaporozhe the largest nuclear power station in Europe, with a net capacity of 5718 MWe. (The second largest station operating is Gravelines, near Dunkerque in France, with a net capacity of 5460 MWe.)

In August and October 2004 Khmelnitsky 2 and Rovno 4 respectively were connected to the grid, bringing their long and interrupted construction to an end and adding 1900 MWe to replace that lost by closure of Chernobyl 1&3 in 1996 and 2000 respectively. They were completed by Energoatom using a consortium of Framatome ANP and Atomstroyexport. See fuller account of K2-R4 in Appendix below.

In 1990 construction of three reactors (units 2-4) at Khmelnitski had been halted, though the site infrastructure for all four units was largely complete. Unit 3 was (and is) 75% complete, unit 4: 28% complete. These have been maintained to some extent since. An intergovernmental agreement with Russia on completing the two units was signed in mid-2010 and a contract with Atomstroyexport was signed in February 2011. Ukraine was hoping to sign a loan agreement for them late in 2012 and resume construction soon after.

**Ukraine power reactors operating**

| **Reactor** | **Type V=PWR** | **MWe net** | **Commercial operation** | **Scheduled close,**  **likely close** |
| --- | --- | --- | --- | --- |
| **Northwest:** |  |  |  |  |
| **Khmelnitski 1** | V-320 | 950 | Aug 1988 | 2018, 2032 |
| **Khmelnitski 2** | V-320 | 950 | Aug 2005 | 2035, 2050 |
| **Rivne/Rovno 1** | V-213 | 402 | Sep 1981 | 2030 |
| **Rivne/Rovno 2** | V-213 | 416 | Jul 1982 | 2031 |
| **Rivne/Rovno 3** | V-320 | 950 | May 1987 | 2017, 2032 |
| **Rivne/Rovno 4** | V-320 | 950 | late 2005 | 2035, 2050 |
| **South:** |  |  |  |  |
| **South Ukraine 1** | V-302 | 950 | Oct 1983 | 2023, 2033 |
| **South Ukraine 2** | V-338 | 950 | Apr 1985 | 2015, 2030 |
| **South Ukraine 3** | V-320 | 950 | Dec 1989 | 2019, 2034 |
| **Zaporozhe 1** | V-320 | 950 | Dec 1985 | 2015, 2030 |
| **Zaporozhe 2** | V-320 | 950 | Feb 1986 | 2016, 2031 |
| **Zaporozhe 3** | V-320 | 950 | Mar 1987 | 2017, 2032 |
| **Zaporozhe 4** | V-320 | 950 | Apr 1988 | 2018, 2033 |
| **Zaporozhe 5** | V-320 | 950 | Oct 1989 | 2019, 2034 |
| **Zaporozhe 6** | V-320 | 950 | Sep 1996 | 2026, 2041 |
| Total (15) |  | 13,168 MWe net (13,835 MWe gross – Energoatom May 2010) | | |

## Life extension and upgrades

Original design lifetime of the Russian reactors was 30 years. Energoatom initially planned to extend the lifetimes of Rovno 1 & 2 and South Ukraine 1 by 15 years and final checking of the pressure vessels (for embrittlement) and the internals of all three units was in 2008-9. A 20-year extension of the operating licences for Rovno 1&2 was granted by the State Nuclear Regulatory Inspectorate of Ukraine (SNRI or SNRC) in December 2010. Energoatom said that more than US$ 300 million had been invested in upgrading the two units since 2004, in collaboration with IAEA. Energoatom has said that Rovno 1&2 are pilot facilities and that it plans to extend all reactor lifetimes similarly. In mid-2012 it announced that the 11 oldest 1000 MWe reactors are to have 20-year life extensions by 2030. In February 2013 the SNRI said that South Ukraine 1 could have life extension after a major upgrade during 2013, and in October it approved plans for a ten-year extension to 2023.

In March 2013 the European Bank for Reconstruction & Development (EBRD) announced a EUR 300 million loan for comprehensive reactor safety upgrading to the end of 2017, matching EUR 300 million from Euratom. The EUR 1.4 billion project will include up to 87 safety measures addressing design safety issues comprising the replacement of equipment in safety relevant systems, improvements of instrumentation and control for safety relevant systems and the introduction of organisational improvements for accident management.

The life extension program is being challenged under the UN Convention on Environmental Impact Assessment in a Transboundary Context – informally known as the Espoo Convention – which has been ratified by 44 countries and the EU. The convention comes under the Economic Commission for Europe and the challenge is on the basis of inadequate environmental assessment.

Ukraine's best-known nuclear power plant was Chernobyl (Chornobyl in Ukrainian). This had the only RBMK type reactors in the country. Unit 4 was destroyed in the 1986 accident, unit 2 was shut down after a turbine hall fire in 1991, unit 1 was closed in 1997 and unit 3 closed at the end of 2000 due to international pressure.

Interruptions in natural gas supply from Russia in January 2006 sharply focused attention on the need for greater energy security and the role of nuclear power in achieving this. A nuclear power strategy involving building and commissioning 11 new reactors with total capacity of 16.5 GWe (and 9 replacement units totaling 10.5 GWe) to more than double nuclear capacity by 2030 was approved by the government in 2006 to enhance Ukraine's energy independence. See Table below.

## Increasing nuclear power capacity

The 2006 strategy envisaged completing **Khmelnitski 3&4,** which were respectively 75% and 28% complete when work stopped in 1990. The government announced in September 2008 that construction on these would resume in 2010 for completion in 2016 and 2017. These completion dates were reaffirmed in mid-2010 and in the mid-2011 energy policy update. In February 2011 it signed a framework contract for construction with Atomstroyexport for AES-92 plants with V-392B reactors similar to those already on the site. In June 2010 an intergovernmental agreement was signed, under which Russia will largely finance the project. Some 85% of the UAH 40 billion (EUR 3.7 billion) project is to be financed through a Russian loan, with 15% funding coming from Ukraine. The loan is to be repaid within five years after the reactors go into service. In July 2012 the government confirmed the feasibility, costings and timing of the project – $4.9 billion total. The loan agreement was expected to be finalized by the end of 2012. At the end of 2013 the energy minister said that construction might resume in 2015.

It was earlier expected that an international tender would open up the choice of technology and in March 2008 Areva, Westinghouse and South Korean suppliers were invited to bid, along with Atomstroyexport and Skoda – all involving pressurized water (PWR) types. In the event only Atomstroyexport and Korea HNP submitted bids, with the former being chosen.

**Ukraine power reactor construction, planned and proposed** (all PWR type)

| Reactor | Type V=PWR | MWe gross | Start construction | Start operation |
| --- | --- | --- | --- | --- |
| **Khmelnitski 3** | V-392 | 1000 | 9/85, 2015? | 2019? |
| **Khmelnitski 4** | V-392 | 1000 | 6/86, 2015? | 2019? |
| **New 1** |  | 1200 | ? | 2020 |
| **New 2** |  | 1200 | ? | 2020 |
| **Replacement 1** |  | 1000 | 2021 | 2026 |
| **Replacement 2** |  | 1000 | 2022 | 2027 |
| **Replacement 3** |  | 1200 | 2024 | 2030 |
| **Replacement 4** |  | 1000 | 2027 | 2033 |
| **Replacement 5** |  | 1000 | 2027 | 2033 |
| **Replacement 6** |  | 1000 | 2028 | 2034 |
| **Replacement 7** |  | 1200 | 2027 | 2033 |
| **Replacement 8** |  | 1200 | 2028 | 2034 |
| **Replacement 9** |  | 1000 | 2029 | 2035 |
| **Total (13)** |  | 14,000 MWe | | |

In the WNA reactor Table, K3&4 are "planned", the other 11 (12,000 MWe) "proposed".

The mid-2011 energy policy revision proposes 2300 MWe of new capacity with decision on technology to be after 2015. Following this there will be a need for replacing plants which are decommissioned in the 2030s. Energoatom proposes to select a standard PWR (or possibly Candu) design from among leading vendors for the remaining planned units after Khmelnitsky 3&4. This will involve consideration of local content in the plants. While Russian VVER technology is the most obvious fit, Energoatom's Atomproektengineering division provided a feasibility study recommending making provision for use of CANDU EC-6 reactors to the Ministry in October 2010.

Chigirin on the Tyasmyn River in the southern Cherkassy Region is proposed as one site for a new nuclear plant.

In connection with the South Ukraine nuclear power plant, the South Ukraine Power Complex also consists of the 11.5 MWe Olexandrivka Hydro Power Plant on the river Pivdenny Buh, generating annually over 25 million kWh; and the 2 x 150 MWe Tashlyk Hydro Pumped Storage Power Plant commissioned in 2006-07, with total annual production of 175 million kWh. A third unit is due to be commissioned here in 2011, and three more re planned from 2015. The hydro units of the South Ukraine Power Complex belong to the country's nuclear utility Energoatom, and they serve as an important regulation of the peak capacity for load-following.

Energoatom has been planning to raise its electricity tariff in order to finance reorganization of the nuclear fuel cycle complex and to implement safety modernizations at all plants. The nuclear tariff is expected to rise further by 2015 to enable funding of life extensions and construction of new plants.

In February 2010 Energoatom signed a cooperation agreement with China Guangdong Nuclear Power Co (CGNPC) relating to nuclear power plant design, construction, operation and maintenance.

## Uranium resources and mining

Ukraine has modest recoverable resources of uranium - 225,000 tU according to IAEA Red Book 2011, 62,000 tU of these recoverable at under $80/kgU, and 131,000 tU according to the Energy Ministry. Uranium mining began in 1948 at Pervomayskoye, and 65,000 tU have been produced so far. Current production is about 1000 tU/yr (960 tU in 2012, 922 tU in 2013). VostgGOK expects increased production in 2014.

The Vostochny Gorno-Obogatitel’niy Kombinat (VostGOK), Eastern Mining and Processing Enterprise or Skhidniy Gorno-Zdobychuval’nyi Kombinat (SkhidGZK in Ukrainian, or Skhidniy HZK) had been producing up to 830 tonnes of uranium per year - around 30% of the country's requirements. This is from several deposits – Ingulskaya and Smolinskaya – at Zheltye Vody or Zhovti Vody (Ukr) in Dnepropetrovsk region, and Safonovskoye in Nikolaev region. The main undeveloped deposit is said to be Mikhailovskoye in Kirovograd region. In both these regions mineralization occurs in metasomatic deposits up to 1300 metres deep. At Ingulskaya block leaching is undertaken, and a heap leach for low-grade ore has been set up at Smolinskaya, where beneficiated ore from radiometric sorting is railed to the central mill. VostGOK is also operating the Vatutinskoye, Central and Michurinskoye underground mines west of Zheltye Vody. Typical grade from these mines in metasomatic deposits is 0.1%U.

Ore is railed 100 to 150 km to the central mill and hydrometallurgical plant at Zheltye Vody. The plant was built in 1958, rebuilt in the 1970s, and is due for further refurbishment. A UAH 400 million ($50 million) reconstruction of the hydrometallurgical plant is planned. VostGOK also plans a heap leach facility at Novokonstantinovskoye to treat one third of its ore, but the high-grade material from there will be railed east to these central facilities.

The **Novokonstantinovskoye** uranium project in the Kirovohrad region was being developed independently of VostGOK by the Novokonstantinov uranium development company, to produce up to 1500 t/yr by 2013, and 2500 t/yr eventually. This is claimed to be the largest uranium deposit in Europe, and 93,600 tU resources at 0.14% are quoted (100,000 tU in a 2013 report). Ceremonial first production was in August 2008, but development then languished. Three levels have been opened up at 680 to 1090 metres depth. Russia's Rosatom had said it was keen to invest in developing the project, but agreement on equity was not reached. The government was seeking partners to help fund the $820 million development cost, but after becoming impatient with disputes, it legislated to put the project under VostGOK from December 2009.\* In October 2010 VostGOK announced that production would commence in 2011, ramping up towards 1050 tU/yr. Russian overtures were again rejected. First production was in June 2011, with 99 tU projected to end of year. Production in 2012 was expected to be 180-190 tU, and then 424 tU in 2013, 760 tU in 2014, 1270 tU in 2015, and 2100 tU in 2017. VostGOK is aiming to invest over UAH 6 billion ($736 million) to develop the Novokonstantinovskoye mine, but financing this depends on securing long-term sales contracts with NAEC Energoatom.

\* This edict was canceled in February 2010, and the regional Public Utility Company Nedra Kirovogradshchiny was then to take over responsibility. However, this was reversed in September, and the project reverted to VostGOK.

In June 2009 VostGOK announced that it planned to develop the Safonovskoye deposit in Kazankovsky District of Nikolaev Region, northwest Ukraine, using in situ leaching (ISL) to produce 100-150 tU/yr from 2011 in a sandstone deposit. A year later the target date was 2012, with 50 tU, reaching 150 tU/yr in 2014. This deposit had been mined with acid leaching to 1983, but mining was discontinued for environmental reasons.

In 2009 VostGOK continued re-treatment of tailings at Smolinskaya mine, and the same is planned for Ingulskaya mine, both for uranium recovery and environmental reasons.

Ukraine is giving priority and investing heavily to boost uranium production and this involves opening the way for foreign investment. It expects to produce 890 tU/yr in 2011 and hopes to fully satisfy its domestic demand of up to 1880 tU/yr by 2015. Projections to 2020 showed fairly steady production from existing mines at about 800 tU/yr, about 2500 tU/yr from Novokonstantinovskoye, and about 1500 tU/yr from new mines. A further target is 6400 tU/yr by 2030.

Australian-based Uran Ltd had agreed with Ukraine's Ministry of Fuel & Energy and VostGOK to carry out a feasibility study for ISL mining of the small Surskoye and Novogurevskoye uranium deposits in the east of the country, near VostGOK's existing operations. However, in 2008 Uran abandoned the prospect.\*

\* The agreements set out terms under which Uran might enter into a Joint Venture over the two sedimentary deposits in the Dnipropetrovsky region. However, in September 2009 the company said that "Following on the repeated failure of the Ukrainian uranium mining enterprise VostGOK to honour a number of agreements with Uran, a decision was made in 2008 to abandon our activities in Ukraine, at least until a more settled and effective political process is established." In 2011 it listed no Ukraine project.

Ukraine also has zirconium resources, and supplies zirconium to Russia.

There are legacy issues with former uranium mining and processing, particularly at the Pridniprovsky Chemical Plant (PHZ) at Dniprodzerzhinsk, not far from the Dnipro River. Nine tailings dams containing 42 million tonnes of mine tailings and 4 PBq of activity and derelict production facilities from operations over 1948-91 are the subject of a large-scale remediation program. PHZ processed ores from the Michurinskoye deposit (near Kirovograd), phosphate ores of the Melovoye deposit (near Shevchenko, now Aktau, Kazakhstan) and raw concentrate from GDR, Hungary and Bulgaria.

## Fuel cycle

Ukrainian uranium concentrate and zirconium alloy are sent to Russia for fuel fabrication. The nuclear fuel produced from these Ukrainian components by TVEL in Russia then returns to Ukrainian NPPs.

The country depends primarily on Russia to provide other nuclear fuel cycle services also, notably enrichment. In June 2007 Ukraine agreed to investigate joining the new International Uranium Enrichment Centre (IUEC) at Angarsk, in Siberia, and to explore other areas of cooperation in the nuclear fuel cycle and building power reactors in other countries. Late in 2008 it signed an agreement for Ukraine's Nuclear Fuel holding company to take a 10% stake in the IUEC based at Angarsk, and in October 2010 this came into effect. Ukraine’s State Concern Nuclear Fuel apparently sells natural uranium to IUEC, which enriches it at Russian plants. Then IUEC sells the enriched uranium to the Fuel Company TVEL, which fabricates fuel assemblies and supplies them to NAEC Energoatom. The first commercial supply was in November 2012 and the next is expected in 2013. The contracted volume is reported to be 60,000 SWU/yr, proportional to the Ukrainian shareholding. Ukraine requires about 1.96 million SWU/yr overall.

In order to diversify nuclear fuel supplies, Energoatom started implementation of the Ukraine Nuclear Fuel Qualification Project (UNFQP). The Project assumed the use of US-manufactured fuel in the VVER-1000 following the selection of Westinghouse as a vendor on a tender basis. In 2005, South Ukraine's third unit was the country's first to use the six lead test assemblies supplied by Westinghouse, which were placed into the reactor core together with Russian fuel for a period of pilot operation. A reload batch of 42 fuel assemblies was provided by Westinghouse in mid-2009 for a three-year period of commercial operation at the unit with regular monitoring and reporting. In addition to the initial supply of fuel from Westinghouse, other aims of the project included the transfer of technology for the design of nuclear fuel.

However, in June 2010, Energoatom signed a long-term fuel supply contract with Russia's TVEL for all 15 reactors. Earlier, Rosatom had offered a substantial discount to Ukraine if it signed up with TVEL for 20 years. TVEL and Westinghouse both bid to build a fuel fabrication plant in Ukraine, and in September 2010 the Ministry of Fuels & Energy selected TVEL. The state-owned holding company Nuclear Fuel signed an agreement with TVEL for a 50-50 joint venture to build a plant to manufacture VVER-1000 fuel assemblies. The US$ 295 million plant is now under construction at Smolino, Kirovograd region, to produce about 400 fuel assemblies (200 tU) per year from 2013. Russia has agreed to transfer fuel fabrication technology by 2020. The site is near Smolinskaya uranium mine. In December 2011 the private joint-stock company Nuclear Fuel Production Plant (NFPP) was set up and will start supplying fuel in 2016. The first phase to 2015 sets up capacity for fabrication of fuel rods and assemblies, the second phase to 2020 involves production of fuel pellets.

An attempt was made in the 1990s to set up a complete suite of fuel cycle facilities other than enrichment, but this failed for political and financial reasons. The December 2006 decision to form Ukratomprom revived intentions to build a fuel fabrication plant. Ukraine has been seeking cooperation with other countries which have experience in the nuclear fuel cycle as a part of its effort to increase its supply of low-cost nuclear electricity and to reduce its imports of natural gas and other energy sources from Russia. In December 2005 Ukraine and the EU signed an energy cooperation agreement which links the country more strongly to western Europe in respect to both nuclear energy and electricity supply.

Tenders were called for a fuel fabrication plant, and in September 2010 Russia’s TVEL was chosen over Westinghouse to build a $212 million plant. One condition is that Ukraine holds a controlling stake in the joint venture company that is to be established to manage the plant, despite relying on TVEL to provide most of the funds to construct it. Another condition is the requirement for the transfer of technology for the manufacture of fuel assemblies under a non-exclusive licence by 2020, for reactors both in Ukraine and abroad. Construction is due to start in mid 2014, with commissioning in 2015. It is assumed that from 2016 the plant will cater all nuclear fuel needs of Ukraine’s nuclear power plants, while surplus products will be exported under separate arrangements with TVEL. The plant is to be doubled in size by 2020.

In May 2008 Ukraine's Ministry of Fuels and Energy signed an agreement with Atomic Energy of Canada Ltd (AECL) to develop CANDU technology. This could provide synergies with the existing Ukrainian VVER reactors by burning uranium recovered from the VVERs' used fuel. (Such recycled uranium has fissile content similar to natural uranium and can be directly used in CANDU reactors). The technology concerned involves either reprocessing or DUPIC – Direct Use of spent PWR fuel In Candu reactors. This has long been mooted by AECL, but is further ahead in South Korea than elsewhere due to their mix of PWR and CANDU reactor technologies. (Use of reprocessed uranium in CANDU reactors is being trialled in China.)

## Radioactive Waste Management

There is no intention to close the fuel cycle in Ukraine, though the possibility remains under consideration. In 2008 the National Target Environmental Program of Radioactive Waste Management was approved. Storage of used fuel for at least 50 years before disposal remains the policy. The new program meets the requirements of European legislation and recommendations of the International Atomic Energy Agency (IAEA) and the European Atomic Energy Community (Euratom). Its implementation will create an integrated system of radioactive waste of all types and categories for 50 years.

Used fuel is mostly stored on site though some VVER-440 fuel is again being sent to Russia for reprocessing. At Zaporozhe a long-term dry storage facility for spent fuel has operated since 2001, but other VVER-1000 spent fuel is sent to Russia for storage, at a cost to Ukraine of over $100 million per year. A centralised dry storage facility for spent fuel was proposed for construction in the government's 2006 energy strategy.

In December 2005, Energoatom signed a US$ 150 million agreement with the US-based Holtec International to implement the Central Spent Fuel Storage Project for Ukraine's VVER reactors. Holtec's work involves design, licensing, construction, commissioning of the facility, and the supply of transport and vertical ventilated dry storage systems for used VVER nuclear fuel, initially 2500 VVER-1000 and 1100 VVER-440 assemblies. This was projected for completion in 2008, but was held up pending legislation. Then in October 2011 parliament passed a bill on management of spent nuclear fuel, and this was approved in the upper house in February 2012. It provides for construction of the dry storage facility within the Chernobyl exclusion area, between villages Staraya Krasnitsa, Buryakovka, Chistogalovka and Stechanka in Kiev Region. The storage facility will become a part of the common spent nuclear fuel management complex of the state-owned company Chernobyl NPP. The total storage capacity of the facility will be 16,529 VVER-440 and VVER-1000 fuel assemblies, and expected to cost $460 million, including 'start-up complex' $160 million. Stage 1 for 3600 fuel assemblies is due to open in 2015.

Used fuel from decommissioned RBMK reactors at Chernobyl is stored, and a new dry storage facility is under construction there. In September 2007 Holtec International and the Ukrainian government signed a contract to complete the placement of Chernobyl's used nuclear fuel in dry storage systems (ISF-2). Removing the radioactive fuel from the three undamaged Chernobyl reactors is essential to the start of decommissioning them. Holtec will complete the dry storage project, begun in 1999 by French Framatome, and plans to use as much of the previous work on the project as possible, with the protection of public health and safety as the overriding criteria. The project is estimated to be worth EUR 200 million (US$ 269 million) and is expected to be completed in mid 2014. There is full endorsement from the Assembly of Donors, who provide funding for Chernobyl remediation and decommissioning.

Also at Chernobyl, Nukem has constructed an Industrial Complex for Radwaste Management (ICSRM) which was handed over in April 2009. In this, solid low- and intermediate-level wastes accumulated from the power plant operations and the decommissioning of reactor blocks 1 to 3 is conditioned by incineration, high-force compaction, and cementation, as required and then packaged for disposal. In addition, highly radioactive and long-lived solid waste is sorted out for temporary separate storage. A low-level waste repository has also been built at the Vektor complex 17 km away.

In 2013, a four-year Ukraine-NATO project began to clean up low-level radioactive waste at nine military facilities in the country. EUR 25 million was budgeted. The wastes will be buried in the Chernobyl exclusion zone.

From 2011, high-level wastes from reprocessing Ukrainian fuel was to be returned from Russia to Ukraine and go to the central dry storage facility.

Preliminary investigations have shortlisted sites for a deep geological repository for high- and intermediate-level wastes including all those arising from Chernobyl decommissioning and clean-up.

A new facility for treatment solid radioactive waste is under construction at the site of Zaporozhe nuclear power plant, to be commissioned in 2015. It will be fitted with a state-of-the-art incinerator of Danish design.

## Decommissioning

Four Chernobyl RBMK-1000 reactors, plus two almost-completed ones, are being decommissioned. Unit 4, which was destroyed in the 1986 accident, is enclosed in a large shelter and a new, more durable containment structure is to be built by 2015.

This shelter project will be funded by the International Chernobyl Shelter Fund facilitated by the EBRD and is expected to cost about EUR 1.2 billion, more than two thirds of which has now been pledged. In September 2007 a EUR 430 million contract was signed with a French-led consortium Novarka to build this new shelter, to enclose both the destroyed Chernobyl-4 reactor and the hastily-built 1986 structure over it. It will be a metal arch 110 metres high and spanning 257 m, which will be built adjacent and then moved into place.

In May 2005, international donors made pledges worth approximately EUR 150 million towards the new confinement shelter. The largest contribution, worth more than EUR 130 million, came from the G8 and the EU. Russia contributed to the fund for the first time and other fund members, which include the USA, increased their contributions, with the Ukrainian government pledging some EUR 15 million. The European Commission has committed EUR 239.5 million since 1997, making it the main donor.

Units 1-3 are undergoing decommissioning conventionally – the first RBMK units to do so – and work will accelerate when the new dry storage facility for fuel is built (see Waste Management above).

## R&D

Ukraine has two research reactors, a very small one at the naval Engineering school and a 10 MW tank type one – VVR-M – which was commissioned in 1960 at the Institute for Nuclear Research in Kiev. This is due to close in 2015 and plans for a $250 million replacement were announced in 2008.

In 2012 the government approved construction of a subcritical neutron source at the Kharkov Institute of Physics and Technology, using LEU. The USA will provide technical assistance and $25 million towards it. The facility is planned to start up in 2014. It is intended for research in nuclear physics as well as isotope production, particularly for nuclear medicine.

## Organisation

In 1996 the former nuclear operating entity Goskomatom spawned a new corporate nuclear utility, Energoatom. Then Goskomatom was replaced by two Departments within the Fuel & Energy Ministry: a Department for Nuclear Energy, responsible for civil nuclear power plants operation, and a Department for Atomic Industry, responsible for the development of nuclear fuel cycle. Energoatom's current priorities are to increase safety, bring load factors up to 83-85%, and extend the working lives of the reactors by 10-15 years (at about US$ 150 million per VVER-1000 reactor).

The regulator is the State Nuclear Regulatory Inspectorate of Ukraine (SNRI or SNRC), now an independent authority (it was until 2001 under the Ministry of Environment Protection & Nuclear Safety).

The 1995 law on Nuclear Energy Use and Radiation Safety establishes the legal basis of the industry and included a provision for the operating plant to have full legal responsibility for the consequences of any accident. The 1995 law on Radioactive Waste Management complements this, and the consequent state program was approved in 2002.

## Nuclear industry structure and the Russian connection

Late in 2006 the government moved to set up a new national nuclear industry entity - Ukratomprom, as a vertically-integrated nuclear holding company reporting to Energy Ministry and cabinet. Ukratomprom was to consist of six state-owned enterprises including Energoatom, the VostGOK uranium mining company, and the Novokonstantinov uranium development company, with assets of some US$ 10 billion, including $6.35 billion for Energoatom. Three major projects were to be launched in 2007, including a $1875 million uranium production venture comprising refurbishment of VostGOK's hydrometallurgical plant and construction of a uranium mill at Novokonstantinov. Then it was announced that Energoatom would not be included in Ukratomprom, and soon afterwards plans were abandoned.

Russia has made strenuous efforts to regain its influence in Ukraine, and early in 2010 various proposals for civil nuclear joint ventures were put forward. In April the Russian president suggested "full-scale cooperation of our nuclear industries," and that the two countries establish a large holding company that would include power generation, heavy engineering and fuel cycle facilities. As a first stage, he suggested a merger involving Ukrainian uranium mining with Russia's Novosibirsk Chemical Concentrates Plant in Siberia, which produces VVER fuel. Also he noted that Ukraine's Turboatom was producing large steam turbines solely for Russia. Furthermore, all Ukrainian reactors need modernization which, he said, could be most effective with close cooperation of Russian enterprises, at the same time as opening access for Ukrainian partners to the Russian market as it greatly expands nuclear capacity. In addition, Russia and Ukraine could collaborate in foreign markets on the basis of financing provided by the Russian government and leading financial institutions. Ukraine's president agreed in principle that some of these particular suggestions might have merit.

Rosatom followed up with the suggestion that if Ukraine signed long-term (25-year) fuel supply contracts with Russia it would enjoy a discount of more than US$ 1 billion. Furthermore, Rosatom was ready to transfer up to 50% of the shares in the Novosibirsk Chemical Concentrates Plant to Ukrainian partners and establish domestic fuel production, either “either [as] a branch of the combine where we can be shareholders together, or a new plant in the Ukrainian territory." Rosatom reiterated its long-standing desire to take a share of Ukraine's Novokonstantinov uranium project, and also proposed a joint venture bringing together the heavy engineering assets of Russia's Atomenergomash and Ukraine's Turboatom at Kharkov.

Energoatom has set up Atomproektengineering to handle new nuclear power projects, including investment, design, and construction. It has already been involved with Khmelnitsky 3&4 (see below). In October 2010 Atomenergomash announced that it and NAEC Energoatom would set up a strategic consortium to localize nuclear equipment manufacture in Ukraine, particularly in relation to Khmelnitsky 3&4.

Ukraine's plans for fuel cycle developments as of mid 2010 are to develop uranium mining and fuel fabrication, but not conversion, enrichment or reprocessing - these being done in Russia, albeit with some Ukraine equity in IUEC (see above).

Ukraine's JSC Turboatom at Kharkov, established in 1934 and now 75.2% government-owned, is among the leading world turbine-building companies. It specializes in steam turbines for thermal and nuclear power plants, and has the capacity to produce 8000 MWe of such per year, with individual units up to 1100 MWe. It has supplied 110 turbines totaling 50 GWe for 24 nuclear power plants. Ukrainian power plants employ 47 Turboatom-made turbines plus 43 Russian ones. Turboatom's major competitors are the Power Machines Co in Russia and Germany's Siemens. Much of its production in 2010 was for Russia.

## Non-proliferation

After the break-up of the Soviet Union, Ukraine negotiated to repatriate nuclear warheads and missiles to Russia in return for nuclear fuel supplies. Ukraine then joined the Nuclear Non-Proliferation Treaty (NPT) as a non-nuclear weapons state. Its safeguards agreement under the NPT came into force in 1998, and in 2005 the Additional Protocol to this agreement was ratified.

## Appendix: The K2-R4 saga

In the 1990s both the government and Energoatom were determined to bring two new reactors – Khmelnitski 2 and Rovno 4 (K2-R4) – into operation as soon as possible. Both reactors were 80% complete when a halt was imposed in 1990.

In 1995 a Memorandum of Understanding was signed between the Governments of the G7 countries, the EC and the Ukrainian government which required closure of the operating Chernobyl reactors. Thus, Chernobyl reactors were shut down – the last in December 2000.

The Memorandum stipulated the agreement on international financial aid to Ukraine to support Chernobyl decommissioning, power sector restructuring, completion of K2-R4 nuclear reactors, thermal and hydro plant rehabilitation, construction of a pumped storage plant, and to support energy efficiency projects in accordance with Ukraine's energy sector strategy.

In 2000 the European Bank for Reconstruction & Development (EBRD) approved (by an 89% vote apart from abstentions) a US$ 215 million loan towards completion of K2-R4. This EBRD funding, though a modest part of the US$ 1480 million estimated to be required, was a key factor in plans for their completion to western safety standards. Conditions on the loan included safety enhancement of all 13 Ukraine nuclear power reactors, independence for the country's nuclear regulator, and electricity market reform.

Following approval of the EBRD loan, the European Commission (EC) approved a US$ 585 million loan to Energoatom. The EC said that approval of this Euratom funding "a few days before the permanent closure of Chernobyl gives a clear sign of the Commission's commitment to nuclear safety ... as well as to the deepening of [EU] relations with Ukraine." It "will finance the completion, modernisation and commissioning of two third-generation nuclear units". The EC pointed out that it and the EBRD had concluded that the project met all safety, environmental, economic and financial criteria.

Russia earlier provided US$ 225 million credit for K2/R4 equipment and fuel, then in 2002 a Russian loan of US$ 44 million for completion of the units was approved. The arrangement covered goods and services from Russia. It followed signing of a US$ 144 million agreement in June, including about US$ 100 million of fuel.

However the promised loans of US$ 215 million and the Euratom's US$ 585 million were deferred late in 2001 because the government had baulked at doubling the wholesale price of power to USD 2.5 cent/kWh as required by EBRD. Ukraine also rejected almost all approved Russian loans. The Ukrainian government then approved estimates for the completion, site works and upgrades for the K2 - R4 nuclear power reactors, at US$ 621 million and US$ 642 million respectively. With local finance and a bond issue, Energoatom proceeded with work on both units.

In July 2004, prior to start-up of the two units, the EBRD finally approved a scaled-down loan of US$ 42 million. This sum was matched by US$ 83 million from Euratom, approved by the EC. The project finances the post-start-up component of a safety and modernisation program developed for K2 and R4.

The loan was approved on condition that revised tariffs are implemented in order to fund upgrading of all 13 operating power reactors in Ukraine to K2-R4 standards that a decommissioning fund is set up and "an internationally agreed level of nuclear liability insurance" is reached.

The program on modernisation and safety improvement of K2-R4 was established taking into account IAEA's recommendations. It consists of 147 "pre-commissioning", as well as "post-commissioning" and "before and after commissioning" measures. In 2003-2004, Framatome ANP, an independent expert of the EBRD, together with the local Riskaudit Company, reviewed the implementation status and sufficiency of the program. They assessed positively the result of this program's implementation to date. The post-commissioning modernization measures were completed in November 2010, under the US$ 125 million budget from EBRD and Euratom.

In August 2004 the Ukrainian President said that Western governments had failed to honour their 1995 undertakings to assist his country in exchange for closing the Chernobyl plant, particularly in relation to the Khmelnitsky 2 and Rovno 4 completion, grid infrastructure and a pumped storage hydro plant.

## Underground recovery process at WIPP begins

Source: http://www.homelandsecuritynewswire.com/dr20140311-underground-recovery-process-at-wipp-begins

Nuclear Waste Partnership (NWP), the management and operations contractor at the Waste Isolation Pilot Plant (WIPP) for the U.S. Department of Energy (DOE), said it has **initiated the first phase of an underground recovery process that will lead to the resumption of nuclear waste disposal operations at WIPP.**

Over the weekend (7 and 8 March), radiological and air quality instruments were lowered down the Salt Handling and the Air Intake Shafts, to check for airborne radioactivity and to determine air quality. NWP says the preliminary findings indicate no detectable radioactive contamination in the air or on the equipment lowered and returned to the surface. Air quality results were also normal. These results were expected because the shafts which were sampled were not in the air flow path coming from the area where the radiation release originated.

“This process is critical in helping determine the proper personal protective equipment needed for our personnel entries,” said Tammy Reynolds, WIPP Recovery Process Manager for NWP. “We will do a final analysis of these samples before we send anyone down. The safety of our employees is foremost during this process.”

“This is a positive way to begin the recovery process. In order to get to this point, a lot of work has taken place and it involved a lot of time-consuming activities,” said Joe Franco, manager of the Carlsbad Field Office. “But the recovery process is underway. We are receiving information that will get us to the next steps in the process.”

After completing required safety inspections of the hoisting equipment and the Salt Handling and Air Intake Shafts, the next step in the recovery process will be sending qualified site personnel into the WIPP underground facility, which may occur as soon as the end of the week.

The specialists entering WIPP will determine the mine’s stability and attempt to identify the source of the release.

Once the team completes an inspection of the shafts to ensure they are safe, they will check for levels of air and surface contamination between the Air Intake and Salt Handling shafts. **At that point, the team will make its way down to the area of the repository where operations were being conducted prior to the radiological release, doing radiological sampling and checking for quality as they go.**

**Then the team will isolate the source of the release and implement a plan to remove the contamination hazard.**

NWP also updated the bioassay results, saying that the results of bioassay testing of employees who may have been exposed during the recent radiation release at WIPP continue to come in. As of 8 March, a total of seventeen employees have tested positive for just over background for contamination in fecal samples (this includes the thirteen employees who were initially tested immediately after the event, and other employees who have been subsequently tested). There has been no detectable contamination in urine samples, which indicates contamination was not inhaled into the lungs.

NP says the levels of exposure are extremely low, and none of the employees is expected to experience any health effects from the exposures.

**The four most recent positive results were at the barely detectable level (about .1 disintegrations per minute), and reflect extremely low levels of exposure.**

# Argon’s RADSIM 44-9 enhances realism of CBRN response training

Source: http://www.army-technology.com/contractors/nbc/argon-electronics/pressargons-radsim-44-9.html?WT.mc\_id=WN\_PR

Argon Electronics has launched a new detector simulator that offers CBRN/HazMat response training instructors yet another way to enhance the reality of exercises. The Argon RADSIM 44-9-SIM is a versatile simulated detector probe for training in the use of Ludlum's 44-9 GM pancake-type detector, and can be used with an extensive range of Ludlum survey meters, rate meters and scalers.

Rather than real radiation sources or radioactive materials, **the Argon RADSIM 44-9-SIM will respond to safe Alpha/Beta simulation sources that can be hidden on a person, enabling students to detect either partial or full decontamination.** Instructors can therefore establish a realistic exercise that enables students to experience the operational features of Ludlum's 44-9 GM pancake-type detector without endangering safety.

The Argon RADSIM 44-9-SIM not only enhances realism and safety but also is compatible with the Argon PlumeSIM® system for wide area tactical field and nuclear emergency response exercises. PlumeSIM® software is used with chemical and radiological detector simulation instruments from Argon, allowing virtual dispersal plumes and hot spots to be set up quickly and simply for trainees to detect. The Argon RADSIM 44-9-SIM is also compatible with other dosimeter, survey/radiac meter, and spectrometer simulators manufactured by Argon Electronics, permitting multi-detector, multi-isotope training to take place within the same scenario.

As with all detector simulators in the Argon Electronics range, the RADSIM 44-9-SIM offers cost-effective training without the need for recalibration and with no preventative maintenance required beyond the occasional replacement of AA alkaline batteries.

## Radiation damage to Chernobyl’s ecosystems helps spread radioactivity

Source: http://www.homelandsecuritynewswire.com/dr20140321-radiation-damage-to-chernobyl-s-ecosystems-helps-spread-radioactivity

**Radiological damage to microbes near the site of the Chernobyl disaster has slowed the decomposition of fallen leaves and other plant matter in the area, according to a study just published in the journal Oecologia. The resulting buildup of dry, loose detritus is a wildfire hazard that poses the threat of spreading radioactivity from the Chernobyl area.** A University of South Carolina release reports that Tim Mousseau, a professor of biology and co-director of the Chernobyl and Fukushima Research Initiatives at the University of South Carolina, has done extensive research in the contaminated area surrounding the Chernobyl nuclear facility, which exploded and released large quantities of radioactive compounds in the Ukraine region of the Soviet Union in 1986.

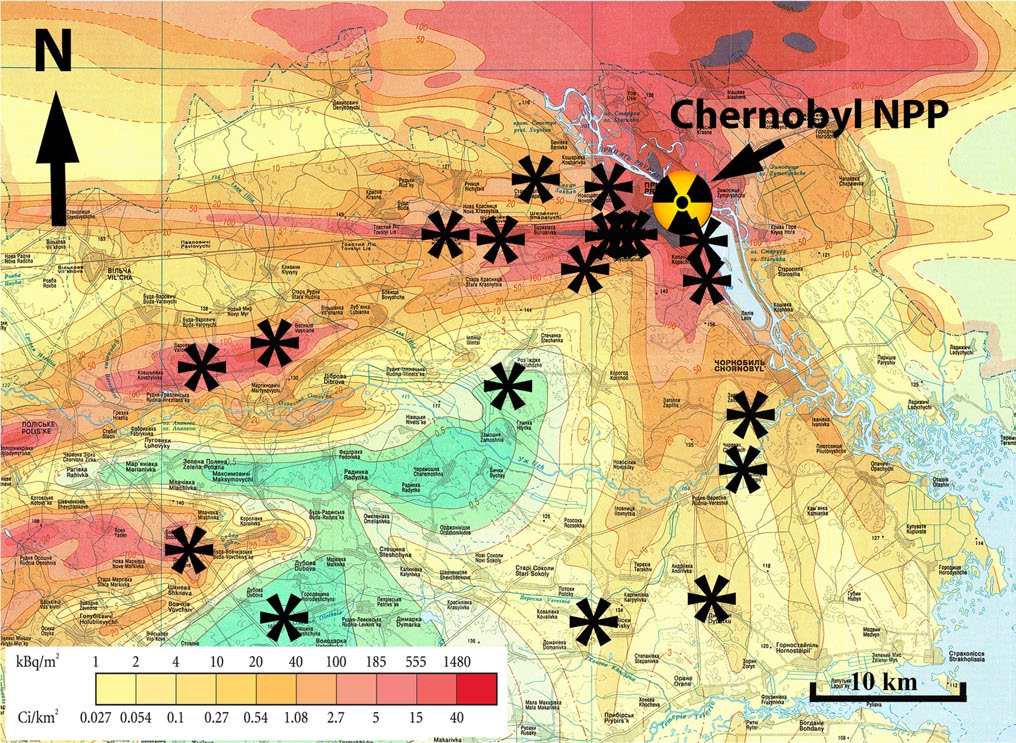
He and frequent collaborator Anders Møller of Université Paris-Sud noticed something unusual in the course of their work in the Red Forest, the most contaminated part of the Chernobyl Exclusion Zone.

“We were stepping over all these dead trees on the ground that had been killed by the initial blast,” Mousseau said. “Some 15 or 20 years later, these tree trunks were in pretty good shape. If a tree had fallen in my backyard, it would be sawdust in 10 years or so.”

Background radiation levels in the Chernobyl area vary widely by location (Image: Oecologia).

They set out to assess the rate at which plant material decomposed as a function of background radiation, placing hundreds of samples of uncontaminated leaf litter (pine needles and oak, maple and birch leaves) in mesh bags throughout the area. The locations were chosen to cover a range of radiation doses, and the samples were retrieved after nine months outdoors.

A statistical analysis of the weight loss of each leaf litter sample after those nine months showed that higher background radiation was associated with less weight loss. The response was proportional to radiation dose, and in the most contaminated regions, the leaf loss was 40 percent less than in control regions in Ukraine with normal background radiation levels.

They also measured the thickness of the forest floor in the same areas where samples were placed. They found that it was thicker in places with higher background radiation.

**The team concluded that the bacteria and fungi that decompose plant matter in healthy ecosystems are hindered by radioactive contamination. They showed a smaller effect for small invertebrates, such as termites, that also contribute to decomposition of plant biomass.**

According to Mousseau, slower decomposition is likely to indirectly slow plant growth, too, given that the products of decomposition are nutrients for new plants. The team recently reported diminished tree growth near Chernobyl, which he says likely results both from direct radiation effects and indirect effects such as reduced nutrient supply.

“It’s another facet of the impacts of low-dose-rate radioactive contaminants on the broader ecosystem,” Mousseau says. “We’ve looked at many other components, namely the populations of animals in the area, and this was an opportunity for broadening our range of interests to include the plant and microbial communities.”

The results also show the potential for further spread of radioactivity.

“There’s been growing concern by many different groups of the potential for catastrophic forest fires to sweep through this part of the world and redistribute the radioactive contamination that is in the trees and the plant biomass,” Mousseau says. “That would end up moving radio-cesium and other contaminants via smoke into populated areas.

“This litter accumulation that we measured, which is likely a direct consequence of reduced microbial decomposing activity, is like kindling. It’s dry, light and burns quite readily. It adds to the fuel, as well as makes it more likely that catastrophically sized forest fires might start.”

*— Read more in Timothy A. Mousseau et al., “Highly reduced mass loss rates and increased litter layer in radioactively contaminated areas,”* Oecologia *(March 2014) (DOI: 10.1007/s00442-014-2908-8); and Timothy A. Mousseau et al., “Tree rings reveal extent of exposure to ionizing radiation in Scots pine Pinus sylvestris,”* Trees *27, no. 5 (October 2013): 1443-53*

# Abu Dhabi sets nuclear standard

Source: http://www.thenational.ae/business/energy/abu-dhabi-sets-nuclear-standard#full

Abu Dhabi is building “gold-standard” safety procedures into its plan to develop four nuclear reactors, a foreign adviser to the government said.

This country could even teach the Japanese a thing or two, experts say, after drawing lessons from Japan’s Fukushima nuclear disaster.

**The UAE is investing in facilities for nuclear power, renewable energy and liquefied natural gas to cut its reliance on oil and will be the first Arab state in the GCC region to have a nuclear plant when the facility starts as scheduled in 2017.**

Barakah plant’s Unit 1, Abu Dhabi

Elsewhere in the Arabian Gulf, Iran generates atomic energy.

“Safety culture has got to be first, and here they are doing that,” says Barbara Judge, a member of an international nuclear advisory council formed by the Abu Dhabi Government.

Tokyo Electric Power Company (Tepco), the Fukushima plant’s operator, “had moved to an efficiency culture” focused on profit over safety, Ms Judge said, speaking in Abu Dhabi last week on the third anniversary of the Japanese nuclear accident.

The Fukushima Dai-Ichi nuclear plant leaked radioactive material after a tsunami triggered by an earthquake struck the facility on March 11, 2011.

Ms Judge, a former chairman of the UK Atomic Energy Authority, is the vice chairman of a committee advising Tepco on the decommissioning of the damaged Fukushima units.

She also serves on Abu Dhabi’s nuclear International Advisory Board, headed by Hans Blix, a former UN chief weapons inspector.

“We respond sincerely” to Ms Judge’s assessment and “will steadily work to improve the safety culture in the company,” Mayumi Yoshida, a Tepco spokeswoman, says.

Emirates Nuclear Energy, the government-owned company building the Abu Dhabi plants, will be a benchmark for safety when the units are built, Ms Judge says.

Officials seeking her views into what went wrong at Fukushima have created strong regulatory oversight for the Abu Dhabi project, something Japan lacked, she adds.

Authorities here are still working on a permanent plan for storing or disposing of nuclear waste, and the Government did not brief advisory board members last week on any new developments, Ms Judge says.

**The UAE plans to generate 25 per cent of its power from four nuclear plants by 2020**, Suhail Mohammed Al Mazrouei, the energy minister, said in October.

The reactors will produce 5,400 megawatts when they are completed, Matar Hamed Al Neyadi, an energy ministry undersecretary, said at the time.

While the UAE’s neighbour Saudi Arabia plans to develop a nuclear power sector in the future, for now it is focused on its gas industry for electricity production.

But foreign companies that formed joint ventures with the state oil firm Saudi Aramco to look for conventional gas in the kingdom’s Empty Quarter, including Russia’s Lukoil, Royal Dutch Shell and Sinopec, have failed to find commercially viable deposits.

So Saudi authorities are now seeking to concentrate the search on unconventional deposits — very deep, high-temperature reservoirs that would require more complex and expensive technologies to commercially exploit.

“The assumptions of the initial gas exploration agreements do not exist anymore because in spite of a decade of exploration, no commercial gas discoveries have been made,” says Sadad Al Husseini, a former senior executive at Saudi Aramco.

“Therefore the exploration programme could be redefined as a change to unconventional gas exploration with higher costs and new buy-back terms,” says Mr Al Husseini, who now owns an energy consultancy firm said.

Lukoil is negotiating a deal with the world’s top oil exporter to tap unconventional gas deposits in the Empty Quarter, the company’s overseas unit said this week.

**Saudi Arabia** has kept its vast oil reserves off-limits to foreigners, but needs natural gas to help cover domestic power demand and conserve oil for export. It invited investors a decade ago to find and produce gas in the Empty Quarter, also known as Rub Al Khali.

Lukoil is still on the hunt for desert gas and is now evaluating the possibility of production from an unconventional deposit.

“This is tight gas. The negotiations are under way. No details on deal and future production plans yet,” says a spokesman for Lukoil Overseas, which operates the group’s foreign upstream projects.

“Yes, we are hopeful and will continue evaluating drilling after signing a deal.”

Because such production would be more expensive than conventional output, the firm is trying to negotiate a higher price with Saudi authorities in its joint venture, industry sources say.

The sources say no deal has yet been reached as further studies need to be carried out by Lukoil and Saudi Aramco to estimate how much unconventional gas was available.

Saudi Aramco and the Saudi oil ministry were not immediately available to comment.

“At this time there isn’t enough data to determine how much gas may be recoverable, what levels of production can be achieved, and what levels of expenditures are likely to be required,” says Mr Al Husseini.

“It appears that the decision-makers may now be thinking that since there are source rocks in the region, there may be some formations where fracking can be successful in generating unconventional gas production,” he adds.

The higher cost of extracting unconventional gas was not the only obstacle to production — scaling up and sustaining unconventional gas operations at a meaningful level of supply would also present major technical challenges, Mr Husseini says.

Shell says it is not currently drilling in its Rub Al Khali venture but says it is in regular dialogue with Saudi officials, without elaborating further.

An industry source familiar with the matter says China’s Sinopec has suspended drilling operations in the Empty Quarter. A Sinopec spokesman could not be reached for comment.

The Saudi oil minister Ali Al Naimi has estimated the kingdom has more than 600 trillion cubic feet of unconventional gas reserves, more than double its proven conventional reserves.

# Missing radioactive material may pose 'dirty bomb' threat - IAEA

Source: http://uk.reuters.com/article/2014/03/21/uk-nuclear-security-iaea-idUKBREA2K10I20140321



March 21 – **About 140 cases of missing or unauthorised use of nuclear and radioactive material were reported to the U.N. atomic agency in 2013,** highlighting the challenges facing world leaders at a nuclear security summit next week.

Any loss or theft of highly enriched uranium, plutonium or different types of radioactive sources is potentially serious as al Qaeda-style militants could try to use them to make a crude nuclear device or a so-called "dirty bomb", experts say.

Denis Flory, deputy director general of the International Atomic Energy Agency (IAEA), said most of the reported incidents concerned small quantities of radioactive material.

But, "even if they can't be used for making a nuclear weapon, they can be used in radioactive dispersal devices, which is a concern," Flory told Reuters in an interview.

In a "dirty bomb", conventional explosives are used to disperse radiation from a radioactive source, which can be found in hospitals, factories or other places that may not be very well protected.

Holding a third nuclear security summit since 2010, leaders from 53 countries - including U.S. President Barack Obama - are expected to call for more international action to help prevent radical groups from obtaining atomic bombs.

At the March 24-25 meeting in The Hague, they will say that much headway has been made in reducing the risk of nuclear terrorism but also make clear that more must be done to ensure that dangerous substances don't fall into the wrong hands.

The Dutch hosts say the aim is a summit communiqué "containing clear agreements" to prevent nuclear terrorism by reducing stockpiles of hazardous nuclear material, better securing such stocks and intensifying international cooperation.

Flory said member states had reported **a total of nearly 2,500 cases to the IAEA's Incident and Trafficking Database since it was set up two decades ago. More than 120 countries take part in this information exchange project, covering theft, sabotage, unauthorized access and illegal transfers.**

**Nuclear security pact delayed**

**In 2012, 160 incidents were reported to the IAEA, of which 17 involved possession and related criminal activities, 24 thefts or loss and 119 other unauthorised activities, its website says.**

"It is continuing, which means there is still a lot of work to do to have that really decrease," Flory said with respect to the statistics. However, there are also "more and more countries which declare incidents. The number of incidents we don't know is probably decreasing."

Because radioactive material is less hard to find and the device easier to make, experts say a "dirty bomb" - which could cause panic and have serious economic and environmental consequences - is a more likely threat than a deadly atom bomb.

Radical groups could theoretically build a crude nuclear bomb if they had the money, technical knowledge and fissile materials needed, analysts say.

One of the biggest challenges ahead is to finally bring into force a 2005 amendment to the Convention on Physical Protection of Nuclear Materials (CPPNM), Flory said.

There are still 27 countries - including the United States - which need to ratify the amendment, which expands the coverage from only the protection of nuclear material in international transport to also include domestic use, transport and storage.

"It is extremely important because this amendment brings a lot of strengthening in the field of nuclear security," he said.

Harvard University professor Matthew Bunn said this month that a U.S. failure so far to ratify the amended convention "has made it far harder" for Washington to pressure others to do so.

"The problem appears to be a combination of lack of sustained high-level attention by both the administration and Congress and disputes over unrelated issues," Bunn said.

Flory, who heads the IAEA's nuclear safety and security department, said he knew that the U.S. administration was "very keen on finishing the process" as soon as possible.

"This is a country where you have a lot of nuclear material, a lot of nuclear facilities and they have a lot of influence on nuclear security."

|  |
| --- |
| EDITOR’S QUESTION  Why we focus so much on to aquizition off “nuclear weapons” and miss the possibility of “dirty long range missiles”? |

# Five assessments of the Fukushima disaster

**By Charles Perrow**

Source: http://thebulletin.org/five-assessments-fukushima-disaster

**Considered in this review:**

* Samuels, Richard J (2013) 3.11: Disaster and Change in Japan. Ithaca and London: Cornell University Press
* Nadesan, Majia H (2013) Fukushima and the Privatization of Risk. Basingstoke: Palgrave Macmillan
* The Independent Investigation Commission on the Fukushima Daiichi Nuclear Accident (2014) The Fukushima Daiichi Nuclear Power Station Disaster: Investigating the Myth and Reality. Chicago: The Bulletin of the Atomic Scientists. London and New York: Routledge
* The Fukushima Nuclear Accident Independent Investigation Commission (2012) "The Official Report." Tokyo: Japanese National Diet
* Lochbaum, David, Edwin Lyman, Susan Q. Stranahan, and the Union of Concerned Scientists (2014) Fukushima: The story of a nuclear disaster. New York: The New Press

The four books and the government report reviewed here are all impressive. Though they cover the same ground—the disaster at the Fukushima Daiichi nuclear plant that began three years ago after a massive earthquake and tsunami—and largely draw upon the same or similar sources, there are distinct differences among them. Samuels covers the actual accident less closely than the others but has the most to say about the history of nuclear power in Japan and the best material on the “nuclear village.” Nadesan has the best information on the radiation effects on the population, which is treated very lightly by the others, and her book has the most compact but broad coverage of all the issues and events. The independent investigation review (hereafter called the citizens’ review) raises the volume of criticism and has nuggets of information that none of the others has, making it quite valuable. The review by the Japanese Diet commission (which I call the Diet report) turns up the volume even further and has important quotes from Fukushima workers and especially those working for subcontractors at the plant. The final book by Union of Concerned Scientists members David Lochbaum, Edwin Lyman, and Susan Stranahan  (hereafter, the UCS review) has the most dramatic and intensive coverage of the accident, as well as superb material on the response to it of the US Nuclear Regulatory Commission.

Readers of the Bulletin will be familiar with most of the basic themes and details of the Fukushima situation, so I will take some basic knowledge for granted and highlight the distinctive contributions of the five volumes considered here, raise some questions about omissions found in most of them, and reflect upon the presumed uniqueness of the disaster.

**A nuclear village too big to fail.** Richard Samuels’ 3.11: Disaster and Change in Japan takes a historical approach to Fukushima. A political scientist with the skills of a historian, he makes it apparent that we should not have been surprised by the disaster. There had been others in Japan, the lessons learned were few and often forgotten, and there will be more. He bases this assessment on a fascinating history of nuclear power in Japan, an industry that was coursing 32.5 billion nuclear dollars a year through the economy at the time of the accident. In 2010, utility revenues were one quarter of all industrial revenues. “If ever a sector were too big to fail, this was it,” he writes (page 112).

The outrage evoked by the other books curdles to cynicism when we take Samuels's long view and see that the alarming corruption, the complacency, the refusal to take foreign help in crises, the political power of private industry, and so on, are just part of Japan’s culture. He has the most thorough discussion of the “nuclear village” phenomenon—the incestuous relationship between the national government, the utilities, and the press—that all other books touch on. He digs carefully into the warnings of possible disaster, noting, for example, that more than half of the members of the committee that set the size of predicted tsunamis, which affected design of the Fukushima plant, came from the nuclear industry. That committee estimated a tsunami that was just one-third the size of the surge that actually came on 3/11/11.

With a historical perspective, Samuels is able to explore an issue barely mentioned by the other books: The motivation to build so many nuclear plants on an earthquake-prone island was based not just on the island's lack of oil and coal. Also important were military considerations: Nuclear power kept the nuclear weapons option open. A former defense minister noted after the disaster (on page 124): “It is important to maintain our commercial reactors because it will allow us to produce a nuclear warhead in a short amount of time. ... It is a tacit nuclear deterrent.” The current minister of defense agrees. Such an interest can trump any interest in safety.

Samuels reviews the changes made in response to public pressure for safe operations—even abandonment—of nuclear power and is skeptical of the government’s reform attempts. A long review of past natural and industrial disasters does not anticipate a promising future. Each of these books' calls for transparency should be read in light of one fact: In late 2013, the National Diet passed a draconian official state secrecy act that provides jail terms for a variety of offenses, including independent helicopter surveillance of the reactors and publishing negative information regarding Fukushima’s nuclear power station. And unfortunately, important books such as those reviewed here are likely to be disregarded by the Japanese nuclear industry; TEPCO, the utility managing the power plants at Fukushima, has published a report saying it did nothing significantly wrong.

**Shifting the risk.** The most general of these Fukushima books, Fukushima and the Privatization of Risk by Majia H. Nadesan, also has the broadest theme: the process through which risk is shifted from organized entities, such as governments and corporations, to private citizens. While the government and TEPCO suffered reputational and financial loses, the greatest economic and social costs have been borne by citizens, and the greatest health costs will take years, even generations, to materialize. The fallout risks will only be realized retrospectively, through epidemiological studies of populations, and Nadesan's examination of exposure levels—the most detailed of any of the books—suggests that thousands will be affected. (All of the books are skeptical of the reassuring “too small to measure” and “not worth investigating” claims of most US experts, almost all Japanese officials, and the major UN organizations. See my article, "Nuclear denial: From Hiroshima to Fukushima.") Helping to shield the government and the utility from the responsibility for the risks posed by the Fukushima catastrophe is the large degree of uncertainty about the amount of radioactive materials released, the precise locations where they settled, their take-up by plants and animals, and the extent of age and gender vulnerability of affected populations. Certainly, citizens are not shielded when such uncertainties enhance the privatization of risks.

And in Japan, the privatization is blatant and ongoing. Japanese citizens have been encouraged to return to areas that were highly contaminated by the disaster, with only minimal attempts at decontamination, thus saving the costs of the monthly stipends the displaced had received. But the privatization of risk can also be subtle. Newspaper headlines based upon expert pronouncements declare that the harm is less radiological than social—the panic and stress caused by unreasonable fears and evacuations. But these books make clear that the government is the source of the stress. The government did not explain why evacuation was necessary, or how long it would continue; it sent thousands of people from areas of low radiation to ones of high radiation; it left the aged and ill abandoned; and citizens were moved as many as six times over a few days or weeks. The stress that was supposedly more damaging than the radiation came from the government, but has been privatized by not acknowledging this source.

In the second chapter of her book, Nadesan examines the development of the industrial-military nuclear complex in Japan. In her analysis, deterrent power is gained simply by stockpiling plutonium that can be used to make weapons; as with Samuels, she offers evidence that the Japanese government had this deterrent very much in mind as it began its massive nuclear power program. The crisis-management efforts of the Japanese and US governments are well covered by all the books, but Nadesan's third chapter has the best documentation of the evidence of fallout and bio-contamination. Her fourth chapter extensively documents the harmful effects of ionizing radiation and reviews the scientific controversy regarding low-level radiation; the quality of these two chapters is not matched in any of the other books. All told, this may be the best current general volume on the accident. Others cover several topics in more depth, but none addresses the radiological hazards as seriously as she, and all lack the general theme of the privatization of risk in nuclear power. (An even more general discussion of the social construction of risk can be found in a new book by University of Colorado Boulder sociology professor Kathleen Tierney, The Social Roots of Risk.)

**The citizens view.** In 2011, shortly after the March 11 disaster, 30 young and mid-career professionals—including natural scientists and engineers, social scientists and researchers, businesspeople, lawyers, and journalists—formed an investigative committee. It was to be independent of any governmental organization. Chaired by Koichi Kitazawa, a former chairman of the Japan Science and Technology Agency, the committee published a report in 2012, with an English translation to follow in 2013, referred to here as the citizens review, to distinguish it from a government report with a similar name. The Fukushima Daiichi Nuclear Power Station Disaster: Investigating the Myth and Reality is a sprawling, repetitive, angry analysis that nevertheless contains valuable material on the accident that does not appear elsewhere.

The material in the preface is not very useful but the book's first chapter is splendid. It covers the first few days of the accident, examining the Japanese Cabinet and the staff at the plant. TEPCO refused to cooperate with the citizens' investigation (or with any other investigation reviewed here), and in particular refused to fully disclose videoconference footage recorded in March 2011, according to the citizens review. Nevertheless, through extensive interviews and documentary evidence, the opening chapter provides a blow-by-blow, even minute-by-minute account of the accident. It highlights something familiar to students of crises: Top management in all of the cabinet agencies experienced "elite panic" (a term coined by Rutgers' Lee Clarke), while the foot soldiers on the ground saved whatever of the day was left to be saved. The workers’ mistakes and errors are understandable, given the chaotic circumstances: working for days with little rest or nourishment, struggling in dense blackness penetrated only by feeble flashlights, dealing with radioactive water and debris all about and a failure of all instrumentation. Micromanagement from the top contributed to the few errors the plant personnel made.

The plant manager knew that venting of the unit 1 reactor vessel was necessary to prevent hydrogen explosions, but permission had to come from Tokyo. It took more than nine hours to get permission to vent and five hours to complete the job, and by then it was too late. The rods in unit one had already melted into a sludge and the pressure vessel was filled with hydrogen, which ignited a few hours later, blowing away the thick concrete walls of the reactor building in the first of two explosions.

All the major topics of the disaster are covered in the other chapters of the citizens review, but the regulatory apparatus comes in for special condemnation in the excellent discussion of the “safety myth” that came to pervade the Japanese nuclear establishment and public. But as Jessica Matthews and James Acton of the Carnegie Endowment for International Peace note in the epilogue, while the first six chapters of the citizens review presents a trenchant and persuasive critique of the weaknesses in Japanese regulations, the review does not apply the same critical standards when examining US regulations for the purposes of comparison. The expert commentary of Matthews and Acton reminds us of the parallel regulatory failures in the US and the huge inventory of spent fuel rods in US reactors.

**The government's surprising report.** The nongovernmental investigating committee that I've called the citizens review was established because a group of people feared that any governmental report would be a whitewash. They were wrong. One member of the private group, in fact, had to resign when the National Diet of Japan asked him to head up an investigation. This was Kiyoshi Kurokawa, a medical doctor and former president of the Science Council of Japan. The nine other members came from universities, institutes, and the Defense Ministry, were renowned in their fields, and included a former Japanese ambassador to the United Nations. The National Diet of Japan Fukushima Nuclear Accident Independent Investigation Commission held 19 meetings from December 2011 to June 2012, with extensive testimony at each meeting. In addition to these sessions, the Diet investigation included more than 900 hours of hearings and interviews with 1,167 people and site visits to nine nuclear power plants. The result is as impressive a report (henceforth called the Diet report) from an elected government body as we are likely to find.

The quotes from the public and Fukushima workers in the Diet report are striking in their detail and their emotional impact. The comments from many of the subcontractors are especially revealing and damning of TEPCO management. While this report has the best coverage of the subcontractors (the bulk of the plant’s staff), there is no mention of the extensive use of criminals from the Japanese mafia, who were hired as temporary workers during the response to the disaster.

The Diet report received widespread coverage in the press, and though the following quotations are familiar, they deserve repeating here, because they effectively summarize the report:

*What must be admitted—very painfully—is that this was a disaster “Made in Japan.”… Its fundamental causes are to be found in the ingrained conventions of Japanese culture: our reflexive obedience; our reluctance to question authority; our devotion to "sticking with the program"; our groupism; and our insularity. …With such a powerful mandate, nuclear power became an unstoppable force, immune to scrutiny by civil society. Its regulation was entrusted to the same government bureaucracy responsible for its promotion. At a time when Japan’s self-confidence was soaring, a tightly knit elite with enormous financial resources had diminishing regard for anything "not invented here." …This conceit was reinforced by the collective mindset of Japanese bureaucracy, by which the first duty of any individual bureaucrat is to defend the interests of his organization.*

*Carried to an extreme, this led bureaucrats to put organizational interests ahead of their paramount duty to protect public safety … Only by grasping this mindset can one can one understand how Japan’s nuclear industry managed to avoid absorbing the critical lessons learned from Three Mile Island and Chernobyl; and how it became accepted practice to resist regulatory pressure and cover up small-scale accidents. It was this mindset that led to the disaster at the Fukushima Daiichi Nuclear Plant.*

**A real-life thriller.** The last book I will discuss—Fukushima: the story of a nuclear disaster—is the best. David Lochbaum, director of the Union of Concerned Scientists (UCS) Nuclear Safety Project; Edwin Lyman, a UCS senior scientist; and Susan Q. Stranahan, a reporter for The Philadelphia Inquirer, present the most detailed and gripping account of the accident offered in these assessments. They interrupt their thriller with coverage of the culture of safety in the government and in the utility industry, and they sharply criticize the US government and especially the US Nuclear Regulatory Commission for also playing fast and loose with this risky and lethal technology and bowing to the demands of the nuclear power industry. Their lucid explanations of the technicalities of the generation of nuclear energy at each point in the crisis wonderfully characterize the complexity of the process, increased many fold by the damage of the earthquake and then the tsunami. It is a thriller that reminds one of Eric Schlosser’s recent account of the explosion of a Titan II nuclear missile during the Cold War in his book Command and Control.

The authors not only put you in the Fukushima plant, minute by minute, but provide something the other books lack: an astonishingly detailed examination of the reactions of the NRC staff in Maryland and of the group of experts the agency sent to Tokyo. With quotations of conversations, pithy emails, and NRC documents, they offer insight not only into the actions of the Japanese authorities, but also into the response in the White House, the Defense Department, and other US agencies. Finally, because of their extensive knowledge of our own nuclear industry and its “lackluster” regulator, the NRC, they are able to put the problem of nuclear safety into a larger framework than the other books.

Their critique of the NRC and its cozy relationship with the nuclear industry (which, they assert, is almost as tight as relationships in Japan) is easy for them to support; the UCS has been documenting this relationship for years. For example, on page 190, they note that it is the NRC, not its Japanese counterpart, that declared in 1985, “[E]xisting plants pose no undue risk to public health and safety.” Furthermore, the authors note that the vulnerability of US reactors in some respects is greater than those in Japan with regard to overloaded spent fuel rod pools. (Think of the Indian Point nuclear plant a few miles from the Bronx, or a South Carolina plant a few miles downstream of a huge and challenged dam.)

But they imply another important vulnerability. It is apparent from the Japanese case that the serious failures did not generally occur at the operating level, but in the top tier of management. Gregory Jaczko chaired the five-man Nuclear Regulatory Commission at the time of the accident and performed admirably, but that was not true of the other four commissioners, who eventually forced Jaczko from the commission. Over his objections, the other commissioners rejected changes to US regulations that should have been made, based on the lessons of Fukushima. The staff of the NRC, on the other hand, performed admirably, both in the crisis mode and the regulatory mode.

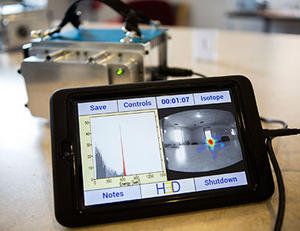
Surprisingly, the UCS book barely mentions any connection between nuclear weapons and its daughter, nuclear power, in contrast to the books by Samuels and Nadesan. Nor does it dwell upon the consequences of the accident in terms of low-level radiation. (For a review of these issues see "Nuclear denial: From Hiroshima to Nagasaki.") Indeed, it goes easy on the international promoter of nuclear power, the IAEA, which was late in feebly stepping up to the Fukushima plate. The UCS book also does not inquire into the evidence that a meltdown in unit 1 may have been in process immediately after the earthquake and well before the tsunami came ashore. None of the books entertains this possibility, but even though workers reported that, before the tsunami hit, cracked pipes were spilling coolant water, that a radiation alarm went off on the perimeter, and that safety devices were energized, fruitlessly, indicating the possibility of a LOCA, or loss of coolant accident. All of this reportedly came before the tsunami arrived at the plant. Since earthquakes are more frequent than tsunamis, this indication that an earthquake may have caused a loss of coolant or even a meltdown would be bad news for the nuclear power industry.

**Finally, none of the books adequately deals with the potential danger of a failure of the unit 4 spent fuel pool. Nuclear power critics have noted that a collapse of the pool at unit 4, now being slowly emptied of used fuel assemblies, or even an inadvertent jostling of the assemblies during removal, could release radiation that would require the evacuation of Tokyo. Even if only the Fukushima plant had to be evacuated, that would mean that the 11,000 fuel assemblies in the reactors and the common pool could not be constantly cooled because workers could not survive the radiation. The former Japanese Ambassador to Switzerland, Mitsuhei Murata, has said that full-scale releases from Fukushima, with 14,000 times as much radiation as the Hiroshima nuclear bomb, “would destroy the world environment and our civilization.”**

***Charles Perrow*** *is an emeritus professor of sociology at Yale University, and a visiting professor at Stanford University's Center for International Security and Cooperation. An organizational theorist, he is the author of six books including* [The Next Catastrophe](http://www.amazon.com/Next-Catastrophe-Vulnerabilities-Industrial-Terrorist/dp/0691129975) *(Princeton, 2011) and the award-winning* Normal Accidents: Living with High Risk Technologies *(Princeton, 1999). His current research focuses on the institutional and organizational aspects of global warming.*

## Innovative nuclear radiation detector reaches the market

Source: http://www.homelandsecuritynewswire.com/dr20140312-innovative-nuclear-radiation-detector-reaches-the-market

A **handheld radiation camera** developed by University of Michigan engineering researchers offers nuclear plant operators a faster way to find potentially dangerous hot spots and leaky fuel rods.

**The new Polaris-H detector lays a gamma-ray map over an image of a room, pinpointing radiation sources with unprecedented precision. At least four U.S. nuclear power plants are using versions of the camera, which is now available commercially through the U-M spinoff company H3D.**

“This technology enables people to ‘see’ radiation,” said Zhong He, a professor of nuclear engineering and radiological sciences at U-M and CEO of H3D. “This should enable the early detection of leaks by locating abnormal radiation, a much better understanding of radiation sources to protect workers, and it could be a tool for the cleanup effort of nuclear waste and fallout, such as in Fukushima in Japan.”

**Radiation safety professionals have called the device revolutionary.** They say it could become the new standard.

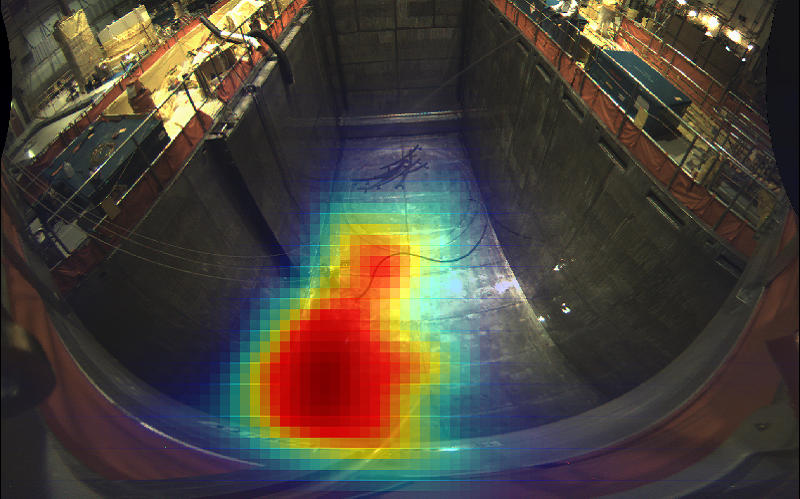
**“We can find things now in 30 minutes that could take weeks to find before,”** said Robert Hite, radiation protection manager at the Cook Nuclear Plant near St. Joseph, Michigan, and early adopter of Polaris-H. “All of our technology that we have — that I’ve worked with for thirty years — doesn’t touch what this shows us.”

A U-M release reports that a radiation imager offers plant managers like Hite a quicker way to identify and locate problems, including radioactive buildup in pipes, stray radioactive particles in otherwise clean areas and leaky fuel rods. Also, in the event of an accident, an imager could monitor radiation plumes and point out contaminated areas.

The **gamma camera operates at room temperature,** which is an improvement for the many plants that currently work with cumbersome, cryogenically cooled detectors. Room-temperature radiation imagers have been poor performers in the past, so many nuclear power plants in the United States rely on non-imaging detectors to find contamination. Locating the source of the problem often means moving the non-imaging detector around the contaminated area to find areas with high radiation counts.

**To use Polaris-H, though, an operator can simply set the camera in the contaminated area, switch it on and then leave the room while it reveals the radiation hotspots and identifies the radioactive elements present.** A 15-foot cord connects the detector and an external touchscreen controller so the operator can give commands and download data remotely. The camera stores radiation detection data on a USB drive that operators can transfer to a computer for in-depth analysis.

**While traditional imagers cost upwards of $200,000, the new cameras are priced below $100,000.**

The technology grew out of a project in He’s lab. The original briefcase-sized Polaris was developed for catching terrorists, but the team quickly realized that the nuclear energy industry could put the technology to use for safety. Five of He’s former graduate students making up the bulk of the company’s staff.

Clean-up verification

The release notes that prototype models are in use at the Cook plant and South Korea’s Institute for Basic Science in Daejeon. Based on feedback from these users over the past year, the team made it possible to operate the camera using a simple red button to start and end measurements.

“Our demonstrations used to last 20 minutes,” said H3D president William Kaye, a recent doctoral graduate in nuclear engineering and radiological sciences. “Now we just switch on the machine and say, ‘Okay, these are all the isotopes, this is where they are, any questions?’”

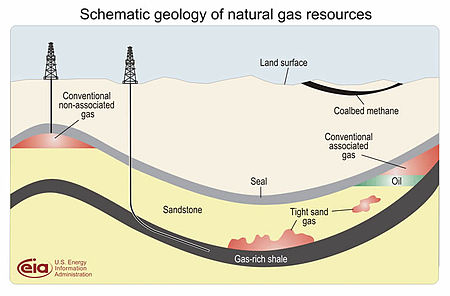
Kaye said that this level of information has not been available in the past, so the H3D team hopes to educate customers about how it can be used. For instance, sometimes the radiation source is ambiguous after detector measurements. A set of pipes might appear to be radioactive, but an image could clearly show whether the radiation was uniform, or whether some pipes were more radioactive than others.

**In addition to the nuclear plants, NASA and the Department of Defense are also using the detectors.**

►**Read also:** http://www.h3dgamma.com/applications.html

## Shale may offer long-term home for nuclear waste

Source: http://www.homelandsecuritynewswire.com/dr20140318-shale-may-offer-longterm-home-for-nuclear-waste

**Shale, the source of the U.S. current natural gas boom, could help solve another energy problem: what to do with radioactive waste from nuclear power plants.** The unique properties of the sedimentary rock and related clay-rich rocks make it ideal for storing the potentially dangerous spent fuel for millennia, according to a geologist studying possible storage sites who made a presentation here today.

The talk was given at the 247th National Meeting & Exposition of the American Chemical Society (ACS), being held 16-20 March in Dallas, Texas.

About 77,000 tons of spent nuclear fuel currently sit in temporary above-ground storage facilities, said Chris Neuzil, Ph.D., who led the research, and it will remain dangerous for tens or hundreds of thousands of years or longer.

“Surface storage for that length of time requires maintenance and security,” he said. “Hoping for stable societies that can continue to provide those things for millennia is not a good idea.” He also pointed out that natural disasters can threaten surface facilities, as in 2011 when a tsunami knocked cooling pumps in storage pools offline at the Fukushima Daiichi nuclear power plant in Japan.

Since the U.S. government abandoned plans to develop a long-term nuclear-waste storage site at Yucca Mountain in Nevada in 2009, Neuzil said finding new long-term storage sites must be a priority. It is crucial because nuclear fuel continues to produce heat and harmful radiation after its useful lifetime.

An ACS release notes that in a nuclear power plant, the heat generated by uranium, plutonium, and other radioactive elements as they decay is used to make steam and generate electricity by spinning turbines. In temporary pool storage, water absorbs heat and radiation. After spent fuel has been cooled in a pool for several years, it can be moved to dry storage in a sealed metal cask, where steel and concrete block radiation. This also is a temporary measure.

Shale deep under the Earth’s surface, however, could be a solution. France, Switzerland, and Belgium already have plans to use shale repositories to store nuclear waste long-term. Neuzil proposes that the United States also explore the possibility of storing spent nuclear fuel hundreds of yards underground in layers of shale and other clay-rich rock. He is with the U.S. Geological Survey and is currently investigating a site in Ontario with the Canadian Nuclear Waste Management Organization.

Neuzil explained that these rock formations may be uniquely suited for nuclear waste storage because they are nearly impermeable — barely any water flows through them. Experts consider water contamination by nuclear waste one of the biggest risks of long-term storage. Unlike shale that one might see where a road cuts into a hillside, the rocks where Neuzil is looking are much more watertight. “Years ago, I probably would have told you shales below the surface were also fractured,” he said. “But we’re seeing that that’s not necessarily true.”

Experiments show that water moves extremely slowly through these rocks, if at all. Various circumstances have conspired to create unusual pressure systems in these formations that result from minimal water flow. In one well-known example, retreating glaciers in Wellenberg, Switzerland, squeezed the water from subsurface shale. When they retreated, the shale sprung back to its original shape faster than water could seep back in, creating a low-pressure pocket. That means that groundwater now only flows extremely slowly into the formation rather than through it. Similar examples are also found in North America, Neuzil said.

Neuzil added that future glaciation probably doesn’t pose a serious threat to storage sites, as most of the shale formations he’s looking at have gone through several glaciations unchanged. “Damage to waste containers, which will be surrounded by a filler material, is also not seen as a concern,” he said.

He noted that one critical criterion for a good site must be a lack of oil or natural gas that could attract future interest.

## New infrared technique aims to remotely detect dangerous materials

### Source: http://news.byu.edu/archive14-mar-infrared.aspx

For most people, infrared technology calls to mind soldiers with night-vision goggles or energy audits that identify where heat escapes from homes during the winter season.

But for two Brigham Young University professors, infrared holds the potential to spot from afar whether a site is being used to make nuclear weapons.

Statistics professor Candace Berrett developed a model that precisely characterizes the material in each pixel of an image taken from a long-wave infrared camera. The U.S. National Nuclear Security Administration funded the project through a grant awarded to BYU engineering professor Gustavious Williams.

The government’s long-term goal for infrared technology is to remotely detect the exact materials, chemicals and gases coming and going from factories or other sites suspected of illegal nuclear production. Berrett and Williams tested their new method of analyzing infrared images with more basic materials using data taken by Lawrence Livermore National Laboratory. The results appear in a report published by the journal Technometrics.

Infrared cameras capture wavelengths of light that are not visible to the human eye. Hyper-spectral infrared cameras capture this light in hundreds of narrow bands. Since different materials reflect or absorb different bands of light, scientists can characterize the materials by analyzing the picture.

Identification of materials would be straightforward if those were the only signals bouncing back at the camera. But other incoming signals, such as the object’s temperature and the weather conditions, muddle the analysis and add noise to the material’s light signature.

The novelty of the BYU study is that it directly separates the incoming signals to provide the material’s unique signature. Other methods deal with the noise by matching the combined signals in a database.

“What we wanted to know is if you didn’t know anything about the material in an image, and we had a  number of pictures over time, could we let the algorithms figure out what the different materials are and separate them out,” Williams said.

The resulting information is more akin to measuring the material with a spectrometer in a lab. Berrett’s model can also group together pixels that are related to each other to map out the various materials in an image.

“If we apply this model we can get distributions on the physical characteristics of each of these pixels and, using those different characterizations, also cluster the pixels with like materials,” Berrett said.

As the technique develops, this could do much more than spot a bomb-making plant. Imagine taking an infrared picture from above a city struck by an earthquake or tornado. In addition to spotting all the gas leaks, it could reveal the exact gases being leaked and their concentrations in different neighborhoods.

“There are already instruments that can do this,” Williams said. “Our algorithms take a different approach but are still at a basic research stage. There are lots of places this research could go.”

**Abstract**

Long wave infrared (LWIR) Hyperspectral imagers (HSI) image a scene by collecting high-resolution spectra at each pixel. The data are similar to a camera image but have a large number of narrow spectral bands rather than the familiar broad three bands of red-green-blue in a traditional digital camera. Materials in LWIR are emissive (rather than reflective) and have unique spectra that can be used for material detection and identification. The measured spectra are a convolution of the material spectra (emissivity), the black body temperature (Planck curve), other interacting environmental spectral sources, and measurement error. One approach to material identification is temperature-emissivity separation (TES), which separates or deconvolves the material spectra from the temperature curve. To accomplish this task, we develop a unique flexible model which combines the mathematical model of the physical processes within a Bayesian nonparametric framework. In addition to offering interpretable estimates of model parameters, this model is able to identify material emissivity spectra and cluster pixels into appropriate material groups. We demonstrate our method using both a synthetic and measured data set. The online supplementary material contains an appendix of the details of the sampling algorithm.

# http://r70.cooltext.com/rendered/cooltext1333426779.pngExposure to IED blasts increases risk of long-term health consequences

Source: http://www.homelandsecuritynewswire.com/dr20140226-exposure-to-ied-blasts-increases-risk-of-longterm-health-consequences

U.S. soldiers exposed to blasts while deployed in Iraq and Afghanistan have an increased risk of developing adverse health outcomes over the long term, such as post-traumatic stress disorder (PTSD) and, in certain cases of traumatic brain injury (TBI), growth hormone deficiency, and persistent post-concussive symptoms including head-aches, says a new report by the Institute of Medicine. The committee that wrote the report focused on health consequences experienced at least six months after a blast.

Tens of thousands of U.S. soldiers serving in Iraq and Afghanistan have been killed or wounded by explosions during those wars. An

NSC release reports that **blasts are the leading cause of death and injury on the battlefield, accounting for about 75 percent of all combat-related injuries in U.S. military personnel.** Several major patterns of injury result from explosions, from injuries caused by the blast wave itself to those caused by fragments of debris propelled by the explosion, to subsequent illnesses from, for example, chemical substances released by a bomb. When the energy from the blast shock wave is absorbed in the human body, it disrupts the natural state of the body at a basic or even molecular level, which can cause tissue damage not immediately apparent after the blast.

“Acute physical and psychological health outcomes in people who survive blast explosions can be devastating, but the long-term consequences are less clear, particularly for individuals who show no external signs of injury from exposure to blast waves or may not even be aware that they were exposed,” said Stephen L. Hauser, chair of the committee that wrote the report, Robert A. Fishman Distinguished Professor, and chair of the department of neurology of the University of California, San Francisco.

**Some evidence suggests that blast exposure can result in long-term hearing damage and muscle or bone impairment such as osteoarthritis.** However, the data on these outcomes were not strong enough to draw a direct cause-and-effect relationship. **Though an association could exist, evidence was more tentative to link blast exposure to long-term effects on cardiovascular and pulmonary function, substance-abuse disorders, and chronic pain in the absence of a severe, immediate injury.** While there is substantial overlap between symptoms of mild TBI and PTSD, limited evidence suggests that most of the shared symptoms could be a result of PTSD and not a direct result of TBI alone.

The committee outlined several recom-mendations for urgent research to inform decisions on how to prevent and better diagnose blast injuries, and how to treat, rehabilitate, and support victims of battlefield trauma in the immediate aftermath and in the long term. In this research agenda, it is especially important to emphasize that blasts create unusual patterns of injury that can affect multiple organs and systems of the body, a complexity that has often been overlooked in previous studies. Understanding these cross-system interactions should be a priority for future research, the committee stressed. It also is essential that future studies use a standardized definition of blast exposure, once it is developed.

For health outcomes associated with blast exposure, the U.S. Department of Veteran Affairs should evaluate the approaches already in place to detect, treat, and rehabilitate blast injuries, the report says. Because injuries from blast may go undetected for long periods, the VA should conduct epidemiologic and mechanistic studies to identify biomarkers of blast injury through advanced imaging and molecular methods that could serve as surrogates of exposure.

The majority of past studies have used self-reported exposure data, rather than objective measures. Therefore, the committee recommended DOD develop and deploy data collection technologies that quantitatively measure components of blast and characteristics of the exposure environment in real-time and also link these data with self-reported exposure histories and demographic, medical, and operational information.

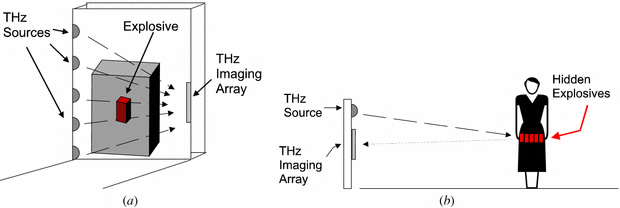
The Institute of Medicine study was sponsored by the U.S. Department of Veteran Affairs. The release notes that this is the ninth volume of its congressionally mandated series on health effects related to military service during wartime, which began in 1998 in response to the growing concerns of ill Gulf War veterans

.

*— Read more in* Gulf War and Health*, Volume 9:* Long-Term Effects of Blast Exposures *(National Academies Press, 2014)*

## Remote explosives detection may see the end of full-body scanners

Source: http://www.homelandsecuritynewswire.com/dr20140227-remote-explosives-detection-may-see-the-end-of-fullbody-scanners

Standing in a full-body scanner at an airport is not fun, and the process adds time and stress to a journey. It also raises privacy concerns. Researchers now report in American Chemical Society’s (ACS) Journal of Physical Chemistry Letters a more precise and direct method for using terahertz (THz) technology to detect explosives from greater distances. The advance could ultimately lead to detectors that survey a wider area of an airport without the need for full-body scanners.

An ACS release reports that R. Kosloff and colleagues explain that **using THz spectroscopy by itself is challenging for sensing far-away explosives. This technology uses beams of electromagnetic radiation that lie between microwaves, like those used in kitchen ovens, and the infrared rays used in TV remote controls.** In addition to screening people for explosives, it is **used at drug companies** for quality-control purposes and, most recently, to study the layers of paint of ancient works of art. With recent advances, the technique is becoming a strong candidate for detecting substances from a distance. **Other researchers have developed remote-sensing THz instruments, but they combine it with a second method to identify substances. Kosloff’s group aimed to use THz directly to eventually develop even better remote sensors.**

**They developed a computational tool and used it to successfully identify two explosives, RDX and TATP, with THz data directly.** RDX is a component of plastic explosives, and TATP is an explosive found in the shoes of the “shoe bomber” in 2009. “The ability to perform experimentally and simulate multidimensional spectroscopy should significantly enhance the screening ability of THz spectroscopy,” say the researchers.

The authors acknowledge funding from the U.S. Department of Homeland Security.

*— Read more in G. Katz et al., “Direct MD Simulations of Terahertz Absorption and 2D Spectroscopy Applied to Explosive Crystals,”* Journal of Physical Chemistry Letters *5 (10 February 2014): 772-76*

## How dogs detect explosives: New training recommendations

Source: http://www.homelandsecuritynewswire.com/dr20140228-how-dogs-detect-explosives-new-training-recommendations

A research team at Indiana University-Purdue University Indianapolis (IUPUI) has helped determine the science behind how canines locate explosives such as Composition C-4 (a plastic explosive used by the U.S. military). **The study found the dogs react best to the actual explosive, calling into question the use of products designed to mimic the odor of C-4 for training purposes.** These findings are the culmination of a four-year contract funded by the U.S. Department of Defense (DOD).

“Appropriately, dogs that are trained to find real explosives are going to find real explosives and not much else,” said John Goodpaster, Ph.D., associate professor of chemistry and chemical biology and director for the Forensic and Investigative Sciences Program in the School of Science at IUPUI.

An IUPUI release reports that the effectiveness of trained detector dogs is well established, but the study sought to determine which chemical compounds cause a dog to recognize a particular explosive and alert to it. Previous studies have suggested that certain non-explosive chemicals emitted by Composition C-4 cause dogs to alert, and that these specific chemicals could be used as mimic substances to train the dogs in place of real explosives.

In the first phase of the study, IUPUI researchers discovered that the non-explosive chemicals given off by C-4 mimics also are present in a variety of everyday plastic objects. Objects tested included PVC pipes, electrical tape, movie tickets, a plastic grocery bag and plastic food wrapping. Several of the tested items emitted appreciable levels of a mimic compound recommended by some vendors for training canines.

The second phase exposed 33 trained canines from the DOD, Department of Justice, Amtrak, and other agencies to these vapors to see if the dogs would respond. The field trials demonstrated that the dogs failed to respond in any significant way to specific odor compounds found in C-4. **The results indicate that if the dogs are trained on the full scent, they will only detect real explosives.**

“The canines are not easily fooled — you can’t pick and choose components of explosive odors and expect the dog to respond,” Goodpaster said. “Dogs are specific and it’s the full scent that causes them to alert.”

The study also sought to better establish the scientific facts needed for canine detection to be legally admissible evidence — an effort that found using mimic compounds could present challenges in court. By training with real explosives, false positives are unlikely in the field. Overall, the team recommended that dogs be trained with actual, not mimic, explosives.

While there is technology available to search for explosives, canines remain the best option because of their speed, sensitivity and ability to search large numbers of items, Goodpaster said.

*— Read more in William Kranz et al., “On the smell of Composition C-4,”* Forensic Science International *236 (March 2014): 157-63*

# Bomb blast targeting tram station in Cairo wounds one person

Source: http://www.terrorismwatch.org/2014/03/bomb-blast-targeting-tram-station-in.html

Since the military ousted Islamist president Mohamed Morsi in July, militants have stepped up attacks against the security forces in Egypt, killing many soldiers and policemen.

However, **attacks on civilian targets have been rare**.

**Another homemade bomb was defused at the same station,** the security officials said.

In February, a bomb that struck a bus carrying tourists near the Taba border crossing in South Sinai killed three people, including three South Koreans.

The Al-Qaeda-inspired Ansar Beit al-Maqdis claimed the attack.

It has also claimed responsibility for high-profile attacks including a car bombing at a police headquarters in Cairo and the shooting down of a military helicopter in the Sinai Peninsula.

The Sinai-based group said the attacks were in revenge for a deadly crackdown by the security forces on Morsi supporters.

More than 1,400 people have been killed in the crackdown, according to Amnesty International. Thousands have also been jailed.

# Suicide bomber uses Iraq police Humvee in attack

Source: http://english.alarabiya.net/en/News/middle-east/2014/03/08/Suicide-bomber-uses-Iraq-police-Humvee-in-attack.html

Authorities in Iraq said **a suicide bomber has used a stolen police Humvee to pass through a military checkpoint and set off his explosives, wounding 14 people.**

The attack happened Saturday in Ramadi, the provincial capital of Anbar province, where Iraqi security forces have been battling militants who took control of parts of the town in late December.

Police say militants stole the Humvee and painted it with military colors to trick soldiers into letting it by.

Elsewhere on Saturday, police say a roadside bomb targeting a military vehicle in Baqouba, 35 miles (60 kilometers) northeast of Baghdad, killed a captain and wounded four soldiers.

Medical officials confirmed the casualty figures for the attacks. All officials spoke on condition of anonymity as they weren't authorized to release the information.

## Computer simulations help predict blast scenarios

Source: http://www.homelandsecuritynewswire.com/dr20140319-computer-simulations-help-predict-blast-scenarios

Simulation-based engineering science (SBES) allows researchers to predict the effects of building explosions and analyze the response of building materials to those threats. Using a $400,000, five-year CAREER grant from the National Science Foundation, **researchers at the University of Missouri developed the Material Point Method (MPM) a computer-generated tool which not only creates blast scenarios that informs blast and impact resistant materials and design, but also is crossing over into Hollywood animation — most recently, Disney’s Oscar-winning animated film, Frozen.**

“Motivated by the need for better simulations that demonstrate impact and penetration phenomena, we developed the MPM more than 20 years ago,” said Zhen Chen, C.W. LaPierre Professor of civil and environmental engineering at the College of Engineering at MU. “Since then, the MPM has been further developed and applied by many global research teams to real-world problems including fire, explosions and impacts in buildings and structures. Our first study on the MPM has been cited more than 400 times, and Disney is now using physics-based simulation methods as they create sequences for their popular animated movies including Frozen.”

The computer-based tests developed using MPM can create scenarios that help determine which materials and designs respond most favorably to impact and blast loadings, Chen said. Using the information and analysis provided by simulations, designers can then **validate the results with laboratory tests before applying them to full-scale construction including stronger building components such as columns, walls and windows.**

A University of Missouri release reports that animators at Disney took note of the Material Point Method and used it to develop snow simulations that mimicked snowball drops and smashes. They also animated the effects of characters walking through snowy backdrops.

“We’re proud of the computational methods we’ve developed and our work in SBES through the years,” Chen said. “The nation’s engineering and science communities have become increasingly aware that SBES is an indispensable tool for resolving a multitude of scientific and technological problems facing our country. An added bonus of having the SBES tool used in animation and popular media is that children, who are more touch-oriented through tablets and smartphones, also are fans of Disney and Frozen. We hope they’ll get excited about STEM (science, technology, engineering and mathematics) fields and that our methods will help shape and inspire the next generation of scientists and engineering researchers.”

The release notes that additionally, an interdisciplinary research team at MU is developing a multiscale MPM for creating alternative energy sources, with the most recent study, “A particle-based multiscale simulation procedure within the MPM framework,” to be published in Computational Particle Mechanics.

****Can the F-35 Fighter Jet fighter be Hacked ?

Source: http://i-hls.com/2014/02/f-35-fighter-jet-can-hacked/

The F-35, the latest fighter jet being developed for the U.S. Armed Forces, has hit another potential snag. This time it’s not questions of the jet’s structural integrity or even questions of relevance in combat. It’s the plane’s vulnerability to hackers.

The F-35′s helmet displays an augmented reality overview, which is drawn from six cameras across the body of the plane. This enables the pilot to look around the cockpit and, instead of seeing the interior of the plane, see directly through the cameras at the world outside.

**This computational capability is all run by a computer system called ALIS. Looks basically like a laptop computer, and the pilot carries it out to the plane and sticks it in a slot right next to him in the cockpit. That contains all the information about the mission he’s gonna fly. The servers which run all of this software take up a room about the size of a shipping container.**

**This is a prime target for a hacker.** If the enemy can hack into all that software that’s running the mission, then the fighter aircraft is defeated without firing a bullet.

According to the Business Insider it seems the ALIS has been given too much power over the F-35. For example, ALIS has the ability to ground planes indefinitely if it detects anything wrong with the plane. Human intervention cannot overrule ALIS, either.

If hackers could manage to infiltrate the network that ALIS relies on, it is very possible that they could brick an entire F-35 fleet. This would render the plane, the most expensive weapons system ever, completely useless.

Experts in the U.S say that the probability of hacking the F-35 is very low because its systems are protected. They also say that **when** hackers get more sophisticated more steps should be taken.

## Latest cybersecurity threat: WiFi virus

Source: http://www.homelandsecuritynewswire.com/dr20140226-latest-cybersecurity-threat-wifi-virus

**Researchers at the University of Liverpool have shown for the first time that WiFi networks can be infected with a virus that can move through densely populated areas as efficiently as the common cold spreads between humans.**

The team designed and simulated an attack by a virus, called **Chameleon**, and found that not only could it spread quickly between homes and businesses, **but it was able to avoid detection and identify the points at which WiFi access is least protected by encryption and passwords**.

A University of Liverpool release reports that researchers from the University’s School of  Electrical Engineering, Electronics and Computer Science simulated an attack on Belfast and London in a laboratory setting, and found that Chameleon behaved like an airborne virus, travelling across the WiFi network via Access Points (APs) that connect households and businesses to WiFi networks.

Areas which are more densely populated have more APs in closer proximity to each other, which meant that the virus propagated more quickly, particularly across networks connectable within a 10-50 meter radius.

Alan Marshall, Professor of Network Security at the University, said: “When Chameleon attacked an AP it didn’t affect how it worked, but was able to collect and report the credentials of all other WiFi users who connected to it. The virus then sought out other WiFi APs that it could connect to and infect.”

Chameleon was able to avoid detection as current virus detection systems look for viruses that are present on the internet or computers, but Chameleon is only ever present in the WiFi network. Whilst many APs are sufficiently encrypted and password protected, the virus simply moved on to find those which weren’t strongly protected including open access WiFi points common in locations such as coffee shops and airports.

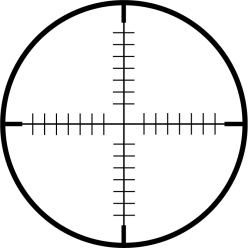
Professor Marshall added: “WiFi connections are increasingly a target for computer hackers because of well-documented security vulnerabilities, which make it difficult to detect and defend against a virus. “It was assumed, however, that it wasn’t possible to develop a virus that could attack WiFi networks but we demonstrated that this is possible and that it can spread quickly. We are now able to use the data generated from this study to develop a new technique to identify when an attack is likely.”

*— Read more in Jonny Milliken et al., “Detection and analysis of the Chameleon WiFi access point virus,” EURASIP* Journal on Information Security *2 (17 October 2013)*

# Hackers target Brazil's World Cup for cyber attacks

Source: http://www.reuters.com/article/2014/02/26/us-worldcup-brazil-hackers-idUSBREA1P1DE2014 0226

Brazilian hackers are threatening to disrupt the World Cup with attacks ranging from jamming websites to data theft, adding cyber warfare to the list of challenges for a competition already marred by protests, delays and overspending.

In a country with rampant online crime, a challenging telecommunications infrastructure and little experience with cyber attacks, authorities are rushing to protect government websites and those of FIFA, soccer's governing body.

Furious about the 33 billion reais ($14 billion) in federal funds being spent on World Cup preparations, more than a million Brazilians took to the streets last June in a wave of mass demonstrations, calling for better public services, greater transparency, and a crackdown on corruption.

Now, hackers say they will join the fray.

"We are already making plans," said an alleged hacker who goes by the nom de guerre of Eduarda Dioratto. "I don't think there is much they can do to stop us."

Reuters contacted Dioratto and other self-proclaimed members of the international hacker network known as Anonymous by finding them online. Though unable to confirm their true identities, Reuters spoke with them in the interest of understanding their threats and what impact they might have on the World Cup.

They said the event offers an unprecedented global audience and an opportune moment to target sites operated by FIFA, the government, other organizers or corporate sponsors.

**"The attacks will be directed against official websites and those of companies sponsoring the Cup," a hacker known as Che Commodore said in a late-night Skype conversation.**

While most of the fretting ahead of the tournament is focused on the completion of stadiums by kickoff on June 12, experts agree that little attention is being paid to Brazil's telecommunications infrastructure.

Problems include overstrained networks, widespread use of pirated software and low investment in online security. To make matters worse, Brazil is home to one of the world's most sophisticated cyber-criminal communities, which is already disrupting ticket sales and other World Cup commerce.

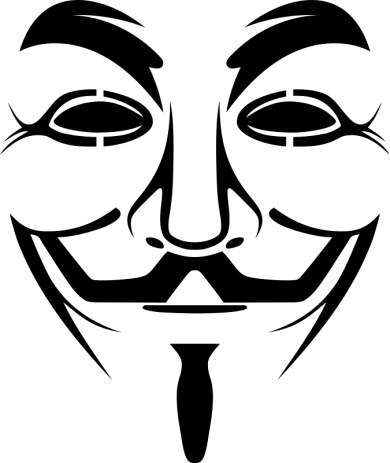
"It's not a question of whether the Cup will be targeted, but when," said William Beer, a cybersecurity expert with the consultancy firm Alvarez & Marsal. "So resilience and response become extremely important."

Brazil says it is ready, or as ready as it can be.

"It would be reckless for any nation to say it's 100 percent prepared for a threat," said General José Carlos dos Santos, the head of the cyber command for Brazil's army. "But Brazil is prepared to respond to the most likely cyber threats."

A FIFA spokesperson declined to comment on online security.

**Fast, damaging and simple**

Known internationally for their high-profile attacks against the U.S. Central Intelligence Agency, Sony and even the Vatican, **Anonymous flexed its muscle in Brazil in 2012 when it disabled the websites of some of the country's biggest banks, including Banco do Brasil, Itaú Unibanco and Bradesco.**

During that attack, dubbed #OpWeekPayment by the hackers, they **launched denial-of-service (DDoS) attacks, in which thousands of computers simultaneously access target websites, jamming them.** The method would be their preferred weapon this time, too.

"It's fast, damaging and relatively simple to carry out," explained Che Commodore.

With that in mind the army created a Cyber Defense Center, which leads a multi-agency task force for the Cup. Besides DDoS attacks, they may also face website defacement and data theft.

The worst-case scenario would be an attack sophisticated enough to cripple Brazil's power grid, communications or air-traffic control systems. But General dos Santos said in a recent interview that authorities aren't expecting anything that bad.

"The probability for that is much lower," he said.

For their part, the Anonymous members said they would not do anything to target the Brazilian people. The government and event organizers, however, are another matter.

And despite the government's preparations, the hackers say they are fully up to speed, and not terribly impressed by what they see as meager defenses.

"It's nothing out of this world", said an activist called Bile Day. "Security remains very low."

Indeed, security experts said Brazil could be caught ill-prepared. The country, with no geopolitical enemies, is not used to being on guard and, as such, may not even be aware of the extent of its vulnerabilities.

"Brazil is a big target, it's neutral and has a challenging infrastructure," said Marcos Oliveira, an executive with U.S. network security firm Blue Coat. "It's the perfect storm."

Aside from the banks, which now invest heavily in online security, Brazilian companies pay little attention to the problem. **And more than half of Brazil's computers run pirate software, which makes them more vulnerable to a denial-of-service attack.**

**Growing breaches**

Brazil is not entirely untested.

The government grew far more sensitive to cybersecurity issues last year after reports that the U.S. National Security Agency spied on President Dilma Rousseff and millions of ordinary Brazilians.

Officials have also tracked a growing number of online security breaches during other big events in recent years. **In 2012, during a United Nations conference on climate change in Rio de Janeiro, the cyber command detected 140 attempted security breaches. Attacks climbed to more than 300 for last year's Confederations Cup, a dress rehearsal for the World Cup.**

"We expect that number to be much higher for the Cup," said General Dos Santos. And they will likely increase once again when Rio hosts the 2016 Olympics.

**ATOS, a French company in charge of information technology networks for the Rio Olympics, said it detected around 255 million security events during London 2012.**

"It's huge," said Michele Hyron, who heads the ATOS team for the Rio games. "And it had absolutely no impact on the Games."

Problems can occur ahead of the events, though, especially in a country with fast-growing Internet access and booming online banking services, but little regulation for either.

Seeking to capitalize on the massive demand for World Cup tickets, criminals are already finding ways to steal from would-be buyers online.

Most of the attacks are so called "phishing," where users are redirected to fake sites of banks and firms and tricked into entering their credit card data. **Online security firm Kaspersky said it is blocking between 40 and 50 fraudulent sites using the theme of the Cup daily.**

"The World Cup is the theme of the moment," said Fabio Assolini, a security analyst with Kaspersky in São Paulo, "and cyber criminals are taking full advantage of that."

# World's biggest cyberattack detected

Source: http://timesofindia.indiatimes.com/tech/tech-news/internet/Worlds-biggest-cyberattack-detected-360-million-accounts-1-25-billion-email-addresses-hacked/articleshow/31133867.cms

An internet security firm has stumbled upon a "mind boggling" and "Godzilla-sized" cache of personal data put up for sale on the online black market by hackers.

**One of the hacker attacks stole over 105 million records making it the single largest data breach in cybercrime history.**

**The trove included credentials from more than 360 million accounts and around 1.25 billion email addresses.**

**The discovery was made by cybersecurity firm Hold Security.** "These credentials can be stolen directly from your company but also from services in which you and your employees entrust data. In October 2013, Hold Security identified the biggest ever public disclosure of 153 million stolen credentials from Adobe Systems. One month later we identified another large breach of 42 million credentials from Cupid Media," the firm said.

They accumulated the data over the past three weeks. The company first tracked over 300 million abused credentials that were not disclosed publicly (that is over 450 million credentials if one counts the Adobe find).

"But this month we exceeded all expectations. In the first three weeks of February we identified nearly 360 million stolen and abused credentials and 1.25 billion records containing only email addresses. These mind boggling numbers are not meant to scare you and they are a product of multiple breaches which we are independently investigating. This is a call to action," it added.

"The sheer volume is overwhelming," said Alix Holden, chief information security officer of Hold Security.

Hold Security says that the email addresses came from all major providers including Google, Microsoft and Yahoo, and that many non-profit organizations and almost all Fortune 500 companies had been affected.

This comes just months after details of 2.9 million people across the globe were stolen in a highly sophisticated cyberattack on Adobe.

Adobe's security team announced recently that the attackers accessed Adobe customer IDs and encrypted passwords on its systems and removed information including customer names, encrypted credit or debit card numbers, expiration dates and customer orders.

# Power grid vulnerable to cyberattack, report says

Source: http://www.bostonglobe.com/business/2014/03/03/report-calls-for-better-protection-power-grid-from-cyberattacks/Z6LUuqBbt4izvdyHOZUW4H/story.html

Despite rising anxiety over the possibility of a cyberattack on the power grid, the industry and government are not set up well to counter the threat, according to a report produced by leading energy security experts.

**Companies are reluctant to share information with one another, a critical step in reducing vulnerability, because they are afraid of being accused of failing to comply with cybersecurity rules, committing antitrust violations, or giving away proprietary information, the report found.**

**And federal rules intended to protect the electric system from cyberattack are inadequate because they do not give companies an incentive to continually improve and adapt to a changing threat, according to the report, released Friday (Feb 28).**

The report was produced by the Bipartisan Policy Center, a Washington nonprofit group, and led by Michael V. Hayden, a former CIA director; Curt Hébert Jr., a former chairman of the Federal Energy Regulatory Commission; and Susan Tierney, a former assistant energy secretary and former utility regulator in Massachusetts.

**The experts also found that while the government had focused on the high-voltage power grid, less work has been done on the lower-voltage distribution system, which could cause problems that would propagate up the chain.**

Cyberwarfare is “a domain that favors the attacker,” Hayden said in a panel discussion Friday. But he said the United States could reduce its vulnerability and improve its ability to recover. He even quoted a line spoken by John Wayne in the film, “Sands of Iwo Jima”:

“Life is tough, but it’s tougher if you’re stupid.”

Most hacking against utilities is done by people who are trying to steal financial data, including that of customers, but experts fear an act of war, or what Hayden called “recreational espionage.”

Not even public utility commissions are well set up for new problems, the report said. Regulated utilities can add security costs to the expenses for which they bill their customers, if the regulators find the expenditures “prudent,” but “many regulators lack the expertise to make these judgments,” the report said.

And many entities on the grid are unregulated in a competitive market, which may make it hard for them to recover their costs.

The report recommended establishing a group like one set up after the Three Mile Island accident in 1979 by the nuclear industry, the Institute of Nuclear Power Operations, to conduct peer-to-peer audits and disseminate best practices.

Outside experts who were not involved with the report endorsed some of its findings. Samuel P. Liles, an associate professor at Purdue, where he works in the Cyber Forensics Laboratory, said that sharing best practices was “a hit or a miss,” although threat information was shared.

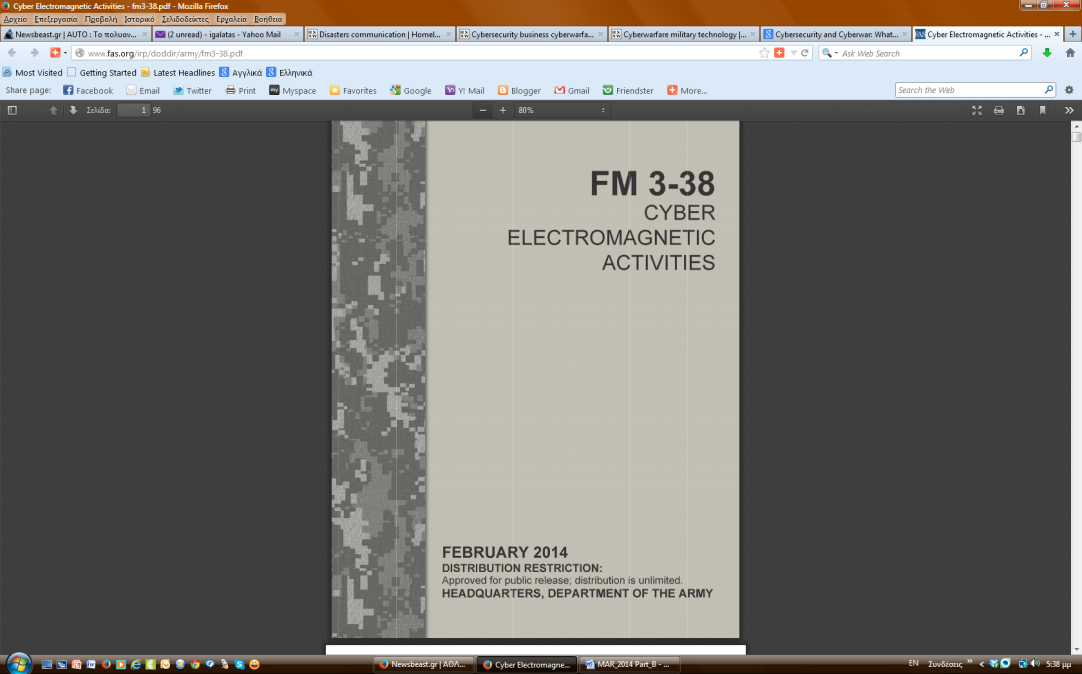
At the Utilities Telecom Council, a trade association of electric and water utilities, Nadya Bartol, a cybersecurity expert, said the report was correct in asserting that utilities might not always come forward with helpful information.

**“If utilities say, ‘I have this vulnerability,’ they might get fined if that’s a violation,” she said. And they may hesitate to talk about their vulnerabilities because, “if I put it out in the public space, I will get hacked more.”**

The report raised the issue that public utility commissioners, who decide which utility expenses are “prudent” and eligible to be passed on to customers, have trouble determining the value of such investments. At the National Association of Regulatory Utility Commissioners, a nationwide organization of state commission members, Miles Keogh, coauthor of a paper on evaluating such investments, said commissioners should approach the problem as a management audit and not get into the details of security.

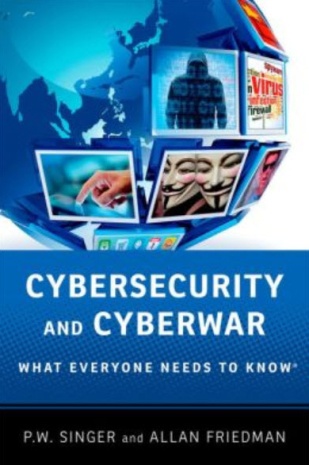
## U.S. Army releases first field manual for war in the electromagnetic spectrum

Source: http://www.homelandsecuritynewswire.com/dr20140306-u-s-army-releases-first-field-manual-for-war-in-the-electromagnetic-spectrum

**The U.S. Army recently released its first field manual for Cyber Electromagnetic Activities (CEMA).** The Pentagon defines cyber electromagnetic activities as activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy the use of such capabilities, and protecting the mission command system.

Defense One reports that the manual reflects the Army’s belief that dominance in electromagnetic capabilities is as important as its cyber-capabilities. In its 2013 Electro-magnetic Spectrum Strategy report, the Pentagon notes that its operations in air, on land, on and under the sea, in space, and in cyberspace are fundamentally dependent on its use and control of the electro-magnetic spectrum.

Electromagnetic spectrum (ES) covers all electromagnetic radiation, including infrared, radar, television, and radio waves. **The Army’s field manual details its electronic warfare operations, which include disabling enemy communications and destroying enemy equipment with large bursts of electromagnetic radiation.**

The manual does not detail how to conduct specific attacks, **but it does offer soldiers examples of what electro-magnetic warfare looks like in terms of protocol, terminology, and command and control.** The Field Manual also offers detailed descriptions of the Army’s cyber-operations chain of command, functions of cyberspace operations, battle protocols, and the multinational and legal considerations for various cyber-actions.

Access to the electromagnetic spectrum is needed to operate several Army operations, from flying a drone to using radar to landing a plane. Some experts question the Army’s grouping of cyber operations with electro-magnetic spectrum warfare. “While there are strong similarities, cyber operations have a broader range of capacities than the traditional electronic warfare strategic role, and can support a wider range of operations. Similarly, the counter-electronic warfare capacity has a more limited scope than the huge needs to defend our military infrastructure from cyber exploitation and disruption,” said Allan Friedman, co-author of the book Cybersecurity and Cyberwar: What Everyone Needs to Know, told Defense One.

**Retired Lt. Gen. Robert Elder, a George Mason University research professor and former Air Force cyber officer, does not agree with Friedman’s position, saying that “the new (field manual) makes it clear that conducting these activities independently may detract from their efficient employment,” he said. “This provides a useful mechanism for the traditional and (cyber electromagnetic activities) communities to effectively communicate with one another.”**

The Army’s renewed focus on electromagnetic spectrum dominance comes at a time when the technology is widely available on the lower end of the market, driven by consumer demand for better wireless broadband networks, but the high level use of electromagnetic technology could be compromised by terrorists and adversaries.

Sergei Gorshkov, former Admiral of the Fleet of the Soviet Union, once remarked**, “the next war will be won by the side that best exploits the electromagnetic spectrum.”** The U.S. Army agrees.

## Securing Industry 4.0

Source: http://www.homelandsecuritynewswire.com/dr20140306-securing-industry-4-0

An increasing number of unsecured, computer-guided production machinery and networks in production facilities are gradually evolving into gateways for data theft. New security technologies may directly shield the sensitive data that is kept there.

You can hear the metallic buzz as the milling machine bores into the work piece. Just a few last drill holes, and the camshaft is complete. The computer-guided machine performed the entire job — thanks to the digital manufacturing data that were uploaded onto its embedded computer beforehand. Everything runs without a hitch, only — the data are stolen.

Manufacturing data determine the production process for a product, and are just as valuable today as the design plans. They contain distinctive, inimitable information about the product and its manufacture. Whoever possesses this info merely needs the right equipment, et voilà: the pirated or counterfeit product is done. Whereas design data are well-protected from unauthorized outside access today, production data often lie exposed and unsecured in the computer-assisted machinery. An infected computer on the network, or just a USB stick, are all a thief would need to heist the data. Or hackers could directly attack the IT network — for instance, through unsecured network components, like routers or switches.

**Encrypting manufacturing data upon creation**

A Farunhofer release reports that researchers at the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt are exhibiting how these security gaps can be closed up at this year’s CeBIT,which will be held 10-14 March 2014. They will be presenting, for example, a software application that immediately encrypts manufacturing data as soon as they emerge. Integrated into computer and equipment, they ensure that both communicate with each other through a protected transportation channel and that only licensed actions are executed. “To the best of our knowledge, no comparable safeguard has previously existed for manufacturing data that reside directly in the machine tool,” states Thomas Dexheimer from the SIT’s Security Testlab.

Digital Rights Management (DRM) controls all important parameters of the assignment, such as designated use, quantity, etc. This way, brand manufacturers are able to guarantee that even external producers can only produce an authorized quantity, as instructed in advance — and no additional pirated units.

His colleague at SIT, Dr. Carsten Rudolph, is more involved with secured networks. At CeBIT, Rudolph will exhibit his “Trusted Core Network.”

“Hackers can also gain access to sensitive production data via unsecured network components. These are small computers themselves, and can be easily manipulated,” says the Trust and Compliance department head at SIT.

In order to prevent this, he called upon one piece of technology which, for the most part, lies dormant (in deep slumber) and, for all intents and purposes, unused on our PCs: the Trusted Platform Module. This relates to a small computer chip that can encrypt, decrypt, and digitally sign the data. Installed into a network component, it indicates which software is running on the component, and assigns a distinct identity to it. “As soon as the software changes in a component, the adjacent component registers this occurrence and notifies the administrator.

Hacker attacks can be exposed quickly and easily this way,” says Rudolph.

“Both security technologies are important building blocks for the targeted Industry 4.0 scenario,” says Dexheimer.

**The term “Industry 4.0” stands for the fourth industrial revolution. After water and steam power, followed by electrical energy, electronics and information technology, now, the cyber-physical systems (IT systems embedded in machinery that communicate with each other via wireless or cabled networks) and the Internet of Things are expected to move into the factory halls. “This revolution can only work if the intellectual property is sufficiently protected. And that’s a tall order, because the targets of production IT will increase exponentially, due to ever growing digitization and networking,” explains Dexheimer.**

At this year’s CeBIT, both researchers — Dexheimer and Rudolph — will present a computer-assisted machine tool using a CAD computer and a 3D printer. SIT’s security software is installed both on the computer and the printer. The data are encrypted on the computer, and decrypted by the printer. The printer also validates the licensed authorization to conduct the print job. To ensure that the data are also securely embedded in the network, the scientists have built a Trusted Platform Module into multiple routers, and are displaying this as a demo.

“An attacker cannot hack this there, because he or she will get nowhere near the built-in key,” explains Rudolph.

## Safeguarding networks when disasters strike

Source: http://www.homelandsecuritynewswire.com/dr20140306-safeguarding-networks-when-disasters-strike

Disasters both natural and human-caused can damage or destroy data and communications networks.

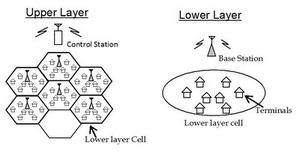
**New algorithm for cloud data**

Much of our computing these days, from browsing Web sites and watching online videos to checking e-mail and following social networks, relies on the cloud. The cloud lives in data centers — massive warehouses filled with thousands of servers that run constantly. Disasters such as earthquakes, tornadoes, or even terrorist attacks, can damage the data centers and the communication links between them, causing massive losses in data and costly disruptions.

An Optical Society of America (OSA) release reports that to mitigate such potential damage, researchers from the University of California, Davis, Sakarya University in Turkey, and Politecnico de Milano in Italy, first analyzed the risk that a disaster may pose to a communications network, based on the possible damage of a data center or the links that connect them to users. Then, they created an algorithm that keeps data safe by moving or copying the data from data centers in peril to more secure locations away from the disaster. The algorithm assesses the risks for damage and users’ demands on the network to determine, in real-time, which locations would provide the safest refuge from a disaster.

“Our content placement solution can be implemented with some modifications on any existing settings of data centers and it is adaptable to different dynamic disaster scenarios,” said researcher Sifat Ferdousi of UC Davis. “This can highly benefit the network providers in designing disaster-resilient cloud networks.”

**Integrating wireless with fiber for temporary emergency networks**

Earthquakes, tsunamis, and other natural disasters can sever the optical fibers that carry data across long distances, leaving telecommunications networks useless. If fiber-optic cables are down, wireless communication can fill the void and be part of a temporary, emergency network. For such a system to work, however, wireless technology would have to be integrated with the fiber-optic network that transports data around the world.

Such an integrated wireless optical system would combine the speed and bandwidth of fiber optics with the mobility and range of a wireless network. This system could also be applied in home networks, in which data is sent via optical cables to the home then broadcasted wirelessly.

One big challenge of an integrated system, however, is to develop the wireless links that can handle the speed and capacity of optical cables. Researchers from Fudan University in Shanghai and ZTE (TX), Inc. in Morristown, New Jersey, have now developed a new antenna architecture that allows for a simple and high-speed integrated wireless optical system. The design relies on two pairs of antennas, explains Jianjun Yu of ZTE. Because each pair is polarized differently and isolated, there’s no interference between the two pairs, allowing for a simpler structure and a larger transmission capacity. The new system achieves a data-transmission rate of 146 gigabits per second (Gb/s), which is the highest bit-rate-per-channel in a wireless signal shown so far, Yu says.

# Quantum cryptography put to work for electric grid security

Source: http://www.lanl.gov/newsroom/news-releases/2013/February/02.13-quantum-cryptography. php?utm\_source=Quantum+Cryptography%3A+Has+the+White+House+Heard+of+It%3F&utm\_campaign=America%27s+Commercial+Air+FleetNeeds+Protection+from+Shoulder-Fired+Missiles&utm\_medium=email

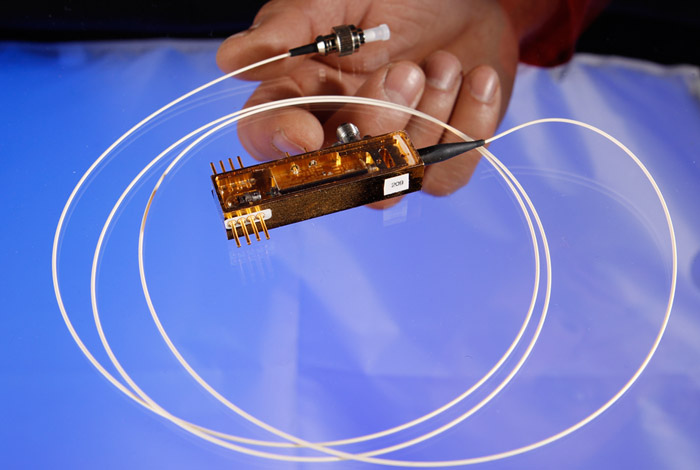
Recently a Los Alamos National Laboratory quantum cryptography (QC) team successfully completed the first-ever demonstration of securing control data for electric grids using quantum cryptography.

The demonstration was performed in the electric grid test bed that is part of the Trustworthy Cyber Infrastructure for the Power Grid (TCIPG) project at the University of Illinois Urbana-Champaign (UIUC) that was set up under the Department of Energy’s Cyber Security for Energy Delivery Systems program in the Office of Electricity Delivery and Energy Reliability.

Novel methods for controlling the electric grid are needed to accommodate new energy sources such as renewables whose availability can fluctuate on short time scales. This requires transmission of data to and from control centers; but for grid-control use, data must be both trustworthy and delivered without delays. The simultaneous requirements of strong authentication and low latency are difficult to meet with standard cryptographic techniques. New technologies that further strengthen existing cybersecurity protections are needed.

Quantum cryptography provides a means of detecting and defeating an adversary who might try to intercept or attack the communications. Single photons are used to produce secure random numbers between users, and these random numbers are then used to authenticate and encrypt the grid control data and commands. Because the random numbers are produced securely, they act as cryptographic key material for data authentication and encryption algorithms.

At the heart of the quantum-secured communications system is a unique, miniaturized QC transmitter invention, known as a QKarD, that is five orders of magnitude smaller than any competing QC device. Jane Nordholt, the Los Alamos principal investigator, put it this way: “This project shows that quantum cryptography is compatible with electric-grid control communications, providing strong security assurances rooted in the laws of physics, without introducing excessive delays in data delivery.”

A late-2012 demonstration at UIUC showed that quantum cryptography provides the necessary strong security assurances with latencies (typically 250 microseconds, including 120 microseconds to traverse the 25 kilometers of optical fiber connecting the two nodes) that are at least two orders of magnitude smaller than requirements. Further, the team’s quantum-secured communications system demonstrated that this capability could be deployed with only a single optical fiber to carry the quantum, single-photon communications signals; data packets; and commands. “Moreover, our system is scalable to multiple monitors and several control centers,” said Richard Hughes, the co-principal investigator from Los Alamos.

The miniature transmitter communicates with a trusted authority to generate random cryptographic keys to encode and decode information

The TCIPG cyber-physical test bed provides a realistic environment to explore cutting-edge research and prove emerging smart grid technology in a fully customizable environment. In this demonstration, high-fidelity power simulation was leveraged using the real-time digital simulator to enable hardware in the loop power simulation to drive real phasor measurement units (PMUs), devices, deployed on today's electric grid that monitor its operation.

“The simulator provides a mechanism for proving technology in real-world scenarios,” said Tim Yardley, assistant director of test bed services. “We're not just using perfect or simulated data, so the results demonstrate true feasibility.”

The power simulation was running a well-known power-bus model that was perturbed by introducing faults, which drove the analog inputs on the connected hardware PMU. The PMU then communicated via the standard protocol to the quantum cryptography equipment, which handled the key generation, communication and encryption/decryption of the connection traversing 25 kilometers of fiber. A phasor data concentrator then collected and visualized the data.

“This demonstration represents not only a realistic power model, but also leveraged hardware, software and standard communication protocols that are already widely deployed in the energy sector,” said William H. Sanders, the Donald Biggar Willett Professor of Engineering at UIUC and principal investigator for TCIPG. “The success of the demonstration emphasizes the power of the TCIPG cyber-physical test bed and the strength of the quantum cryptography technology developed by Los Alamos.”

The Los Alamos team submitted 23 U. S. and foreign patent applications for the inventions that make quantum-secured communications possible. The Los Alamos Technology Transfer Division has already received two licensing inquiries from companies in the electric grid control sector, and the office plans an industry workshop for early 2013 when the team’s patents will be made available for licensing.

The Los Alamos team is seeking funding to develop a next-generation QKarD using integrated electro-photonics methods, which would be even smaller, more highly integrated, and open the door to a manufacturing process that would result in much lower unit costs.

.

# Russia's Cyber-Weapons Hit Ukraine: How to Declare War Without Declaring War

**By Alec Ross**

Source: http://www.huffingtonpost.com/alec-ross/russias-cyber-war\_b\_4932475.html

The playground fights I got into when I was a kid had closely observed, unwritten rules: you could punch, you could kick and you could even choke your opponent, but you couldn't use a weapon. Pick up a rock or a stick and bring that into the fight and you were going to earn the derision, and maybe a butt-kicking, from the entire playground crowd.

Similarly, during the Cold War there were some important, unspoken rules about combat. It was okay if militaries of Soviet and American satellite States fought and killed each other, but it was not okay for an American or Soviet soldier to engage one another directly, lest the uneasy equilibrium in that Great States conflict between the world's two superpowers be thrown off balance.

Today, utilizing cyber weapons falls into the category of largely being accepted (even if unhappily) as part of how countries exercise their power while falling short of the line of armed conflict treated as an act of war.

We will see if this can hold.

**The latest example of firing off a cyber weapon is a Russian cyber weapon called Snake, also known as "Ouroboros" after a serpent drawn from Greek mythology.** Ouroboros is wrecking havoc on Ukrainian government systems. It is interesting in that it has the characteristics of both a product of the intelligence services (the ability to surveil) but also of the military (the ability to physically destroy computer networks).

By targeting the Ukrainian government with Ouroboros, the Russians are able to effectively engage in an aggressive, kinetic act without actually declaring war or countries reacting like it is an act of war.

This will not last forever. If certain capabilities of Ouroboros go live then we will see if the playground rules hold. **If the Russians deploy cyber weapons with network-destroying capabilities into other countries, there might well be one country that reacts as though the launch of a cyber weapon is no different than the launch of a missile.** You see where it goes from here.

The absence of a set of broadly-held norms and treaties governing the use of cyber weapons has not led to the firing of guns or launching of missiles, but this will not always be the case. We need something more than playground rules.

* **Ouroboros** ► **Greek:** *oura* (tail) + *vrosi* (to eat) 🡺 snake/dragon eating each own tail.

**Alec Ross** is a senior fellow at Columbia University's School of International and Public Affairs. During the first Obama term, he served as senior adviser for Innovation to Secretary of State Hillary Clinton.

►**Read also this “strange” article:** http://projectumbrella.net/articles/Uroboros-Virus

## “Hacker schools” grow to meet growing demand for programmers

Source: http://www.homelandsecuritynewswire.com/dr20140321-hacker-schools-grow-to-meet-growing-demand-for-programmers

The increasing demand for computer programmers in the job market has led to the growth of “hacker schools,” an alternative to traditional education that offers students a quicker, cheaper, and effective way to learn computer programing.

There is a shortage of qualified job applicants in the computer software category, according to Tino Mantella, director of the Technology Association of Georgia. A recent survey by the group found roughly 4,000 open high tech positions in Georgia, and it often takes up to six months for employers to find the right candidates.

GovTech reports that hacker schools do not offer certificates or diplomas, instead they claim to target students who currently have degrees in other fields but who want a career change. Dr. Jenny Grace, an eighteen-year ob-gyn, told GovTech that she decided to shift careers to computer science, but was unable to dedicate two to four years to traditional education. Grace attended Tech Talent South, an Atlanta-based hacker school which offers a two month computer science course. Upon completion of the course, Grace was able to code and landed an internship with a local software developer.

Shane Pike, head of EngineerJobs.com, an online classified advertising site for engineering jobs, agrees that hacker schools are helping fuel the supply of tech savvy job applicants. “People have been seeing this shortage for a long time,” he said. “That’s the reason these alternative schools are popping up. I’ve been hiring software engineers since 1998. It’s always been hard to find good ones.”

Hacker schools have spread to other cities with high-tech markets like New York, Boston, and San Francisco. The Iron Yard, a hacker school based in South Carolina, will open in Atlanta at the end of March. More than sixty students have graduated from The Iron Yard’s Greenville, South Carolina campus. William Haynes, CEO of Sabia Technology, a South Carolina router manufacturer, recently hired a programmer from The Iron Yard. “We have a huge need for inquisitive and smart programmers who can create a structure rather than conform to one,” Haynes said. “When you hire from one of these schools, you get an enthusiastic and focused individual who has just spent their most recent months focused on learning, creating and developing in areas where they’ve never been before.”

The Iron Yard’s program takes three months and costs $9,000, while Tech Talent South’s two-month program costs $6,250 for full-time students and $4,250 for part-time students. The Iron Yard guarantees job placement in six months or students may request a refund.

Hacker School in New York requires students to have some prior programing experience because it operates a free education course, and charges an average $20,000 recruiting fee to employers who hire its graduates.

Though hacker schools are meeting a demand in the market for computer programming education, some industry experts disagree with the method. Jeff Atwood, a software developer and author of the blog Coding Horror, criticized hacker schools, saying “they imply that there’s a thin, easily permeable membrane between learning to program and getting paid to program professionally.”

Hacker schools have not been subjected to federal regulations, but Richard Simms, co-founder of Tech Talent South, said, “programs like ours are unique in that they don’t confer or claim to confer degrees of higher education or professional or occupational licenses. So, like in many aspects of tech, there may not be a neat fit with the existing regulatory framework. (We) will be prepared to adapt to any regulatory developments in our part of the country.”

# Cybercriminals use fake MH370 websites to steal data

Source: http://www.terrorismwatch.org/2014/03/cybercriminals-use-fake-mh370-websites.html

Cybercriminals are exploiting the disappearance of a Malaysia Airlines plane by luring users to websites purporting to offer the latest news in order to steal their personal information, an Internet security firm warned Tuesday.

Trend Micro urged Internet users to exercise caution when clicking on links shared on social media for news of flight MH370, which mysteriously vanished from the radar in the early hours of March 8 while on its way from Kuala Lumpur to Beijing.

There is no trace of the aircraft or the 239 people on board, despite a massive international search.

Trend Micro said its global network of research, service and support centres TrendLabs had spotted an executable file disguised as a video that, when clicked, allowed scammers to collect a user's data, such as his or her IP address.

"Given the heightened interest in the missing flight, it was only time (before) cybercriminals used it to their advantage," TrendLabs expert Paul Oliveria said in a statement.

Another scam enticed Facebook users to click a link that leads to a page with the heading: "(BREAKING NEWS) Malaysia Plane Crash into Vietnam sea MH370 Malaysia Airlines is found!"

When the link is clicked, users are taken to a fake page with a "ready to play" video. Further clicks will prompt the user to share the link before the video can be viewed.

"Sharing the video, of course, helps cybercriminals spread their malicious link to other users," Trend Micro said in a statement.

After sharing, the user will be asked to verify his age by completing a 'test'. The test was "nothing but another survey scam," it said.

Trend Micro added that cybercriminals have previously used tragedies such as last year's Super Typhoon Haiyan in the Philippines and the deadly bomb attack on the Boston Marathon to lure unsuspecting users to malicious websites.

# French cyberwarfare expert elaborates on fear of tipping off terrorists at Vancouver conference

**By Gillian Shaw (**Vancouver Sun March 13, 2014)

Source:http://www.vancouversun.com/news/French+cyberwarfare+expert+elaborates+fear+tipping+terrorists+Vancouver+conference/9613614/story.html

*Earlier I wrote about French cyberwarfare specialist Eric Filiol’s decision to withdraw his presentation from CanSecWest Vancouver, the security conference now underway in Vancouver. After I posted that story, I heard back from Eric, who emailed me a note explaining his decision to withdraw from the conference. I was then able to interview Eric, who is in France, by phone. Basically, I learned he made the decision not to present his findings to CanSecWest because he realized he would be outlining a blueprint that could be used to terrorists or others intent on destroying critical infrastructure in the United States or other countries. Here is the story I wrote from that interview:*

VANCOUVER — An eminent French cyberwarfare specialist scheduled to present a talk at a Vancouver security conference has withdrawn his presentation, saying he fears sharing the results of research that shows how open data can be mined by terrorists could result in attacks against the United States or other countries.

**The talk, “Hacking 9/11: The next is likely to be even bigger with an ounce of cyber,” was to be presented at CanSecWest Vancouver 2014 by Eric Filiol, who heads up the Operational Cryptography and Computer Virology lab in Laval, France, and is a 22-year veteran of the French military with a background in intelligence and computer warfare.**

But Filiol withdrew his research presentation in which he would have shown how open data can be mined, making it possible to mount large-scale attacks and bring down critical infrastructure such as transportation, power, financial and emergency services, with as few as 10 attackers.

In a telephone interview from France, Filiol said he made the decision to withdraw from the conference because he realized that in sharing his research he would be revealing a technique that, in the wrong hands, could be used to launch an attack.

“It could be misused by the bad guys,” said Filiol, who added that his decision was not ordered by the French government. He said his decision was prompted by moral and legal considerations.

“Just imagine I publish how to strike the USA and people use that. It would be a nightmare. There is a point you have to speak to yourself and say you cannot do that.”

Filiol said the proliferation of open data, not cyberwarfare, poses the larger threat to countries’ critical infrastructures. Used by terrorists, it could lead to attacks of the magnitude of 9/11.

**“You would be surprised what we can find in open data,”** he said. “I think it’s nonsense, it’s total madness. Nation states should be aware of that and be careful about the data they release.”

He said while governments and corporations worry about cyberwarfare, the reality is that cyberattacks can do little damage compared to real-world attacks by small groups armed with information they can extract from data being made freely available.

“I think the big threat nowadays is the huge quantity of open data,” he said, adding that while the risk may not be obvious, mathematical modelling can reveal vulnerabilities.

From open data, he said, people planning attacks can extract “hidden information that may be very critical because it is revealing a very interesting point of weakness — where to strike, what is very important in critical infrastructure.

**“I think the biggest threat is that everything is available to an attacker if they combine the data with mathematical modelling. I think in the forthcoming years we will see very dramatic attacks.”**

Filiol, whose lab is carrying out simulations in its research, said he had to withdraw from the Vancouver conference because he would have to present the scientific proof of his research findings, and in doing so, the technique would be made public.

“Cyber attacks will always be used, but in a very limited way,” said Filiol. He said in the case of cyber attacks seeking to exploit a software vulnerability, the attackers don’t know if the vulnerability has been patched or other circumstances that might limit the impact of their attack.

“You can patch software, but you cannot change the place of a building. You cannot change the map of railway lines,” he said.

CanSec conference organizer Dragos Ruiu said it was the view of the French Ministry of the Interior and the Department of Defense that the topic was better discussed among closed user groups. Ruiu dismissed criticism that the withdrawal of the presentation amounted to censorship by the French government.

The withdrawal of the report prompted criticism from some security experts, and ignited the debate over “security through obscurity.”

“This is an age-old debate — security through obscurity is the magic phrase,” said Ruiu. “The big debate is whether you should be hiding this stuff or whether you should be trying to find a fix as soon as possible.”

****Countries must be more prepared for crises, UN warns

Source: http://www.thenational.ae/uae/countries-must-be-more-prepared-for-crises-un-warns

Abu Dhabi – With the number of global conflicts rising and a world that is growing increasingly dangerous and unpredictable, the United Nations has urged countries to be more prepared to respond to crises.

Antonio Guterres, the UN High Commissioner for Refugees (photo), said the multiplying conflicts had become increasingly more difficult to address while the capabilities of nations to solve them have become more limited.

**“Preparedness and response is something we badly need in today’s world – a world that is dangerous and unpredictable,”** he said. “We don’t know where the next crisis will be and unpredictability has become the name of the game.”

He said the number of new conflicts had multiplied in recent years, in countries including Mali, Cote d’Ivoire and Libya, while old conflicts, in Afghanistan and the Republic of Congo, remained.

“Today, we no longer live in a unipolar world,” he said. “We live in a kind of chaotic world, there’s no global governance system and power relations became unclear. There are very limited capabilities for nations to solve crises, like in Syria, and the capability to address the needs of people becomes more difficult.”

**In the past 35 years, the Arab region has faced 272 crises that have led to the death of more than 100,000 people.**

“These challenges or responsibility of facing them require readiness to deal with all the phases of emergencies and ensure their competent management and full recovery,” said Dr Nabil Elaraby, the Arab League’s secretary general. “This is why all experts and specialists focus on resilience and the capability of facing challenges.”

**Climate change, food and water security, and urbanisation have become more interlinked.**

“They create conditions for us to create a multiplication of disasters with more frequent and more dramatic consequences, like drought, which occurs every two years now,” Mr Guterres said. “Resources and capacities are not growing as far as the needs that we witness in today’s world, so it’s important to have preparedness and response.”

Dr Elaraby said the nature of some crises and disasters would require a high level of preparedness at all levels in the country.

“This would require a change in mentality in the way of dealing with emergencies and crises,” he said. “It’s always better to be well-prepared rather than facing the emergency or crisis when it happens.”

He said it had become one of the most important and urgent topics in the region.

“Almost every country is affected by disasters, emergencies and crises, regardless of their advanced capabilities. Response to such incidents requires an advanced infrastructure and specific response plans, which need constant updates amid the unexpected and continuous crises in some countries.”

Mr Guterres said partnership was key.

“As an organisation, we have 2,400 people working in and around Syria,” he said. “We’ve been able to mobilise almost US$1 billion (Dh3,67bn) of donations to support Syrian refugees last year and help 4.5 million people. Every single day, 130,000 relief items were moved, so the whole year represents a massive effort.”

**More than seven million Syrians are displaced.**

“Nowadays, crises are longer, they go on and on, seeming never to end,” he said. “Our objective is to be able to mobilise the people and equipment necessary to support 600,000 displaced in 72 hours, wherever that displacement takes place.”

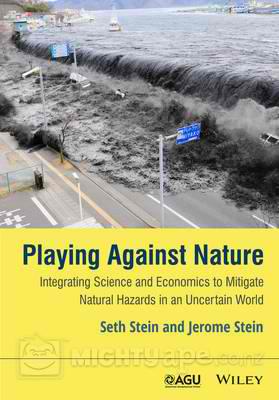
He thanked Sheikha Fatima bint Mubarak, mother of the nation, and Sheikha Jawaher bint Mohammed Al Qasimi, the wife of Sharjah’s ruler, for their contributions.

**“Nobody can do it alone, we need to do it together,”** he said. “Partnership is essential for success, with the government, civil society and international organisations. This is particularly true in the UAE and the Gulf.

“It is the devotion deeply rooted in the best values of Islamic tradition and law, and the devotion of personalities like these that give us strength and courage to go on against all odds preparing ourselves and responding to dramatic crises that make more and more people suffer in today’s world.”

# Planners need to think carefully about costs and benefits to outsmart nature during disasters

Source: http://www.medicalnewstoday.com/releases/272800.php?tw

The dramatic images of natural disasters in recent years, including hurricanes Katrina and Sandy and the Tohoku, Japan, earthquake and tsunami, show that nature, not the people preparing for hazards, often wins the high-stakes game of chance.

"We're playing a high-stakes game against nature without thinking about what we're doing," geophysicist Seth Stein of Northwestern University said. "We're mostly winging it instead of carefully thinking through the costs and benefits of different strategies. Sometimes we overprepare, and sometimes we underprepare."

Stein discussed his research in a presentation titled "How Much Natural Hazard Mitigation is Enough?" at the American Association for the Advancement of Science (AAAS) annual meeting in Chicago. His presentation was part of the symposium "Hazards: What Do We Build For?" held at the Hyatt Regency Chicago.

Stein is the William Deering Professor of Geological Sciences in Northwestern's Weinberg College of Arts and Sciences. He is the author of a new book, **"Playing Against Nature: Integrating Science and Economics to Mitigate Natural Hazards in an Uncertain World"** (Wiley, 2014) and the book "Disaster Deferred: A New View of Earthquake Hazards in the New Madrid Seismic Zone" (Columbia University Press, 2010).

Sometimes nature surprises us when an earthquake, hurricane or flood is bigger or has greater effects than expected. In other cases, nature outsmarts us, doing great damage despite expensive mitigation measures or causing us to divert limited resources to mitigate hazards that are overestimated.

**"To do better we need to get smarter,"** Stein said. **"This means thoughtfully tackling the tough questions about how much natural hazard mitigation is enough. Choices have to be made in a very uncertain world."**

Stein's talk used general principles and case studies to explore how communities can do better by taking an integrated view of natural hazards issues, rather than treating the relevant geoscience, engineering, economics and policy formulation separately.

**Some of the tough questions included:**

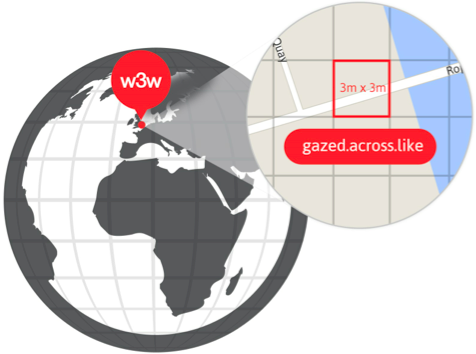
* How should a community allocate its budget between measures that could reduce the effect of future natural disasters and many other applications, some of which could do more good? For example, how to balance making schools earthquake resistant with hiring teachers to improve instruction?
* Does it make more sense to build levees to protect against floods or to prevent development in the areas at risk?
* Would more lives be saved by making hospitals earthquake resistant or by using the funds for patient care?

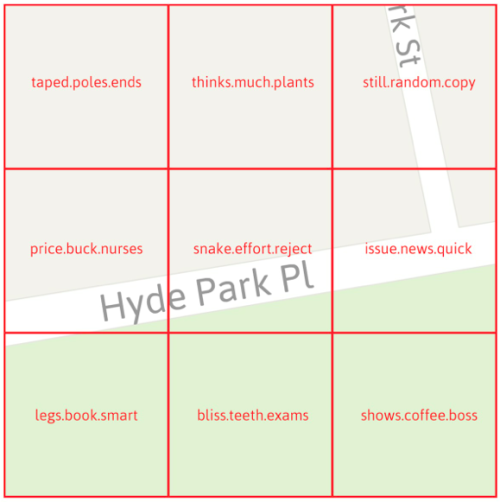
The choice is difficult because although science has learned a lot about natural hazards, Stein says, **our ability to predict the future is much more limited than often assumed.** Much of the problem comes from the fact that formulating effective natural hazard policy involves combining science, economics and risk analysis to analyze a problem and explore costs and benefits of different options in situations where the future is very uncertain.

**Because mitigation policies are typically chosen without such analysis -- often by a government mandate that does not consider the costs to the affected communities -- the results are often disappointing.**

# Crisis Mapping without GPS Coordinates

Source: http://irevolution.net/2014/02/25/crisis-mapping-without-gps-coordinates/

[](http://irevolution.files.wordpress.com/2014/02/screen-shot-2014-02-24-at-9-14-20-pm.png)I recently spoke with a UK start-up that is doing away with GPS coordinates even though their company focuses on geographic information and maps. The start-up, **What3Words.com**, has divided the globe into 57 trillion squares and given each of these 3-by-3 meter areas a unique three-word code. Goodbye long postal addresses and cryptic GPS coordinates. Hello planet.inches.most. The start-up also offers a service called OneWord, which allows you to customize a one-word name for any square. In addition, the company has expanded to other languages such as Spanish, Swedish and Russian. They’re now working on including Arabic, Chinese, Japanese and others by mid-January 2014. Meanwhile, their API lets anyone build new applications that tap their global map of 57 trillion squares.

When I spoke with CEO Chris Sheldrick, he noted that **their very first users were emergency response organizations.** One group in Australia, for example, is using What3Words as part of their SMS emergency service. “This will let people identify their homes with just three words, ensuring that emergency vehicles can find them as quickly as possible.” Such an approach provides greater accuracy, which is vital in rural areas. “Our ambulances have a terrible time with street addresses, particularly in The Bush.” Moreover, many places in the world have no addresses at all. So What3Words may also be useful for certain ICT4D projects in addition to crisis mapping. The real key to this service is simplicity, i.e., communicating three words over the phone, via SMS/Twitter or email is far easier [](http://irevolution.files.wordpress.com/2014/02/screen-shot-2014-02-24-at-9-41-58-pm.png)(and less error prone) than dictating a postal address or a complicated set of GPS coordinates.

How else do you think this service could be used vis-à-vis disaster response?

## HHS proposes rules to govern health-care facilities’ disaster preparedness

Source: http://www.homelandsecuritynewswire.com/dr20140321-hhs-proposes-rules-to-govern-health care-facilities-disaster-preparedness

The Centers for Medicare and Medicaid Services (CMS), a federal agency within the Department of Health and Human Services, has proposed new requirements for health-care facilities intended to ensure these facilities are prepared to care for patients during disasters. The regulations aim to prevent the service disruptions which occurred during Hurricane Sandy and Hurricane Katrina, when an estimated 215 deaths occurred in hospitals and nursing homes in Louisiana.

“In New Orleans it seems very likely that dozens of lives could have been saved by competent emergency planning and execution,” the proposed rule said. **The proposal which will impact more than 68,000 institutions, was issued on 27 December 2013, and is open for comment until the end of March 2013.**

The New York Times reports that in response to the proposal, the American Hospital Association, in an advisory to its members, said that federal officials “may have significantly underestimated the burden and cost associated with complying with this rule.”

**The proposal requires that all nursing facilities and group homes have plans to maintain emergency lighting, fire safety systems, sewage/waste disposal options, and temperatures at a safe level for patients during power losses. Inpatient facilities must be capable of tracking displaced patients, provide care at alternate sites, and handle volunteers during disasters.** Transplant centers would need to have alternative hospitals for patients awaiting organs, which the Times notes is a challenge because transplant centers maintain different criterias.

The proposed regulations do not require hospitals to maintain water supply systems which might be needed to support decontamination stations, bathrooms, and air conditioning.

Some industry experts sayt that the CMS should instead support emergency management standards developed by the Joint Commission, an organization that accredits health care facilities, or standards developed by the National Fire Protection Association, whose recommendations should cover “90 percent or 95 percent of things that may go wrong,” said Robert Solomon, who oversees the association’s building and life safety codes.

**One of the most contested requirements requires all hospitals and nursing homes to test backup generators for extended periods at least once a year rather than the currently recommended once every three years.** Critics warn that the four-hour, full-load tests could be costly. The proposal also requires health care facilities to protect power sources against damage from floods and other hazards, but only newly installed systems are capable of meeting that requirement, due to regulatory codes.

Retrofitting current power systems could be too expensive, but some hospitals are already taking a proactive approach. New York University’s Langone Medical Center is investing in a multimillion-dollar cogeneration plant capable of operating independently of the power grid. The project, planned before Hurricane Sandy in which the hospital lost power and millions of dollars in damages, is expected to provide a reliable source of power and climate control during extended power grid failures.

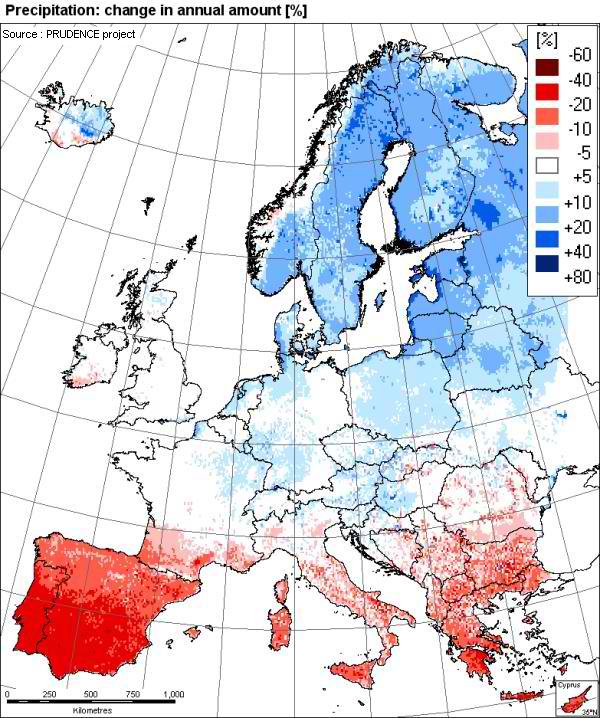
The proposal, which applies to seventeen types of health care providers, will require many facilities to adopt the regulations in order to participate in the Medicare and Medicaid programs. The CMS will have three years to finalize the rule, and the Times reports that if the requirements become law, the financial impact will be an average of $8,000 for hospitals the year the rule takes effect, and roughly $1,262 per year for skilled nursing facilities. Some facilities will be required to spend more depending on their size of operation.



|  |
| --- |
| Some interesting applications for disaster and emergency management  **Source:** <http://lehd.ces.census.gov/applications/> |

****Flood risk in Europe could double by 2050

Source: http://www.homelandsecuritynewswire.com/dr20140304-flood-risk-in-europe-could-double-by-2050

**Current flood losses in Europe are likely to double by 2050,** according to a new study published in the journal Nature Climate Change by researchers from the International Institute for Applied Systems Analysis (IIASA), the Institute for Environmental Studies in Amsterdam (IVM), and other European research centers. An IIASA release reports that socioeconomic growth accounts for about two-thirds of the increased risk, as development leads to more buildings and infrastructure that could be damaged in a flood. The other third of the increase comes from climate change, which is projected to change rainfall patterns in Europe.

“In this study we brought together expertise from the fields of hydrology, economics, mathematics and climate change adaptation, allowing us for the first time to comprehensively assess continental flood risk and compare the different adaptation options,” says Brenden Jongman of IVM, who coordinated the study.

**The study estimated that floods in the European Union averaged €4.9 billion a year from 2000 to 2012. These average losses could increase to €23.5 billion by 2050.** In addition, large events such as the 2013 European floods are likely to increase in frequency from an average of once every sixteen years to a probability of once every ten years by 2050.

The analysis combined models of climate change and socioeconomic development to build a better estimate of flood risk for the region. IIASA researcher Stefan Hochrainer-Stigler led the modeling work on the study.

He says, “The new study for the first time accounts for the correlation between floods in different countries. Current risk-assessment models assume that each river basin is independent. But in actuality, river flows across Europe are closely correlated, rising and falling in response to large-scale atmospheric patterns that bring rains and dry spells to large regions.”

“If the rivers are flooding in Central Europe, they are likely to also be flooding Eastern European regions,” says Hochrainer-Stigler. “We need to be prepared for larger stress on risk financing mechanisms, such as the pan-European Union Solidarity Fund (EUSF), a financial tool for financing disaster recovery in the European Union.”

For example, the analysis suggests that the EUSF must pay out funds simultaneously across many regions. This can cause unacceptable stresses to such risk financing mechanisms. Hochrainer-Stigler says, “We need to reconsider advance mechanisms to finance these risks if we want to be in the position to quickly and comprehensively pay for recovery.”

IIASA researcher Reinhard Mechler, another study co-author, points out the larger implications arising from the analysis. He says, “There is scope for better managing flood risk through risk prevention, such as using moveable flood walls, risk financing and enhanced solidarity between countries. There is no one-size-fits all solution, and the risk management measures have very different efficiency, equity and acceptability implications. These need to be assessed and considered in broader consultation, for which the analysis provides a comprehensive basis.”

Hochrainer-Stigler presented testimony based on this research at a recent public hearing on the European Union Solidarity Fund (EUSF) with the European Commission.

*— Read more in Brenden Jongman et al., “Increasing stress on disaster-risk finance due to large floods,”* Nature Climate Change *(9 January 2014)*

## What use are apps when your web infrastructure is underwater?

**By Nigel Linge**

Source: http://www.homelandsecuritynewswire.com/dr20140304-what-use-are-apps-when-your-web-infrastructure-is-underwater

This winter has seen unprecedented high winds and flooding resulting in widespread and in some cases, long-lasting power outages in the United Kingdom, particularly in the west of England. Time and time again, companies have advised their customers to go online to check their Web sites for the latest information. Some organizations have even created apps specifically designed to assist flood victims; others have established Facebook self-help groups. There is a fundamental problem here: There are two primary ways in which we gain access to the Web, via a landline and using a mobile connection. Within our homes the landline connects to a wireless router and also, for a lot of homes, a cordless telephone, both of which need electrical power to work. **So, when the lights go out, your router and cordless phones are useless. The result is that at times of crisis, the customers in most need are often the ones with no access.**

**According to OFCOM, 80 percent of adults in the United Kingdom had access to the Internet in 2013 and each spent about thirty-five hours online each month.** And half of all adults in the United Kingdom access the Web using their mobile phones, spending an average of five hours online per month.

**The average U.K. household has three Internet enabled devices and more than 17 percent of homes are connected to the Internet via superfast broadband services.** For many people, the Internet is the first port of call for virtually everything.

Businesses have responded in turn and now see having a Web site and online services as a top priority. And we are often urged to seek information online before attempting to contact customer support over the phone. Some might say we have become too reliant on the Internet. More reliant than our infrastructure justifies.

There are two primary ways in which we gain access to the Web, via a landline and using a mobile connection. A landline connects our homes to the local telephone exchange. For those customers with superfast broadband connections, the majority of these pass through a piece of street furniture called a primary connection point, recognizable as a green metal cabinet. That cabinet needs electrical power, as does the local telephone exchange.

Within our homes the landline connects to a wireless router and also, for a lot of homes, a cordless telephone, both of which need electrical power to work. So, when the lights go out, your router and cordless phones are useless.

Very few people have the means to power these devices without mains electricity. The local telephone exchange does have electrical backup which includes emergency diesel generators but the green street cabinets providing superfast broadband only have batteries that keep them going for about four hours.

Therefore the only thing that is going to work in your home is a traditional analogue telephone plugged directly into your landline. Have you still got one? If your laptop’s battery is charged and you kept an old modem and dial-up Internet account then you could connect for a couple of hours but you’ll be back in the 1990s in terms of speed.

What about a mobile connection using a smart phone or broadband dongle? **Surely these can get you online.** That depends on how severe the power outage is and how good the local infrastructure is. Your mobile connection relies on establishing radio transmission with the nearest mobile base station. These can be identified by their aerial masts and are normally visible at the side of roads or on top of buildings.

They vary in size and many are well above the ground keeping them away from floods. However, while they all have battery back-up, generally these are only designed to cope with short duration power cuts. As we have witnessed this year, long duration power outages will result in the base stations shutting down. That is bad news for your mobile phone signal, which is likely to be lost.

Of course, street furniture and other key pieces of infrastructure could themselves be submerged under water or have been damaged, which will prolong any Web outage.

Since Christmas 2013, BT’s infrastructure arm Openreach has published several MBORCs (matters beyond our reasonable control) declarations. These in effect state that conditions are so extreme that the company is not able to restore service within normal expectations. Major disruption to the environment does inevitably stop the engineers themselves from physically getting to or gaining access to sites to carry out repairs. As is the case for so many other vital services, it is difficult to tell when the Internet will be restored. It’s even harder for residents in Somerset to find this out.

**Organizations that rely on the Web as their primary means of delivering customer services need to become far more aware of the fragility of our infrastructure and crucially the dependency of the Web on having a supply of electricity to make it work. At times of crisis, the customers in most need are often the ones with no access.**

**Nigel Linge** is Professor of Computer Networking and Telecommunications at University of Salford.

## Planning for future ecological challenges

Source: http://www.homelandsecuritynewswire.com/dr20140319-planning-for-future-ecological-challenges

**How can communities dodge future disasters from Mother Nature before she has dealt the blow?** Researchers are taking a unique approach to the issue and gaining input and support from community stakeholders. Daniel Murphy, a University of Cincinnati assistant professor of anthropology, will present findings on 20 March at the 74th annual meeting of the Society for Applied Anthropology (SFAA) in Albuquerque, New Mexico.

The presentation reveals an innovative, interdisciplinary research technique for approaching climate change vulnerability which is called Multi-scale, Interactive Scenario-Building (MISB).

A University of Cincinnati release reports that the project focuses on **two geographic case studies:** Big Hole Valley in Montana — a high-altitude ranching valley — and Grand County in Colorado, a resort community west of Denver and south of Rocky Mountain National Park.

The researchers conducted a series of one-on-one interviews at those sites to get an array of community contributors thinking and planning for future ecological hazards, and to consider the impact of those decisions.

The researchers posed three scenarios involving future drastic climate changes. The one-on-one interviews involved around thirty people for each region, ranging from ranchers to teachers, small business owners, hunting guides, county planners and representatives from federal and state agencies. Ecologists on the research team would then predict the impact of the suggested planning.

**The three possible scenarios were:**

* Some Like it Hot — Describes years and years of consistent summer drought.
* The Seasons, They’re a-Changing — Describes changes in seasonality, such as significantly increased rainfall in the spring.
* Feast or Famine — Describes big swings in temperature and precipitation between years.

“Areas like the Big Hole depend on snow to irrigate their hayfields,” explains Murphy, “so little snowfall could pose a big problem. Not only does it affect their hay crop, but in a region with the Arctic Grayling, a candidate for endangered listing, the water shortage would affect wildlife. Because of these scenarios, more groups were open to conservation efforts. All community interests were able to see the benefits of conservation efforts.”

Murphy says scenarios to remove or shrink grazing allotments for ranchers were also big concerns, since ranchers would turn to grazing allotments to offset the effect of drought on herds.

“Flood irrigation, for example, has environmental impacts that are really, really good. So, we looked at the impact of stopping flood irrigation and switching to center pivot irrigation. It could rob the groundwater, it would evaporate off the soil and it wouldn’t go back into the river, so river levels would go down and stress the fish. So in examining that scenario, ranchers could see how this feeds back and that’s the iteration,” says Murphy.

Murphy adds that one of the major concerns in Grand County, Colorado, is also water, because much of the snow melt there feeds into a lake that’s a reservoir for Denver’s water. “Ranchers, irrigators and home owners are concerned about rising water prices if there is less snow, so that was a conflict that seemed to emerge there.”

Murphy says that in both Grand County and Big Hole Valley, the second scenario was perceived as an opportunity, because despite any temperature increases or other issues, it involved continuous rain in the spring.

The release notes that Murphy is now exploring climate vulnerability in Ohio’s Appalachia near the Wayne National Forest in southeast Ohio, where he says future flooding could pose a threat.

“A lot of research in this area tends to focus on past vulnerability or past adaptation, and from my perspective, that’s come and gone. The real opportunities lie in the future, and we’re examining how city planners, urban planners and extension agents can utilize our research in future decision-making,” says Murphy.

## Storm surges, rising sea levels threaten New Jersey’s beach-centered tourism industry

Source: http://www.homelandsecuritynewswire.com/dr20140318-storm-surges-rising-sea-levels-threaten-new-jersey-s-beachcentered-tourism-industry

**Sea level at the Jersey Shore could rise by thirty-one inches by the year 2050, posing a threat to New Jersey’s $38 billion tourism industry.** Planning and design firm Sasaki Associates says that  state tourism officials should begin to look for additional hot spots in New Jersey to contribute to tourism-generated revenue. Jason Hellendrung, principal of Sasaki Associates, says that the potential for more harsh storms and sea level rise calls for better promotion of what else New Jersey has to offer tourists aside from the beach.

APP.com reports that Sasaki is one of ten teams selected by the U.S. Department of Housing and Urban Development’s (HUD) Rebuild by Design competition to propose a plan to promote resilience with innovative planning and design in Hurricane Sandy-affected areas.

**“No one paid that close attention until Sandy. That was a wake-up call,”** Hellendrunbg told Asbury Park Press. “New Jersey’s tourism industry, it’s a plus-or-minus $30 billion number, so how can we grow it so, if or when we see another storm in the future, we don’t take another crippling blow?” According to Hellendrung, New Jersey could lose $526.6 million in annual tax revenue if sea level rises by thirty-one inches. Just an increase of twelve inches in sea level could swallow 43,823 acres from Sandy Hook to Long Branch and Point Pleasant Beach to Beach Haven, the locations considered most vulnerable, leading to $13.77 billion in assessed property value to disappear.

As part of its proposal in the planning and design competition, Sasaki Associates is focusing on tourism in Ocean County because many of the city’s beach towns were destroyed by Hurricane Sandy; Ocean County also generates the third most tourism dollars annually in New Jersey, bringing in roughly $4.2 billion in tourism-related revenue in 2012, falling behind Cape May County at $5.2 billion and Atlantic County at $7.6 billion, according to the state’s annual tourism report. Ocean County is urged to promote tourists activities on the mainland, offering visitors opportunities to explore what lies beyond the beach thereby extending or altering their beach visit instead of canceling it.

“Unfortunately, there’s always going to be another storm,” said Tony MacDonald, director of Monmouth University’s Urban Coast Institute. **“Everyone is really focused on the recovery efforts, but this also provides a really good opportunity to plan for the future.”**

## Climate change, population pressures leading to rethink of floating cities

Source: http://www.homelandsecuritynewswire.com/dr20140324-climate-change-population-pressures-leading-to-rethink-of-floating-cities

The concepts have existed for decades, but governments and financiers, responding to the growing threat of rising tides, pollution, and overpopulation to coastal urban centers, are now beginning to take a more serious look at floating cities..

The Guardian reports that areas of infrastructural decay around the world could benefit from reconstruction at sea. Mentioned are the vast slums of Makoko, in Lagos, which suffer from intense yearly flooding. As an example of the problem solving involved, local architect Kunle Adeyemi and his team have proposed a series of floating A-frame constructions which would completely replace the neighborhood. In order to prove the idea, the group successfully built a floating school for the community. The team even goes on to “use docking stations with centralized services, rather like hooking up a caravan to power, water, and drainage lines at a campground.”

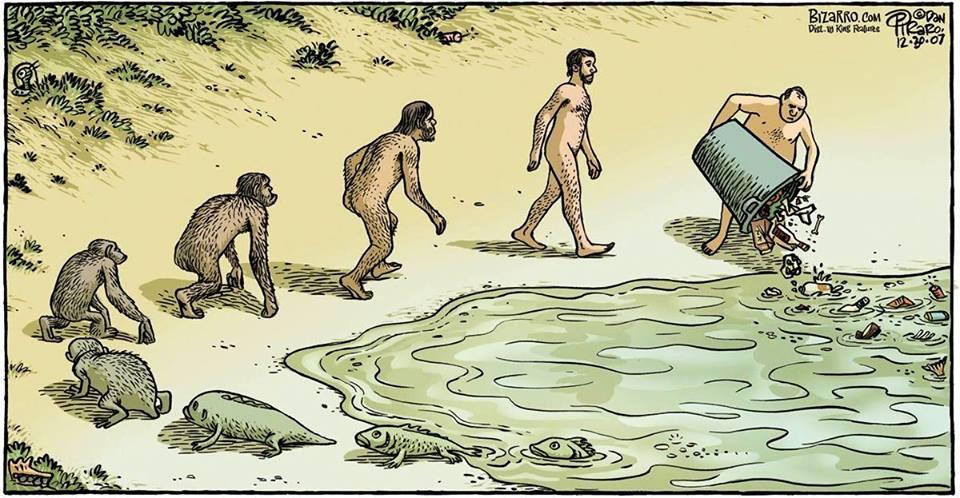
Elsewhere in Europe, the Guardian notes, “a floating village at London’s Royal Docks has the official nod, and Rotterdam has a Rijnhaven waterfront development experiment well under way.”

Jacque Fresco, an American architect, has concerns about overpopulation on land and has spent much of his career designing similar structures through his Venus Project. His work also considers the challenges of sea-based construction and the materials research which would be necessary to make it a reality.

Members of the Seasteading Institute and the coastal engineering firm DeltaSync even go as far as to trace out the socio-political implications of sea construction. As theGuardian points out, “Patri Fiedman (of The Seasteading Institute) claims to be in active negotiations with potential host nations that would give the villages political autonomy… communities would serve as experiments in governance.”

There are already efforts underway already to create aquatic communities, and the success of these could help determine the feasibility of the idea.

The World (photo above) is a privately owned 644-foot yacht in which 165 condominiums are available for purchase by residents as a co-ownership of the vessel itself. Also, Freedom Ship is aproposed mile-long barge which could feasibly contain 40,000 residents and a crew of 20,000. Directors of the project claim substantial Asian investor interest for the ship’s $11 billion proposed budget.



# http://r70.cooltext.com/rendered/cooltext1333431858.pngFully prepared for the worst

Source: http://www.thenational.ae/business/industry-insights/the-life/fully-prepared-for-the-worst

**The two earthquakes in Iran that in 2013 sent tremors rippling across the UAE caused a certain amount of alarm if not minor panic.** They showed that a number of organisations are not as prepared as they should be to handle a disaster. Farther afield, the explosions in Boston and the subsequent manhunt for the perpetrators rose questions in cities around the world about just how prepared they would be in the face of terrorist attacks.

Nicholas Bahr (photo) is the regional manager of the Middle East office of the consultancy Booz Allen Hamilton in Abu Dhabi. He is also an expert in emergency response planning. He would like to see better business continuity planning in the UAE and across the Middle East.

**This means every government body and business would figure out in advance what their key services are, what the threats are, and what systems could be put in place - and tested - to reduce the effect of disaster. Such a drill would apply in the case of a cyber attack, a natural disaster or a political crisis.**

"In the past, a lot of companies have looked at emergency preparedness ... emergency management [and] how to manage after an event and then maybe crisis communication during an event," Mr Bahr says. "Now what we are looking at is different. It's called business continuity: how do you manage your business in the middle of an event. It's sort of building up resilience."

**This idea of business continuity is relatively new but catching on.** It's also had more importance since the National Crisis and Emergency Management Authority introduced a business continuity standard in December.

This was created by looking at such standards in Britain, Australia, New Zealand, Switzerland and Singapore, in the context of the UAE's activities and services. It's the first business continuity standard in the Arab region.

The situation in the UAE is particularly interesting because of the large number of expatriate workers, according to Mr Bahr. One scenario that needs to be considered is a potential mass flight of foreign workers.

"What happens if expats leave suddenly [in] a mass exodus like what happened with the invasion of Kuwait by Saddam Hussein?" he says. "Here we have things like 70 per cent of the nurses in Abu Dhabi [being] from the Philippines, so imagine if relations between the Philippines and the UAE break down for whatever reason. Then all of a sudden you have a situation.

"Again, I think the concept is: how do I make myself, my company, my government more resilient so that as the vagaries, the unpredictableness of the world occur, I can just respond in a cost-effective and sustainable way?"

While the likelihood of a disastrous earthquake hitting the UAE is small (the country sits in the middle of a tectonic plate rather in the more dangerous location of where two plates meet), Mr Bahr says he noticed some less than desirable behaviours and consequences when separate tremors hit this month.

**First,** he saw many people evacuate their buildings by taking the elevator. As in the situation of a fire, people should get out of the building via the stairs. **Second,** he noted that few managers told occupants they could re-enter their buildings. **Third,** many people jumped in their cars to leave the area only to end up in a gridlock.

Unpredictable events "could be devastating for an economy so it's really important to plan ahead and think about it and test it," he says."**This street by noon [last week] was like a parking lot**. People just left and got in their cars and went home early; which is fine - but because of the [lack of] coordination there was very little traffic movement and statistically most people have less than a full tank of gas in their car at any one time. So imagine if there is a real call for evacuation: what do you do when cars start running out of gas getting out of the centre of activities?"

Mr Bahr concludes: "I think for me what I would like to see is all of us doing - government and industry together because I am a very firm believer it should be done jointly - is really come up with these business continuity programmes. It's really a joint effort because we are really joint entities now. We are not really black boxes."

### What is ISO 22301?

Source: http://www.iso27001standard.com/what-is-iso-22301

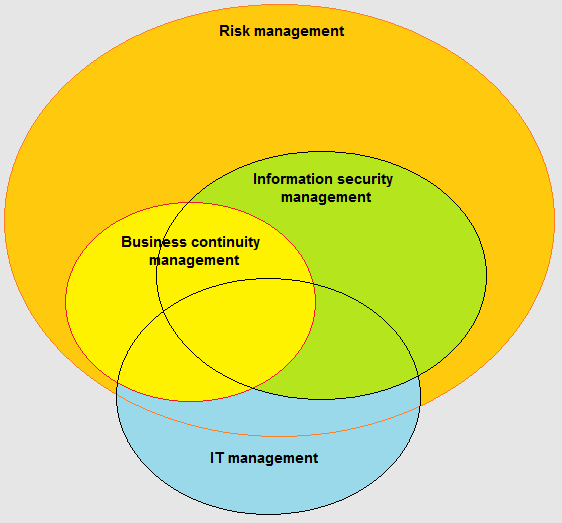
The full name of this standard is ISO 22301:2012 Societal security – Business continuity management systems – Requirements. This standard is written by leading business continuity experts and provides the best framework for managing business continuity in an organization.

One of the features that differentiate this standard compared to other business continuity frameworks/standards is that an organization can become certified by an accredited certification body, and will therefore be able to prove its compliance to its customers, partners, owners and other stakeholders.

### Relationship with BS 25999-2

ISO 22301 has replaced 25999-2 – these two standards are rather similar, but ISO 22301 could be considered an upgrade from BS 25999-2.

### What are the benefits of business continuity?

When implemented properly, business continuity management will decrease the possibility of a disruptive incident, and if such incident occurs an organization will be ready to respond in an appropriate way, and thus drastically decrease the potential damage of such incident.

### Who can implement this standard?

Any organization – large or small, for profit or non-profit, private or public. The standard is conceived in such a way that it is applicable to any size or type of organization.

### How does business continuity fit into overall management?

Business continuity is part of overall risk management in a company, with overlapping areas with information security management and IT management.

►Note: Risk management is part of overall corporate management.

### Basic terms used in a standard

* Business Continuity Management System (BCMS) – part of an overall management system that takes care business continuity is planned, implemented, maintained, and continually improved
* Maximum Acceptable Outage (MAO) – the maximum amount of time an activity can be disrupted without incurring unacceptable damage (also Maximum Tolerable Period of Disruption – MTPD)
* Recovery Time Objective (RTO) – the pre-determined time at which an activity must be resumed, or resources must be recovered
* Recovery Point Objective (RPO) – maximum data loss, i.e., minimum amount of data that needs to be restored
* Minimum Business Continuity Objective (MBCO) – the minimum level of services or products an organization needs to produce after resuming its business operations

### 

### Content of ISO 22301

The standard includes these sections:

|  |  |  |
| --- | --- | --- |
| Introduction  0.1 General  0.2 The Plan-Do-Check-Act (PDCA) model  0.3 Components of PDCA in this International Standard  1 Scope  2 Normative references  3 Terms and definitions  4 Context of the organization  4.1 Understanding of the organization and its context  4.2 Understanding the needs and expectations of interested parties  4.3 Determining the scope of the management system  4.4 Business continuity management system | 5 Leadership  5.1 General  5.2 Management commitment  5.3 Policy  5.4 Organizational roles, responsibilities and authorities  6 Planning  6.1 Actions to address risks and opportunities  6.2 Business continuity objectives and plans to achieve them  7 Support  7.1 Resources  7.2 Competence  7.3 Awareness  7.4 Communication  7.5 Documented information | 8 Operation  8.1 Operational planning and control  8.2 Business impact analysis and risk assessment  8.3 Business continuity strategy  8.4 Establish and implement business continuity procedures  8.5 Exercising and testing  9 Performance evaluation  9.1 Monitoring, measurement, analysis and evaluation  9.2 Internal audit  9.3 Management review  10 Improvement  10.1 Nonconformity and corrective action  10.2 Continual improvement  Bibliography |

### 

### Mandatory documentation

If an organization wants to implement this standard, the following documentation is mandatory:

* List of applicable legal, regulatory and other requirements
* Scope of the BCMS
* Business Continuity Policy
* Business continuity objectives
* Evidence of personnel competences
* Records of communication with interested parties
* Business impact analysis
* Risk assessment, including risk appetite
* Incident response structure
* Business continuity plans
* Recovery procedures
* Results of preventive actions
* Results of monitoring and measurement
* Results of internal audit
* Results of management review
* Results of corrective actions

### 

### Related standards

Other standards that are helpful in implementation of business continuity are:

* ISO/IEC 27031 – Guidelines for information and communication technology readiness for business continuity
* PAS 200 – Crisis management – Guidance and good practice
* PD 25666 – Guidance on exercising and testing for continuity and contingency programmes
* PD 25111 – Guidance on human aspects of business continuity
* ISO/IEC 24762 – Guidelines for information and communications technology disaster recovery services
* ISO/PAS 22399 – Guideline for incident preparedness and operational continuity management
* ISO/IEC 27001 – Information security management systems – Requirements

►**You can download the full related package from:** http://www.iso27001standard.com/en/free-downloads