October 2015

# CBRNE NEWSLETTER TERRORISM

E-Journal for CBRNE & CT First Responders

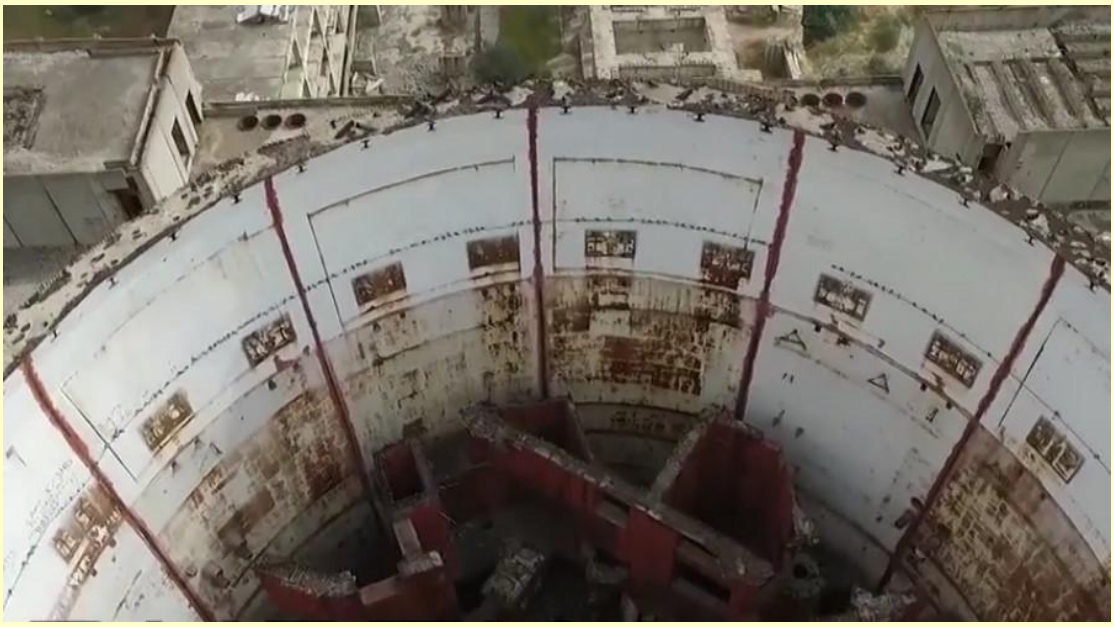
10 years

CBRNE-Terrorism Newsletter


www.cbrne-terrorism-newsletter.com

# Drone captures rare footage of abandoned Chernobyl-era nuclear plant in Crimea

Source: https://www.rt.com/news/316529-drone-video-nuclear-plant/





Sept 25 – Footage captured from a bird's-eye view of a Chernobyl-era nuclear power plant in Crimea shows its heart – the reactor. The unfinished plant has been standing abandoned for almost three decades.

Rare drone footage shows the decaying infrastructure of the Crimean Atomic Energy Station on the banks of Aqtas Lake in the eastern part of the peninsula, the construction of which was started in 1975.

The video shows the whole territory of the crumbling nuclear plant including the building for the main

energy block and cooling system from up above.

The project of the plant, which was supposed to supply the whole peninsula with energy, was abandoned in 1989, three years after the Chernobyl nuclear power plant catastrophe.

One of the alleged reasons for aborting construction was the location of the Crimean plant on a geologically volatile site. However, some blame the project's closure on lack of funds due to the economic problems in the Soviet Union.

**At the time when the construction was abandoned, the first nuclear unit was 80 percent finished and the second was 18 percent finished. However, no nuclear fuel had been stored at the facility.**
The Crimean power plant was reportedly one of the most expensive nuclear power plant projects to ever be abandoned before being finished.
From 1995 to 1999, the building housed the famous Kazantip musical festival carried out under the slogan "a nuclear party in a reactor."

# Fukushima disaster was preventable: Study

Source: http://www.homelandsecuritynewswire.com/dr20150923-fukushima-disaster-was-preventable-study

Sept 23 – The worst nuclear disaster since the 1986 Chernobyl meltdown never should have happened, according to a new study.
In the *Philosophical Transactions A of the*

*Royal Society*, researchers Costas Synolakis of the USC Viterbi School of Engineering and Utku Kânoğlu of the Middle East Technical University in Turkey distilled thousands of pages of government and industry reports and hundreds of news stories, focusing on the run-up to the Fukushima Daiichi disaster in 2011. They found that "arrogance and ignorance," design flaws, regulatory failures, and improper hazard analyses doomed the coastal nuclear power plant even before the tsunami hit.
"While most studies have focused on the response to the accident, we've found that there were design problems that led to the disaster that should have been dealt with long before the earthquake hit," said Synolakis, professor of civil and environmental engineering at USC Viterbi.
"Earlier government and industry studies focused on the mechanical failures and 'buried the lead.' The pre-event tsunami hazards study, if done properly, would have identified the diesel generators as the linchpin of a future disaster. Fukushima Daiichi was a sitting duck waiting to be flooded."

**Regulatory failures**
USC reports that the authors describe the disaster as a "cascade of industrial, regulatory and engineering failures" leading to a situation where critical infrastructure — in this case, backup generators to keep cooling the plant in the event of main power loss — was built in harm's way.
At the four damaged nuclear power plants (Onagawa, Fukushima Daiichi, Fukushimi Daini, and Toka Daini), 22 of the 33 total backup diesel generators were washed away, including 12 of 13 at Fukushima Daiichi. Of the 33 total backup power lines to off-site generators, all but two were obliterated by the tsunami.
Unable to cool itself, Fukushima Daiichi's reactors melted down one by one.
"What doomed Fukushima Daiichi was the elevation of the EDGs (emergency diesel generators)," the authors wrote. One set was located in a basement, and the others at 10 and 13 meters above sea level — inexplicably and fatally low, Synolakis said.

**Warnings ignored**
Synolakis and Kânoğlu report that the Tokyo Electric Power Co. (TEPCO), which ran the plant, first reduced the height of the coastal cliffs where the plant was built, underestimated potential tsunami heights, relied on its own internal faulty data and incomplete modeling, and ignored warnings from Japanese scientists that larger tsunamis were possible.
Prior to the disaster, TEPCO estimated that the maximum possible rise in water level at Fukushima Daiichi was 6.1 meters — a number that appears to have been based on low-resolution studies of earthquakes of magnitude 7.5, even though up to magnitude 8.6 quakes have been recorded along the same coast where the plant is located.

This is also despite the fact that TEPCO did two sets of calculations in 2008 based on datasets from different sources, each of which suggested that tsunami heights could top 8.4 meters — possibly reaching above ten meters.

**Wake-up call**

During the 2011 disaster, tsunami heights reached an estimated 13 meters at Fukushimi Daiichi — high enough to flood all of the backup generators and wash away power lines.

Additionally, the 2010 Chilean earthquake (magnitude 8.8) should have been a wake-up call to TEPCO, said Synolakis, who described it as the "last chance to avoid the accident." TEPCO conducted a new safety assessment of Fukushima Daiichi but used 5.7 meters as the maximum possible height of a tsunami, against the published recommendations of some of its own scientists. TEPCO concluded in November 2010 that they had "assessed and confirmed the safety of the nuclear plants," presenting its findings at a nuclear engineering conference in Japan.

"The problem is that all of TEPCO's studies were done internally; there were no safety factors built in the analysis, which anyway lacked context. Globally, we lack standards for the tsunami-specific training and certification of engineers and scientists who perform hazard studies, and for the regulators who review them, who can in principle ensure that changes be made, if needed," Synolakis said. "How many licensing boards have tsunami-specific questions when granting professional accreditation?"

Lacking tsunami specific training, certification and licensing, the potential for similar mistakes to occur in hazard studies for other coastal nuclear power plants exists, he said. He points to recent studies around the world where lack of experience and context produced tsunami inundation projections with Fukushima-size underestimation of the hazard.

*— Rea more in Costas Synolakis and Utku Kânoğlu, "The Fukushima accident was preventable," Philosophical Transactions A of the Royal Society (21 September 2015).*



# Welcome to North Korean Nuclear Weapons 101

**By Kyle Mizokami**

Source: http://www.nationalinterest.org/feature/welcome-north-korean-nuclear-weapons-101-13940

Sept 26 – The Democratic People's Republic of Korea (DPRK) has pursued a nuclear weapons program for decades. In 2006, despite sanctions and economic hardship, North Korea tested its first nuclear weapon. It has since conducted two more successful tests in 2009 and 2013.

That is pretty much the extent of unclassified knowledge about Pyongyang's nuclear arsenal.

North Korea openly admits it has nuclear weapons. In fact, the hermit kingdom brags about its arsenal and regularly threatens to annihilate its enemies. Other than that, North Korea has been vague about its nukes and declines to discuss details.

It's no surprise that little is known about North Korea's nuclear program. Information about a country's nukes can be hard to come by, even in free societies like Israel's. But the Stalinist-inspired North Korean dictatorship is one of the most isolated regimes on Earth, and information coming in and out of the country is tightly controlled.

As a result, almost all discussion about the North Korean nuclear program is based on guesses and estimates. We can make some very good guesses about the country's nuclear goals, but invariably some guesses will be better than others. Here are five guesses we can make about the North Korean nuclear program.

**1. Nuclear weapons are meant to guarantee the security of the regime**

The 1991 Persian Gulf War was not just a disaster for Saddam Hussein. On the other side of the world, the North Korean regime stood by and helplessly watched as the Iraqi military — outfitted similarly to the Korean People's Army — was destroyed in a matter of days. A revolution in military affairs, combined with a new generation of weapons and tactics demonstrated the increasing irrelevance of sheer numbers.

The lesson was clear: the days of North Korea's military might protecting

the regime were over. Kim Jong Il, who assumed power in 1994, made the production of nuclear weapons — and the means to deliver them — his number one priority.

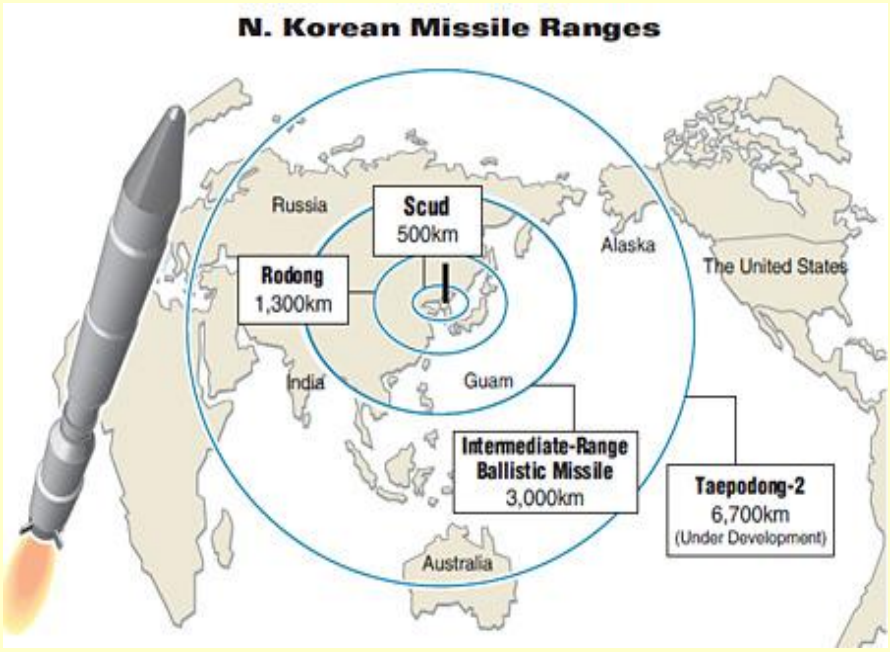
Being described as a member of the "Axis of Evil" in 2001 undoubtedly added to his sense of urgency. Nor did Allied military action in 2011 against Muammar Gaddafi's Libyan regime after it gave up its program to develop weapons of mass destruction reassure Pyongyang.

Kim succeeded in his plan. Thanks to North Korean nuclear weapons and the uncertainty surrounding them, the United States and South Korea seem unlikely to undertake major military action against Pyongyang, lest it trigger a nuclear response from the DPRK. The North Korean regime is now virtually invulnerable to outside threats.

The North Korean bomb is now a key part of the regime's survival strategy. It may be *the* survival strategy.

**2. The number of North Korean nuclear weapons is unknown**

We know the North has had at least three nuclear weapons — the three it tested. We don't know how many more it has stockpiled. North Korea has not stated how many nuclear weapons it has, and nobody outside of Pyongyang knows for sure. Estimating North Korea's nuclear arsenal is made even more difficult because its early weapons may have been inefficient designs with a relatively low explosive yield.




In 2008, North Korea declared it had 38.5 kilograms of weapons-grade plutonium. It also has highly enriched uranium (HEU) that it can use to build a nuclear weapon, but the DPRK has not declared how much of the material it has. North Korea also claims it restarted the Yongbyon nuclear plant in 2013, meaning it has been producing fissionable material for the last two years.

In 2012, analyst David Albright estimated North Korea had enough material to build up to eleven nuclear weapons. In 2015, the US-Korea Institute at SAIS estimated it had between ten and sixteen devices, of those between six and eight were made of plutonium and another four to eight made out of HEU. Further, the institute claimed that under the projected worst case scenario, North Korea could have 100 weapons by 2020.

**3. Current methods of delivery for the North's nukes are unknown**

There are a limited number of ways to deliver a nuclear weapon to a target. Bombs, artillery shells, and missiles based on aircraft, ships or ground vehicles are all possible delivery systems. Most, but not all, require miniaturization and ruggedization to allow them to survive the journey to the target.

North Korea may have mastered none of these systems, or it may have mastered all of them.

North Korea has worked for decades to improve its missile force, turning intermediate-range ballistic missiles into something that can hit the United States. It has also been working on making a weapon small and durable enough to arm a missile. North Korea claimed that its 2013 nuclear test involved miniaturizing a weapon.

In its 2014 defense white paper, South Korea stated the North Korean regime has the ability to place a nuclear weapon atop a ballistic missile. Joel Wit and Sun Young Ahn of the U.S.-Korea Institute assess the North as being able to fit a nuclear weapon on a Nodong medium range nuclear missile or Taepodong-2 long-range ballistic missile.

Even if miniaturization has eluded the DPRK, there remain other ways it could deliver a nuclear weapon. It

could simply dig a tunnel and set off a weapon somewhere south of the demilitarized zone. Nor is Incheon or Seoul that far away from the border. Another option would be to load it onto a commercial ship and slip it into the port city of Busan.

**4. The North's nuclear doctrine is unknown**

Under what circumstances would North Korea use nuclear weapons? Does it have a "no first use" policy? Does it consider nukes offensive or defensive weapons? Maybe both? Are Pyongyang's nukes strategic or tactical?

Outsiders — which is everyone outside of North Korea — have no firm answers, a disturbing notion since understanding under what circumstances North Korea would use a nuclear weapon is essential to avoiding a nuclear war.

Other countries are more explicit. China and India, for example, have both made a pledge of "no first use" of nuclear weapons. Neither will use nuclear weapons unless they are nuked first. It's an admirable policy of restraint and pre-tension signaling. North Korea, not surprisingly, has taken a different tack and nuclear ambiguity has become an essential part of the Kim's nuclear strategy.

Not understanding the terms under which North Korea will use nukes has a chilling effect on any potential military action. Tit-for-tat artillery exchanges in retaliation for bombarding South Korean territory might potentially trigger a nuclear war. Rolling the combined might of the South Korean and U.S. armies up to the entrance of the Ryugyong Hotel might not trigger nuclear war. We really don't know. Which just might be the whole point.

**5. Giving away nukes would probably end the Kim regime**

Nuclear weapons have become the guarantor of the Kim dynasty. But by pushing so hard for nuclear weapons, the Kims may have fallen into a trap of their own making.

North Korea has long maintained that it preserves the "real" spirit of the Korean people. It safeguards this gem of Koreanness from the imperialist United States and the puppet government in Seoul. That's the whole point of heavily arming itself and cutting itself off from the outside world.

The Kim dynasty has defined the United States as the antithesis of Koreanness. The Yankee imperialist enemy has helped legitimize multi-generational rule by the Kim family, as well as justify repressive security measures, harsh living conditions, lack of economic progress and the generally low level of prosperity.

If Kim Jong Un were to cut a deal with the United States and other powers to relinquish his nuclear weapons, he would be acknowledging that the existential threat no longer exists. And if there's no longer a threat to North Korea, why should the people tolerate deprivation, sacrifice and the Kims?

North Korea's nuclear arsenal is not going away anytime soon. It will likely continue to grow. Getting to the bottom about the many uncertainties about Pyongyang's nuclear program will help the rest of the world deal with as ever more dangerous and complex situation. Ambiguity may conceal weakness. It may also conceal strength.



*Kyle Mizokami is a defense and national security writer based in San Francisco who has appeared in The Diplomat, Foreign Policy, War is Boring and The Daily Beast. In 2009 he cofounded the defense and security blog Japan Security Watch.*

## Nuclear TSUNAMI: ISIS wants to wipe hundreds of millions from face of the earth

Source: http://www.express.co.uk/news/world/607737/ISIS-plan-Islamic-nuclear-holocaust-wipe-hundreds-millions-from-face-earth

Sept 30- **The claim comes from a veteran German journalist who is the only reporter to have been allowed to operate as an 'embed' with ISIS and escape alive.**

Jürgen Todenhöfer, 75, a former MP with Angela Merkel's CDU party, became a reporter in 2000 and has specialized in war reporting.

He spent 10 harrowing days on the ISIS frontline, dodging bullets and death threats, while being chauffeured around by none other than the UK's own scumbag traitor 'Jihadi John' – real name Mohammed Emwazi.

Todenhöfer's conclusions – detailed in a book called 'Inside IS - Ten Days In

The Islamic State' - make chilling reading.
He believes the west cannot militarily defeat

the self-styled Caliphate rulers and writes: “The terrorists plan on killing several hundred million people.
"The west is drastically underestimating the power of ISIS."
Shockingly, he even compares them to a "nuclear tsunami preparing the largest religious cleansing in history."
Critics say Todenhöfer, 75, was only allowed to get so close to ISIS because of his reputation as a vociferous critic of U.S. policy in Iraq and Afghanistan.
But he said: "This project was opposed by my family for seven months.
"My son ultimately accompanied me - against my will. He meant to protect me. And he filmed there."
He managed to make contact with his family only once, from an Internet cafe on the third day following their arrival, but their mobile phones were taken from them by their hosts.
He said” "My family didn't hear from us for seven days. It was very difficult for my daughters."
Todenhöfer added the trip came about after intense negotiations with "the leadership of the Caliphate, via Skype, over several months, hammering out the security details."
He made his will before leaving and said: "Of course I'd seen the terrible, brutal beheading videos and it was of course after seeing this in the last few months that caused me the greatest concern in my negotiations to ensure how I can avoid this. Anyway, I made my will before I left.
"People there live in shellholes, in barracks, in bombed-out houses. I slept on the floor, if I was lucky on a plastic mattress. I had a suitcase and a backpack, a sleeping bag.
"My impressions? That they are much stronger than we here believe.
“They now control land greater in size than the United Kingdom and are supported by an almost ecstatic enthusiasm the like of which I've never encountered before in a war zone.
“Every day hundreds of willing fighters from all over the world come.
"The beheadings have been established as a strategy which they wanted to spread fear and terror among their enemies. This worked well - look at the capture of Mosul taken with less than 400 fighters!
"They are the most brutal and most dangerous enemy I have ever seen in my life.
"I don't see anyone who has a real chance to stop them. Only Arabs can stop IS. I came back very pessimistic."



## HHS Enhances Radiological, Nuclear Attack Preparedness with New Products to Treat Severe Burns

Source: http://www.hstoday.us/single-article/hhs-enhances-radiological-nuclear-attack-preparedness-with-new-products-to-treat-severe-burns/c9cdbc921ca3b080d5efabfaee24d97c.html

**Disaster readiness could soon be making new treatment options available for routine burn care from mass casualty radiological or nuclear events,** according to the Department of Health and Human Services (HHS).

HHS announced that four novel products to treat severe thermal burns will be developed and acquired under contracts with HHS's Office of the Assistant

Secretary for Preparedness and Response (ASPR).


"The products are intended to enhance the available treatment options for disaster response and are being designed to find uses in routine clinical burn care," HHS said.

HHS said the ASPR's Biomedical Advanced Research and Development Authority (BARDA) "will leverage authority granted under the Project BioShield Act of 2004 to purchase one of the products currently available commercially and fund late-stage development and procurement of the other three. These products will be added to the Strategic National Stockpile (SNS) or managed by vendors to help protect people from burn injuries resulting from radiological and nuclear threats."

"The detonation of an improvised nuclear device would produce intense heat, resulting in many patients with severe burns," HHS said Wednesday in announcing the new treatment options.

"The treatments for such burns require complex procedures including surgical skin grafting that is resource-intensive and technically demanding," HHS said, noting that, "With only 127 burn centers nationwide, a mass casualty incident of this scale could easily overwhelm the nation's burn care infrastructure," a point *Homeland Security Today* has repeatedly reported.

"To protect health and save lives from the impacts of multiple types of disasters, we have to address critical challenges in burn care," explained BARDA Director Robin Robinson, Ph.D. "These products are intended to offer greater options and help create a continuum of care in a mass casualty incident; together they have the potential to eliminate resource-intensive steps, shorten hospital stays and improve patient outcomes."

**The first product, Silverlon**, could improve care for burn patients before they reach the hospital and can receive a surgical treatment for their burn injuries.

Silverlon, manufactured by Argentum of Geneva, Illinois, is a long-acting silver-impregnated nylon bandage available commercially and used widely to cover acute wounds and first- and second-degree thermal burns. The silver helps control bacterial growth within the dressing, HHS

explained, saying, "This product is being purchased through an interagency agreement with the Defense Logistics Agency at the Department of Defense, which has an existing purchasing arrangement with Argentum. The five-year contract is valued at $20 million, and the product will be delivered over the term of the contract."

**The other three products** are being developed to address challenges in burn care treatment, which HHS said, "BARDA will fund [the] pivotal clinical studies necessary for the companies to submit applications for approval from the Food and Drug Administration [FDA]. While this late-stage product development takes place, BARDA will begin procuring the products for the SNS. Wide-scale use of the products could be permitted by FDA in a disaster response under an Emergency Use Authorization."

Each of these three contracts have options for funding additional studies as deemed necessary by the FDA and to make additional purchases necessary to enhance national preparedness to

respond to radiological and nuclear events.
Under a five-year, $40.4 million contract, MediWound of Israel will develop NexoBrid, a topical gel made of pineapple-based enzymes and designed to dissolve the damaged or dead skin tissue to create a clean wound-bed for skin grafting.
"If successful," HHS said, "NexoBrid could eliminate the need to surgically remove damaged or dead tissue, a technically-demanding and time-intensive step in burn care, and may decrease the required amount of skin grafting which could speed recovery."
The contract has a total value up to $112.8 million.
Meanwhile, Stratatech Corporation of Madison, Wisconsin will advance its development of a novel cell-based skin substitute made from living human cells called StrataGraft under a


five-year, $59.9 million contract as part of an effort by BARDA.
"If successful," HHS stated, "StrataGraft could reduce the need to remove healthy donor-skin from the person's own body to graft over the burned skin, instead offering an off-the-shelf alternative to using animal or cadaver skin for skin grafts."
This contract has a total value up to $246.7 million.
In addition, under a five-year, $16.9 million contract, Avita Medical Americas, LLC of Northridge, California, will advance the development of a device called ReCell, which produces a topical spray derived from a small sample of the patient's own skin. This topical spray may enhance skin growth, allowing burn surgeons to use smaller skin donor grafts, and stretch grafts over a larger burn wound," HHS said.
This contract has a total value up to $79.5 million.
With these agreements, HHS said "using Project BioShield authorities, BARDA has supported the development and procurement of 16 medical countermeasures – vaccines, drugs and other medical products needed for emergencies – since 2004, including products needed to treat some of the health impacts of ionizing radiation, as well as drugs or products to treat illness from anthrax, smallpox and botulism."
HHS is the principal federal agency for protecting the health of all Americans and providing essential human services, especially for those who are least able to help themselves.
ASPR leads HHS in preparing the nation to respond to and recover from adverse health effects of emergencies, supporting communities' ability to withstand adversity, strengthening health and response systems and enhancing national health security.

Within ASPR, BARDA provides a comprehensive integrated portfolio approach to


the advanced research and development, innovation, acquisition and manufacturing of vaccines, drugs, therapeutics, diagnostic tools and non-pharmaceutical products for public health emergency threats.

These threats include chemical, biological, radiological and nuclear (CBRN) agents, pandemic influenza and emerging infectious diseases.

## ISIS Attempts To Get Nuclear Weapon And The World Is Sleeping

Source: http://i-hls.com/2015/10/isis-attempts-to-get-nuclear-weapon-and-the-world-is-sleeping/

The terror organization known as ISIS is trying to get its hands on nuclear weapons in order to cause a massive explosion that will kill millions of people, claims a German journalist who stayed with the organization. This claim is joined by intelligence assessments in several countries.

The journalist Jurgen Todenhofer, 75, an ex-parliament member of the party of Angela Merkel, has turned in the year 2000 into a reporter specializing in reports from battlefields. In a report published on the English Express website, he wrote that ISIS is planning a nuclear attack to destroy millions of people. This report is only a comfirmation of intelligence suspicions around the world.

"The danger is substantial and great but what is being done today against ISIS is a bad joke", says an Israeli expert.

Civilian nuclear reactors contain highly enriched Uranium which terrorists might use in order to build nuclear bombs.

The atom bomb which annihilated the Japanese city of Hiroshima at the end of WWII contained about 60 kgs od Uranium of the kind that creates a chain reaction. The American device, called "Little Boy", was activated above the doomed port city with a fairly simple rifle-like mechanism. The mechanism launched a part of the Uranium 235 inside the bomb, which was below critical mass, towards another part of the bomb. The combined mass of the two was greater than the critical mass, causing an explosion equivelant to 15,000 tons of TNT. The bomb which destroyed the city of Nagasaki several days later was made of Plutonium and not Uranium and its activation required a more advanced technology.

Although several countries have produced over 100,00 nuclear weapons, and despite incidents which nearly occured over the past sixty years, there hasn't been a nuclear annihalation such as this since. Howevere, today we are witnessing another alarming threat: Up to a few years ago, Al Qaeda was thought to be striving towards nuclear terror weapons. Today experts say the Al Qaeda looks like pre-school compared to ISIS.

In an article which appeared a few years ago in Scientific American, a concern was raised that a terror organization will lay its hands on Highly Enriched Uranium (HEU), build some crude explosive device with a rifle-like mechanism and use the resulted nuclear weapon against a city. HEU is Uranium where the concentration of Uranium 235, the isotope that can support a nuclear chain reaction, reaches over 20% of the weight.

The engineering required to build an atomic bomb of the rifle-like kind is so basic, that the physicists who designed "Little Boy" conducted to nuclear experiments before using it. They had no doubt that should the "rifle" fires, the bomb will indeed explode. That is why experts agree that a well-funded terror group could produce such rifle-like mechanism. Some have voiced actual concert that suicide bombers could penetrate HEU storage facilities, build an improvised nuclear device and blow it up before security can even respond.

**Producing HEU is obviously not an option for non-countries, but stealing it or acquiring it from the black market surely is: There are about 1,800 tons of this matter around the world, produced during the cold war, mainly by the United States and the USSR. Today HEU can be found in civilian facilities as well as military ones and it is far less secured (Uranium fuel to produce electricity in nuclear power plants is usually enriched with only a small amount of Uranium 235 – abour 3% – 5% of the weight).**

**Over 50 tons of HEU are currently in civilian use and are spread around the world to support around 140 reactors designed to scientific research, industrial use or to create radioactive isotopes for medical purposes. These sites are usually located in urban**

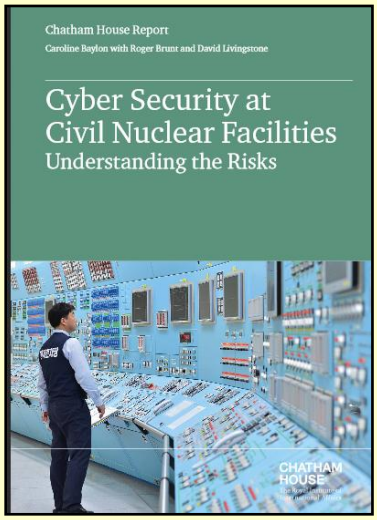
**environments and their guarding, guards and security systems wise, is minimal. Most concerning is Russia's HEU reactors which constitutes a third of the global total and to which more than half of civilian-used HEU is connected.**

So intelligence experts haven't a doubt – ISIS wants to create a nuclear explosion. This puts a somewhat odd light around the so-called war the West is running against this organization. A few jet planes and some ground battles cannot defeat this organization that combines a lot of money with the will to commit the most atrocious terror attacks that can be described.

If the world doesn't wake up, the worst is still to come.

# Cyber Security at Civil Nuclear Facilities: Understanding the Risks

Source: https://www.chathamhouse.org/publication/cyber-security-civil-nuclear-facilities-understanding-risks#sthash.Y9HJUmzJ.dpuf




Oct 05 – The risk of a serious cyber attack on civil nuclear infrastructure is growing, as facilities become ever more reliant on digital systems and make increasing use of commercial 'off-the-shelf' software, according to a new Chatham House report.

The report finds that the trend to digitization, when combined with a lack of executive-level awareness of the risks involved, means that nuclear plant personnel may not realize the full extent of their cyber vulnerability and are thus inadequately prepared to deal with potential attacks.

**Specific findings include:**

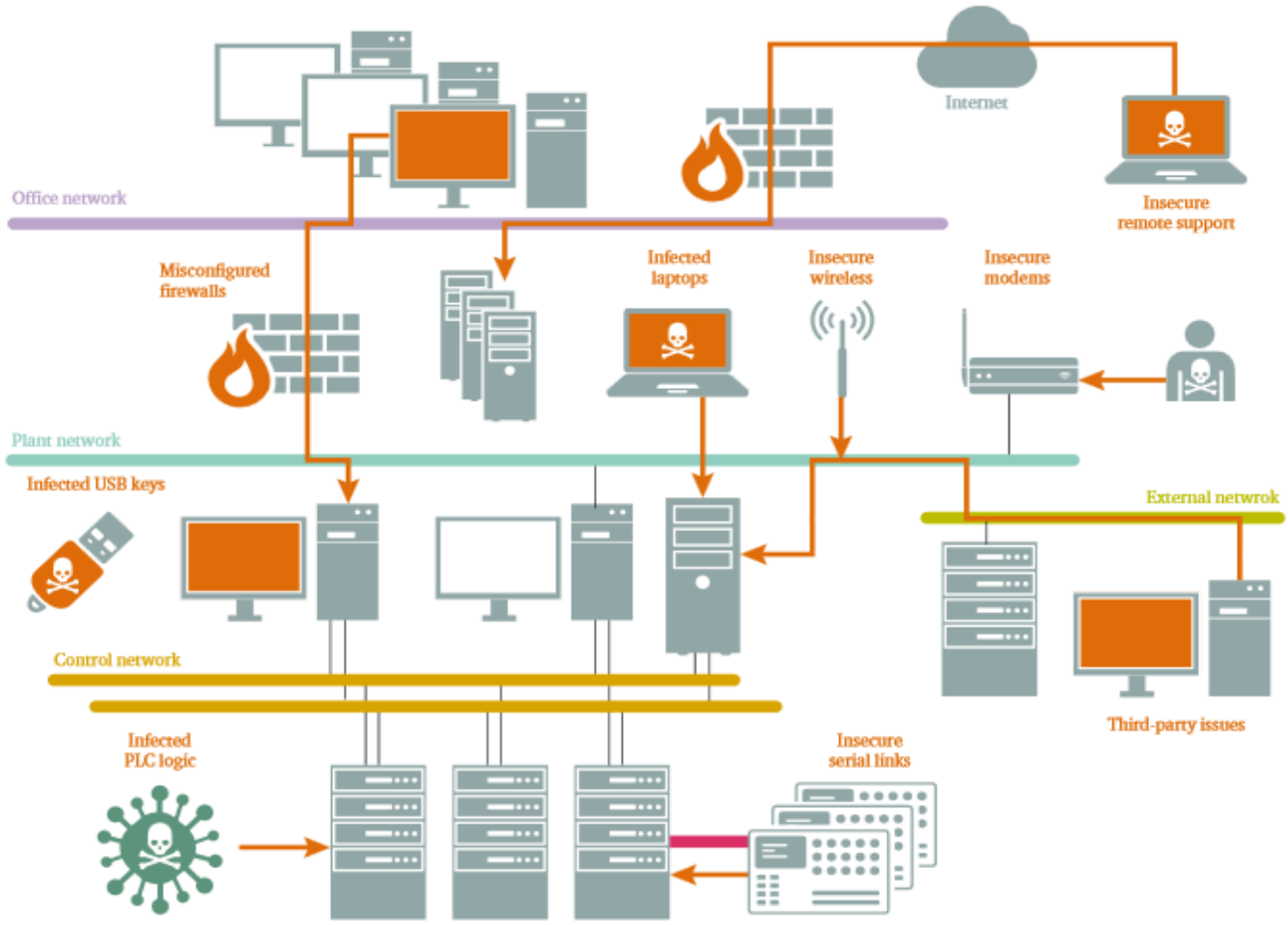
- The conventional belief that all nuclear facilities are 'air gapped' (isolated from the public internet) is a myth. The commercial benefits of internet connectivity mean that a number of nuclear facilities now have VPN connections installed, which facility operators are sometimes unaware of.
- Search engines can readily identify critical infrastructure components with such connections.
- Even where facilities are air gapped, this safeguard can be breached with nothing more than a flash drive.
- Supply chain vulnerabilities mean that equipment used at a nuclear facility risks compromise at any stage.
- A lack of training, combined with communication breakdowns between engineers and security personnel, means that nuclear plant personnel often lack an understanding of key cyber security procedures.
- Reactive rather than proactive approaches to cyber security contribute to the possibility that a nuclear facility might not know of a cyber attack until it is already substantially under way.

In the light of these risks, the report outlines a blend of policy and technical measures that will be required to counter the threats and meet the challenges.

**Recommendations include:**

- Developing guidelines to measure cyber security risk in the nuclear industry, including an integrated risk assessment that takes both security and safety measures into account.
- Engaging in robust dialogue with engineers and contractors to raise awareness of the cyber security risk, including the dangers of setting up unauthorized internet connections.
- Implementing rules, where not already in place, to promote good IT hygiene in nuclear facilities (for example to forbid the use of personal devices) and enforcing rules where they do exist.
- Improving disclosure by encouraging anonymous information sharing and the establishment of industrial CERTs (Computer Emergency Response Team).
- Encouraging universal adoption of regulatory standards.

**Figure 1: Potential control system vulnerabilities**




Source: Eric Byres, Byres Security.

▶ **Read the full report at:**
https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20151005CyberSecurityNuclearBaylonBruntLivingstone.pdf

# FBI helps foil several plots to sell nuclear material in Moldova's black market

Source: http://www.homelandsecuritynewswire.com/dr20151007-fbi-helps-foil-several-plots-to-sell-nuclear-material-in-moldova-s-black-market

Oct 07 – **Over the past five years, four attempts by Russian gangs in Moldova to sell nuclear material have been thwarted by the FBI and Moldovan authorities.**

**The AP reports that the most recent case was in February when a smuggler, who specifically sought a buyer from Islamic State, offered undercover agents a large amount of radioactive caesium. The FBI provided a Mercedez Benz to an undercover police officer posing as a connected gangster.**

**The would-be smuggler wanted €2.5 million for enough radioactive material to contaminate several city streets. He was recorded at a club in the Moldovan capital Chisinau, telling the police informant who posed as a potential client: "You can make a dirty bomb, which would be perfect for the Islamic State. If you**

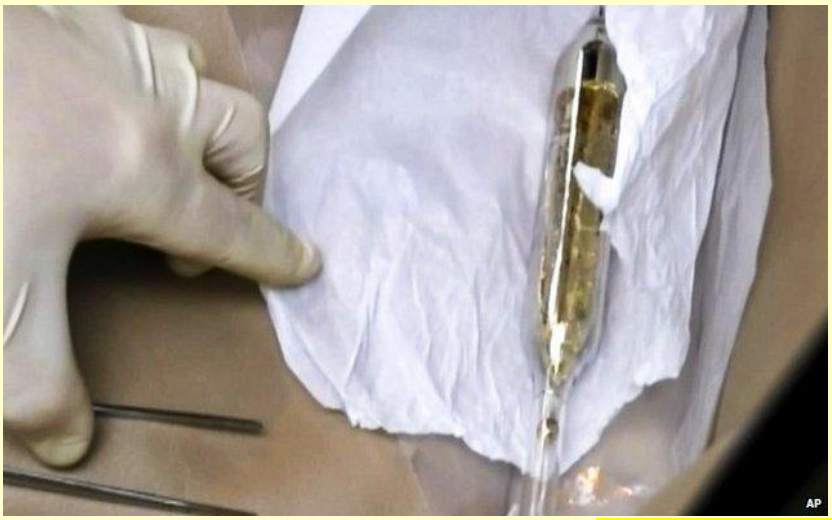
**have a connection with them, the business will go smoothly."**

The BBC reports that the alleged kingpins behind the different plots received only short prison sentences, and that few of them have resumed nuclear smuggling.

Moldova - timeline of nuclear smuggling

- 2010: 1.8kg of Uranium-238 seized in Chisinau when three people tried to sell it for €9m (£6.6m; $10m)
- 2011: Six detained for trying sell 1kg of weapons-grade Uranium-235 for €32m; they said they also had access to plutonium
- 2014: Smugglers allegedly tried to sell 200g of Uranium-235 from Russia to undercover security agents for $1.6m; 1.5kg of Uranium-235 seized close to Moldovan border in Ukraine
- 2015: Undercover agent bought ampoule of Caesium-135; materials contaminated with Caesium-137 found in central Chisinau

Experts say that the radioactive material involved likely have come from Russian hospitals, and that so far there have been no indications that large quantities of deadlier fissile materials have been sold in Moldova's nuclear black market.




Case files shared with AP by the Moldovan authorities show that smugglers have been exploiting the breakdown in cooperation between Russia and the west.

"We can expect more of these cases," said Constantin Malic, a Moldovan police officer who investigated all four cases. "As long as the smugglers think they can make big money without getting caught, they will keep doing it."

The BBC notes that the files revealed a pattern in how the cases were handled, suggesting that there are flaws in Moldova's anti-smuggling strategy. In all four cases, the Moldovan authorities arrested low-level suspects in the early stages of a deal, allowing the ringleaders a chance to escape with their nuclear contraband.

**The most serious nuclear smuggling case began in the spring of 2011, with the investigation of a group led by a Russian named Alexandr Agheenco, aka "the colonel," believed by the Moldovan authorities to be an officer with the Russian FSB.**

**A middle man working for Agheenco was recorded trying to arrange the sale of bomb-grade uranium, U-235, and blueprints for a dirty bomb to a man from Sudan. When Agheenco got away the police had no information whether he had more bomb-grade nuclear material.**



## Severe accident progression without operator action

**Prepared by:** CNSC staff – Ottawa, ON, Canada

Source: http://www.nuclearsafety.gc.ca/eng/resources/research/technical-papers-and-articles/2015/2015-severe-accident-progression-without-operator-action.cfm

Oct 10 – After the Fukushima Daiichi accident in 2011, one of the many actions committed to by the Canadian Nuclear Safety Commission (CNSC) in its Integrated Action Plan was an assessment and video representation for the public of how a full station blackout could progress in a CANDU reactor in Canada. This video was posted online in January 2013. The CNSC has now followed up with this technical paper, which

assesses the timing of a hypothetical blackout, using the Darlington Nuclear Generating Station for illustration.

**For the assessment, it was necessary to make the extremely unrealistic assumption that operators take absolutely no action after a full station blackout.** The assessment is not used to determine the effect of releases, but rather to assess the potential time and magnitude of releases to determine what operator action can be taken to prevent releases. The assessment identifies the multiple points when operator action becomes critical to stop the progression of an accident. Also, the assessment shows there is adequate time for operator action.

CNSC staff reviewed and agreed with the results of the Darlington Level 2 probabilistic safety assessment (PSA) performed by Ontario Power Generation (OPG), including the analysis of OPG's highly unlikely station blackout scenario, which assumed no operator intervention took place. In this scenario, external electrical power sources, standby diesel generators and emergency power generators are unavailable.

CNSC staff's summary of OPG's data paid attention to how reactors currently operating in Canada offer multiple layers of defence-in-depth to prevent accidents. The postulated initiating event of a prolonged station blackout in itself is extremely unlikely and would require multiple failures of plant safety systems to occur. It also depends on the control room staff failing to perform the most basic control room actions in accordance with established safety procedures.

**In such a hypothetical event, a release of radioactivity into the environment due to severe core melt can occur at around 11 hours (first stage of release) after this unmitigated station blackout begins. Twenty-three hours into the scenario, the containment integrity can be compromised due to structural failure, leading to a second stage of release at around 25 hours. Lastly, molten core–concrete interaction is expected to occur at around 58 hours, at this point releasing additional fission products into the containment and the environment.**

The results of the MAAP4-CANDU severe accident analysis performed by OPG as part of its Level 2 PSA for Darlington indicate that a simple action carried out by the control room staff would provide approximately 8 to 10 hours of additional passive core cooling by supplying readily available water to the boilers. Based on operating procedures, control room staff are instructed to open safety relief valves to depressurize the boilers and allow gravity to feed the water into the boilers. This action could be accomplished from the main control room or secondary control area, and the control room staff would have over 1 hour to perform it. Following this action, field operators would have ample time to connect the portable emergency mitigating equipment and thus secure a continuous supply of coolant to the boilers. Successful connection of emergency mitigating equipment could fully halt progression of the accident. Such actions are regularly exercised and are highly likely to succeed in terminating accident progression and preventing releases of radioactive material to the environment.

**The likelihood of such an accident described in this scenario is very low because of the multiple safety defences in place.** Nonetheless, since the Fukushima accident, nuclear power plants in Canada have implemented numerous safety enhancements focusing on the prevention and mitigation of severe accidents. These safety enhancements would further reduce the likelihood of severe core damage resulting from a prolonged station blackout and the potential for radioactive releases.



## 3D Printed Nuclear Weapons are Coming! (But Not Really)

**By Scott J Grunewald**

Source: http://3dprint.com/99382/3d-printed-nuclear-weapons/

Oct 07 – The history of newspaper publishing is rich with improbable doomsday scenarios that are hyped up beyond seriousness, especially when someone invents some new technology that is difficult to understand. Facts or reality only seemed to matter in the thinnest sense of the words, and an actual grasp of the technology being demonized was never really required. For the most part, large nationally distributed newspapers have done a pretty good job of leaving those days of

sensationalism behind them. So I was pretty surprised when I saw this recent blog post from the Monkey Cage section on the Washington Post. Honestly, had I not known what website I was on, and double checked the URL, I would have assumed that I was reading a story written by a crackpot conspiracy theorist. It is probably one of the most absurdly inaccurate and misleading stories about 3D printing technology that I've ever seen. The title of the post? "*You can print your own guns at home. Next it will be nuclear weapons. Really*."

Yes, really, that is the actual title of an article that was written for the blog of a nationally distributed and well respected newspaper. In the article written by Daniel C. Tirone and James Gilley (Yes, it took two people to write it) the pair piggyback their handwringing over 3D printable weapons onto the current rash of mass shootings in the United States. While the subject of gun violence in the country is a serious and important topic that we need to address, I'm going to be a little cynical and suggest that maybe using the tragedies of mass murders to try and legitimize what comes uncomfortably close to straight up fear mongering is kind of gross. That's just me and my having a pesky soul. The article proceeds to completely misrepresent what actual 3D printed guns can do before suggesting that 3D printing will soon be able to create biological weapons and even produce actual nuclear weapons.

**Here are a few excerpts of the frankly staggering amount of wrong that this article contains.**

**"The ability to 'print' or manufacture guns privately will allow individuals to bypass**

**background checks, the primary way that guns are regulated today. And that challenge will expand exponentially as the technology advances, one day enabling individuals to print chemical, biological and nuclear weapons of mass destruction at home."**

**"How do you run background checks on someone who can print a gun at home?"**

Well, you don't I guess. But you also don't run background checks on people who make their own firearms using traditional gun manufacturing methods with plans that are easily accessible to anyone online either. Yes, that's right, anyone can download plans to make their own guns from the internet and have been doing so since the internet existed. You can even check out books at your local library that walk you through the process.

But okay, sure, let's pretend that it isn't almost the same thing just for argument's sake.

**"This is not a futuristic speculation; 3-D printed handguns are already on the street. The government is struggling to respond to these guns, which are hard to detect and deadly."**

The 3D printable Liberator gun

Except for the part where any "3-D printed handguns" currently on the street are about as deadly as a BB gun, sure. The 3D printed handgun that they are worried about is the Liberator handgun from Defense Distributed by the way. While it is certainly impressive that a working firearm was made using 3D printed parts, it is hardly a weapon that needs to be feared. It is made of fragile plastic, capable of firing only a single shot, and isn't especially small or easy to hide. I still have to take off my shoes when I board an airplane after a single failed shoe bomb, if law enforcement was really afraid of 3D printed guns then they wouldn't be 'struggling' to put measures in place to screen for them.

Now I don't want to diminish the actual issue of 3D printed handguns here in the least. Truthfully, the government is going to need to find a way to regulate 3D printed weapons at some point. And I see no problem with people looking forward and trying to bring the issue up for discussion. Had Tirone and Gilley stopped here I probably wouldn't have even noticed the story, but they've only just begun working themselves up into histrionics.

**"First, terrorists are now more willing to utilize WMD than before. Bruce Hoffman has argued that while at one point the conventional wisdom was that terrorist groups had no desire to inflict mass casualties, the 9/11 attacks and the rise in religiously motivated**

**terrorism showed that this logic no longer holds."**
**"Second, the opportunity to use WMD will expand as 3-D printing makes these weapons more available. In the past, only countries could reliably manufacture WMDs, given the formidable technical and economic investments involved."**

Both of these statements are vaguely true I guess, but exactly what type of "WMDs" will be 3D printable? What technologies will be employed to create them? If you know anything about the 3D printing industry, then you're probably pretty aware of what the major 3D printing applications and technologies are. There isn't a 3D printer in existence that can just pop out guns or chemical weapons, at least not without an enormous investment of money and time.

**"When will 3-D printing become advanced enough to produce WMDs? Though it sounds like science fiction, the best projections suggest that it will happen within a few decades. The technology to print from standard metals such as steel and titanium already exists, allowing for firearms far stronger than the roughly made and fragile plastic handgun."**


Metal gun 3D printed by Solid Concepts.

Sure, metal parts can currently be 3D printed… using special 3D printers that cost tens if not hundreds of thousands of dollars. And yes, there have been some metal guns manufactured by large 3D printing services bureaus, but they cost about $12,000 to produce. For a single gun. I know it is easy to assume that criminals are stupid, but that level of fiscal irresponsibility is quite a stretch.

And even had the article stopped here it probably wouldn't have ended up on my radar, but Tirone and Gilley continue:

**"Progress in mixed-materials printing, which can currently use 14 materials in the same printer, is being made both in the laboratory and among hobbyists. Work in biological materials is expanding at a rapid pace, with scientists printing human organs, medications and even hamburgers; bacteria and chemicals aren't far behind. Production is also moving beyond simple items, allowing for the fabrication of increasingly complex objects."**
**"As an example, SpaceX is utilizing innovative 3-D printing techniques to manufacture components for its spacecraft and rocket engines. It should also be possible to use 3-D printers to print components needed to produce nuclear weapons, potentially even from fissile materials such as uranium or plutonium."**

Yes, metal 3D printers can now somehow 3D print uranium and plutonium. I suppose someone could, possibly, invest millions of dollars into developing technology capable of 3D printing with radioactive materials. But how exactly does that suddenly make radioactive materials available on the free market where terrorists can purchase them? I mean, if any terror group had some uranium or plutonium just laying around they could already make a dirty bomb for a few hundred dollars, why are they going to bother to invest millions of dollars into a machine that will make it look pretty?

The answer? They won't. It is completely absurd to suggest that terror groups will be using expensive and highly advanced technology to do things that they can already do for a lot cheaper. ISIS is not going to buy themselves a metal 3D printer in order to craft themselves roadside IUDs. Criminals who want guns are not going to spend $12,000 on a 3D printed metal gun when they can just go buy the real thing for a few hundred dollars. And they're most certainly not

going to buy 3D printers to make one-shot plastic guns when they have access to metal guns for a fraction of the cost. That just isn't how reality works.

There is a very real need to have some conversations about 3D printed weapons and emergent technology like additive manufacturing. But these are not conversations that should be had by journalists who don't seem to be even trying to understand the technology that they're writing about. Journalists don't need to be scientists to write about technology, god knows that I'd be a hypocrite if they did, but they should at least make an attempt to understand exactly what it is that they're writing about.

I know newspapers, even their blogs, usually have tight deadlines. But it doesn't take a lot of research to discover that a 3D printer capable of using materials strong enough for a dangerous gun are far too expensive to be practical. It doesn't take a lot of research to discover that metal 3D printers are material-specific and they can't just 3D print anything from any metallic material. And oh man it doesn't take a lot of research to discover that they most certainly cannot magically create uranium or plutonium for goodness sake. I know some tech sites like to call the 3D printer a precursor to Star Trek's replicators, but we're a few centuries away from that, I promise.

# We Asked Two Experts if We Should Be Worried About the Islamic State Getting Nuclear Weapons

**By Mark Hay**

Source: http://www.vice.com/read/how-worried-should-we-be-about-the-islamic-state-getting-nuclear-weapons-1007

Oct 07 – On Wednesday, the Associated Press published a report showing just how easy it is for radioactive material smugglers to operate in Eastern Europe. Stories of authorities busting smugglers dealing in cesium or even uranium aren't that uncommon, but they rarely stir up too much concern because the volumes being trafficked in these isolated incidents are far below what you'd need to build a nuclear device—and some of the shady types involved turn out to be scammers selling duds.

But the AP report—dominated by one undercover cop who downed vodka shots to ease his nerves before buys—suggests that Moldova is a virtual free-for-all for smugglers of radioactive material, who often dodge prison time. And perhaps most alarming of all, one of these bold dealers was determined to dish his wares directly to the Islamic State back in February.

**To understand just what kind of danger these networks and deals pose, VICE reached out to Dr. Beyza Unal, an international security expert focusing on nuclear issues at the London think-tank Chatham House, and Scott Stewart, a security analyst at the geopolitical intelligence and advisory firm Stratfor.**

**They told us that there's no reason to lose your shit about the prospect of terrorists getting "nukes" because of these black-market networks. But that's not the only kind of weapon you can make from radioactive material.**

**VICE: How likely is it that, if an extremist buyer did make a deal with a nuclear materials smuggler, they could make a seriously dangerous weapon?**

**Beyaz Unal:** First of all, there's confusion between radioactive material, which is used for dirty bombs, and uranium and plutonium, which can be used for an improvised nuclear device.

**Scott Stewart:** We know al Qaeda was scammed and they paid a lot of money for [fake nuclear material]. Frankly, if you're a real [ex-]KGB colonel who has access to highly-enriched uranium (HEU), you're going to be able to sell it to someone better than terrorists. You'd sell it to the Iranians, North Koreans, even the CIA, because the Agency's been buying this stuff for decades.

**If terrorists aren't likely to be able to buy the stuff you need to make a nuke, what sort of materials might they actually get their hands on?**

**Stewart:** A lot of [the material that actually gets sold to terrorists] could be something that's just slightly radioactive or even a little more potent like cesium.
**Unal:** It's relatively easy to acquire radiological materials because they have dual uses in hospitals, industrial facilities. And the safeguarding of hospitals is not well established.
**Stewart**: Because of what's happened in Syria and Iraq, groups like the Islamic State already have access to radioactive material because of emitters that were left in hospitals or other places.

**So are you more worried about radioactive smuggling networks or about unattended radiological elements in hospitals?**
**Stewart:** With the model of terrorism that we're looking at today—these radicalized people who live here, who're becoming our most common terrorist threat—I would be more worried about somebody who already works at a hospital or a construction site and has access to these things.

**What kind of weapons could they make with these easier-to-access radiological materials?**
**Unal:** In this case they could make a radiological dispersion device—a dirty bomb.
**Stewart** As far as the actual construction of a dirty bomb, it's very simple. It's basically strapping radioactive material to [a conventional explosive].

**How destructive would these dirty bombs be?**
**Stewart**: A dirty bomb is not a weapon of mass destruction. You're not going to cause mass fatalities. Most of the people who will die from a dirty bomb are going to die from the explosive material itself rather than radiation. The biggest dirty bomb in history was Chernobyl [where] you had some long-term deaths from cancer, but the immediate accident didn't have many deaths.
**Unal**: It will cause huge impacts on the psychology of the public. If it's used on a subway, they will not use the subways and people who aren't even contaminated would consider themselves [to be] contaminated and they would go to the hospitals, so the hospital system can be paralyzed.
They would disrupt the economy as well as potentially kill people. That would be the aim.



**So what's the risk of an actual, successful dirty bomb attack?**
**Unal:** Although the probability of use of radiological use is low, the consequences would be high, so the risk is high.
**Stewart:** While [the Islamic Sate is] good at conducing insurgent and terrorist operations within their territory, doing that remotely requires a very precise set of terrorist tradecraft and that's just not something that they've demonstrated. If I [as a hypothetical Islamic State operative] have got to go to Minneapolis instead of Mosul, I have to operate in a clandestine fashion. I have to gather and make explosives. I have to make my own mechanism for the firing chamber of the IED. We've seen al Qaeda do that, but they've struggled since 9/11 to do much in the West.
They're [both] having trouble getting operatives into the United States to commit terrorist attacks. Getting radioactive material in is another hurdle higher.

**Given the scale of radiological material smuggling, especially in light of the AP story, what's the best way to mitigate the physical and psychological dangers posed by terrorists getting their hands on these materials?**
**Unal:** Safeguarding hospitals, export controls of dual-use materials, getting more nations into the International Atomic Energy Agency (IAEA) tracking database (today in includes only 125 states), increasing the safety and security in critical places like border control and ports is important. And for dual-use materials, there's always a non-radioactive option that could be used for commercial purposes, but because they're expensive, states do not use them. So I think we need to do more to find alternatives.
**Scott Stewart:** There's been a very robust effort on the part of the US government to limit access to this material. It's not something that's been neglected by any means.

There's been a long history of concern over dirty bombs. There was a huge spike around the time of José Pedilla and last year there was supposedly some cesium loose in Kazakhstan. A lot of that concern's stoked by not having a good understanding of what a dirty bomb is and

what it's capable of. A lot of it is just education and keeping that in perspective with everything else.

## To Maintain Ties during Afghan War, US Ignored Pakistan's Nuclear Smuggling

Source: http://www.terrorismwatch.org/2015/10/to-maintain-ties-during-afghan-war-us.html

Oct 10 – **The US went soft on Pakistan's nuclear smuggling efforts during former President Ronald Reagan's administration, fearing that any action would upset their bilateral ties at a critical time of the Afghan war, according to new declassified documents.**

The documents were declassified amid reports that the Obama Administration is considering a civil nuclear deal with Pakistan.

Declassifying a number of documents, the National Security Archive (NSA) said that the Reagan administration had an internal debate over policy towards Pakistan's developing nuclear capability.

The debate led to **a letter from President Reagan to Pakistani dictator Muhammad Zia-ul-Haq, never before published, asking for a commitment to low levels - five per cent - of nuclear enrichment.**

Five per cent would amount to a "red line", which some in Washington believed would trigger sanctions, although President Reagan's letter did not directly threaten to cut aid in the event of non-compliance.

Through the 1980s, the war in Afghanistan had priority over Pakistan's nuclear programme and President Reagan and his top advisors did not want to take any action that would jeopardise Pakistan's role as a conduit for US aid to the Mujahadin, NSA said in a media release.

In his letter dated September 12, 1984, Ronald Reagan wrote of his "appreciation" that Zia-ul-Haq had made the assurance on five per cent, further stating that higher levels of enrichment above five per cent "would have the same significance" as the other nuclear activities, such as unsafeguarded reprocessing which "I had personally discussed with you and would have the same implications for our security programme and relationship."

Ronald Reagan said enrichment above five per cent was "no different" from the other activities, but the letter did not make explicit the threat of an aid cut-off.

NSA said the Soviet war in Afghanistan, and US support for Pakistan's aid to the mujahidin, was the context for President Reagan's points on nuclear proliferation.

That Afghanistan was the overwhelming priority was also evident in draft talking points that were prepared for Ambassador Hinton: Washington remained "fully committed to supporting you in our common effort."

The talking points went on at some length about nuclear issues, including the importance of Pakistani assurances and the need for Indian-Pakistani dialogue, but they included no reference to penalties if Pakistani cooperation was found wanting, NSA said.

Significantly, the talking points refer to Washington's "judgment" that it is "likely that at some point India will take military action to pre-empt your military programme".

Such a possibility had been discussed in previous national intelligence estimates, NSA said.

Consistent with the allusion to an Indian threat, the talking points included an inducement for Pakistan to adopt safeguards on its nuclear facilities: in light of the threats that Pakistan faced, "we would be prepared to act promptly to discourage or help deter such action as you move toward safeguards".

Whether this offer, close to a security guarantee, was actually made to General Zia-ul-Haq remains to be learned, NSA said.

It added that a wide-ranging 1985 CIA report analysed General Zia's "gamble" on a close strategic relationship with the US, waged in the face of broad domestic opposition which was deeply suspicious of Washington and fearful that Pakistan would be embroiled in a conflict with the Soviet Union.

To keep India and the Soviet Union at bay, Zia-ul-Haq wanted to pursue a close security relationship with Washington and secure increased aid to support military modernisation.

To avoid "pressure" from Moscow, however, Zia-ul-Haq opposed any publicity for US indirect aid to the insurgents in Afghanistan, although he wanted it to keep flowing to prevent the Soviets from consolidating their position, it said.

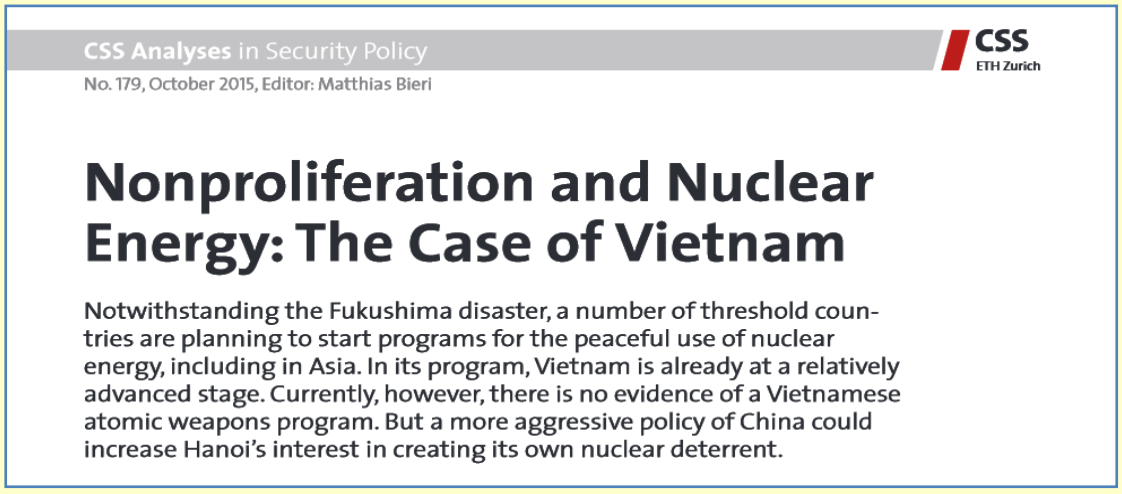
The CIA saw Zia-ul-Haq and the Pakistani public generally as deeply committed to a nuclear weapons capability as security against India; accordingly, if Washington cut aid to Pakistan for non-proliferation reasons, CIA analysts argued that Zia-ul-Haq would reduce support for the resistance in Afghanistan and intensify work on nuclear weapons development.

An aid cutoff could even lead to General Zia's overthrow or resignation in light of his gamble on close relations with the United States, NSA said referring to the documents.

## Nonproliferation and Nuclear Energy: The Case of Vietnam

**By Oliver Thränert**

Source: http://www.css.ethz.ch/publications/pdfs/CSS-Analyse179-EN.pdf






Notwithstanding the Fukushima disaster, a number of threshold countries are planning to start programs for the peaceful use of nuclear energy, including in Asia. In its program, Vietnam is already at a relatively advanced stage. Currently, however, there is no evidence of a Vietnamese atomic weapons program. But a more aggressive policy of China could increase Hanoi's interest in creating its own nuclear deterrent.

***Dr. Oliver Thränert** is the head of the Think-Tank at the Center for Security Studies (CSS) at ETH Zurich. He is the author of numerous publications including "Das nukleare Nichtverbreitungsregime und Autokratien" (DGAP Yearbook 2014).*

## U.S. to clean up site of a 1966 nuclear weapons accident in Spain

Source: http://www.homelandsecuritynewswire.com/dr20151020-u-s-to-clean-up-site-of-a-1966-nuclear-weapons-accident-in-spain

Oct 20 – **On 17 January 1966, a B-52 bomber carrying four hydrogen bombs collided with a KC-135 tanker plane during mid-air refueling off the coast of Almería, Spain, killing seven of the eleven crew members. Two of the bombs were recovered intact from the sea, but the other two leaked radiation into the surrounding countryside when their plutonium-filled detonators went off, strewing 3kg of radioactive plutonium 239 around the town of Palomares.**

Following the accident, the U.S. military shipped 1,700 tons of contaminated soil to South Carolina, and the whole thing was forgotten.

To show that the U.S. clean-up resolved all health concerns, the Spanish minister of tourism, Manuel Fraga, accompanied by the U.S. ambassador to Spain, took a televised swim in the sea.

In the early 1990s, however, health concerns were reawakened when tests revealed high levels of americium, an isotope of plutonium, and further tests showed that 50,000 cubic meters of soil were still contaminated. The Spanish government appropriated the land in 2003 to prevent any commercial use of it.

The *Financial Times* reports that on Monday in Madrid, Secretary of State John Kerry and the Spanish foreign minister José Manuel García-Margallo, signed an agreement to clean up the site and "store the contaminated earth at a suitable location in the United States."


The radioactive material will likely be shipped to an area of Nevada which is already contaminated from numerous nuclear tests carried out in the 1950s.

Margallo said the process would begin soon but gave no details.

The *FT* notes that analysts see a relationship between the clean-up announcement and the agreement by Spain to allow the United States to increase the number of U.S. military personnel in the country. The number of Marines at the base in Morón in southern Spain is to be increased from 850 to 2,200, and to 3,000 in the event of a crisis.

The U.S. navy base at Rota, near Cádiz, is set to become the largest in the Mediterranean.

The analyst note that what has accelerated the pace of negotiations on both the clean-up and the increase military presence in the fear in Washington that the December election may see the rise to power of a left-leaning government less sympathetic to U.S. concerns.



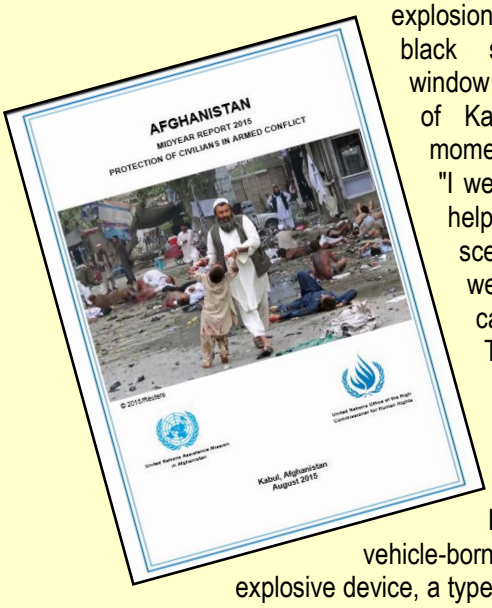

Copyright © 2005 Pittsburgh Post-Gazette

# IEDs: A Daily Nightmare for Afghans

Source: http://www.voanews.com/content/improvised-explosive-devices-daily-nightmare-afghans/2965078.html


FILE - An Afghan Army soldier searches for land mines with a metal detector during an exercise on defusing improvised explosive devices in Jalalabad, east of Kabul, Afghanistan.

Sept 15 – Mohammad Nasir Atmar was at home one day in August when he heard a huge explosion and saw plumes of black smoke outside his window in the Macroryan area of Kabul city. It was a moment of terror.




"I went down to see if any help was needed at the scene," he said, "as there were a lot of civilian casualties."

The attack happened in a residential area built by the Soviets, killing 12 people and injuring 66 others.

It was carried out by a vehicle-borne improvised explosive device, a type of IED that is used by insurgents to target the Afghan National Security Forces and their NATO counterparts but often affects innocent civilians.

Ordinary Afghans are bearing most of the brunt of the current conflict, which is in its 15th year.

Nicholas Haysom, the U.N. secretary-general's special representative and head of the U.N.'s assistance mission in Afghanistan, said in a report in August that Afghans had suffered a lot and that it was time for the violence to end.

"Afghan civilians have suffered far too long from this destructive conflict," he said. "The devastating consequences of this violence against civilians as documented in this report should serve to strengthen the broad conviction that peace is urgently needed."

**Development deterred**

The Taliban are active across Afghanistan but are most visible in the country's south and east. Local and international organizations are reluctant to implement development projects in areas where the Taliban have a powerful presence, fearing attacks and roadside bombs.

Shahab Hakimi, director of the nongovernmental Mine Detection Dog Center in Afghanistan, said IEDs are a hurdle for development in in the country. Last Thursday, he said, "two engineers who wanted to go and help build a clinic in Charkh district of Maidan Wardak province drove over an IED and died. The project was postponed after the incident."

A resident of the Shajoy district of Zabul province who did not want to be named for security reasons told VOA that a lot of bridges have been blown up on the Kabul-Kandahar highway by the insurgents and that noncombatants suffer as a result, especially during the flooding season.

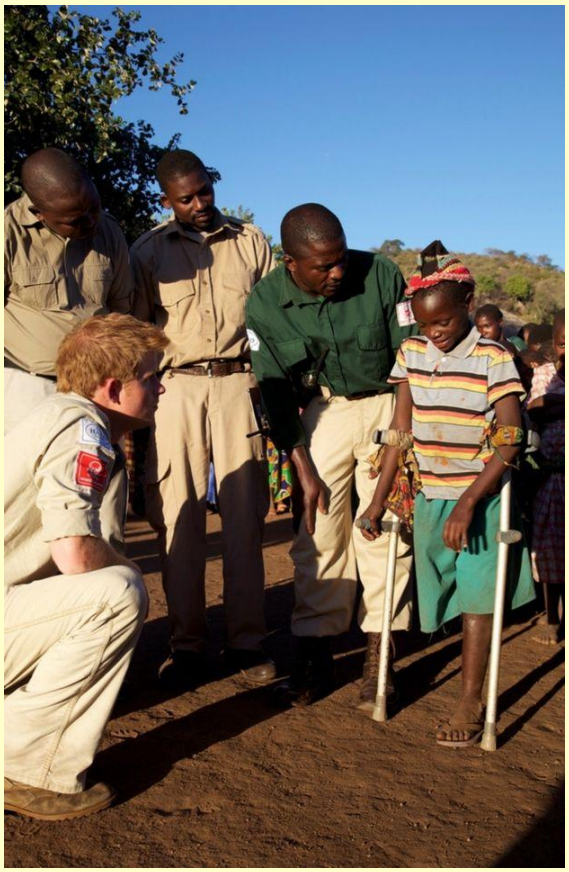
According to the U.N. report released last month, in the first half of this year alone, more than 4,900 civilian casualties have been documented — nearly 1,600 deaths and about 3,300 wounded. Nearly the same number of people were also killed and injured during the same period in 2014.
According to the report, 90 percent of the civilian casualties resulted from ground engagements, with IEDs as the second leading cause of civilian deaths after targeted killings.

**Blind weapons**
IEDs are blind weapons that target innocent civilians indiscriminately, said Mohammad Sediq Rashid, director of the Mine Action Coordination Center of Afghanistan, which organizes demining efforts in the country.
“IEDs continue to target innocent civilians," he said. "Every month, nearly 100 innocent people are killed and injured by IEDs across Afghanistan.” There have been dozens of incidents across the country in which buses carrying civilians drove over roadside bombs and were blown up, killing or injuring innocent people.
Alizai, a resident of southern Helmand province, told VOA that he and his family live in constant fear because of IEDs. According to Alizai, IEDs are planted indiscriminately, and only a few insurgents are in charge of them.
“[And when the insurgents die] in airstrikes or during battles with Afghan National Security Forces, no one knows where they planted their IEDs," he said. "This made life hellish for ordinary Afghans as they fear traveling on roads.”
Afghanistan once was at the top of the list of countries that have the most unexploded ordnance and mines. The mine detection center's Hakimi said that because a lot of the ordinance had been cleared away, donor countries have reduced their aid for the work
He said, however, that IEDs are going to be a continuing problem for Afghanistan, since it has been cleared only of mines that were planted in previous wars and unexploded ordinance left over from various warring factions.

# The Halo Trust celebrates 'mine-free' Mozambique

Source: http://www.bbc.com/news/uk-scotland-south-scotland-34269859

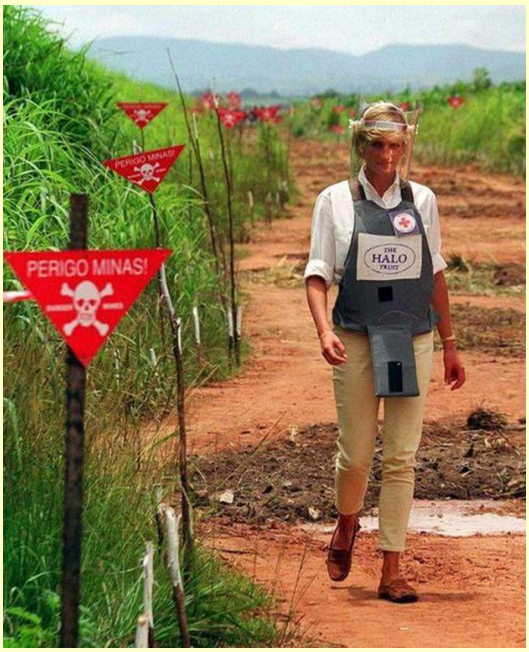




Sept 17 – A Scottish land mine charity is marking the end of a 22-year campaign to clear Mozambique of land mines.
The country was one of the most mined in the world after a civil war but it is expected to declare itself officially "mine-free" on Thursday.
The Halo Trust, which is based in Thornhill, Dumfriesshire, has taken a lead role in the lengthy operation.
The charity said its personnel cleared more than 171,000 landmines - about 80% of the total destroyed in the country.
It is a major achievement and one which improves the safety of Mozambique's 26 million citizens, the charity said.

**'Really brilliant'**
Calvin Ruysen, the Halo Trust's regional director for southern Africa, said it will also allow the country to develop its infrastructure, access gas and coal, increase tourism and attract international investment.
He added: "Only recently I was out in Mozambique, visiting some areas that were cleared which consisted of a couple of bridges

and viaducts that carry a railway.
"We could have cleared about 300 mines from around these few areas and now we can see the transformation.




"We can see farmers farming the land productively. We can see children playing safely and we can see workers now able to commute to work more safely.
"Further, and this is really brilliant, is that the manager of the railway line has talked about how the clearance enables his maintenance teams to upgrade the line and increase the amount of cargo they are able to transport, not only through Mozambique but across to Zimbabwe as well.

Princess Diana walked through a landmine during a visit to Angola with the Halo Trust shortly before her death in 1997

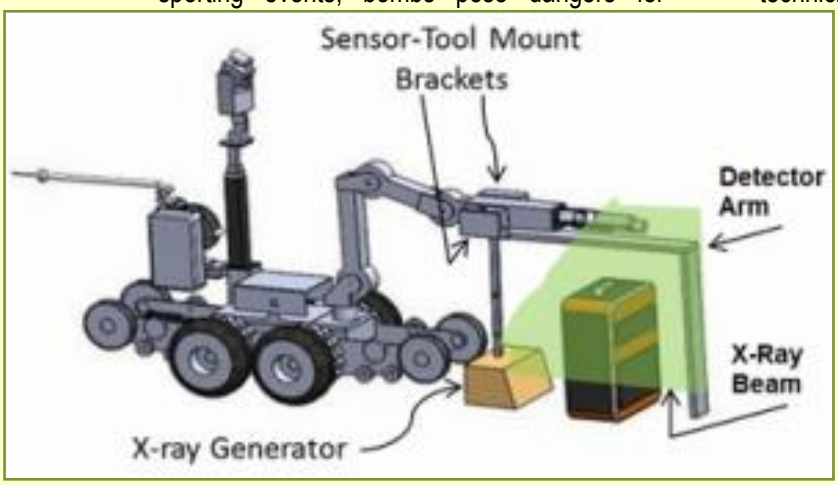
"So the impact, the effect, can be felt not only at the very local level but nationally, across whole regions."
Prince Harry spent two days with The Halo Trust in Mozambique in 2010.
His mother, Princess Diana, was famously pictured walking through a minefield when she visited the same charity in Angola.
Image copyright Halo Trust Image caption Prince Harry met people who had been injured by landmines during his visit to the Tete province of Mozambique Image copyright PA Image caption Princess Diana walked through a landmine during a visit to Angola with the Halo Trust shortly before her death in 1997
Mr Ruysen said 1,600 Mozambican men and woman were employed by the trust to demine the country.
He added: "This clearance will be an example to other mine-affected countries that it is possible to be free of mines and that is extremely important."
He said the charity had worked successfully with the government of Mozambique and the international community, which funded the work.
"We can deliver these results in other mine affected countries with the right resources," he said.



## X-ray Scanning Rover offers a new level of explosives detection

Source: http://www.homelandsecuritynewswire.com/dr20150929-xray-scanning-rover-offers-a-new-level-of-explosives-detection

Sept 29 – From conflict zones to airports to sporting events, bombs pose dangers for innocent civilians as well as the bomb technicians who regularly risk their lives to investigate suspicious objects and render the devices safe. Technology solutions can help first responders to see hidden dangers.




To this end, the Department of Homeland Security Science and Technology Directorate's First Responders Group (FRG) is developing the X-Ray Scanning Rover (XSR) to be a responder's eyes. It quickly and accurately scans packages and bags for leave-behind improvised

explosive devices (LBIED) while keeping responders out of harm's way.

S&T says that while other handheld scanning systems require multiple images to be stitched together, the XSR provides a complete 3-D, multi-view picture of the entire object being scanned in real time, saving first responders precious time. This technology offers an alternative to other large, bulky, expensive options that may have limited ability to operate in remote areas or rough terrain.

"One of the advantages of this system is that it can process images at a very fast speed," FRG XSR Program manager Christine Lee said. "The X-Ray Scanning Rover takes one continuous scan, and then responders have a clear, high resolution picture of any potential threats in real time. This saves valuable time in scanning objects during critical situations."

The XSR meets another requirement of the bomb squad community by embedding the detection technology within the bomb squad's current robotic operating systems — this means they don't have to buy an additional robot.

Whether being used at a roadside checkpoint, a national landmark, or at a public gathering, the XSR deploys easily in multiple environments to provide security screening when needed.

Presently, FRG is integrating the XSR onto existing, commercially-available, midsize robots that are widely used by civilian bomb squads by mounting the X-ray generator onto the sensor-tool bracket of the robotic arm. In order to fully free up the robotic arm for other use, a design approach is being pursued to deploy the X-ray generator on the ground after the object or LBIED has been scanned.

Unlike most existing scanners that use pulsed X-ray energy for detection, the XSR robot features a continuous, fan-shaped operating X-ray beam, permitting a higher degree of penetration through dense packaging.

The prototype also includes 3-D coordinates that mark the location of an explosive device within a suspicious package, a capability previously not found in scanners.

"The project offers new ways to serve on a multi-capacity level," Lee explained. "This will go a long way to provide a viable option for bomb threat responders."

S&T notes that FRG met with subject matter experts in August 2015 for a critical design review. The feedback obtained from the review will be incorporated into two new prototypes, which FRG expects to be ready by summer of 2016. The prototypes will be delivered to selected bomb squad units across the U.S. for field testing.



## Bomb detectors fraudster ordered to pay £1.2 million

Source: http://www.homelandsecuritynewswire.com/dr20151002-bomb-detectors-fraudster-ordered-to-pay-1-2-million

Oct 02 – Gary Bolton, a convicted fraudster who made millions selling fake bomb detectors around the world, has been ordered by a court to pay more than £1 million.

In August 2013 Bolton, 49, from Chatham in Kent, was sentenced to seven years in jail for the sale of more than 1,000 useless detectors that he claimed could track down bombs, drugs, ivory, and money.


The prosecutor, Sarah Whitehouse QC, told the Old Bailey during a confiscation hearing that Bolton had made about £6.8 million from his criminal activities, but that his assets were much lower.

The BBC reports that Judge Richard Hone QC ordered Bolton to pay £1,265,624, including more than £400,000 from the sale of his house — excluding 5 percent of the proceeds owed to his partner, Carly Wickens, who attended court with Bolton's mother, Grace Bolton.

The judge gave Bolton three months to pay the money — most of which deposited in British or foreign bank accounts – or face a seven additional years in jail.

Bolton produced and sold his fake detectors between January 2007 and July 2012.


**Numerous witnesses described how Bolton, with no experience in science, research, training, or security, had built a £3 million per year company selling the devices around the world for up to £10,000 each.**

**The devices were nothing more than crudely made boxes with handles and antennae that he created at home and at the offices of his company in Ashford, Kent.**

**In his sales pitch, Bolton claimed the devices worked with a range of 700 meters at ground level and up to 2.5 miles in the air, saying they were effective through lead-lined and metal walls, water, containers, and earth.** "Double-blind" tests in 2001 showed, however, that the devices had a successful detection rate of 9 percent.

Bolton was one of several defendants convicted for their part in fake bomb detector scams.

In 2013, James McCormick, a British businessman, was convicted of having made millions in profits from selling fake bomb detectors to Iraq, Georgia, and several other countries (see "U.K. businessman convicted of selling fake explosives detectors," HSNW, 30 April 2013). McCormick bought $20 golf ball finders in the United States, then sold the devices, which had no working electronics, for $40,000 each. The Iraqi government used more than $40 million in U.S. aid money to buy 6,000 of the devices, despite being warned by the U.S. military that the devices were a sham. The Iraqi military used the fake detectors at check-

points, leading to scores of soldiers and civilians being killed by suicide trucks which went through the check points undetected. Some police units in Kenya still use the devices.

## New Liquid Scanner is Approved to Airport Security Industry's Highest Standard

Source: http://www.hstoday.us/single-article/new-liquid-scanner-is-approved-to-airport-security-industrys-highest-standard/8c3c4083093bb2379bdca26e960544aa.html


At this year's DSEI exhibition, Link Microtek unveiled a new liquid explosive detection system (LEDS) that has been rigorously tested by an independent laboratory and approved to the airport security industry's highest level: ECAC Standard 3.

Jointly developed by Link Microtek and technology partner EMISENS, the EMILI 3 liquid scanner is a Type B LEDS as defined by ECAC (European Civil Aviation Conference), which means that it is designed for non-invasive screening of individual, unopened bottles or other containers. Achieving ECAC Standard 3 demonstrates that EMILI 3 satisfies the most stringent requirements relating to threat detection and low false alarm rates.

**The new scanner can identify the contents of an unopened container in as little as a second and is believed to be the fastest LEDS of its type currently available.** Coupled with its ease of use, this exceptionally fast speed of operation minimises the impact on passengers and makes the scanner ideal as a front-end detection device for high-throughput lanes at airport security checkpoints.

As each container is placed on the sensor plate, the display indicates almost immediately whether the contents are harmless or a threat such as liquid explosives or their precursors, with 'Pass' shown on a green background and 'Fail' on a red background. On occasion, an orange screen will appear, requesting additional information about the item under test; the operator simply enters this via touch-screen selection menus to complete the process.

EMILI 3 employs a combination of patented dual-mode RF/microwave, infra-red and gravometric sensing technologies. Since no X-rays, high-power lasers, static magnetic fields or high voltages are involved, the scanner has none of the health-and-safety concerns associated with other types of equipment.

Measuring just 720 (H) x 540 (W) x 540 (D) mm and weighing only 25kg, the scanner has a small enough footprint to be installed on any table top, with no special services required, and there are no consumables to replenish.



## Bomb squad called in after mother finds her flower vase was an unexploded WW2 shell

Source: http://www.telegraph.co.uk/news/newstopics/howaboutthat/11907374/Bomb-squad-called-in-after-mother-finds-her-flower-vase-was-an-unexploded-WW2-shell.html

A woman was shocked to discover that the flower vase she had used for 30 years was an unexploded bombshell.

Kathryn Rawlins, 45, from Atherstone, Warwickshire, had found the shell when she was 15 years old buried in the playing fields at her school.

Assuming that it safe, and thinking it would make a nice vase, she had kept it filled with her favourite flowers for more than three decades - until she saw a documentary featuring World War One bombs in Coventry - and feared her vase may have actually been an unexploded shell.

After calling police, MoD experts dashed in to take away the vase and remove the explosive - before returning the vase to Mrs Rawlins.

She said: "The police said that the shell had the potential to have

killed anybody that was within about 20 metres of it and could well have taken the house down.
"It's funny to think that I had it on my mantelpiece the entire time - it's just become a part of my family now."
"I have had the shell on the mantelpiece for three decades now and even took it to university. I used to stick plastic roses out of the top of it when I was dancing around to Madonna.
Mrs Rawlins, who works as a careers advisor at a secondary school, originally dug up the shell on the route home from school with two friends when they were 15 and used their hands and rocks to excavate the device.
Because her friend assured her that the shell was safe, Mrs Rawlins made it a prominent feature of her life and used it as a flower vase in her student digs.
She said: "My two friends and I dug the shell up on the way home after school. I saw something sticking out of the ground, which we dug up over a couple of days.
"We used our hands and rocks to get the shell out and the boys I was with jimmied the conical top of the shell off.

"We thought we needed to make sure it was safe and my friend said he would do it, but in hindsight he didn't.
"The shell became a part of my life ever since and I even kept it when I got married."
But it was only through a coincidence that Mrs Rawlins, a married mother-of-two, realised that she might have left unexploded ordnance on her coffee table over the years after she took a day off work through illness.
What she had always believed to be a harmless ornament had aroused suspicion after Kathryn watched a daytime documentary on unexploded wartime shells that had been dropped on Coventry by German zeppelins during the First World War.
Mrs Rawlins said: "I had seen that there had been a couple of devices found in the area since World War One, from a Zeppelin attack, so that brought it back into my mind that I needed to get the device checked.
"I made the strangest call to the police non-emergency hotline. I started off the conversation by telling them not to panic and attempted to describe the shell that I had.
"I told them it was 12 inches in length and three

inches across at its base. The top of it has a conical tip, which can be unscrewed.
"I used to unscrew it and put the flowers out of the top.
"It's really heavy to hold and has some writing that looks like it could be German around the top."
"In the end I just sent them a photo of the shell I'd been using as a vase. After the police saw that, they had an officer at my house within the hour.
"The situation then became very serious after the police told me that they would have to take the shell to the local barracks as the Ministry of Defence needed to examine it.
"It was a little bit worrying.
"The police brought it back to me when they assured me the shell had been made safe though, so I'll carry on using it for my flowers.
"I took it into school to show the kids; they loved it."

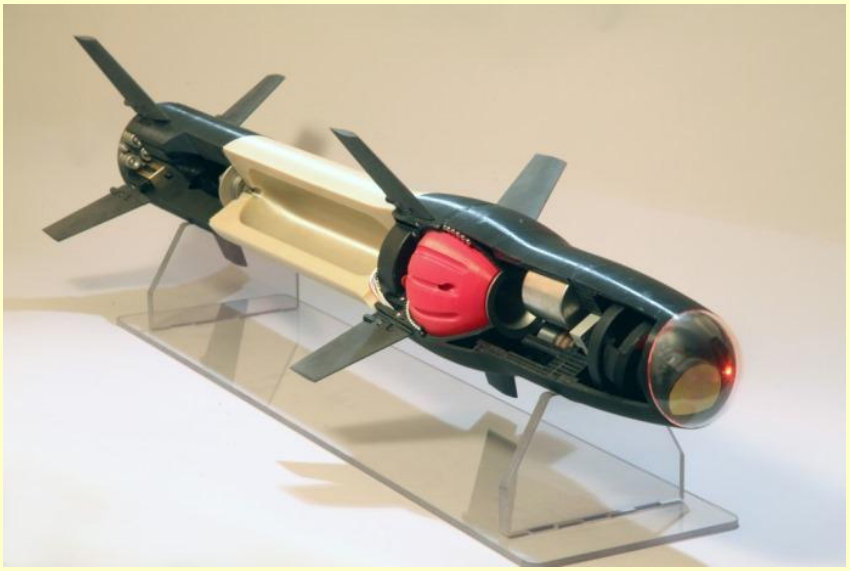
# With 3D-Printed Guns Beyond Control, DIY Nukes Are the Chic New Concern

**By J.D. Tuccille**

Source: https://reason.com/archives/2015/10/06/with-3d-printed-guns-beyond-control-diy

Oct 06 – On Thursday, after the Umpqua Community College shooting, President Obama took to the airwaves to blame the murderous acts of a motivated, vicious individual on America's unique status as "the one advanced nation on Earth in which we do not have sufficient common-sense gun-safety laws" (maybe Norway and France could show us how to do it right).

The president's words rang hollow to many observers. Perhaps that's because he openly boasted of politicizing the issue even while remaining vague as to the definition of



Raytheon 3-D printed guided missile

"common-sense gun-safety laws," maybe it's because these crimes remain horrible and resistant to analysis but fortunately rare, or it could be that the legal restrictions on guns the president and his chums have touted over the years have won compliance only from the reflexively law-abiding and defiance from anybody else, even as it's never been easier to ignore such laws.

Just days before President Obama's speech, a police official in essentially gun-free Japan lamented to *Vice News* that a struggle among Yakuza organized crime factions threatened to turn violent, and that the country's tight weapons restrictions seemed powerless in the face of home-built drones wielding bombs, and **3D-printed guns**.

"Even if a gang has no weapons on hand, they just need the right equipment," warned a detective with the Hyogo Police Department. "**Print, kill, melt the gun.** Those new guns will be hard to trace…. Escalation could be very fast and very bloody."

That the powerful crime syndicates—the organizations themselves are legal, with corporate headquarters, logos, and political connections somehow separate from their illegal activities—would bother to print guns rather than smuggle them in or "borrow" what they need from government contacts may be a testament to the technology's growing maturity.

In 2014, just a year after the original 3D-printed gun was unveiled by Cody Wilson, Japan's Yoshitomo Imura was the first person imprisoned for 3D-printing a firearm. His capture was no feat of forensic scrutiny; Imura had publicized his successes with little apparent regard for the legal status of his efforts.

"This has shown that anyone can illegally manufacture guns with a 3D printer, flaunting their knowledge and skill, and it is an offense to make our country's strict gun controls into a dead letter," the judge in the case reportedly huffed.

But dead those controls pretty much are—and so are those elsewhere. "Proposed legislation to ban 3D printing of weapons may deter, but cannot completely prevent their production," the U.S. Department of Homeland Security had conceded by then. "It is very difficult to do anything about it," a Europol official agreed.

Yoshitomo Imura's revolver design has since been refined, with functioning examples produced elsewhere and the plans available for download around the world. Aficionados can print their own ammunition now too.

In this artisanal age, perhaps the Yakuza agree with so many others that craft-produced products have much to recommend them over their commercial counterparts. Who

doesn't love that extra authenticity?

With home-brewed guns growing in sophistication, easily produced even without specialized skills, and nearly impossible to thwart, it's about time for the concerned class to get their panties in a bunch about something new. That fresh and shiny fear revolves around 3D-printed weapons of mass destruction.

"Within a few years, the greatest challenge to the government's ability to control firearms will be advances in additive manufacturing, popularly known as '3-D printing,'" Louisiana State University's Daniel C. Tirone and James Gilley recently trumpeted in a *Washington Post* op-ed that the Yakuza may have found intriguing.

Touting their larger treatment of the topic in the *Journal of Policing, Intelligence and Counter Terrorism*, Tirone and Gilley warned that "[t]he ability to 'print' or manufacture guns privately will allow individuals to bypass background checks, the primary way that guns are regulated today. And that challenge will expand exponentially as the technology advances, one day enabling individuals to print chemical, biological and nuclear weapons of mass destruction at home."

**Even a techno-enthusiast such as myself has trouble making the jump from printable mechanical objects like firearms to "My First WMD" kits on every petty tyrant's and terrorist's wishlist. Nukes? Really?**

**But chemical printing is already a thing, promising not just eased pharmaceutical research, but the ability to print otherwise expensive-to-produce orphan drugs (or illicit intoxicants) "at point of need." As of this year, 3D printers can operate at the molecular level, potentially building even live tissue from the ground up. Though not uranium any time soon.**

"It should also be possible to use 3-D printers to print components needed to produce nuclear weapons, potentially even from fissile materials such as uranium or plutonium," Tirone and Gilley insist.

The authors extrapolate more than a little to arrive at their worries about a desktop bomb in a box. But who knew 20 years ago that the ultimate rebuttal to gun control dreams would be automated home-based manufacturing with widgets priced within most people's budgets? Maybe the Yakuza and other evil-doers of the future really will order their nerve gas factories from Amazon (pro tip: go with Prime membership if you want delivery in time for the Spring offensive).

Tirone and Gilley suggest that, when it comes to modern DIY technology, governments must act in ways "countering its potential for mass destruction."

That's a little vague and open-ended. My guess is that we'll have to listen to a president of the future fret that as "we do not have sufficient common-sense DIY-safety laws," hinting at a grab-bag of impractical and unenforceable restrictions on 3D printers, CNC machines, traditional tools, and devices we have yet to imagine.

It's clear that the cat is out of the bag when it comes to people's growing ability to make whatever they damned well please, guns included, no matter what governments may want. And the professional worry warts can't see any end in sight.



*J.D. Tuccille is a former managing editor of Reason.com and current contributing editor.*

# Brazil Police Safely Detonate Bomb Found In Heart of Sao Paulo

Source: http://www.bernama.com/bernama/v8/wn/newsworld.php?id=1177027

Oct 06 – Police on Monday detonated an explosive device discovered at a taxi stand in Brazil's largest city, thereby averting a potential national disaster.

The device, comprising a small cylinder of gas, cables and a timer, was left inside a backpack near a main intersection in Sao Paulo's financial district.

Once a police robot equipped with an X-ray scanner detected the device, a specialist with the bomb squad safely detonated the explosives, Mayor Iron Ferreira said in a statement.

The nearby intersection was closed to vehicles and pedestrians for nearly three hours.

Besides the offices of financial institutions and other major companies, the area where the bomb was found is home to a hospital and a cultural center.


Authorities are reviewing footage from security cameras in the zone in search of the person who left the backpack at the taxi stand, Mayor Ferreira said.

## Deadly ISIS landmines plague Peshmerga

Source: http://rudaw.net/english/kurdistan/07102015

After more than a year of fighting, it is clear that even after the Peshmerga secure victories and recapture territories, the Kurdish forces are still exposed to the wrath of the Islamic State.

This hard-learned fact was underscored again last week when a sweeping Peshmerga offensive through western Kirkuk province was stopped less than 20 km from the ISIS stronghold of Hawija by one of the jihadists' most brutal and effective weapons: landmines.

"Our forces face death against the landmines," said Dr Kemal Kerkuki, a Peshmerga commander on the frontline in west Kirkuk.

"ISIS makes them very complex and very dangerous."

Mines are also a deadly factor in southeastern Kirkuk province, where nearly 6,000 of the explosives have been discovered. General Sirwan Barzani, commander of the Makhmour-Gwer front, said dozens of Peshmerga have died trying to diffuse the bombs.

In fact, Barzani estimates that landmines have caused 75 percent of the Peshmerga deaths on the frontline he holds against ISIS.

"They are our biggest problem," Barzani said.

Since seizing large parts of Iraq and Syria last year, ISIS has become synonymous for asymmetrical battle tactics, such as car-bombs, suicide attacks and improvised explosive devices, or IEDs.

These strategies, which evoke fear in ISIS opponents and have slowed progress in the fighting, seem only to intensify as the group digs in and defends the areas under its control.

"ISIS is currently attacking our front with chemical weapons, mortars and gunfire," said Kerkuki on Monday from a base a few kilometers from the front where several Peshmerga were killed in landmine explosions less than an hour before the interview.

The Peshmerga's three-prong, 3,500-fighter offensive, their fourth major assault in western Kirkuk, had recaptured a string of villages as well as the strategic Ghara Heights and a stretch of the Kirkuk-Samarra highway. In all, 140 square kilometers had been taken back from ISIS.

Even so, Kerkuki was not resting easily. He said he had only a few minutes before he returned to the fight.

"We control the key to Hawija," Kerkuki said, pointing to a projection screen that time-lapsed the Peshmerga's progress against ISIS. "See, we have all the high places now, and ISIS just has the plains."

The commander admits, however, that his men have been unable to safely navigate the no-man's land because of the mines, IEDs and

other intricate booby-traps built by the terrorists.
"In the last offensive, only one person was wounded by gunfire," Kerkuki said. "The rest were injured or killed by landmines."
Colonel Masoud Salih, a veteran Peshmerga officer and instructor at Zakho Military Academy, told Rudaw's Zhelwan Z. Wali that ISIS had a high-functioning system in place to ensure that its troops have access to mines and other explosives.
"[ISIS] has powerful military engineers in the group's self-proclaimed capital of Raqqa in Syria. They have factories manufacturing booby traps and landmines in Raqqa, which are then distributed to their controlled areas in Iraq and Syria," said Salih, 35, in a phone interview.
"Whenever there is an attack against them they ambush the forces, including the Peshmerga, the Iraqi Army and forces in Syria, with landmines," he added.
Mines and explosives aren't the only ISIS threats. During the interview, Kerkuki retrieved a bulky, white drone shot down by one of his fighters a few days earlier. A GoPro camera had been duct-taped to the nose of the device.
"We watched the video from the memory, and it revealed so much about our position and frontlines," Kerkuki said.
In answer to how many ISIS drones have gathered intelligence on the Peshmerga and have not been shot down, the commander sighed and said, "Too many."
He added that the lack of sophisticated demining equipment and skilled mine-removal engineers were hurting the Peshmerga.
"The landmines are slowing us down," he said. "Until we can bring in teams to remove them, we have to wait."

## Thief steals radioactive items from Los Alamos National Lab

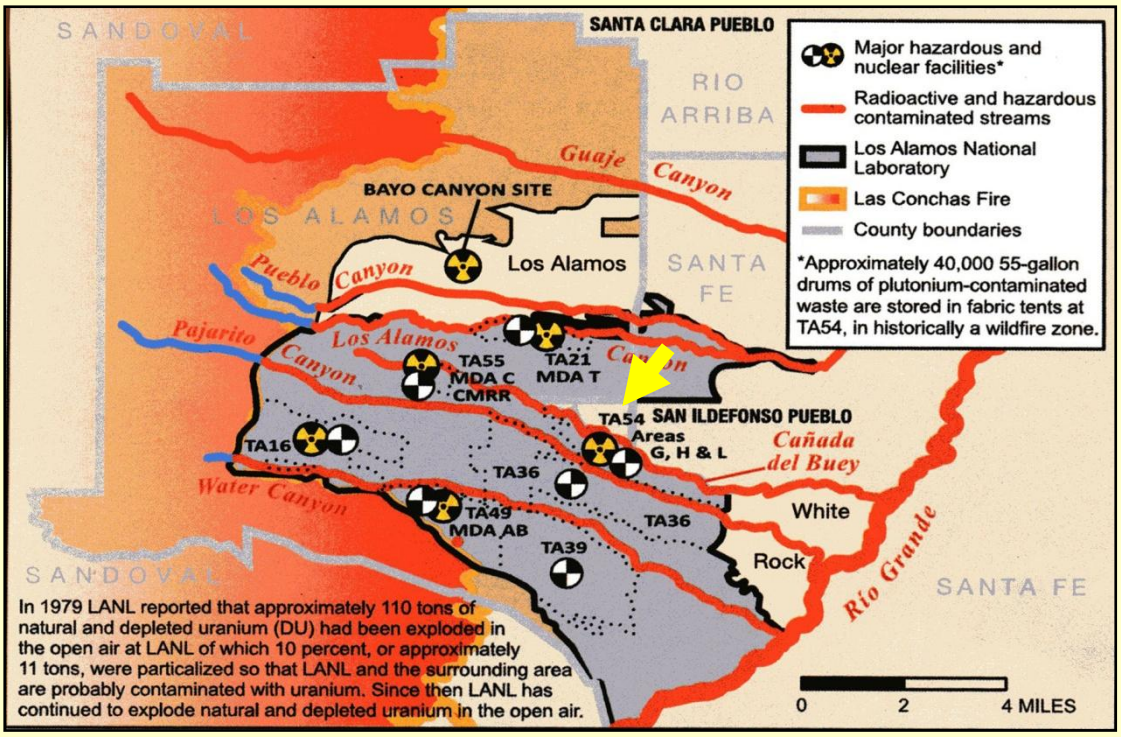
Source: http://krqe.com/2015/10/13/thief-steals-radioactive-items-from-los-alamos-national-lab/

Oct 13 – Not a very smart thief, stealing lab tools contaminated with radiation from Los Alamos National Laboratory.
Investigators believe a LANL contractor might

have done just that, and put the public at risk in what is just the latest problem with theft at the high security lab.

Los Alamos Police are calling the man a "person of interest," but not a suspect.
Richard Atencio, an employee of Compra Industries, had total access to LANL's Technical Area-54, which is a radioactive waste storage area.
The incident started as a theft, but quickly turned into a full-on HAZMAT situation last month.
According to a search warrant, on September 29, a witness saw a man in a brown shirt throwing things out of the trunk of a Honda Accord into bushes on LANL grounds. The man was tossing the things across the way from TA-54, where items have been reported missing over the past year.

Los Alamos Police came out to the scene of the dump and found a laundry list of stuff. One of the items, a band saw, had "TA-54" on it, meaning it was likely contaminated. Turns out, it was,




along with a pair of gloves and a bag.

Police tracked down Richard Atencio, who was wearing a brown shirt and owns a Honda Accord.

When officers searched Atencio's Accord, they noticed his trunk carpet was missing.

A HAZMAT sweep of his car found radiation levels on Atencio's steering wheel, gear shift and passenger door.

The FBI then searched Atencio's Española home on October 9, suspecting he might have contaminated his own stuff.

No LANL property or radioactive items were found.

Atencio has not yet been charged with anything. LANL didn't comment on the thefts; the company that Atencio works for, Compra Industries, didn't get back to KRQE News 13.

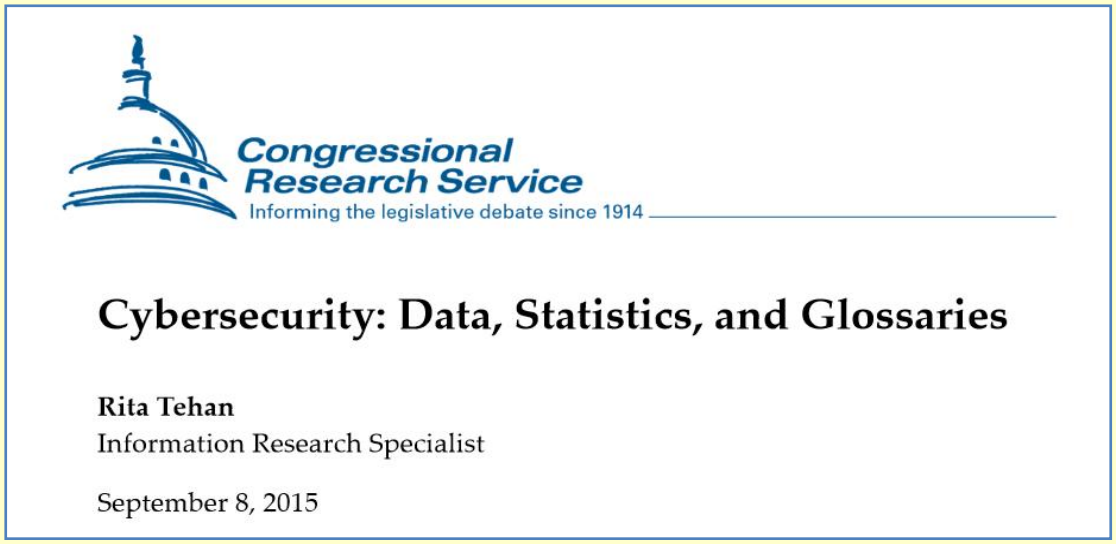
**The search warrant also revealed a disturbing fact, that there have been 76 reported cases of theft of LANL property by LANL employees in the last year.**



**EDITOR'S COMMENT:** "Not a very smart thief…" the article begins with. Was this the core problem? Or the BS security of Los Alamos National Laboratory??? And the thief was smart enough to steal and avoid radio-contamination! Perhaps when LANL's reported thefts reach to 100 certain measures will be taken…

## Cybersecurity: Data, Statistics, and Glossaries

Source: http://www.fas.org:8080/sgp/crs/misc/R43310.pdf


Congressional Research Service
Informing the legislative debate since 1914

Cybersecurity: Data, Statistics, and Glossaries

Rita Tehan
Information Research Specialist

September 8, 2015

This report describes data and statistics from government, industry, and information technology security firms regarding the current state of cybersecurity threats in the United States and internationally. These include incident estimates, costs, and annual reports on data security breaches, identity thefts, cybercrimes, malwares, and network securities.

## Gender Gap Widens in Male-Dominated Cybersecurity Industry

Source: http://www.nbcnews.com/tech/tech-news/gender-gaps-widens-male-dominated-cybersecurity-industry-n434986



**Women account for just one out of 10 cyber security professionals**, as the gender gap widened over two years in a male-dominated field with a drastic workforce shortage, a survey showed.

ISC2, the largest organization that certifies cyber professionals, said on Monday that a poll of nearly 14,000 information security professionals in developed countries found that just 10 percent were women. That is down from 11 percent two years ago, said ISC2 official Elise Yacobellis.

"It is certainly alarming to see it go down to 10 percent," Yacobellis said in interview.

One reason for concern is a talent shortage. ISC2 reported earlier this year that 62 percent of respondents said their organizations did not have enough security professionals.

"We have a huge workforce shortage. If we brought more women into this field, I believe that gap would lessen," Yacobellis said.

The survey also found pay inequalities. Some 47 percent of men reported annual salaries of at least $120,000, compared to 41 percent of women.

It comes amid a broader debate about the lack of women in the technology industry, especially high-profile firms like Google Inc and Apple Inc. Women account for roughly a third of workers at many tech firms, with fewer in leadership and technology roles.

## 5 Cyber Security Threats For 2015

Source: https://tech.co/cyber-security-threats-for-2015-2015-10

Oct 10 – Currently, there are increasingly large numbers of cyber attacks in the nation. In fact, the FBI now ranks cybercrime as one of its top law enforcement activities. President Barack Obama, in his recently proposed budget, said that he would drastically raise the spending on cybersecurity to around $15 billion. From fraud and identity theft to commercial hacking

assaults, cybersecurity has never been so important for governments, businesses and other organizations.

Hacking experts throughout the world have warned that there are more security threats in the near future, as web identity thieves are gradually getting more and more educated and sophisticated. While some of the conventional cybercrimes like internet password fraud will be prevalent in 2015, there will be more espionage attacks on a larger scale and the Internet of Things will even be considered as a huge risk. **Read on to learn some of the cyber security threats for 2015 that you should watch out for:**

**Ransomeware**

Ransomware is a specific kind of malware, which when infected, restricts you to access to a computer system. This will become more refined in its targets and methods. Experts predict that the variants of ransomware that hurt the security software that are installed within a computer may particularly target the endpoints which sign up with cloud-based storage solutions like Google Drive, Dropbox, OneDrive and many more. On detecting the endpoint, ransomware will exploit the stored personal credentials of the logged-in user and will even infect the cloud storage that is backed up. McAfee has warned that ransomware attackers will try out as many ways possible to shell out ransom payments from their victims.

**Cyber espionage**

No matter how tight-lipped the governments may be about their involvement in different activities to fight against their cyber enemies, cyber espionage is gradually becoming the strongest weapon for most of the national governments. The long term players will gradually become better gatherers of information and newcomers will only look for ways of stealing money.

**The Internet of Things**

Are you aware of the Internet of Things? Well, if answered No, then this is the connection of different devices like cars and home appliances to the Internet. But sadly enough, this will always be the Internet of Vulnerabilities. Founder of Cyber Senate, Jamison Nesbitt echoed the beliefs of the experts who said that the Internet of Things is one of the biggest cybersecurity risks of 2015. The unique security challenges will come in terms of the total number of devices that are connected at present. The IoT will be embedded into every market from the energy industry to the healthcare industry.

**Increase in cyber theft**

Stealing online financial information is not a new thing. Stealing debit or credit card data online has become a profitable business for cyber criminals. However, as there are new methods of paying for goods like mobile payments, there is again a new opportunity for cyber hackers, especially when retailers don't store confidential data securely. This would require cyber criminals to target the personal cards and that wouldn't result in huge scale breaches or burglary.

**Precarious passwords**

Passwords that are easy-to-crack are going to pose a big risk in 2015. There has always been a risk of weak passwords and this is a known fact but this may still lead to some of the highest-profile attacks like the very recent iCloud attack.



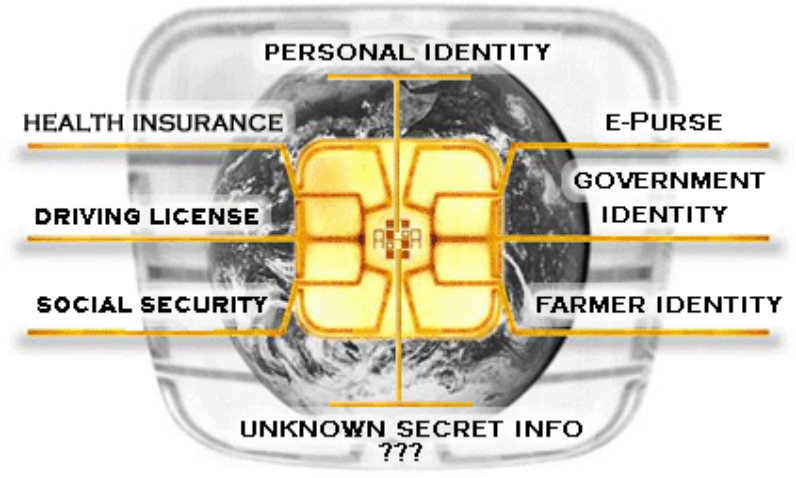
## FBI Issues Warning on New EVD Chip Cards

Source: http://www.hstoday.us/single-article/fbi-issues-warning-on-new-evd-chip-cards/277e0651a8e4def1e2fcd49e73de8d27.html

The FBI has issued a warning about new chip credit and debit cards being issued to consumers, saying, "When using the EMV (Europay, MasterCard and Visa) card at a PoS terminal, consumers should use the PIN, instead of a signature, to verify the transaction."

"By October 2015, many US banks will have replaced millions of traditional credit cards, which rely on data stored on magnetic strips, with new credit cards containing a microchip known as an EMV chip," the FBI said. But, "While EMV cards offer enhanced security, the FBI is warning law enforcement, merchants, and the general public that these cards can still be targeted by fraudsters."

The FBI warned that the "small gold chip found in many credit cards" referred to as "an EMV chip," "chip-and-signature," "chip-and-pin" or "smart" cards are now the global standard for credit card security, and, "Unlike traditional credit cards that store data on a magnetic strip,




EMV cards store card data in tiny integrated circuits and are authenticated when the cardholder inputs a PIN into a point of sale (PoS) terminal."

"Although EMV cards will provide greater security than traditional magnetic strip cards, they are still vulnerable to fraud," the FBI warned this week, noting that, "EMV cards can be counterfeited using stolen card data obtained from the black market. Additionally, the data on the magnetic strip of an EMV card can still be stolen if the PoS terminal is infected with data-capturing malware. Further, the EMV chip will likely not stop stolen or counterfeit credit cards from being used for online or telephone purchases where the card is not physically seen by the merchant and where the EMV chip is not used to transmit transaction data."

"Consumers should closely safeguard the security of their EMV cards," the FBI stressed, saying, "this includes being vigilant in handling, signing and activating a card as soon as it arrives in the mail; reviewing credit card statements for irregularities; and promptly reporting lost or stolen credit cards to the issuing bank. When using the EMV card at a PoS terminal, consumers should use the PIN, instead of a signature, to verify the transaction. This fully utilizes the security features built within the EMV card. Consumers should also shield the keypad from bystanders when entering their card PIN."

The FBI explained that, "With traditional credit cards, the magnetic strip on the back of the card contains data and personal information about the cardholder. This information is used to authenticate the card at the PoS before the purchase is authorized."

"While most EMV cards still retain the traditional magnetic strip and the cardholder's signature on the back of the card, they offer the additional enhancement of the microchip embedded into the card," the FBI stated. "This allows merchants to verify the card's authenticity by the cardholder's personal identification number (PIN), which is known only to the cardholder and the issuing financial institution. In addition, EMV cards transmit transaction data between


the merchant and the issuing bank with a special code that is unique to each individual transaction. This provides the cardholder greater security and makes the EMV card less vulnerable to hacking while the data is transmitted from the PoS to the issuing bank."

The FBI's advisory urged merchants "to require consumers to enter their PIN for each

transaction, in order to verify their identity," and "if a consumer uses a signature, merchants should ask to also see a government-issued photo identification card to verify the cardholder's identity."

The FBI further encouraged merchants to handle EMV cards and their data with the same security precautions they use for standard credit cards.

"Merchants handling sales over the telephone or via the Internet are encouraged to adopt additional security measures to ensure the authenticity of cards used for transactions," the FBI cautioned. "At a minimum," the Bureau stated, "merchants should use secure servers and payment links for all Internet transactions with credit cards, and information should be encrypted, if possible, to avert hackers from compromising card information provided by consumers. Credit card information taken over the telephone should be encrypted, and any written copies of the card information should be securely disposed."

"Retailers have long-argued that PINs are essential to providing cardholders with the security that they deserve. The FBI's alert should be a wake-up call to the banks and card networks that continue to stand in the way of making PIN authentication the standard in the US just as it has been around the world for years," said Brian Dodge, executive vice president of the Retail Industry Leaders Association, (RILA), the trade association of the world's largest and most innovative retail companies.

"Retailers have invested billions to implement new chip-enabled card readers in stores nationwide. Now, retailers are asking banks and credit unions to meet that commitment by issuing new chip cards with PINs," Dodge said.

RILA said in a statement that, "It is high time for banks and credit unions to heed the words of both the FBI and the Federal Reserve and issue consumers the most secure standard of payment—chip-and-PIN cards."

Continuing, RILA said the FBI's "warning states what retailers have been saying all along, which is that the new chip cards issued by banks need an accompanying PIN. Retailers have consistently urged banks and credit unions to ditch the signature and adopt the PIN. US banks and credit unions have argued that the chip is enough, and will prevent counterfeit chargess from being made."

RILA stressed that, "The FBI alert also urges retailers to require that PINs be used at the point of sale. Unfortunately, merchants cannot force consumers to enter a PIN if a card has been issued without one, and further, card network rules prohibit merchants from requiring a PIN when one exists."

"The deployment of EMV chip cards in the United States represents an important step forward. But we should not stop there," Federal Reserve Gov. Jerome Powell told *The American Banker*, adding, "New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions."

**A 2013 study by the Federal Reserve found that using PINs in debit card transactions reduced fraud by 700 percent.**



## Cyber Wars: From Regional Nuisance to Global Threats

Source: http://i-hls.com/2015/10/cyber-wars-from-regional-nuisance-to-global-threats/

**Today's small wars and border conflicts are being fought online and under the radar, but the conflicts could escalate into real world wars.**

Last year, a full-blown hacking war erupted between India and Pakistan, with groups on each side defacing websites belonging to organizations in their rival nation. "We're seeing this as a common form of attack," says Martin Libicki, senior management scientist with the RAND Corp. "This is a relatively easy attack to carry off, and the cost in terms of damage isn't very large." But as it continues to develop, cyber warfare has the potential to cause a lot more harm than mischief and nuisance. Cyber warfare has become an extension of traditional small war politics. In most cases it isn't meant to cause physical or even economic damage but is one that is more of mass annoyance or mass distraction.

Outside the economic harm it caused, the alleged North Korean cyber attack on Sony is an example of how it fits into the mass annoyance category.


Sometimes a cyber attack is another way of spying on another country. In 2014, North Korea was also accused of a cyber attack on South Korea's Korea Hydro and Nuclear Power Co Ltd. That attack didn't cause physical damage but it may have been conducted to gain plant blueprints and test data. This is a clear example of the way cyber warfare has become an extension of the classis war, this time in the form of espionage.

**As noted by the documents leaked by Edward Snowden, countries spy on one another all the time—and this includes allies spying on each other. But most security breaches are likely kept quiet to avoid the embarrassment that comes along with it.** But what if the reprucussions for cyber attacks become become too dangerous? For instance, government operatives, as in spies or sources, can be compromised through these kinds of breaches. We haven't yet witnessed a situation where things get out of hand, but it is surely a possible future scenario and some believe it is only a matter of time before someone cross some line.



## Police Car Hacks: Under the Hood

Source: http://www.darkreading.com/vulnerabilities---threats/police-car-hacks--under-the-hood/a/d-id/1322604


The recent hacks performed on two different Virginia State Trooper vehicles were nowhere near as sexy as the live-drive Jeep Cherokee remote attacks by renowned car hackers Charlie Miller and Chris Valasek. For one thing, they required initial physical tampering or access to the 2012 Chevrolet Impala and 2013 Ford Taurus, which are much lower-tech than the Internet-equipped 2014 Cherokee.

They also weren't tested with a police officer--or a journalist--behind the wheel. But in some ways, they are more scary, with the potential for an officer's vehicle to be a target and how they showed that older vehicles with few networked features are not immune to hacking.

I got to see the researchers' work firsthand earlier this month at the VSP's Driver Training Complex tucked away in rural Virginia's old tobacco country.
Here's a look at the work the Mitre team did on the unmarked Chevy Impala. In this video, the researchers demonstrate a prototype plug-in module built by working group member Kaprica Security to mitigate the car attacks created by the Mitre team. When the device is in place, the attacks don't execute. But when the driver removes it, the attacker (sitting in the backseat) is able to control the vehicle via his smartphone:
This second video, which was shot on behalf of the public-private partnership that worked on the police car-hacking project, is an overview of all of the attacks the researchers waged on the two vehicles, including locking an officer in the vehicle from the inside, engaging the wipers and fluid, starting the car remotely and wreaking havoc on the dashboard gauges, including the speedometer.It also shows in action the mitigation techniques by Kaprica Security and Mission Secure Inc. (MSi):
Among the organizations that worked on the project were the Virginia State Police, the University of Virginia, Mitre Corp., Mission Secure Inc. (MSi), Kaprica Security, Spectrum, Johns Hopkins Applied Physics Lab, Digital Bond Labs, the Aerospace Corporation, and the Virginia Department of Motor Vehicles. The research was conducted in coordination with the US Department of Homeland Security's Science and Technology division and the US Department of Transportation's Volpe Transportation Systems Center.

▶ **Watch the videos' mentioned at source's URL.**

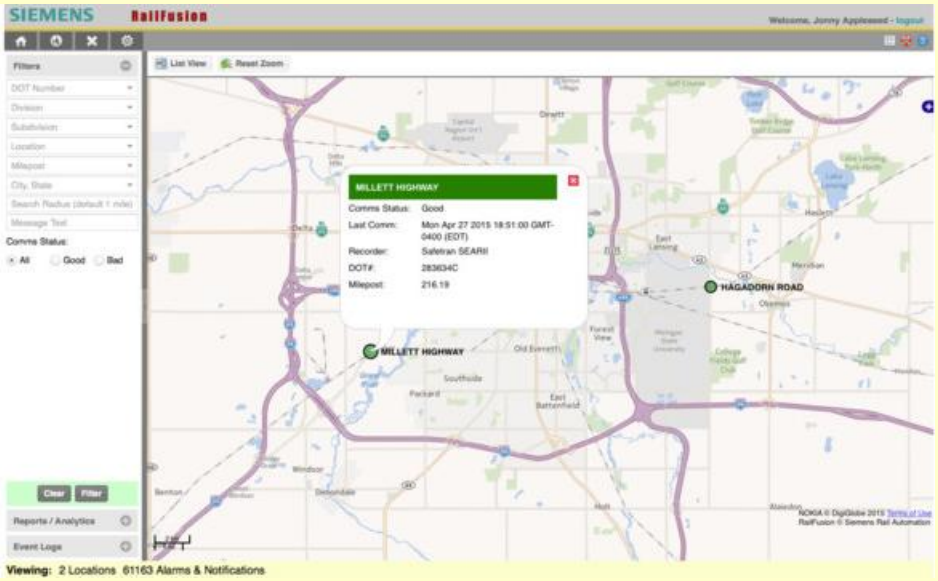
***Kelly Jackson Higgins*** *is Executive Editor at DarkReading.com. She is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise Magazine, CommunicationsWeek, Virginia Business magazine, and other major media properties. Jackson Higgins was recently selected as one of the Top 10 Cybersecurity Journalists in the US. She began her career as a sports writer in the Washington, DC metropolitan area, and earned her BA at The College of William & Mary.*



## Smarter, Safer Trains

Source: http://i-hls.com/2015/10/smarter-safer-trains/

Oct 15 – **At the beginning of October Siemens introduced RailFusion – a software designed to make our trains infrastructures safer and more efficient.**




This new software, already at its pilot stages in North America, monitors and analyzes data points across an entire railroad's infrastructure, including onboard and wayside assets, such as road crossings and end-of-train devices. All the data is transferred into the company's database in real-time and analyzed in order to identify trends so as to better plan their operations and fix issues before they become a problem, without having to leave the office.
By inserting intelligence behind the captured data, the software can evolve to include predictive capabilities that will help railroads identify trends to better plan their operations and fix issues before they become a problem, resulting in greater time and

cost savings. Ways the cloud-based system helps with smarter decision-making for railroads include enabling devices located on rail infrastructure to communicate with one another to remotely determine the status and effectiveness of maintenance activities, road crossings and locomotive operation; accessing live crossing occupation information in order to direct first responders to the quickest and most available route to save time in an emergency; identifying incorrect device behavior, such as false crossing activation and offering remote control to authorized operators, allowing them to address the traffic situation; analyzing patterns along the railroads based on historical data so railroads can more accurately plan their operations to become more reliable and efficient and offering operators of all skill levels a platform to manage complex rail infrastructure.

Once again the Big Data age shows how it can make our lives more efficient by analyzing countless pieces of information in real-time. But like any technological innovation that offers efficiency and comfort – it is important to make sure that it is protected against cyber attacks and terrorists, it being connected to the internet.

## 190 students hurt in China's fire drill; 9 critical

Source: http://www.beijingnews.net/index.php/sid/236891391

Sept 25 – Over 190 students were hospitalized, nine of them in critical condition, after inhaling smoke during a fire drill at a school in northwestern China's Gansu province, state media reported today. As many as 412 students of the junior middle school at Tianshui City of the province participated in the fire and air raid drill on September 18, according to the Tianshui government. "During the drill, smoke guns were used to simulate a true fire scene. Many students began to cough and vomit after inhaling the smoke," an official statement said. More than 190 people received medial treatment.

**EDITOR'S COMMENT:** We always urge planner to conduct realistic exercises but common logic should prevail as well! It is different to play this scenario with adults than with children. Light smoke environment would be enough compared with full capacity of smoke generators. On the other hand, this misfortune reveals the truth on what is expected to happen in a real life scenario. I only hope that the 8 patients into critical condition will survive and be well and that responsible authorities will make the most of this drill ("lessons learned") to avoid deaths in a future incident.

## Robots to pull wounded soldiers off battlefield

Source: http://www.homelandsecuritynewswire.com/dr20150925-robots-to-pull-wounded-soldiers-off-battlefield

Most Americans have seen at least one war movie, where at some point a fresh-faced young private is hit with some shrapnel. From the ground, he calls out for the unit medic — another young guy, from another small town, whose quick reaction and skill just may save his life. In the near future, however, it may no longer be another soldier, who comes running to his side. Instead, it might be an Army-operated unmanned aerial or ground vehicle, said Maj. Gen. Steve Jones, commander of the Army Medical Department Center and School and chief of the Medical Corps.

"We have lost medics throughout the years because they have the courage to go forward and rescue their comrades under fire," Jones said. "With the newer technology, with the robotic vehicles we are using even today to examine and to detonate IEDs [improvised explosive devices], those same vehicles can go forward and retrieve casualties."

The U.S. Army reports that Jones spoke at an Association of the U.S. Army-sponsored medical conference near the Pentagon, 22 September.

"We already use robots on the battlefield today to examine IEDs, to detonate them," he said. "With some minor adaptation, we could take that same technology and use it to extract casualties that are under fire. How many medics have we lost, or other soldiers, because they have gone in under fire to retrieve a casualty? We can use a robotics device for that."

Jones said unmanned vehicles used to recover injured soldiers could be armored to protect those soldiers on their way home. But the vehicles could do more than just recover soldiers, he said. With units operating forward, sometimes behind enemy lines, the medical community could use unmanned aerial vehicle systems, or UAVs, to provide support to them.

"What happens when a member of the team comes down with cellulitis or pneumonia? We have got to use telemedicine to tele-mentor them on the diagnosis and treatment," he said, adding that UAVs could be used for delivering antibiotics or blood to those units to keep them in the fight. "So you don't have to evacuate the casualties, so the team can continue its mission."

**Sensors**

Other technology that Jones said already exists, sensors that could monitor a soldier's vital signs, for instance, might also one day make their way to the battlefield, being worn by soldiers full time.

"Army Medical Research and Materiel Command is actually developing physiological sensors that soldiers can wear," Jones said. "And in a few years, they will be able to field this. They can be wearing the sensors and we can just monitor them. And we can do that remotely."

The general likened the sensors to something like a "Fit Bit," which soldiers might wear now to monitor their heart rate and steps taken.

"This is just a step forward that will monitor other physiological parameters," he said. "Do they need to push more water? How many calories have they consumed? There is a lot of information we can provide commanders that they can use to manage their soldiers."

The same sensors could be used to triage casualties automatically, so that those injured soldiers whose vital signs are the worst are the ones who get rescued first.

"If you see a casualty whose heart rate is way up, whose respiratory rate is way up, that may be an indication they lost a lot of blood, and need treatment now, as opposed to a casualty whose vital signs are stable and you wouldn't have to treat as quickly," he said.

The same sensors can also be installed on unmanned aerial vehicles that might one day rescue soldiers when they go down.

Jones also discussed the use of "GoPro" cameras on soldiers to document wounds and treatment that is administered. Such video, he said, can be transmitted real-time to follow-on treatment facilities where it can be used by physicians there to better understand exactly what treatment a soldier has already received. Additionally, such footage could be used to provide feedback to the medics who performed the initial care to help them improve their skills. The Army says it is doing something similar now, he said, through the use of medical simulators.

"[We] train combat medics in simulators and record treatment they provide and play it back for them," he said. "We show them how they entered the scene, how they surveyed their casualties, how they decided which casualty to treat or not treat. And then we talk to them about the treatment they actually provided."



# Teams of computers and humans more effective in disaster response

Source: http://www.homelandsecuritynewswire.com/dr20150925-teams-of-computers-and-humans-more-effective-in-disaster-response

Sept 25 – **Over the past five years, researchers from Oxford University have been working on a collaborative project called ORCHID to develop new ways for humans and computers to work together.**

This week, the team from Oxford joined their academic collaborators from the University of Southampton and University of Nottingham at the Royal Academy of Engineering to showcase their work. Oxford Science blog spoke to Dr. Steven Reece, a Senior Research Fellow at the University's Pattern Analysis and Machine Learning Research Group, to find out how the Oxford team has been using its research to help disaster response teams.

***OxSciBlog: ORCHID attempts to integrate humans — and all of their foibles — with computers, so that they can work together as so-called human-agent collectives. Why is it important?***

*Steven Reece*: Ninety percent of all recorded data that exists in the world has been generated in the past two years. This data is vast and mostly unstructured, made up of all kinds of text documents, photographs and videos. The problem is that humans and computers look at this data very differently. Humans are very good at understanding unstructured data — they can interpret the meaning of text and understand events depicted in a photograph better than any software, for example — but they can't work through that much of it. Computers, on the other hand, are better than humans at

processing and spotting patterns in vast amounts of data very quickly. Human-agent collectives (HACs) take the best of both worlds, creating flexible teams of computers and humans to interpret large, unstructured data sets.

***OSB: How do these HACs work?***

*SR*: Traditionally, humans tell computers what to do; HACs turn that relationship on its head and allow computers to take control occasionally and request information from humans. Of course, humans and computers have their foibles: they can be unreliable, malicious, selfish and, in the case of humans, they can even get bored. But it was the goal of ORCHID to figure out how to mitigate these foibles: how to incentivize humans to contribute to the HAC, track performance, maintain the best teams and record the sources of information and decisions that are made.

*OSB: Can you describe the kind real-world problems you've been applying that thinking to?*

*SR*: As just one example, crisis responders need to know the extent of a natural disaster, what aid is required and where they need to get to as quickly as possible. This is what's known as "situation awareness." With the proliferation of mass media, a lot of data is now generated from the disaster zone via photographs, tweets, news reports and the like. With the addition of first responder reports and satellite images of the disaster area, there is a vast amount of relevant unstructured data available for situation awareness. A crisis response team will be overwhelmed by his data deluge — perhaps made even worse by reports written in languages they don't understand.

But the data is also hard to interpret by computers alone, as it's difficult to find meaningful patterns in such a large amount of unstructured data, let alone understand the complex human problems that described within it.

***OSB: How can you use HACs to help?***

*SR*: Firstly, we can farm out satellite images and text to the "crowd." People want to help and they will happily use their skills to interpret a small number of text samples or satellite images. Computers can then build a model connecting features in the data to the interpretations supplied by the crowd. The computer can then use this model to trawl through the rest of the data and "interpret" what it sees using these features. The computer decides what data to farm out to the crowd and who should be recruited from the crowd based on their reliability. The individuals in the crowd can decide if they want to take part and what tasks they are prepared to do. The computer aggregates the crowd responses intelligently and, in so doing, determines their individual reliabilities automatically. So we can use combinations of humans and computers to successfully aggregate and interpret vast amounts of unstructured data. This is just one example of where HACs can be used in disaster response — another is the coordination of a vast fleet of UAVs visually mapping aid requirements across the disaster area.

***OSB: Have you been able to try any of these ideas in the real world?***

*SR*: We've implemented the first approach I just explained, actually. It's in a system called "CrowdScanner," and we used it for real immediately after the first major Nepal earthquake in April of this year. We used the crowd to locate settlements from satellite images, identified settlements that were not mapped on open sources such as OpenStreetMap, and our Search and Rescue partners deployed teams to reconnoiter these settlements.

***OSB: Was it successful? Did you run into any pitfalls when marrying up computers and humans?***

*SR*: First of all, the good news! It is not difficult to find a competent crowd to help out in a disaster situation. We are, however, finding it really difficult to build systems that are relevant to the disaster response community — mainly because we are trying to guess what their critical information requirements might be.

We were able to respond to the Nepal crisis because we just happened to have a working platform that we could adapt to the Nepal situation along with a satellite data source, and Rescue Global, who we were working with, were able to marry this data with their requirements of water filter placement and life detector placement. We were able to respond in a timely manner as a result.

In general, though, we're in the dark as to the generic problems faced by the crisis response community and specifically where we can help. Although we've attended field exercises with various disaster

response organizations we need to sit down with them. That way, we'll be able to abstract information about where they work and their requirements to the level where we can start designing generic situation awareness algorithms to help them.

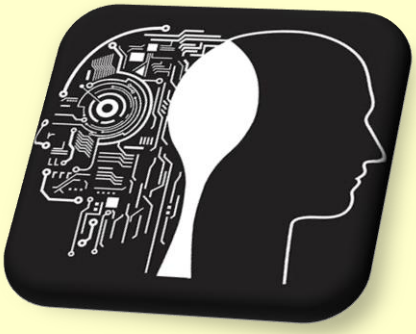
***OSB: So what's next for the disaster response work?***

*SR*: Imagine a service where people could post their resources, such as the availability of an aircraft or their plan to visit a location in the disaster area. This resource could be married with a crisis response team who want to use it to achieve their own goals, and machine learning can be used to link the responders' requirements to the people with the resources using crowd interpretations of the resource providers' offers. Another idea is that we could try to determine the probability of life in a collapsed building after an earthquake, to help responders prioritize their search. Crowdsourced interpretations of drone or satellite footage could be used to identify salient features and machine learning can then determine the probability of life.

There are many ways machine learning can be used in disaster response. The key now is to sit down with crisis responders and develop relevant data processing algorithms that will actually save lives.

## A.I. Program To Assist Us In Making Decisions

Source: http://i-hls.com/2015/09/a-i-program-to-assist-us-in-making-decisions/



Sept 27 – A joint project between NASA and the U.S. Department of Homeland Security (DHS) resulted in a smart program that will do just about anything in order to provide its user with the information they need. The program, which will be connected to the Internet and the Cloud, could ask other programs questions regarding information it lacks. The project is meant to create a sort-of "personal assistant" to give first responders a complete and overall picture about conditions in the field.

The new system is really a computerized version of human reasoning and a decision-making system. In just 16 months, the first prototype, called **AUDREY (Assistant for Understanding Data through Reasoning, Extraction and sYnthesis)**, will be tested.

Don't be alarmed, the program will not replace human beings, but assist them in analyzing countless pieces of information. It's true there are many systems to process and analyze data, but they usually require large computers and many servers. AUDREY, on the other hand, is a program that can be used on our personal computers.

The system can be tailored to individual users. For example, the firefighter headed into a burning building may need different information than the on-site commander or a helicopter crew. The system can recommend which units respond to an emergency based on who is closest, what types of equipment they carry or how busy they are at the time. It also could warn of the presence of dangerous chemicals or tell firefighters when a floor is in danger of caving in.

**The special thing about AUDREY is its flexibility, that is, the ability to be applied in various fields**. Another unique feature is its future capability to work with mathematical formulae. For example, firefighters often have to make an educated guess as to how much equipment or what types of equipment they might need, but they could be lacking certain information. The program, then, could calculate the required equipment according to weather conditions, a direct video footage from the helicopter in the field and even data from wearable sensors on the firefighters' uniforms. AUDREY could also talk to other AUDREY systems when it lacks certain data. When NASA's Mars Rover, for example, saw something unexpected, it would simply ignore it because it does not know what it does not know. On the other hand, when AUDREY realizes it is missing critical information and will try to get the answer some way or another.

Although the program is first and foremost meant to be used by first responders, project officials foresee it joining a wide range of users – military fighters, plant workers and even citizens.


## empowering preparedness globally

Resilience Guard is a boutique consultancy that provides specialist business continuity and crisis management consultancy services to organisations in Switzerland and across Europe. We offer a menu of specialist services tailored to your industry sector that allows you to choose as much, or as little, help as you need. These include:

- Business continuity management
- Crisis management
- Risk management
- Business assurance

Resilience Guard GmbH
Kreuzplatz 2, CH-8032 Zürich, Switzerland
T +41 (0) 44 266 10 62
F +41 (0) 44 266 10 62
E info@resilienceguard.ch

www.resilienceguard.ch

ResilienceGuard
Business Continuity | Crisis Management

# Social Media as a Sensor – Leveraging Crowd-Sourced Data for Early Warning and Response

**By Sara Estes Cohen**

Source: http://www.ghinternational.com/blog/social-media-as-a-sensor-leveraging-crowd-sourced-data-for-early-warning-an#.Vg9qQZc42z8


**A recent story published on Wired.com discussed the findings of group of researchers at the Indiana University School of Informatics and Computing who developed a method for predicting changes in the Dow Jones Industrial Average through the analysis of Twitter updates. The research team leveraged open-source mood-tracking tools like OpenFinder to sort Tweets into positive and negative bins based off of emotionally charged words, the research team was able to predict the ups and downs of the stock market at closing bell three days later to within 86.7% accuracy.**

Now consider leveraging data collected in this manner via Twitter and other social media tools for other types of predictions. The implications of this type of data collection for early warning and/or confirmation of information – social media as a sensor – are significant if applied to the field of public safety.

Earlier this year, Federal Computer Week highlighted a group of Namibian officials who, with assistance from an international team of experts including representatives from NASA and the National Oceanic and Atmospheric Administration (NOAA), developed a geospatial application tapping and combining satellite imagery and river-height sensors to get an early read on possible flooding in Namibia. Leveraging sensory data, officials are now able to predict, prepare for, and respond to events much sooner than previously possible. Furthermore, aggregating and geospatially depicting data provides contextual understanding of a large volume of information very quickly.

By combining social media data with geospatial analysis, officials may be able to prepare for and respond to a disaster faster than ever before. Sensory data like that collected via river-height gauges and seismic monitors, when combined with social media data and/or sentiment analysis, provides both the "what," or that an event has just occurred or is about to occur, and the "who," the "why," and the "how" – or the context of an event, including the public's level of understanding, its reaction to and knowledge of factual information, may even assist in predicting second and third-level events that might arise as a result of the original disaster.

Emergency response officials already monitor seismic data provided by the United States Geological Survey (USGS) for early detection of earthquakes. Why not combine seismic data with key word searches for "earthquake," "shaking," etc. within specific geographical locations? Going further, why not overlay both seismic data and geospatially mapped data from Twitter with historical event data, critical infrastructure data, hazard and mitigation data, etc.? The resulting mash-up could provide an unprecedented level of contextual understanding to response agencies experiencing resource cutbacks and struggling to keep up with the volume of information available on the internet.

Despite the benefits of collecting crowd-sourced data during an emergency, it has not yet been adopted by incident response agencies for a variety of reasons. Many in the incident response community are reticent to social media data a valid information source. In large part, this is due to the difficulty in vetting the potentially vast amounts of data during a major operation. The inability to process this information, in turn, raises other issues for decision-makers, including potential liability concerns. To a lesser degree, the incident response community is steeped in tradition, with a strong proclivity to favor only proven methods and tools for the conduct of their mission. Dramatically divergent concepts

are likely to meet with some cultural resistance. For agencies to begin using social media and other types of sensory data for early warning and response, several changes must occur. First, rather than constantly monitoring Tweetdeck or similar other tools and attempting to physically sift through the data that is rapidly coming in from social media, news wires, etc., imagine if a predetermined aggregation and filtering mechanism could automatically filter through the information and geographically map it so you could look at all the information in context to an event as it unfolds. Incoming Tweets and sensory data could then be visualized as points on a map, and additional tools could enable you to pull in relevant information from other sources including government agencies, public information offices, and non-governmental organizations. This information too could be automatically sorted and mapped for further analysis. Additional tools could then enable more rapid and accurate analysis of the information allowing for efficient and effective decision making. Virtual USA, the Department of Homeland Security's flagship program, sponsored by the White House Open Government Initiative and DHS Secretary Napolitano, has already made these concepts a reality.

Second, although social media tools enable access to a great deal of information from multiple sources prior to and during an incident which can, in turn, greatly enhance decision making and situational awareness, the wide scale use of social media during an event can also present significant challenges in monitoring and sorting through large amounts of data in order to authenticate information for real time decision making.

To harness crowd-sourced and sensory data most effectively, agencies need the ability to successfully aggregate, filter, integrate, map, prioritize, assign, and follow up on data collected via these methods. Accomplishing this requires that:

- Data aggregation and analysis tools to be developed to assist organizations in decision making;
- Data should be geospatially enabled for additional context; and
- Applicable governance framework, policies and challenges (e.g., liability and privacy issues, etc.) must be identified and addressed.

Leveraging crowd-sourced and sensory data may prove useful for alert and early warning of several types of events, including:

- Shooting and other violent acts as they occur;
- Disease, outbreaks, symptom clusters;
- Bird and other animal deaths;
- Floods, tornados, wildfires, and other natural events; and
- Traffic.

I am interested in hearing what others have to say about the types of data that might serve to assist public safety organizations in responding to events within their jurisdictions. Often it is the real-world application and identification of an information gap that drives the development of new and innovative technologies and methodologies.



***Sara Estes Cohen*** *is a Project Manager for G&H International Services, Inc. and currently working in community support and management for DHS First Responder Communities of Practice, a trusted network and platform for homeland security professionals to communicate, collaborate, and share resources.*

## Smart ambulances: the hi-tech future of accident and emergency healthcare

Source: http://www.euronews.com/2015/10/02/smart-ambulances-the-hi-tech-future-of-accident-and-emergency-healthcare/

Every year all over Europe ambulances come to the aid of millions of people. A study suggests almost half of the cases could be treated on the spot and not need hospital care. On that basis a European research project aims to create a Smart Ambulance that can respond quickly and comprehensively to emergencies.

It is hoped that very soon medics will be able to give an accurate early diagnosis in the so-called he 'golden hour' after an incident that could decide the fate of the patient.

SMART AMBULANCE EUROPEAN PROCURERS PLATFORM

"The ambulance will be equipped in such a way with ICT technology, so the ambulance crew can actually work with people inside the hospital," said Declan Henegan, editor of Ambulance Today Magazine. "That also means that the quality of the diagnosis made on scene within the ambulance is going to be more exact, and could mean that the patient goes to one hospital instead of another hospital."

**Room for improvement**

Currently, most ambulances are cramped and confined spaces with sometimes difficult access to




equipment. That doesn't help when trying to treat a patient's injuries on the move, according to London-based paramedic Elaine Parris: "It's not ideal to keep going here, standing moving, whereas, for instance (it's better) if things are all available in front of you, easy to grab. The other thing we are unable to do is to get round the other side of the patient, even the cupboards don't tend to open as much as

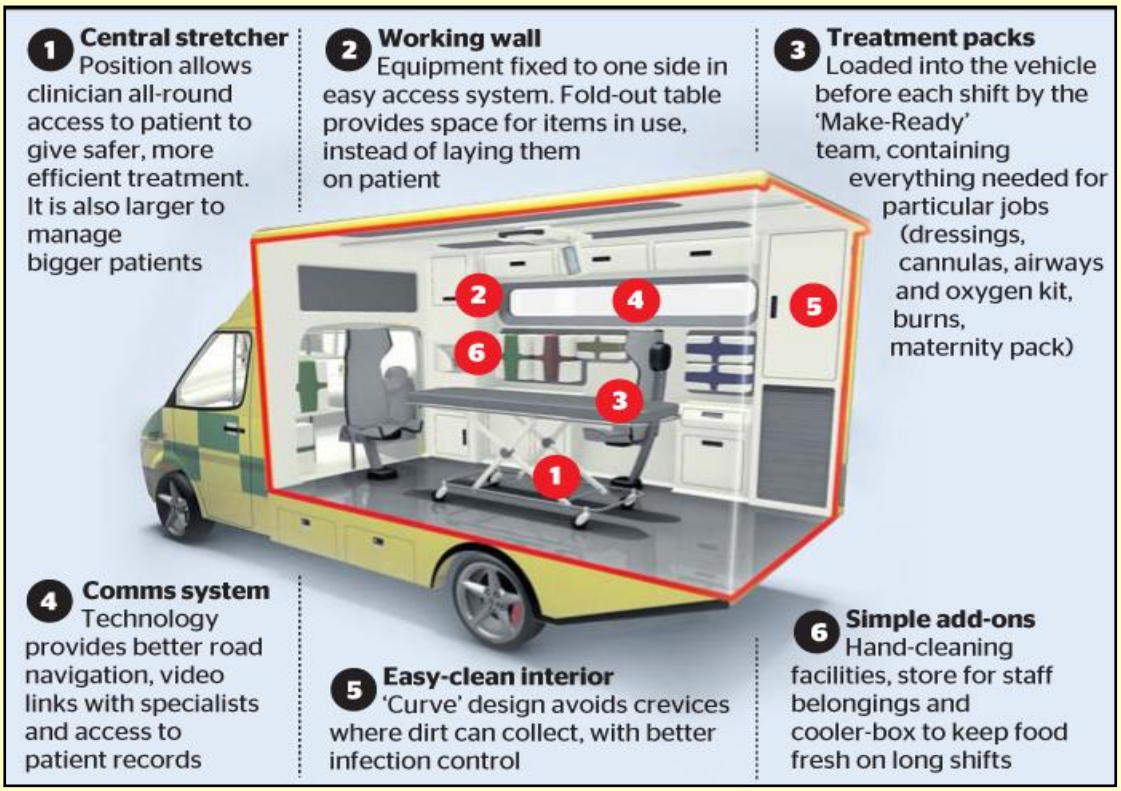
they need to. I could then be putting myself right across the patient, who potentially could be vomiting."

Researchers involved in the Smart Ambulance project created a prototype specifically designed to address those issues. Gianpaolo Fusari, a designer at London's Royal College of Art demonstrated the layout to Futuris: "A digital diagnostic and communications system monitors the patient and sends data to hospitals.

"Putting the stretcher at the center of the ambulance allows the paramedics to treat the patient from all sides. Another innovation is these 'treatment packs'. You just change the pack for a new one when it's used," he said.

**Some of the most promising ideas include:**

- a side-loading trolley layout that also removes the separation between the front of the cab and the treatment space, leaving enough room for one paramedic to have 360-degree access to the patient; built-in washing facilities
- a repositionable monitoring and communications system
- larger windows in the sides and roof to allow more natural light inside the ambulance
- the reconfiguration of consumables into treatment packs.






**Making life-saving decisions**

The most crucial aspect of the smart ambulance is its ability to send and receive data, which helps medics make diagnostic decisions. Andy Newton, Chair at College of Paramedics expects this feature to be further enhanced in the future: "Technology is always moving forward, and at an increasing pace. I think we will see more use of internet enabled technologies, such as telemedicine We have in this project, also, the capability of carrying a mobile laboratory in the vehicle, to use diagnostics such as ultrasound, and X-ray technology is also on the horizon."

It is hoped these ambulances will soon by offering a higher standard of potentially life-saving emergency treatment in many EU countries.

## Developing new modelling tool for better crisis management

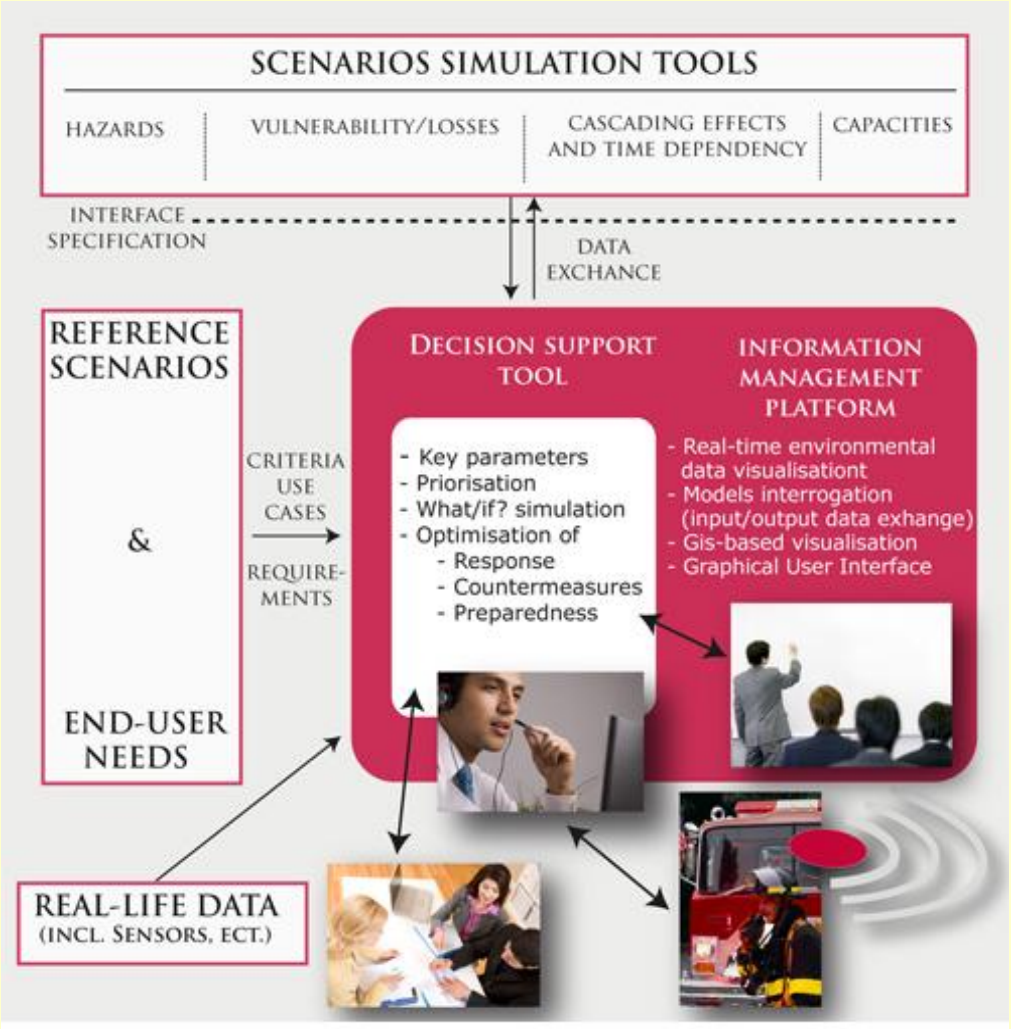
Source: http://www.homelandsecuritynewswire.com/dr20151005-developing-new-modelling-tool-for-better-crisis-management

Oct 05 – Crisis managers and key decision makers routinely face situations that exceed the capacity of local response networks. Furthermore, natural and man-made disasters often do not respect regional or national boundaries, spilling out across borders and creating new unforeseen problems. For these reasons, decision makers need the tools to better understand crisis impacts and have immediate access to multi-organizational and multi-national expertise if and when required.

CORDIS reports that the EU-funded **CRISMA project** sought to address this pressing need through the development of an adaptable online simulation tool. This tool

helps policy makers and those directly involved in crisis management to prepare for events by visualizing complex crisis scenarios, which often require the integration of expertise from multiple sectors and can involve significant financial and ethical concerns.

End uses include land-use and infrastructure planning on a long-term basis, the optimization of operational crisis management plans and support for the preparation, execution and assessment of field exercises. The project consortium also believes that potential exists for the private sector to use the simulation model.




**The CRISMA framework has been specifically designed to enable end users to build up their own crisis scenarios and then integrate both new and legacy models and tools into one simulation system. The adaptability of this architecture was achieved by following an open approach; much of the core framework functionality is served by open source software, which can easily be replaced if and when necessary.**

Furthermore, the CRISMA framework anticipates future technological changes and can accommodate several types of Web services. The modular design allows future developers to add new building blocks when needed, either in open source or closed source, in line with the end user's own business model. Crisis managers and other decision makers can combine models, data and expertise from different sources in order to create a wider perception of crisis scenarios.

During the project, a number of pilot schemes were set up to cover a range of different crises. These included a winter storm event in northern Finland; the submersion of coastal defenses in western France; an accidental container spillage off the coast of Israel; an earthquake and forest fire in Italy; and a multi-hazard mass casualty incident in Germany. Workshops with potential end users were organized to illustrate pilot scheme results and to highlight the potential of the new tool.

The long term sustainability and uptake of the CRISMA results will be assured through recommendations from decision makers and external high-level experts in the CRISMA advisory board.

The project was officially completed at the end of August 2015. A report on CRISMA's final results was published in September 2015, while key successes were shared at the project's final conference in June 2015.

# Study Finds Schools are Underprepared for Pandemics and Natural Disasters


Source: http://www.infectioncontroltoday.com/news/2015/10/study-finds-schools-are-underprepared-for-pandemics-and-natural-disasters.aspx

Missouri schools are no more prepared to respond to pandemics, natural disasters, and bioterrorism attacks than they were in 2011, according to a study published in the October issue of the American Journal of Infection


Control. A team of researchers from Saint Louis University collected and analyzed survey responses from **133 nurses serving elementary, middle, and high schools in Missouri** to determine whether schools were any more prepared for another pandemic than they were based on a similar study conducted in 2011. Pandemic preparedness is not only critical because of the threat of a future pandemic or an outbreak of an emerging infectious disease, but also because school preparedness for all types of disasters, including biological events, is mandated by the U.S. Department of Education.

**Researchers found that on average, schools still reported having less than half of the measured indicators for preparedness.** Although in general, schools were much better prepared for natural disasters than biological events, nurses agreed on the equal importance of being prepared for both. **Particular gaps were found in bioterrorism readiness--less than 10 percent of schools have a foodservice biosecurity plan and only 1.5 percent address the psychological needs that accompany a bioterrorism attack.** This part of the study expanded upon the 2011 study, which did not evaluate bioterrorism preparedness.

**In addition, only 1.5 percent of schools require that staff receive an annual flu vaccine.**

"Infectious disease disaster planning among Missouri schools does not appear to have progressed much over the last four years since a similar nationwide study was conducted, and most Missouri schools are not meeting many national and professional organization recommendations and guidelines," state the study's authors. "A critical finding from this study is that only a very small percentage of schools are addressing student psychological needs as part of disaster planning. Numerous researchers have emphasized the important role schools will play in meeting student and staff psychological needs during and after disasters."

The researchers conclude that U.S. schools must continue to address gaps in infectious disease emergency planning, including developing better plans, coordinating these plans with local and regional disaster response agencies, and testing the plan through disaster drills and exercises. Whenever possible, school nurses should be involved in these planning efforts, as healthcare professionals can best inform school administrators about unique aspects of pandemic planning that need to be included in school disaster plans.



# Running to the Police, Not Away From Them

**By Rodrigo (Roddy) Moscoso**

Source:http://www.domesticpreparedness.com/First_Responder/Law_Enforcement/Running_to_the_Police%2c_Not_Away_From_Them/

**Building sustainable communities is a long-term effort that includes reestablishing positive relationships between police departments and the communities they serve. Repairing these damaged relationships means changing the visual perception,**

**improving communication, providing education, and building awareness for the community members.**

Since the August 2014 riots in Ferguson, Missouri, following the police shooting death of Michael Brown, significant media attention has been placed on the public's perception of law enforcement officers and their use of force. Several cases captured on video – including the death of Eric Garner in New York City during a sidewalk arrest – have latched on to the narrative that the police have become, to some, a source of fear rather than protection, an enemy rather than an ally.

**Broken Relationships**

The April 2015 riots in Baltimore, Maryland, following the death of Freddie Gray while in police custody served as another stark example of the significant distrust that exists between law enforcement officers and portions of the community that they are charged to "protect and serve." Although the events that unfurled will be analyzed for years to come, the unfortunate reality for the city of Baltimore is that significant parts of its citizenry appear to have lost faith in the police; they do not look to them for help in times of crisis.

During the Baltimore protests, Mayor Stephanie Rawlings-Blake made the critical decision to order the police to "create a space" for the protestors, acknowledging later that doing so had also given "those who wished to destroy space to do that [as well]." However, when some unknown number of "bad actors" looted and set fire to their own neighborhoods within this space, the local population did not call out for assistance from the police gathered only blocks away. Worse, the police knew that they were not wanted. This broken relationship played out on live television, and became yet another example in a yearlong series of events highlighting a line between the police and the citizenry.

In some areas, the "us vs. them" viewpoint has become "the norm," illustrating the modern relationship between police officers and the communities they serve. This fractured bond benefits neither the public nor the police and inevitably leads to further distrust and more-frequent instances of conflict and even violence. The questions now are how to better define the relationship and how to make it happen.

**One Police Chief's Perspective**

"In times of crisis, we want people to run to the police, not away from them," said David Mitchell, director of public safety and chief of police for the University of Maryland at College Park (UMD), in a personal interview on 16 June 2015. Mitchell, who has served in cabinet-level positions in Maryland and Delaware as state police superintendent and secretary of the Department of Safety and Homeland Security, respectively, believes that a culture shift in law enforcement – not more training – is what is needed to improve the relationship between the general public and the police.

He worries that law enforcement has "lost legitimacy" with the public. "Our business is to sell safety, and to do so we must redefine our success as, 'the creation of sustainable neighborhoods'," Mitchell added. He is also leery of what he sees as an overreliance (and focus) on crime data used internally by police departments to measure crime rates across distinct geographic areas.

"CompStat is often used by [police] executives to embarrass individuals, which does not necessarily achieve important public safety outcomes. It's a useful tool to be sure, but it is not able to measure our success in building positive relationships with our community," he said, adding that, "the number of arrests made and tickets issued are not necessarily measures of success."

Mitchell also believes that the manner in which the police respond to the community during incidents is equally important. These efforts include:

- *Visual perception* – "We don't dress in BDUs [battle dress uniforms], we use uniforms of the day," said Mitchell noting that BDUs do not necessarily present an "approachable presence" and may create a visual perception of force that is not conducive to building a positive relationship with the community.
- *Communication* – "Ongoing communication is also key to building trust," said Mitchell. The UMD Police Department uses multiple communications channels to keep the community informed of events, large and small, taking place in the area.

  "We use Nixle to send targeted, geo-fenced alerts to faculty and students not just about public safety related

issues, but also to alert them of road closures, construction issues, etc.," he noted. Doing so establishes a "dialogue" that serves to open communication channels that "work both ways" and to encourage people to value and rely on the information coming from the police department.

- *Education* – The UMD police department educates students and faculty on how to respond collaboratively during a significant event, such as on-campus active shooter. "We teach 'Run, Hide, Fight' to our community," said Mitchell. "It is critically important, and it gives our students and faculty a sense that we are working together during these types of situations," he added.
- *Awareness* – Training and communication also helps to avoid the potential confusion caused by a lack of awareness of who the police are, "We can't meet each other for the first time during a crisis," said Mitchell.
- *Documentation and review* – The UMD Police Department documents "every use-of-force incident," including when an officer only "pulls a gun," for later review and analysis. Mitchell noted that the department is currently reviewing its use-of-force training with "a new focus on de-escalation techniques."

Mitchell also believes that leveraging technology is another way to build trust. Examples include:

- *Body-worn cameras* – "We use body-worn cameras, and the officers love them," said Mitchell, noting that the technology creates an "objective observer" that both parties can acknowledge (and perhaps adjust their behavior to) during a police interaction.
- *Gunshot detection* – The UMD is in the process of installing "ShotSpotter" gunshot detection solution in and around campus, which will facilitate a more efficient and timely response to locations where gunshots have occurred.
- *Social media monitoring* – The UMD monitors social media proactively in order to identify incidents that may require a police response. "Social media allows us to establish a real-time dialogue with our community," said Mitchell. "We want them to tell us what is happening, that's why we are here," he added.

**Long-Term Dividends**

Building "sustainable communities" is a long-term effort and one that will require vigilance and a consistent effort by all community members, including the general public, businesses, government, and public safety. Rebuilding the trust between law enforcement and the public is a critical step in this process. "We 'sell' safety, and that means that we have to deliver it. And we will be more successful if the community sees us as a full partner in achieving safety," said Mitchell.

Following the events of the past year, this may be a "tough sell." Building trust is also not something that is ever accomplished quickly. However, small and incremental steps can reap dividends over the long term. Starting a dialogue, even one way, can be a good first step.



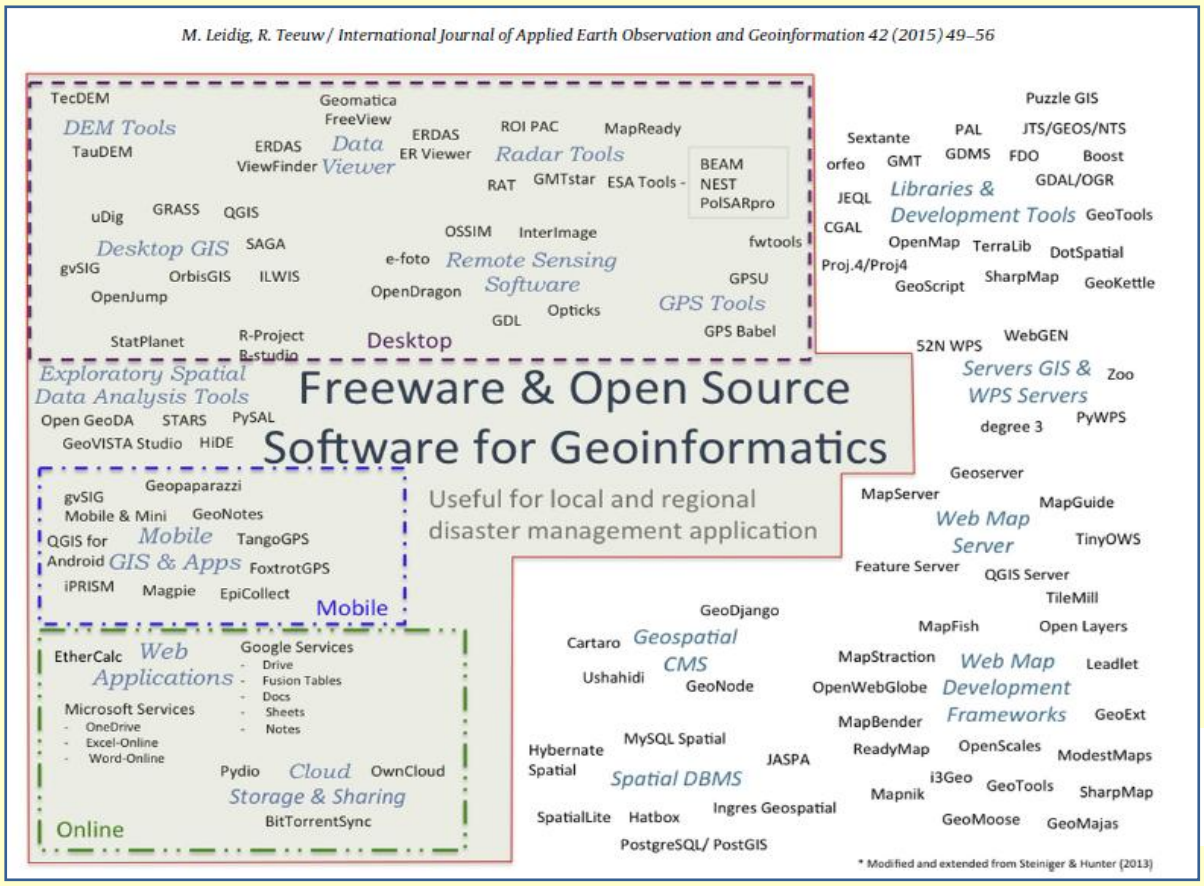
***Rodrigo (Roddy) Moscoso*** *currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.*

## Free software: A review, in the context of disaster management

Source: http://www.sciencedirect.com/science/article/pii/S030324341500121X

This article examines the nature of freely available geospatial software and information systems in the context of disaster management. The use of geospatial data is crucial to effective disaster management, from preparedness to response and recovery. However, to make efficient use of available data and information – before, during and after a disaster – reliable software is required. The software applications examined in this paper range from

Geographical Information Systems, to the processing of remotely sensed images, crowd-source mapping, web applications and content management systems. Trends and challenges are considered, and guidelines are given, to foster and encourage the provision of information by Freeware and Open Source Software. Free geoinformatics can help to optimize the limited financial, technological and




manpower resources that many organisations face, providing a sustainable input to analytical activities.

**Highlights**

- We examine the nature of freely available geospatial software and data in the context of disaster management.
- The reviewed software applications range from GIS to remote sensing, crowd-source mapping and content management systems.
- Free geoinformatics can help to optimize the limited financial and technological resources that many organisations face.
- Trends and challenges are considered, guidelines are given.

# Virtual Exercises - A Cost-Effective Option

**By Dawn Thomas**

Source: http://www.domesticpreparedness.com/Training/Exercises/Virtual_Exercises_-_A_Cost-Effective_Option/

**Some exercises require a hands-on environment, whereas others can thrive in a virtual training space. FUSION X is one federally sponsored exercise that has evolved from a tabletop event at a single location to a virtual training for participants, who require flexibility and cost-effectiveness, at various locations throughout the United States.**

Oct 14 – Those responsible for their organization's preparedness efforts have often been told that they must find ways to do more with less. With budgets tightening even further,

exercises are a likely victim of this trend, as large exercises can be extremely costly to sponsors. However, with continuing and increasing threats associated with natural incidents, industrial accidents,


and deliberate acts, members of the homeland security enterprise need the opportunity to practice their skills in meaningful ways. For those supporting preparedness at the local, state, regional, tribal, and federal levels, this means considering new possibilities for exercising targeted audiences using less expensive methods, but without sacrificing value.

**Exercising Fusion Centers**

On 2 August 2012, the Department of Homeland Security (DHS) Office of Intelligence and Analysis (I&A) sponsored FUSION X, a timely one-day exercise that allowed eight fusion centers to share information and analysis across their National Network of Fusion Centers (National Network) partners. Over the preceding years, DHS had invested a great deal of time and money to support the development of individual fusion center capabilities, including the publication of fusion center guidelines and baseline operational standards. By 2012, internal capabilities grew, and DHS I&A determined that the next logical step was to begin testing information receiving, gathering, analysis, and dissemination across the National Network. Their exercise design included elements of both a tabletop and a functional exercise, with players sitting at different tables and receiving injects that drove interaction.

Exercise support personnel occupied a simulation cell and provided pieces of the puzzle as the scenario advanced. Additionally, each table had a facilitator and an evaluator, who recorded exercise play and developed an after-action report for each table. After the exercise, the lead evaluator gathered and aggregated all exercise data, and developed an after-action report for the National Network. Although DHS I&A and the participants considered the exercise a success – and important strengths and areas for improvement were identified – the cost (both in time and money) was not insignificant. Analysts were away from their desks for two to three days, and a large support staff was needed to facilitate and record the exercise.

In 2014, DHS I&A embarked on an effort to conduct the second exercise in the FUSION X series, using the same tabletop concept as the one used in 2012. As the planning process proceeded, issues of funding and level of effort put the project on hold, and the exercise was postponed. With a continued belief in the value of simultaneously exercising multiple members of the National Network, the newly formed DHS I&A Continuity and Exercise Programs Branch and their exercise planning team began developing a new version of FUSION X – a functional exercise that would take place in a completely virtual, yet secure, environment.

**Moving to a Virtual Training Ground**

The exercise, conducted in July 2015, covered a large geographic footprint, but with no travel required. Players were located in fusion centers in Arizona,

Colorado, Idaho, New Mexico, Utah, and Wyoming, in addition to DHS Watch and Warning Center in Washington, DC. Continuity and Exercise Programs Branch leadership and members of the exercise support team (composed of an exercise director, simulation cell staff, and evaluators) were also spread out, participating from Washington, Virginia, Texas, New Mexico, and Washington, DC.

Although the exercise support team provided training, fusion centers were responsible for providing their own facilitators and evaluators. The former were responsible for: (a) supporting scenario development; (b) injecting their pieces of the Master Scenario Events List; and (c) leading discussion at their respective locations. The latter were responsible for: (a) documenting exercise play; (b) gathering participant feedback forms; and (c) providing their analysis of events through exercise evaluation guides. In addition to making observations on the execution of the fusion centers' critical operational capabilities, the exercise support team also collected and aggregated reflections on the design, conduct, and evaluation of a virtual exercise, including the following:

- The virtual exercise allowed analysts to better mimic their day-to-day roles and responsibilities by more accurately replicating their work environments. The injects – in the form of social media posts, situation reports, and memos from the various intelligence community partners – reflected the information received during a typical workday, and participants were able to respond authentically. Moreover, with a growing effort to gather, analyze, and share information gained through social media and other electronic methods, the virtual environment provided an excellent background for demonstrating fusion center capabilities.
- FUSION X 2015 was less expensive to execute and demanded less time from exercise planners and players than an exercise where participants come together at a single location. Although the Continuity and Exercise Programs Branch made an initial investment in developing an exercise that could be successfully executed in the virtual environment, planners at the national and fusion center levels avoided travel costs, hours lost to travel, and an investment in backfill. Moving forward, the exercise can now be repeated with other groups of fusion centers with minimal time, effort, and investment.
- The exercise planning team had excellent coordination with fusion center planners, using Homeland Security Information Network (HSIN) Connect to host the traditional Homeland Security Exercise and Evaluation Program (HSEEP) planning processes and to share all exercise documents with the planning team. However, players needed much more direction on exercise "rules of engagement." Uncertainty about when to engage each other versus when to engage the simulation cell slowed the pace of play during the first few hours of the exercise.
- Players practiced, or were introduced to, virtual tools of their trade. During FUSION X 2015, players used HSIN's situational awareness platform (SitAware) as one of their methods of communication. Although not all fusion centers had used SitAware in the past, they recognized during the course of the exercise its value for sharing information during fast-paced incidents.

The execution of FUSION X 2015 provided valuable insight into not only how fusion centers can more efficiently exercise their analysts, but also how virtual exercises might be used to serve a wider homeland security audience. In looking toward other applications of virtual exercises, organizations should ask the following three questions when determining whether a virtual exercise might be appropriate for them:

- "Does how we want to exercise translate into a virtual world?" Although many organizations have made good use of virtual training for tactical procedures – for example, hazardous materials, active shooter response – virtual exercises may be less appropriate for these operations. A virtual exercise does not allow responders to practice hands-on operations, such as donning and doffing personal protective equipment, practicing technical processes such as sampling, or exercising the use of equipment that is paramount to their operations.
- "Does what we want to exercise translate to a virtual world?" For those considering an exercise based on a capability such as operational

coordination or public information and warning, a virtual exercise might prove effective. Organizations can place players in the virtual chairs like the ones they occupy in the real world, which encourages information sharing via the mechanisms they use each day. Social media, which is part of the daily information-gathering practices of many emergency responders and receivers, can be seamlessly integrated into the Master Scenario Events List of a virtual exercise.

- "Does the scope of our intended exercise translate to the virtual world?" The scope of some exercises allows for easy and effective virtual play, providing more realism than a tabletop exercise. For example, jurisdictions may want to exercise the critical first 30 minutes of a response, when people are not yet at their desks and are forced to share information and make decisions from wherever they are. Likewise, virtual prevention exercises – done in small increments over a long period of time – may allow players to exercise analytical tradecraft while still effectively performing their daily activities. Finally, exercises that include a large number of participants from different geographical locations may be a good fit for a virtual approach.

Virtual exercise will not be appropriate for all organizations or for all exercises. However, in an environment of limited budgets and extensive virtual communication, organizations should consider the value of shifting their exercise paradigm into the virtual world.

***Dawn Thomas*** *is an associate director of CNA's Safety and Security division, where she has been supporting homeland security planning, training, and exercises for 11 years. She holds a B.S. from Carnegie Mellon University, and an M.A. from The Hebrew University of Jerusalem.*

## How To Make First Responders More Efficient

Source: http://i-hls.com/2015/10/how-to-make-first-responders-more-efficient/



Oct 11 – Imagine a scenario where whoever came to save you is injured during the rescue effort. Perhaps they were burned from the raging fire, or inhaled too much smoke or broke a limb. Rescuers who have themselves been

injured surely can'not help you or anyone else during trouble, which calls for the critical need to better emphasize the safety of first responders.

A conference which was held on Thursday at the Israeli Air Force Center and organized by SIBAT, the Ministry of Public Security, and the Bird foundation, dealt with innovations in the field of first responders. During the conference, Mr. Dan Cotter, head of the first responders group at the Science and Technology directorate of the Department of Homeland Security, noted the ways in which first responders' work can be made more efficient. Cotter claims that one of the most important elements to do so is to ensure their safety.

In order to do so, an efficient communication is needed. Cotter mentioned that about two years ago a great tragedy occurred in the US, when hundreds of firemen tried to put out a large fire in the state of Arizona, during which 19 team members died. Authorities announced that they cannot make contact with the fire fighters and a helicopter was dispatched to search for them. The fire services, however, later confirmed that they have died in the fire. Had they had communications to transmit their exact location and alert them on the weather conditions, and more specifically on the dangerous changes in wind – they might have been saved.

**From exercises in the past and from operations in the field, it is well-known that lack of communications does not prevent first responders from carrying out their mission, but there is little doubt that the lack of advanced technological platforms for cooperation different teams is a gap that should be addressed as soon as possible.**

Zvika Kanfer, Head of Science & Technology Division at the Ministry of Public Security, also addressed the gaps in first responders' capabilities. According to Kanfer, **there is a need for technologies to provide real-time data regarding the location of first repsonders, their proximity to different dangers as well as detecting and analyzing active and passive threats in the field.** There is also a need to develop systems that could scan from a distance the event scene while monitoring vital signs, in order to track down injured team members and casualties. Finally, Mr. Kanfer noted as well the issue of protection means for first responders, mostly in wearable technologies, as well and the issue of communications between the teams.

All that is left is to present the existing needs to the global market industries and have them come up with solutions. Dr. Eitan Yudilevich, CEO of Bird Foundation, which aims for cooperation between Israeli and American companies from different technological fields, stated that the foundation supports projects from various sectors, allowing following what is happening beyond the wall, smart antennas and even technologies meant to better and more accurately distribute the water from fire fighting helicopters over the fires. First responders, it seems, are about to undergo a makeover in the not-so-distant future.



## New Technologies for Israel's First Responders

Source: http://i-hls.com/2015/10/new-technologies-for-israels-first-responders/

Oct 13 – In recent years, technology has been focusing on better equipping first responders in different conditions and scenarios.

A conference held on Thursday at the Air Force Center, organized by SIBAT (Ministry of Defense), Ministry of Public Security, and the Bird foundation, focused on innovations for first responders. During the conference, Major General Eyal Caspi, Head of Operation Department, National Fire and Rescue Authority, stated the changes in needs and service that the state of Israel is providing its citizens during the past few years in the field of fire fighting. The gaps revealed after the great fire in Mount Carmel in December 2010 have raised an immediate need to search for ways of bettering response in the field.

In order to draw conclusions, a team was established and was requested to learn from other countries in the world how they operate and deal with the dangers of fires. Caspi mentioned that he traveled, along with others in the field, to several states including Greece and Spain for this matter. Ever since then changes have been made in the structure and abilities of the fire department.

Among the findings of the delegation and headquarters, it was discovered that countries of the west are much more

organized and prepared for events of fire than Israel in terms of technological means, manpower etc. **The delegation was surprised to see that the countries technological systems were made in Israel. It seems that Israel is great in developing, manufacturing and installing systems abroad but has forgotten to take care of itself.** Another issue revealed has to do with the number of firefighters in Israel. **While other western countries have a firefighter for every 1,000 civilians, Israel has only one firefighter for every 6,000 civilians.** This factor is more relevant, naturally, to the central cities, as the periphery the gap is probably even greater.

After the faults were revealed, several changes were made in the Israel fire service. A greater emphasis was put on coordination between operative services – home front command, the police and others. More fire stations were added, growing from 115 to 134 stations, allowing the responding teams to get to the scene much faster, from an estimated 17 minutes to 10 minutes. The vehicles were also upgraded – Israel has purchased 134 additional fire trucks and additional 14 firefighting aircrafts. The future will see an 6 additional helicopters to complete this aerial fire fleet. However, the manpower issue is still in need of improvement, even with the existing force of volunteers.

There are several central challenges the fire department in Israel has to face – the threat of rockets, skyscrapers, underground challenges and natural disasters. The threat of rockets on Israel has grown substantially in recent years and home front command remains the newest member of the defense services. Everyday life must be kept in case of rockets fired over Israel, and that has to do, of course, with the responding bodies – the police, fire department and the emergency medical services. **We can also recognize difficulties for the fire teams operating in skyscrapers and underground structures, such as underground parking lots.** The problem has to do with the difficulty to track people in such structures due to bad reception. Buildings in Israel can reach over 200 meters in height and parking lots can have seven underground levels.

In conclusion, despite the improvement in the Israeli fire department's capabilities, technological and human solutions are still required. The citizens of Israel should be safe in case of a fire and, whether high above ground or many floors under it, have someone to rescue them, and of course the firefighters need to return safe and sound.



# 6 made-in-Israel devices for disaster relief

Source: http://www.israel21c.org/6-made-in-israel-devices-for-disaster-relief/

When disaster strikes anywhere in the world, Israelis are always among the first on the scene to offer search-and-rescue, first aid and secondary medical care.

Some of the most critical pieces of equipment they take with them to help victims of earthquakes, fires, typhoons, hurricanes and terror attacks are home-grown.

But these innovative devices are not just for Israeli aid workers. Here are six blue-and-white innovations that emergency responders in many countries keep at the ready in case of disasters. More are in development, to be discussed at today's seminar on product innovation for first responders in Herzliya.

1. **Water-Gen**

After any kind of mass disaster, access to drinking water is a pressing concern. International aid workers regularly rely on a range of Israeli innovations to purify, store and transport the precious liquid. Among the most widely deployed solutions are the portable machines made by Water-Gen of Rishon LeZion to generate drinking water from the atmosphere and to purify

existing water sources.
In November 2014, Foreign Policy magazine chose Water-Gen founder Arye Kohavi as one of its 100 Leading Global Thinkers of the Year "for pulling potable water from thin air." Water-Gen received the 2014 Frost & Sullivan European Technology Innovation Leadership Award and was on Fast Company's list of most innovative companies for 2014.

2. **Pocket BVM**

Among the Israeli medical innovations that Israeli volunteers brought to Nepal last May to treat earthquake victims was the Pocket BVM (bag valve mask), a uniquely collapsible version of an essential resuscitation and respiratory support device.




United Hatzalah paramedic Dov Maisel helped invent this product, commercialized in 2007 by Jerusalem-based MicroBVM (microbvm.com) and now used by the US military, NATO forces, the Israel Defense Forces and civilian emergency medical response teams. Pocket BVM folds into a protective case, allowing EMS workers to fit 20 of the devices into the space of two regular-sized resuscitators.

3. **SkySaver**


The personal rescue device is contained in a backpack. Photo: courtesy

Introduced in 2005 as the Spider Rescue System, the Israeli-made SkySaver personal rescue device can evacuate a person weighing up to 300 pounds from a building up to 120 stories tall. The device is worn like a backpack and includes a fire-resistant cord that can rappel rescued people to safety. With its R&D and marketing in Jerusalem, SkySaver's

sales office is now based in New York.

4. **Emergency bandage**

A variety of trauma wound dressing products made by First Care Products originated with the Emergency Bandage (also trademarked as the "Israeli bandage") invented by former Israeli military medic Bernard Bar Natan and widely used by first-responders in more than 50 countries to stanch bleeding from hemorrhagic wounds. It features a patented pressure applicator.

This is the bandage that Arizona medics used in 2011 to save the life of US Congresswoman Gabrielle Giffords after she was shot. In 2012, Texas-based PerSys Medical Group acquired First Care Products and has continued introducing related products to the emergency-care market.

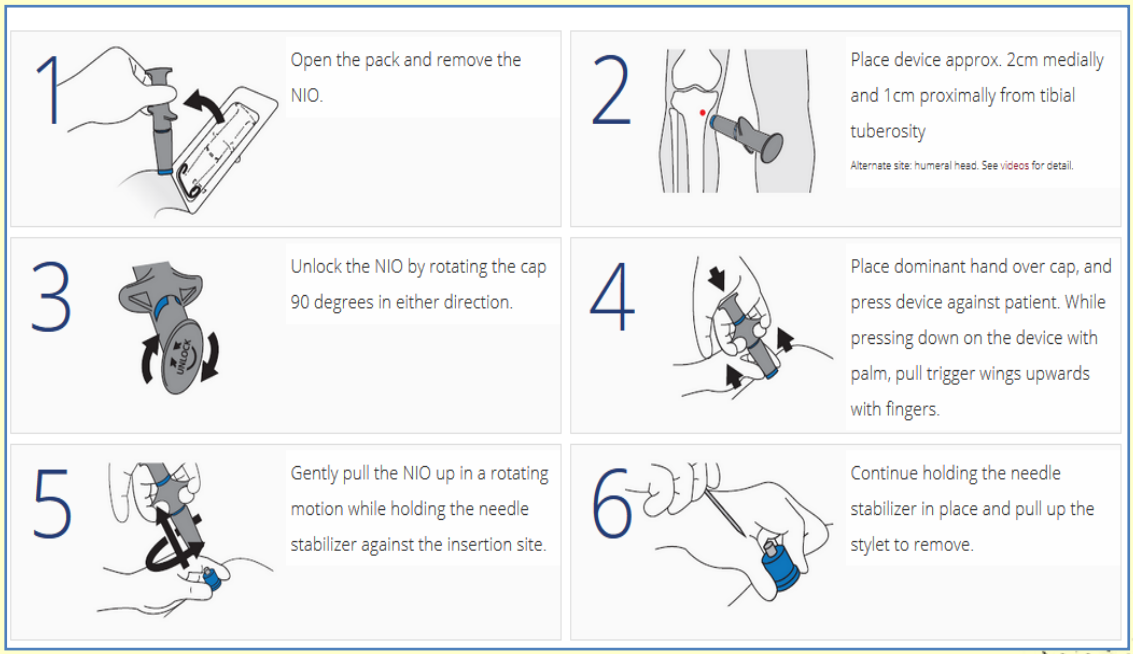
5. **Agilite Instant Harness** and **Injured Personnel Carrier**

Established by IDF and US Army veterans, Agilite makes a line of lightweight rescue harnesses, including the world's smallest Class II rappelling harness that was used to save the lives of South African miners trapped underground in 2013.

The Tel Aviv-based company also makes the Injured Personnel Carrier, a novel hands-free folding device that allows one rescuer to carry an incapacitated person like a "human backpack."



6. **Bone Injection Gun (automatic intraosseous device)**




Paramedics often have to inject medications before evacuating a patient, whether for resuscitation or preventing a blood infection in a crush wound. Opening a vein line is


difficult or impossible in many scenarios, such as in the dark or when a patient is trapped under rubble.
The spring-loaded Bone Injection Gun introduced by WaisMed of Herzliya in 1994 was the world's first automatic intraosseous infusion device. Paramedics in more than 55 countries have used it to introduce medication directly into the bone marrow, which is just as effective as an IV. The paramedic only has to feel for the bone to get it positioned correctly. In 2014, WaisMed rolled out the newest version, the NIO, and was acquired by PerSys Medical.

## MDA Concludes Two Weeks of Saving Lives

Source: http://i-hls.com/2015/10/mda-concludes-two-weeks-of-saving-lives/

Oct 14 – During the past two weeks, which started with the murder of Eitam and Na'ama Henkin, Magen David Adom (MDA) forces all over the country stood on call and arrived quickly to mass casualty scenes in order to saves lives quickly and professionally. From the beginning of October to today (October 13th), the number of injured from the string of terror attacks is 7 dead and 99 wounded – 10 severely wounded, 15 moderately wounded and 67 with light injuries, along with 26 suffering from anxiety.
It has been a busy couple of weeks for the MDA forces across Israel due to the wave of terror attacks washing over the country. For the past several days, MDA forces stood on call, offering medical treatment and medical evacuation to 99 people with different levels of injuries.
For the past couple of weeks, the number of casualties from deadly terror attacks is 7: 2 in the West Bank shooting attack (October 1st), 2 in the stabbing attack in the old city of Jerusalem (October 3rd), 2 in the bus attack in Armon HaNatziv in Jerusalem, and 1 in the car attack in Jerusalem (both on October 13th). MDA forces across the country offered life-saving medical treatment to 99 wounded – 10 severely wounded, 15 moderately wounded and 67 with light injuries, along with 26 suffering from anxiety.



## The Israeli MDA Presents its New Command and Emergency Vehicles

Source: http://www.tlvfaces.com/israeli-mda-presents-new-command-emergency-vehicles/

50 feet in length, 12 feet high, weighing 32 tons, a generator and an attached 900-liter diesel-fuel container: This is one of the most advanced command vehicles in the world, and the only one of its kind ever assembled for the MDA. The cameras installed in the vehicle can rise to a height of about 60 feet and cover a wide area. Fully functioning MDA call centers can receive calls for aid from several disaster areas, and the truck includes a fully functioning meeting room as well.
The command truck allows rescue personnel in the field to use radio, Wi-Fi and internet even in situations where the communications infrastructure fails, as is often the case during large-scale disasters. This will allow rescue and emergency personnel to continue functioning almost without interruption, in order to keep saving lives in the most efficient manner.
The command vehicle was assembled in England, based on a Dutch DAF truck. The project was a part of the organization's general response to the Carmel fire disaster, and the entire process took four years. During the Carmel fire MDA personnel had to overcome many challenges, the most pressing of which was frequent communications failures,

making it very hard for them to coordinate their efforts with the other rescue personnel in the field. After the fires MDA focused on enhancing its capabilities, in preparation for future national disasters. The new command vehicle is a part of these efforts.




Rescue force worldwide have contacted the MDA about the new vehicle and its capabilities. It can allow personnel in the field to continue operating during national disasters even if cellular networks, land-lines, and radio communications all fail.
In addition to the new command truck the MDA presented other new vehicles:

The jeepbulance", advanced emergency response vehicles, an advanced emergency response motorcycle, the advanced T3 Segway, and others. The MDA also presented its new Chevrolet Suburban, ordered and assembled especially for the Israeli organization – a rescue vehicle designed to overcome difficult terrain, such as ravines or sandy beaches

# Climate change heat a greater threat than sea level rise, says Mapua professor

Source: http://www.stuff.co.nz/environment/climate-news/72591034/climate-change-heat-a-greater-threat-than-sea-level-rise-says-mapua-professor

**Mapua's Dr Tord Kjellstrom has researched the impact of climate change heat stress on manual labourers for 20 years. He says people are already dying but the loss of production, particularly in hot countries, could drive a major global economic decline.**

Imagine you are your grandchild living in a world which has not tamed climate change. You are cradling your newly born grandchild in your arms. What life would you wish for the infant?

It is a scenario Dr Tord Kjellstrom uses to illustrate the growing threat of climate change.

Kjellstrom is the co-ordinator of the eight-member Ruby Coast Research Centre (RCRC) which is based in Mapua gathers and and provides international research and data on the impact of the rising global temperature on human health to leading global organisations and decision makers.

"We have to act now to protect our future families and the environment. Mitigation is extremely important because adaption or protection are not going to help the poor people in tropical countries."

For nearly 20 years Kjellstrom, and more lately the RCRC team, have researched the impact of climate change heat-stress on working people and the lost production and resulting downward slide in national Gross Domestic Product (GDP).

Kjellstrom, is a softly spoken medical doctor and also holds a masters in mechanical engineering. He has 40 years experience of teaching and research in environmental and occupational health, and epidemiology. He has held professor positions in universities in Sweden, New Zealand, Australia, and United Kingdom.

He worked 12 years at the World Health Organization in Geneva and was the WHO's Office of Global and Integrated Environmental Health director ,with responsibility, for climate change and health from 1994 to 1997.

Kjellstrom said it is not storms or rising sea levels that will be climate change's greatest threat to human life in the next 100 years - but heat exposure. He says it is here already and people are dying.

"I think somehow that some of the experts want to keep the calculations around heat exposure and its effects low-key," Kjellstrom said. "I don't know why."

Researching and disseminating data and publications about the health impacts of rising heat levels is a focus of the RCRC.

The centre makes its research available through keynote speeches, academic journals, commissioned reports, book chapters, and a website climatechip.org which points to the groups, publications, power points, analysis tools and interactive pinpoint data on temperature trends at thousands of locations around the world.

The work highlights Kjellstom's primary concern - that rising heat and associated stresses and deaths will hit the globe's temperate, tropical and subtropical zones the hardest.

"We have 4000 million people already at risk."

The ideal core body temperature for humans is around 37 degrees C. Once it rises to 39C heat stress and strain sets in, organs can be damaged and at higher temperatures death may occur.

Kjellstrom said poor workers were already dying in parts of the world from kidney disease and heart failure in locations ranging from the sugar cane fields of El Salvador and Nicaragua to Qatar where 185 workers died in 2013 building stadiums and infrastructure for the 2022 FIFA World Cup in sweltering conditions.

Poor manual workers in hot countries faced major hurdles, he said. They had to work to survive, they could often not carry or source enough potable water to hydrate daily, they usually lived without cooling systems and they faced major migration barriers.

The overall results were health impacts, deaths and was lower production output.

"There are millions and millions of people who do all the work by

hand. When it gets up to a certain heat level you can not keep up the pace of work," he said.
He acknowledged the issue of heat was not a big problem in New Zealand.
"But if you are in the south of India and the average temperature in the afternoon is 45 degrees and it goes on for maybe three or four months it's extremely difficult for people to keep up the work.
"So people as individuals will have health effects, lose income and be less productive.
"If that is among self-employed farmers, it is a family economy that is affected. But if you estimate, like we have done, what might be the impact on a country we are talking about several per cent loss of GDP.
"If you lose two per cent of your annual GDP over a 30 years period your average income in the country will be half as much as it could have been."
Even small changes in temperature impact on people.
"Even now construction workers in hot parts of the year can not work in the afternoons. This aspect of heat and how it affects people's lives has, until recently been more or less ignored or not given much emphasis.
"For the first time the IPCC report in 2014 mentioned these health impacts of heat. One could argue that is an achievement of this team in Ruby Bay because I was involved in putting material, together with my colleagues here, for the report. The further analysis we are currently doing will hopefully change the attitude towards this whole thing."
Members of the RCRC team also include Bruno Lemke, Matthias Otto, Olivia Hyatt, David Briggs, Chris Freyberg, Lloyd Hasson and Lauren Lines.

## IPCC projections "wildly over optimistic": Climate expert

Source: http://www.homelandsecuritynewswire.com/dr20151014-ipcc-projections-wildly-over-optimistic-climate-expert

Oct 14 – As a new chairman is appointed to the Intergovernmental Panel on climate Change (IPCC), a University of Manchester climate expert has said headline projections from the organization about future warming are "wildly over optimistic."


In an article published today in *Nature Geoscience* Professor Kevin Anderson says that IPCC claims that "global economic growth would not be strongly effected" are unrealistic and that if we are to meet the 2°C warming target, wealthy and high emitting individuals will need to make dramatic cuts in the energy they use and in the material goods they consume — they will have to accept immediate and fundamental changes to their way of life — at least until the transition away from fossil fuels is complete.
U Manchester reports that Anderson also says that many climate scientists are censoring their own work in order for their results to be more politically palatable, something that does society a "grave disservice."
Anderson's claims are a wake-up call to Professor Hoesung Lee, who was installed at the new IPCC chair last week and are well timed in the lead-up to the climate negotiations in Paris, which take place later this year.
A statement last year from the IPCC said that "to keep a good chance of staying below 2°C, and at manageable costs, our emissions should drop by 40–70 percent globally between 2010 and 2050, falling to zero or below by 2100," and that mitigation costs would be so low that "global economic growth would not be strongly affected."
Anderson notes that, "If the IPCC's up-beat headlines are to be believed, reducing emissions in line with a reasonable-to-good chance of meeting the 2°C target requires an accelerated, but still evolutionary, move away from fossil fuels; they notably do not call for an immediate and revolutionary transition in how we use and produce energy. Yet, in my view, the IPCC's own carbon budgets make it abundantly clear that only a revolutionary transition can now deliver on 2°C."

According to Anderson, the IPCC's positive outcomes are: "Delivered through unrealistically early peaks in global emissions, or through the large-scale rollout of speculative technologies intended to remove CO2 from the atmosphere.

"In stark contrast, I conclude that the carbon budgets associated with a 2°C threshold demand profound and immediate changes to the consumption and production of energy.

"The complete set of 400 IPCC scenarios for a 50 percent or better chance of meeting the 2°C target work on the basis of either an ability to change the past, or the successful and large-scale uptake of negative-emission technologies. A significant proportion of the scenarios are dependent on both. That is unrealistic."

According to IPCC research, it is cumulative emissions of CO2 that matter in determining how much the planet warms by 2100. The IPCC concludes that no more than 1,000 Gt of CO2 can be emitted between 2011 and 2100 for a 66 percent chance, or better, of remaining below a 2°C rise.

However, between 2011 and 2014 CO2 emissions from energy production alone amounted to about 140 Gt of CO2. To limit warming to no more than 2°C, the remaining 860 Gt of CO2 (out to 2100) must be considered in relation to the three major sources of CO2; those released in cement manufacture, changes in land-use, and, most importantly, energy production.

Anderson concludes: "The severity of such cuts would probably exclude the use of fossil fuels, even with carbon capture and storage (CCS), as a dominant post-2050 energy source. If we are to meet the 2°C target, us wealthier high emitting individuals, whether in industrial or industrializing nations, will have to accept radical changes to how we live our lives — that or we'll fail on 2°C.

*— Read more in Kevin Anderson, "Duality in climate science," Nature Geoscience (12 October 2015).*



## Hunger levels "serious" or "alarming" in 52 developing countries: Report

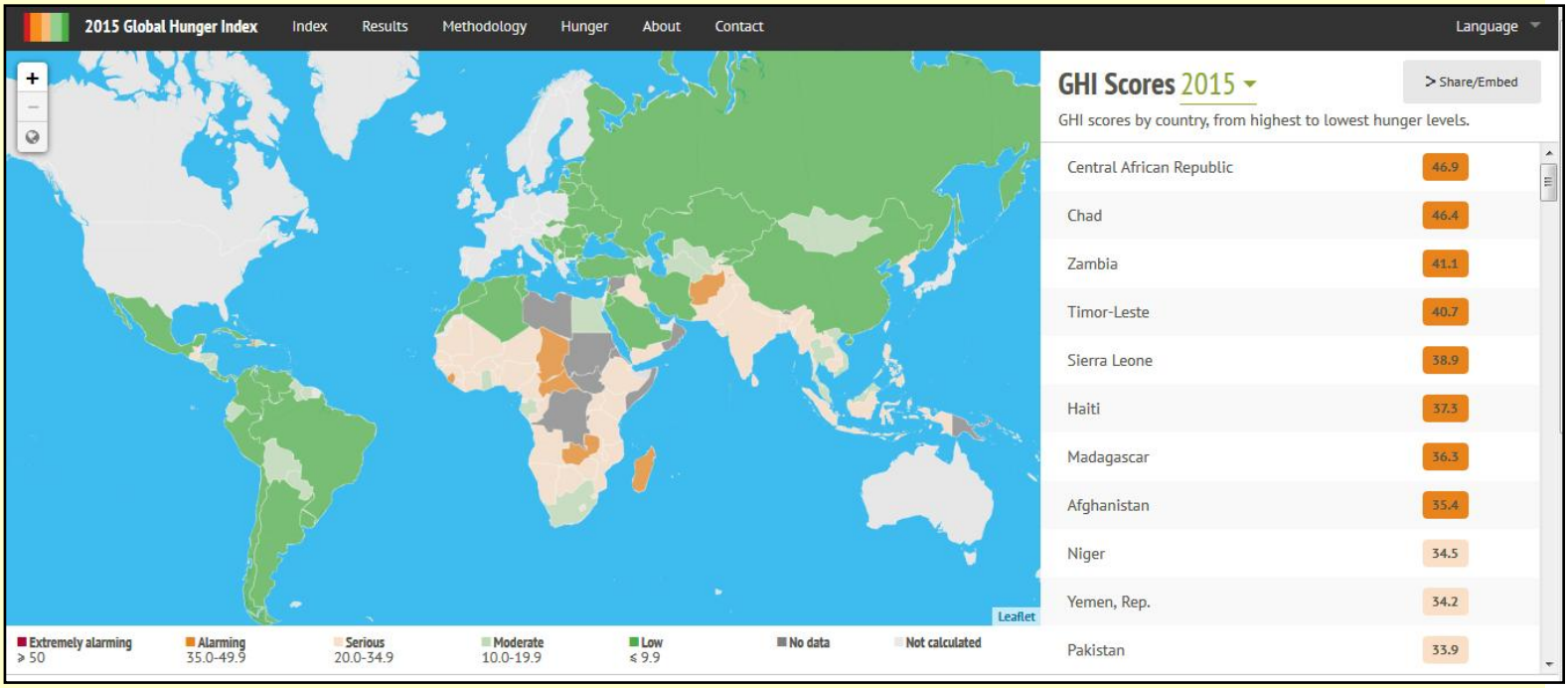
Source: http://www.homelandsecuritynewswire.com/dr20151020-hunger-levels-serious-or-alarming-in-52-developing-countries-report

Oct 20 – Despite progress in reducing hunger worldwide, hunger levels in 52 of 117 countries in the 2015 Global Hunger Index remain "serious" (44 countries) or "alarming" (8 countries). The Central African Republic, Chad, and Zambia had the highest hunger levels in the report, which was released last week by the International Food Policy Research Institute, Welthungerhilfe, and Concern Worldwide.

Conflicts can be strongly associated with severe hunger, according to the report, which focused on armed conflict and the challenge of hunger in the main essay. The countries with the highest and worst Global Hunger Index (GHI) scores tend to be those engaged in or recently emerged from war. The two worst-scoring countries both experienced violent conflict and political instability in recent years. In contrast, in Angola, Ethiopia, and Rwanda, hunger levels have fallen substantially since the end of the civil wars of the 1990s and 2000s.

IFPRI reports that the report outlined some bright spots in the fight to end world hunger. The level of hunger in developing countries has fallen by 27 percent since 2000, and 17 countries reduced their hunger scores by at least half since 2000. Among those countries are Azerbaijan, Brazil, Croatia, Mongolia, Peru, and Venezuela. Some of the world's poorest countries could not be included in the report due to unavailable data. As a result, the picture of global hunger may be worse than reported here.

IFPRI notes that global hunger is a continuing challenge with one in nine people worldwide




chronically undernourished and more than one quarter of children too short for their age due to nutritional deficiencies. Nearly half of all child deaths under age five are due to malnutrition, which claims the lives of about 3.1 million children per year.

This year's report sheds light on an unheralded achievement of the past fifty years. "Calamitous famines," those that kill more than one million people, seem to have vanished.

"War and conquest have long been the drivers of mass starvation. Although humanitarian responses are far faster and more proficient than in the past, we still need to attend to the perils of armed conflict and inhumane policies generating severe hunger," said Alex de Waal, author of the essay and executive director of the World Peace Foundation and research professor at Tufts University. "The world has enough food, enough logistics, enough knowledge, to end severe hunger: achieving that is a matter of political will only."

Between 1870 and 2014, 106 instances of famine and mass starvation each killed 100,000 people or more. Despite a decrease in wars over recent decades, the number of violent conflicts and conflict-related deaths has recently increased from an all-time low in 2006.

"We are more confident today than ever before that we can end hunger, provided we do not rest on our accomplishments," said Shenggen Fan, IFPRI director general. "We must keep pushing, keep partnering, and keep innovating until nutrient-rich foods become sustainably accessible, available, and used by everyone in order to reach their full potential."

"More than 80 percent of those affected by armed conflict stay within their countries. They are the ones who suffer most from severe food insecurity," said Welthungerhilfe president Bärbel Dieckmann. "We need to do more to support these people and to help restore their livelihoods. However, unless we address the root causes of armed conflict, the progress made in reducing hunger will not last."

"Conflict is development in reverse. Without peace, ending poverty and hunger by 2030 will never be achieved. The time has come for the international community to make conflict prevention, mitigation, and resolution a far higher political priority," Concern CEO Dominic MacSorley said. "Diplomatic muscle and political will is urgently needed in equal measure to prevent the appalling levels of poverty, suffering and horrific brutality that seem commonplace in too many of today's conflicts."

**Refugees and hunger**

- When famine occurs today, it is usually the result of armed conflict.
- An average of 42,500 people per day fled their homes last year. Approximately 59.5 million people are displaced

by conflict worldwide, more than ever before.
- Although refugees are more visible, 87 percent of those affected by conflict do not flee their homes — and tend to fare worse than those displaced.
- With the current migrant crisis, there is a need for a global response to support those fleeing conflict and persecution within or outside their home countries.

*— Read more in Klaus von Grebmer et al., 2015 Global Hunger Index: Armed Conflict and the Challenge of Hunger (IFPRI, 2015).*