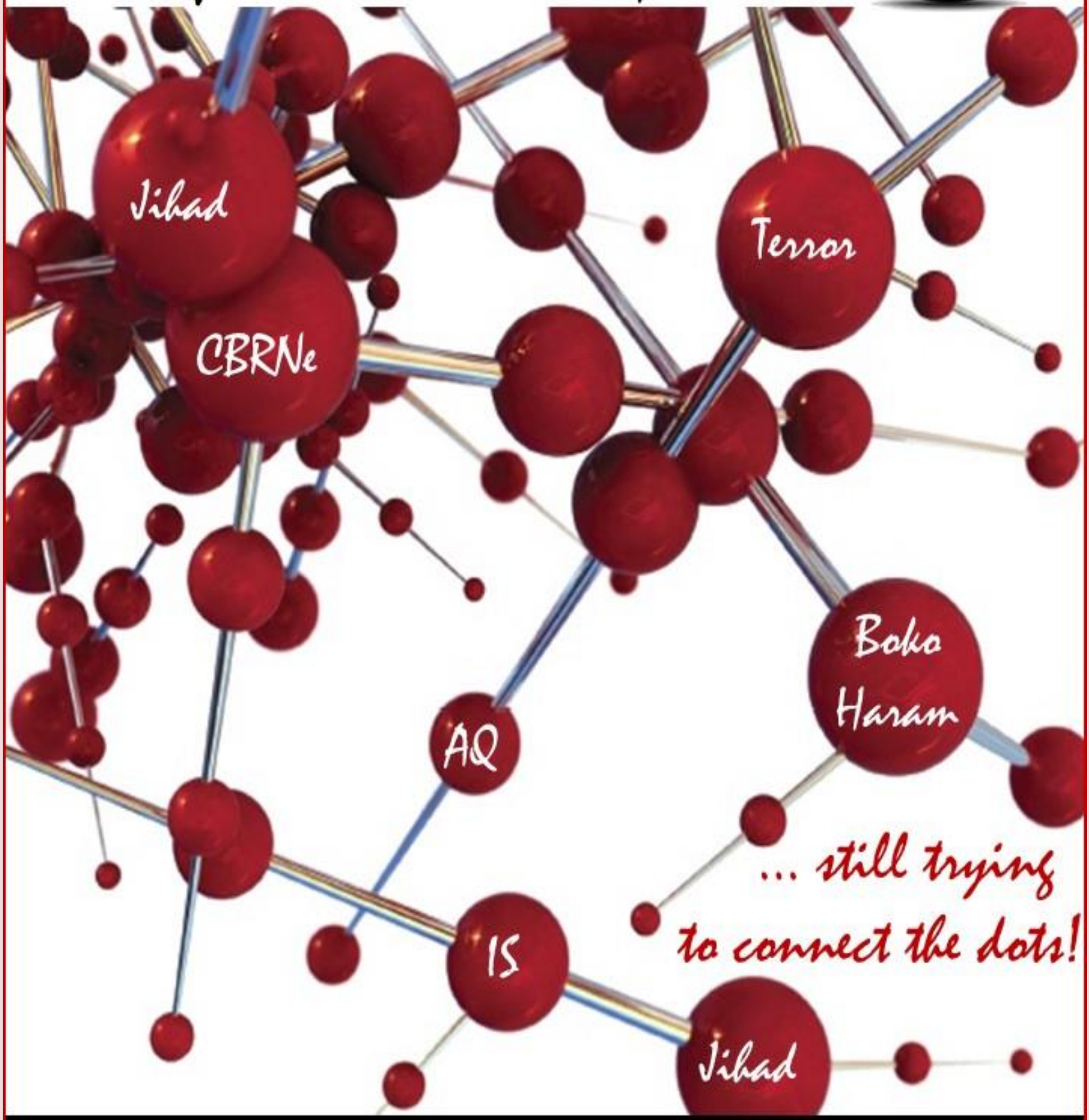
CBRNE NEWSLETTER TERRORISM

April 2016

E-Journal for CBRNE & CT First Responders



www.cbrne-terrorism-newsletter.com

ISIS Wants a Dirty Bomb, a Weapon of Mass Disruption

Source:https://www.inverse.com/article/13180-isis-wants-a-dirty-bomb-a-weapon-of-mass-disruption

Mar 22 – ISIS, which has claimed responsibility for the attack in Brussels today, and associated radicals have been increasingly active in Belgium during the months leading up to this latest act of terror. In November, a man living near Brussels and linked to the Islamic State group was arrested; according to an investigation by the nonprofit Center of Public Integrity, **officials found evidence he was surveilling a Belgian nuclear facility with the goal of creating a dirty bomb.**

If you are unfamiliar with the family tree of explosives, a dirty bomb is meant to disseminate chaos and mayhem. However, it will not result in the high body counts popularly associated with radioactive weaponry. What makes a dirty bomb "dirty" is the dispersal of radioactive material. The explosion itself is conventional — likely result of a bomb a containing nitrogen compounds, like dynamite or TNT — rather than a result of nuclear activity. To make a dirty bomb is to simply wrap radioactive waste or material around a high explosive.

But if it sounds "simple" on paper, it's much harder to do in practice. No terrorist group or single operator has ever set one off, two decades of murderous aspirations to the contrary. "Constructing a dirty bomb is more difficult than most imagine," as journalist Jason Burke wrote at *Foreign Policy* in 2009 when discussing al Qaeda's dirty bomb plans:

"Although the International Atomic Energy Agency warns that more than 100 countries have inadequate control of radioactive material, only a small percentage of that material is lethal enough to cause serious harm. It also requires considerable technical sophistication to build a device that can effectively disperse radioactive material. Some have also voiced the fear that militants might obtain a 'prepackaged' working nuclear warhead from Pakistan. However, that would only be a plausible scenario if an Islamic regime came to power, or if high-ranking elements of the Pakistani military developed greater sympathy for the Islamists than currently exists."

Consider **José Padilla,** the paunchy radicalized American perhaps most frequently associated with a dirty bomb plot. Padilla was not, in fact, charged with his dirty bomb designs, because he was unable to progress beyond planning to whirl buckets of uranium over his head to separate the U-235 isotope for his nuclear device.

The fissile materials at the center of a nuke — like enriched uranium — are both prohibitively difficult to create and obtain. Daily life, that said, is far from radioisotope-free. There are thousands of known radioactive materials, wrote Center for Technology and National Security Policy researchers Peter D. Zimmerman and Cheryl Loeb in a 2004 report. But "only a few stand out as being highly suitable for radiological terror. **These are cobalt-60 (60Co), strontium-90 (90Sr) (and its short-lived daughter, yttrium-90), cesium-137 (137Cs), iridium-192 (192Ir), radium-226 (226Ra), plutonium-238 (238Pu), americium-241 (241Am), and californium-252 (252Cf)."**

Limited as they are, such radioactive sources can be found in research institutions, hospitals, industry, or construction. Cancer treatments use iodine-131 and cobalt-60, smoke alarms use americium-241. But amassing enough material without tripping federal failsafes is tough. So is handling it. People who encounter unusual concentrations of nuclear material — woodcutters in Georgia, scavengers pawing through an abandoned chemo clinic in Brazil — have given themselves severe radiation poisoning.

Ultimately, were a dirty bomb to be detonated, biosecurity and environmental health experts believe most of the loss of life would come from the blast itself. Exposure to radiation, one report estimates, would increase the lifetime likelihood of cancer on par with "smoking five packages of cigarettes." If you didn't inhale any particles and carefully scrubbed yourself clean, the risk would be even lower. The majority of the devastation would be psychological and economic — the site of the explosion, and the incorporeal specter of radiation in the public mind, would remain a lasting reminder of a terrorist attack.

The Nuclear Regulatory Commission, in fact, doesn't even consider dirty bombs weapons of mass destruction. **Instead, the NRC says, consider them weapons of mass disruption.**

EDITOR'S COMMENT: A short article but well written – especially the last sentence! Even "experts" continue to use the word "destruction"; but when comes to terrorism all CBRNE improvised devices of dissemination are "weapons of mass disruption". Weaponized CBRNE agents are causing destruction but this means war between states – not terrorism. Of course disruption caused will have enormous implications as well but not as much as Hiroshima or Halabja.

ISIS obtaining nuclear weapons "obviously a concern": British defense secretary

Source: http://www.homelandsecuritynewswire.com/dr20160324-isis-obtaining-nuclear-weapons-obviously-a-concern-british-defense-secretary

Mar 24 – **British defense secretary Michael Fallon said the prospect of ISIS or another terror group with the "technical know-how" obtaining nuclear weapons is "obviously a concern."**

Fallon said it was important to ensure that terror groups could not "get their hands on nuclear weapons" and said the United Kingdom was doing its part by maintaining strict export controls on the necessary technology.

Responding to questions after a speech on the U.K.'s Trident nuclear weapons system, Fallon said: "It is obviously a concern that we will see non-state actors with the finance and perhaps some of the technical know-how seeking to get hold of nuclear weapons.

"That is why we maintain very strict export control criteria for the technologies involved and why we need to be on our guard."

The *Sun* reports that world leaders are set to meet in Washington, D.C. later this month for discussions about how to prevent nuclear terrorism. It is the fourth such summit since 2010.

In its Strategic Defense and Security Review 2015, the U.K. government said the risk of terrorists obtaining nuclear, chemical, or biological weapons may increase in the coming years.

Home Secretary Theresa May has outlined the steps the government was taking to bolster security at home in the wake of the Brussels attacks. **She said the U.K. Border Force had increased the number of officers at ports in Belgium and France and introduced "enhanced searches" of inbound tourist vehicles.**

She confirmed that a £34 million investment to increase the capacity of armed police units able to respond to a Paris-style attack in the United Kingdom would also see forces outside London benefit, following concerns about cuts to capacity in Greater Manchester and Merseyside.

May said that the United Kingdom must also "do more to counter the poisonous and repugnant narrative peddled by Daesh [ISIS] and expose it for what it is — a perversion of Islam, built on fear and lies."

May criticized comments made by Donald Trump, who claimed on Wednesday that Muslims were "absolutely not reporting" suspected terrorists and needed to "open up to society."

May said Trump was "just plain wrong" in his assessment.

"People in Muslim communities around the United Kingdom are as concerned as everybody else in the U.K. about both the attacks that have taken place and about the perversion of Islam underlying the ideology that has led to violence," she said.

Neil Basu, deputy assistant commissioner of the U.K. Counter Terrorism Policing Network, also condemned Trump's comments, warning that they risked "playing into the terrorists hands and making people feel hate."

The Threat of Nuclear War

US Army's Depleted Uranium Licencing Saga Highlights Post-Conflict Contradictions

By International Coalition to Ban Uranium Weapons, March 26 2016

It has taken a decade but the US Nuclear Regulatory Commission (NRC) has finally granted the US Army a licence to possess and manage DU weapon residues at 15 US installations. However the domestic regulatory framework imposed by the NRC stands in stark contrast to the absence of obligations governing the management of contamination caused by US military actions in Iraq and elsewhere.

The U.S. Nuclear Deterrent Triad. Can the U.S. Afford to Modernize it?

By Brian Kalman, Edwin Watson, and South Front, March 24 2016

Dr. Paul Craig Roberts, who served as an Assistant Secretary of the Treasury for Economic Policy in the Reagan administration, shares his view that there is a real likelihood of a nuclear war breaking out. Below are the main points covered in this radio programme.

What Path for the UN Security Council to Resolve the Conflict on the Korean Peninsula?

By Ronda Hauben, March 21 2016

The Armistice Agreement that ended the fighting of the Korean War was signed on July 27, 1953. While the Armistice Agreement provided for a cease fire, it did not end the Korean War.

Japan: Nuclear Security Risks' Exposed by Secret Plutonium Shipment: NGOs

By Pan Orient News, March 20 2016

Tokyo- (PanOrient News) A coalition of five non-governmental organizations warned today that a shipment of weapons-grade plutonium scheduled to depart the port of the Japanese Tokai nuclear station in Ibaraki prefecture this coming weekend highlights the failure, but also the proliferation risks, of the current Japanese nuclear policy.

The US Just Admitted that 14 Airmen in Charge of 150 Nuclear Missiles — Are Cocaine and Molly Addicts

By Andrew Emett, March 20 2016

Tasked with guarding 150 nuclear missiles at F.E. Warren Air Force Base in Wyoming, fourteen airmen are under investigation for allegedly using cocaine. Last year, three launch officers, known as missileers, pleaded guilty to using ecstasy after an investigation into illegal drug possession uncovered roughly 100 officers involved in a cheating scandal.

Terror attack calls Lusby nuke plant safety into question

Source: http://www.somdnews.com/breaking/terror-attack-calls-lusby-nuke-plant-safety-into-question/article_f2de8e18-ca8c-55f7-a011-c824fc4bd204.html

Mar 28 – The recent news of a planned attack on nuclear plants in Brussels has raised concern over whether America's nuclear reactors are easy targets for terrorists, but Lusby nuclear plant officials say the local plant is safe.

Exelon Generation's Calvert Cliffs Nuclear Power Plant was singled out in a Fox News Insider broadcast Friday, due in part to its proximity to the nation's capital. The report said nuclear power plants in the United States are vulnerable to ground-based and water-borne attacks.

"Our design basis threat is specific to those two things. We have to protect against those," said Tuane Young, manager of site security. "We are no soft target."

A design basis threat, also known as DBT, is the threat against which an asset must be protected.

The nearly 2-mile scenic trek from Route 4 down Calvert Cliffs Parkway

would mislead one to think anyone could just pull up to the two nuclear reactors at the plant with ease. According Young, that is very far from the truth.

"Due to its location and the network of barrier systems in place, perimeter fencing and manned vehicle checkpoints are not required to keep our plant, our workers and our community safe," stated Young. "Calvert's robust defenses include highly trained paramilitary personnel qualified in antiterrorism techniques; state-of-the art cameras and detection systems; military grade weaponry; and a network of engineered barrier systems and fences to repel unauthorized access."

"Manned vehicle checkpoints are not required at many U.S. nuclear facilities," said Young. "We search every vehicle that comes into the protective area. All personnel, all materials, all vehicles have to be searched … no exception."

The multi-level security checkpoint for visitors rivals any major international airport, with layer upon layer of screenings to ensure one doesn't bring in dangerous physical or chemical weapons, or bring out any nuclear contaminants.

Plant employees were not exempt from scrutiny and were also required to go through a magnetometer to check for metal, as well as an explosive detector. Everyone is under constant camera surveillance from the moment they turn onto the parkway leading to the plant.

While most of the plant's security personnel have logged many years of experience in the military and law enforcement before coming to Calvert Cliffs, they are still required to keep their skills up to date.

"When an employee is hired on the security organization, they go through initial training in excess of 360 hours before they ever get to pick up a gun and come out here. Then continually training annually is over 160 [hours]. They are constantly training," said Young.

"We carry a couple of different weapon systems and we have to qualify on both day and night and a tactical course of fire," shared Young. "We are practicing, practicing, practicing throughout the year as required by the [Nuclear Regulatory Commission]."

While Young wouldn't reveal the weapons systems or where the plant's security forces are deployed, or allow photos of any of the security apparatuses on the 1,500-acre campus, he did acknowledge the plant adjusts its security strategy based upon events worldwide.

"Patrols are out there 24/7. If we feel we want to increase our presence at a specific location for deterrence, we make that decision based upon situations," said Young.

The security fleet, for all of Exelon's 23 nuclear reactors nationwide, is tied in with the Department of Homeland Security's National Terrorism Advisory System, which issues timely alerts about terrorist threats to the public, government agencies, first responders, airports and other critical infrastructures like the Calvert Cliffs plant.

According to Young, NRC and homeland security held a security advisory committee meeting March 23 in the wake of the March 22 terrorist attacks in Brussels to brief all nuclear plant security forces.

Neil Sheehan, NRC public affairs officer, confirmed the agency is aware of the attacks in Brussels and subsequent events, and is monitoring the situation as information becomes available.

"U.S. nuclear power plants are maintaining their existing robust security posture at this time. **Plants conduct ongoing access authorization and behavior observation programs for any personnel with unescorted access to a plant site,"** shared Sheehan. "We have no specific, credible threat to prompt us to take additional steps."

Despite the good news of no imminent danger to the plant, Young says his fleet is always ready.

"[For] the design basis threat that we are required to protect against, we are in that posture daily. We have a protective strategy that supports our land-based, vehicle-borne threat all of the time," said Young. "We don't have relaxed security at a nuclear power."

There are also numerous water barriers and buoys and a host of security along the Chesapeake Bay to guard the plant against water-borne attacks.

Young revealed Exelon has a law enforcement response plan with the Calvert County Sheriff's Office and Maryland State Police to protect Calvert Cliffs and the local community. In fact, both agencies met with Young and his team Friday to review the response plan.

Coordination to keep the residents of Calvert County safe is not just a local law enforcement effort. The Federal Bureau of Investigations is also involved.

"FBI frequently visits the site … and has a response plan also for this area and Baltimore," said Young.

The bureau is scheduled to visit within the next week, according to the plant's top security officer, to review the agency's own plan with him.

One thing is for certain: Young is vested in the Lusby plant and is confident in his security team.

"My family lives here. I have been in security for 33 years, 10 years of nuclear weapons security in the military," said Young. "This is safest place I've ever worked in my life. I am not saying that because I am an employee. I'm passionate about what I do, as well as our security force. They are here to protect the public from any threat and I trust they will do it without second guessing."

Experts: ISIS may be looking to access radioactive materials for weapons

Source: http://uppermichiganssource.com/news/nation-world/experts-isis-may-be-looking-to-access-radioactive-materials-for-weapons

Mar 29 – **From the terror attacks in Paris in November to those in Belgium last week, more evidence is now piling up that members of the Islamic State may be setting their sights on nuclear power plants.**

The New York Times recently reported the security clearances of several Belgian nuclear industry employees have been revoked. Additionally, Belgian police found hours of surveillance footage of high level nuclear researcher in the home of an ISIS leader.

Gary Ackerman, Director of the Unconventional Weapons and Technology Division for START, said the discovery raised many new questions.

"They might have been doing it to collect intelligence so they could either coerce or some other way gain access into a nuclear facility," Ackerman said.

.

However many experts now are focused not on the ability of terrorists to access nuclear materials but radioactive materials. They call it "weapons of mass disruption" as opposed to "weapons of mass destruction."

In other words radioactive material also known as a dirty bomb

"The highly enriched uranium is now located in less than 25 countries. In contrast, radiological materials are located in well over 130 countries," said Andrew Bieniawski, Vice President of the Nuclear Threat Initiative.

Bieniawski added those materials are located in places like hospitals, universities and industrial centers, locations.

"If you stop them from getting the materials then they cannot use them to make a bomb or some kind of dispersal device and it's all about locking down and securing those materials," he said

Nuclear Power Plants: Pre-Deployed WMDs

By Karl Grossman

Source: http://www.counterpunch.org/2016/03/28/nuclear-power-plants-pre-deployed-wmds/

Mar 28 – That's what nuclear power plants are. And that's another very big reason—demonstrated again in recent days with the disclosure that two of the Brussels terrorists were planning attacks on Belgian nuclear plants—why they must be eliminated.

Nuclear power plants are sitting ducks for terrorists. With most positioned along bays and rivers because of their need for massive amounts of coolant water, they provide a clear shot. They are fully exposed for aerial strikes.

The consequences of such an attack could far outweigh the impacts of 9/11 and, according to the U.S. 9/11 Commission, also originally considered in that attack was the use of hijacked planes to attack "unidentified nuclear power plants." The Indian Point nuclear plants 26 miles north of New York City were believed to be candidates.

As the Belgian newspaper *Dernier Heure* reported last week, regarding the plan to strike a Belgian nuclear plant, "investigators concluded that the target of terrorists was to 'jeopardize national security like never before.'"

The Union of Concerned Scientists in a statement on "Nuclear Security" declares:

"Terrorists pose a real and significant threat to nuclear power plants. The 2011 accident at Fukushima was a wake-up call reminding the world of the vulnerability of nuclear power plants to natural disasters such as earthquakes and floods. However, nature is not the only threat to nuclear facilities. They are inviting targets for sabotage and terrorist attack. A successful attack on a nuclear plant could have devastating consequences, killing, sickening or displacing large numbers of residents in the area surrounding the plant, and causing extensive long-time environmental damage."

A previously arranged "Nuclear Security Summit" is to be held this week in Washington, D.C. with representatives of nations from around the world and with a focus on "nuclear terrorism."

Last week, in advance of the "summit" and in the wake of the Brussels suicide-bombings at the city's airport and a subway line, Yukiya Amano, director general of the International Atomic Energy Agency (IAEA), said: "Terrorism is spreading and the possibility of using nuclear material cannot be excluded. Member states need to have

sustained interest in strengthening nuclear security. The countries which do not recognize the danger of nuclear terrorism is the biggest problem."

However, a main mission of the IAEA, ever since it was established by the UN in 1957 has been to promote nuclear power. It has dramatically minimized the consequences of the catastrophic accidents at Chernobyl and Fukushima and routinely understated all problems with atomic technology.

The "Nuclear Security Summit," with the IAEA playing a central role, is part of a series of gatherings following a speech made by President Barack Obama in Prague in 2009 in which he said "I am announcing a new international effort to secure all vulnerable nuclear material around the world."

In a press release this past August, White House spokesman Josh Earnest said this week's meeting "will continue discussion on the evolving [nuclear terrorism] threat and highlight steps that can be taken together to minimize the use of highly-enriched uranium, secure vulnerable materials, counter nuclear smuggling and deter, detect, and disrupt attempts at nuclear terrorism."

And, like the IAEA—formed as a result of a speech by U.S. President Dwight Eisenhower promoting "Atoms for Peace" at the UN—officials involved with nuclear power in the U.S. government and the nation's nuclear industry have long pushed atomic energy and downplayed problems about nuclear power and terrorism.

As the Union of Concerned Scientists (UCS) says in its "Nuclear Security" statement, "The adequacy of a security system depends on what we think we are protecting against. If we have underestimated the threat, we may overestimate our readiness to meet it. The NRC [U.S. Nuclear Regulatory Commission] has sometimes used unrealistically modest assumptions about potential attackers. The design basis threat (DBT) is the official definition of the security threats power plant management is required to protect against….After 9/11, UCS criticized the DBT for nuclear plants on these grounds, among others."

UCS says the NRC "ignored the possibility of air-and water-based attacks…it did not address the possibility of large attacking groups using multiple entry points, or of an attack involving multiple insiders…it concentrated on threats to the reactor core, failing to address the vulnerability of spent fuel storage facilities." Since 2011, says the UCS, the NRC "finally revised its rules to address the threat of aircraft attack for new reactor designs—but at the same time has rejected proposed design changes to protect against water- and land-based attacks."

There is "also concern about the testing standard used," notes UCS. "In July 2012, the NRC adopted the new process. However, as a result of industry pressure, the standards were watered down.."

Further, says UCS, testing is "currently required only for operating reactors, leaving questions about the adequacy of protection against attacks on reactors that have shut down, but still contain radioactive materials that could harm the public if damaged."

A pioneer in addressing how nuclear power plants are pre-deployed weapons of mass destruction has been Dr. Bennett Ramberg. As he wrote in his 1980 landmark book, *Nuclear Power Plants as Weapons for the Enemy: An Unrecognized Military Peril*, despite the "multiplication of nuclear power plants, little public consideration has been given to their vulnerability in time of war."

As he writes in a piece in the current *Foreign Affairs,* "Nuclear Power to the People: The Middle East's New Gold Rush," spotlighting the push now by many nations in the Middle East to build nuclear power plants, **"Whatever the energy promise of the peaceful atom, evidently lost in the boom are the security risks inherent in setting up reactors in the Middle East—and not just the commonly voiced fear that reactors are harbingers of weapons. The real risk is the possibility that the plants themselves will become**

targets or hostages of nihilist Middle East militants, which could result in Chernobyl and Fukushima-like meltdowns."

"Given the mayhem that Islamic State (also called ISIS) and kindred groups have sown in the region and their end-of-days philosophy, the plausibility of an attempted attack on an operating nuclear power plant cannot be denied," writes Ramberg.

In fact, the plausibility of an attempted attack cannot be denied in the Middle East—or anywhere in world.

Says Ramberg: "If terrorists did strike a nuclear power plant in the Middle East, the nuclear fallout would depend on the integrity of reactors' own containment systems and the ability of emergency personnel to suppress the emissions, a difficult challenge for even the most advanced countries, as Japan found in Fukushima. Ongoing terrorism, civil strife, or war at the time the reactor is compromised would only complicate matters."

Moreover, he notes, "all nations in the Middle East share an increasingly practical alternative—solar energy."

Nations around the world, likewise, would be able to get along fine with solar, wind and differing mixes of other safe, clean, renewable energy—not susceptible to terrorist attack.

All 438 nuclear power plants around the world today could—and should—close now. The insignificant amount of electricity they generate—but 10 percent of total electric use—can be provided by other sources.

And green energy makes for a less costly power and a far safer world in comparison to catastrophic-danger prone and unnecessary nuclear power. We must welcome energy we can live with and reject power that presents a deadly threat in so many ways.

***Karl Grossman**, professor of journalism at the State University of New York/College of New York, is the author of the book, The Wrong Stuff: The Space's Program's Nuclear Threat to Our Planet. Grossman is an associate of the media watch group Fairness and Accuracy in Reporting (FAIR). He is a contributor to Hopeless: Barack Obama and the Politics of Illusion.*

Harvard researcher warns ISIS may be on the brink of using nuclear weapons

Source: http://www.dailymail.co.uk/sciencetech/article-3516207/Harvard-researcher-warns-ISIS-brink-using-nuclear-weapons.html#ixzz44Toh3JkV

Mar 30 – The possibility of a nuclear-armed ISIS may not be as far-off as many experts suggest, a Harvard researcher has warned.

In a recent report for Project on Managing the Atom from Harvard's Belfer Center, Matthew Bunn explains how the threat of nuclear terrorism is rising as extremist groups continue to evolve.

While there has not been any concrete indication that ISIS is pursuing nuclear materials, the researcher says that the actions and rhetoric of the group suggest its need for such powerful weapons.

THREAT OF NUCLEAR TERRORISM

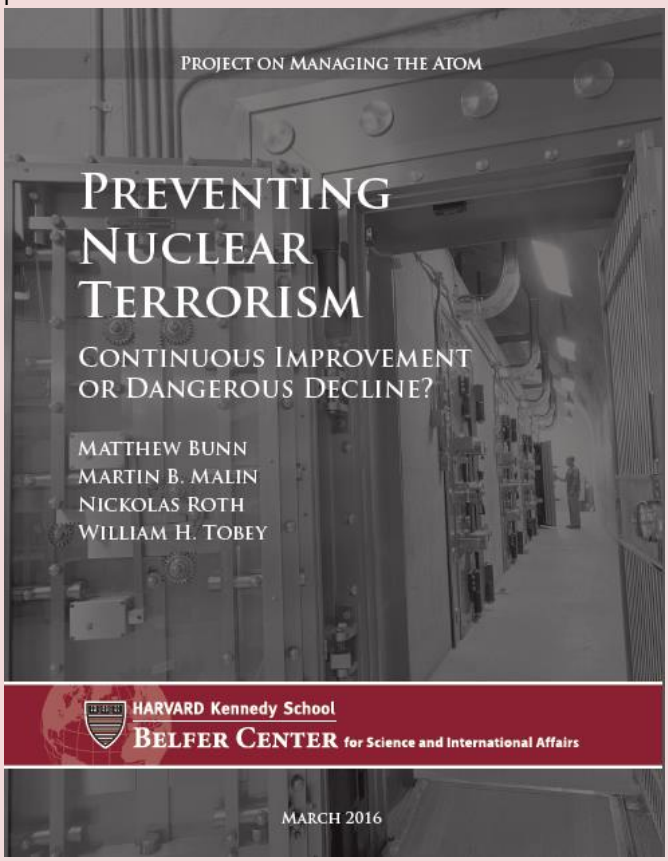
The report details the threat of three types of nuclear or radiological terrorism.

- Detonation of an actual nuclear bomb
- Sabotage of a nuclear facility
- Use of a 'dirty bomb' to spread radioactive material

Each of these comes at a different level of risk, and the authors focus for the most part on the potential danger from the use of an actual nuclear bomb, as these results would be 'most catastrophic.'

Nuclear sites may see tightened security, but there are also numerous other locations where radioactive materials can be acquired, and are less protected.
Hospitals and industrial sites, for instance, also contain such materials in a more easily accessible location,' the researcher explains.

In recent years, there have been numerous occasions of suspicious events relating to nuclear facilities in Belgium, Defense One points out.



While it would be difficult to ISIS or other terror groups to obtain the knowledge of security features and access nuclear materials, Bunn explains that the evidence of such intentions are growing.

The report precedes the 2016 Nuclear Security Summit, which will take place between March 31 and April 1.

According to the authors, the summit will help to determine the feasibility of terrorist groups getting their hands on nuclear materials.
The threats come from the possibility of three types of nuclear or radiological terrorism, the authors write: detonation of an actual nuclear bomb, sabotage of a nuclear facility, or use of a 'dirty bomb' to spread radioactive material.

Each of these comes at a different level of risk, and the authors focus for the most part on the potential danger from the use of an actual nuclear bomb, as these results would be 'most catastrophic.'
Still, the other types of threats do not come without consequences.
'The radiation from a dirty bomb, by contrast, might not kill anyone—at least in the near term—but could impose billions of dollars in economic disruption and cleanup costs,' the authors write.
'The effects of sabotage of a nuclear facility would depend heavily on the specific nature of the attack, but would likely range between the other two types of attack in severity.
'The difficulty of achieving a successful sabotage is also intermediate between the other two.'
In order to reduce the chance of these attacks, the report explains that effective and sustainable nuclear security will be necessary.
But, while progress has been made in recent years, the researchers say the work is not done.
Nuclear sites may see tightened security, but there are also numerous other locations where radioactive materials can be acquired, and are less protected.
Hospitals and industrial sites, for instance, also contain such materials in a more easily accessible location, the researcher explains.
'Making a crude nuclear bomb would not be easy, but is potentially within the capabilities of a technically sophisticated terrorist group, as numerous government studies have confirmed,' the authors write.
Though the probability of such an event may not be high as of yet, the potential consequences would be catastrophic, the researchers say, and this should act as a motivator for improved nuclear security measures worldwide.

EDITOR'S COMMENT: A report worth reading!

10 Devastating Radiation Accidents They Never Tell You About

Source: http://listverse.com/2016/03/26/10-devastating-radiation-accidents-they-never-tell-you-about/

Mar 26 – Humanity has been experimenting with nuclear power for decades, so it's no surprise that a few accidents have occurred along the way. Actually, there've been more than a few. Chernobyl, Three Mile Island, and Fukushima are hardly the only times that people, power plants, or neighborhoods have been irradiated.

10 SL-1

Photo credit: Idaho National Engineering and Environmental Laboratory

Stationary Low-Power Plant No. 1 (SL-1) was a small nuclear reactor located at the Idaho National Laboratory, which is in southeastern Idaho. It began operation in 1958 as part of a prototype nuclear power plant for the military and was used to train nuclear technicians. SL-1 was housed inside a large steel silo.

On December 23, 1960, SL-1 was shut down for maintenance. It was scheduled to resume operation on January 4. Three men, John Byrnes, Richard McKinley, and Richard Legg, were responsible for preparing the reactor the night before. They arrived at around 4:00 PM.

Alarms went off at the laboratory's firehouse at 9:01 PM. Firefighters arrived with radiation detectors and found nothing amiss. The control room looked perfectly normal, though none of the three men were there. When the firefighters began to approach the stairs leading to the silo, however, their detectors indicated dangerous amounts of radiation.

Soon, men equipped with radiation suits and better detectors arrived. Two of them reached the top of the stairs and finally got a look at the reactor. The inside of the silo was a nightmare. Water from SL-1 flooded the floor, which was also littered with debris. Byrnes lay dead in it, and McKinley lay nearby, moaning. Legg was still nowhere to be found.

Four men ran in and carried McKinley out on a stretcher. They got him into an ambulance, but he died a few minutes later. No one knew what to do with his radioactive body, so they drove it out into the desert and covered it with lead blankets for the time being. Legg was found later that night, impaled against the ceiling of the silo by a control rod. It took six days to retrieve his body.

It was eventually determined that an explosion occurred when Byrnes lifted SL-1's central control rod far more than was necessary to restart the reactor. The reaction went out of control instead. It was speculated that this was accidental; perhaps the rod was stuck, had to be yanked, and then slid out too far. Others believe that Byrnes intentionally lifted the rod to commit suicide, since his marriage was falling apart.

It took months to dismantle SL-1 and decontaminate the pieces. The men's hands had to be removed from their bodies and buried as radioactive waste. Byrnes, McKinley, and Legg were buried in lead coffins.

9 Church Rock Uranium Spill

Photo credit: EPA

Not counting nuclear bomb tests, what was the largest release of radioactive material in US history? If you guessed Three Mile Island, you're wrong. That unenviable title belongs to a dam break in Church Rock, New Mexico.

Church Rock is a small town located inside the Navajo Nation in northwestern New Mexico. It was once a major uranium mining site. There are 20 abandoned uranium mines and processing mills in the area. Most of the uranium was mined for use in nuclear weapons. For every pound of concentrated uranium produced, thousands of pounds of tailings were also created. This radioactive byproduct was often dumped in tailings ponds.

On the morning of July 16, 1979, at a processing mill operated by the United Nuclear Corporation, a tailings dam broke, releasing 94 million gallons of contaminated wastewater and 1,100 tons of radioactive tailings into the Puerco River. At around 6:30 AM, Church Rock resident Robinson Kelly went outside to find the Puerco, a normally dry arroyo, rushing with yellow-tinted water. Kelly described it as the "foulest" odor he'd ever smelled.

The water released by the dam had a pH of 2 and was filled with radioactive uranium, radium, thorium, polonium, and many other metals, which were deposited in the riverbed. By 8:00 AM, radiation was detectable 80 kilometers (50 mi) downstream in Gallup, New Mexico. In total, 130 kilometers (80 mi) of the Puerco were contaminated. By noon, the waters had receded enough for people to wade across the arroyo to retrieve livestock. Those who did so developed blisters and sores on their legs and feet. Shortly after the dam was repaired, the river was 6,000 times more radioactive than acceptable levels.

The Navajo Tribal Council asked to have Church Rock declared a disaster area but was denied. Some of the contaminants in the wastewater emit alpha radiation and can cause cancer. That radiation doesn't go away overnight. Thorium-230 has a half-life of 80,000 years, for example.

8 NRX

Photo credit: Padraic Ryan

The NRX reactor at Chalk River Laboratories in Chalk River, Ontario, began operation in 1947 and was used for experiments by the United States and Canada. The reactor could have up to 12 control rods lowered into it. Seven were enough to completely stop any reaction. Four of them, referred to as the safeguard bank, were linked to lower simultaneously. The control rods were moved by magnets, meaning that if the magnets failed, the rods would automatically fall into the reactor and shut it down. A pneumatic air pressure system was used to raise the rods or even to quickly push them down faster than gravity could alone.

All of those safety measures still weren't enough. On December 12, 1952, someone working in the basement below the reactor accidentally opened the valves linked to the control rods' pneumatic system, reducing the air pressure above the rods. Several rods began to rise out of the reactor. The supervisor ran down to the basement and closed them, which should have pushed the rods back down. But for reasons not fully understood, they didn't fall all the way back into the reactor.

The supervisor called the control room and told an operator which numbered buttons to push to make the pneumatic system force the rods down. However, he accidentally gave the number for the button that withdrew the safeguard bank. The supervisor realized his error right away, but the technician had already put the phone down and pressed the buttons.

The reactor's power output began to ramp up dramatically. The technicians eventually managed to get it back down, but not before one or more explosions inside the reactor created several ruptures, leaking 1 million gallons of radioactive water and releasing radioactive gas into the atmosphere.

The water had to be pumped out and dumped in shallow trenches not far from the Ottawa River. The NRX reactor had to be buried as radioactive waste. (A new one was constructed.) Future US president Jimmy Carter was involved in the cleanup.

Chalk River Laboratories had another incident involving a different reactor in 1958. A fuel rod caught fire, spreading fission products throughout its building. The ventilation system was also jammed open, releasing gas downwind. Technicians had to repeatedly run by the fire and toss wet sand on it to extinguish it.

7 Baneberry

Photo credit: National Nuclear Security Administration

Baneberry was a 10-kiloton nuclear bomb that was detonated 270 meters (890 ft) underground at Yucca Flat, part of the Nevada Test Site, on December 18, 1970. Underground nuclear testing had been the norm since 1963 as a result of the Partial Test Ban Treaty, and such tests were certainly less hazardous than good, old-fashioned 1950s mushroom clouds. A week before Christmas in 1970, however, geology threw scientists a curveball.

Baneberry was detonated at 7:30 AM, and everything seemed normal. Then, at 7:33, a fissure opened up about 90 meters (300 ft) from the bomb's emplacement hole, and radioactive dust and gas spewed into the sky. It continued to do so even after the ground above the detonation collapsed. (Such collapses are normal for underground detonations.) Gas visibly vented for another 24 hours.

The cloud from the test was visible from Las Vegas, something that hadn't happened in years. The radioactive dust reached a height of 3,000 meters (9,800 ft) and was carried into several

adjoining states. Fallout from the unexpected plume rained down on 86 test site workers. Two of them died from leukemia four years later.
Testing at the Nevada Test Site was suspended for six months while the cause of the Baneberry incident was investigated. It was determined that the ground into which the device was inserted had an abnormally high water content, causing the fissure to open.

6 Acerinox Plant

Acerinox is a Spanish company that produces stainless steel. In May 1998, a cesium-137 source ended up at one of their scrap metal reprocessing plants, located in Los Barrios, Cadiz. Although the plant had monitoring equipment to catch dangers like this, the source made it through and was melted in one of the ovens.
A radioactive cloud was promptly released into the atmosphere. The plant's chimney detectors didn't catch that, either, but France, Germany, Austria, Switzerland, and Italy did. Radioactivity was about 1,000 times greater than normal, and the ashes produced at the plant were radioactive enough to be dangerous.
Six plant workers suffered minor cesium-137 contamination. The plant had to be decontaminated, as did two other facilities that received its waste. The incident resulted in 40 cubic meters (1,400 ft^3) of contaminated water, 2,000 metric tons of radioactive ash, and 150 metric tons of contaminated equipment. The cleanup and lost productivity at the plant amounted to $26 million. As far as radiation incidents go, it was a happy ending.

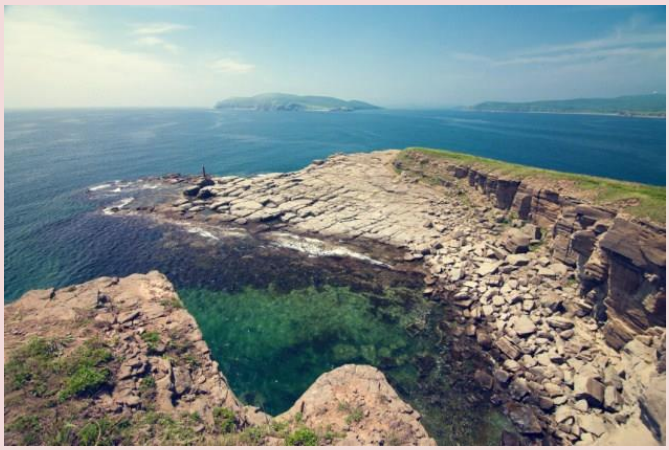
5 Chuetsu Earthquake

Photo credit: kariwa-npp2

The Kashiwazaki-Kariwa Nuclear Power Plant (KKNPP) in Japan's Niigata Prefecture can generate more power than any other power plant in the world—when it's running. Since it became fully operational in 1997, one scandal after another has repeatedly forced it to shut down some or all of its seven reactors. Examples include concealing evidence of stress cracks and covering up the fact that the plant was built near fault lines.
That last bit came to light after the Chuetsu earthquake occurred on July 16, 2007. The magnitude 6.8 quake's epicenter was only 24 kilometers (15 mi) offshore from the plant. The shaking was greater than the plant was designed to withstand; it was built before Japan updated their earthquake standards in 2006.
The ominous dry run for the later Fukushima Daiichi disaster damaged KKNPP and its reactors. The Tokyo Electric Power Company acknowledged that 1,200 liters of slightly radioactive water leaked into the sea and that dozens of barrels of low-level nuclear waste broke open during the quake. An exhaust pipe leaking radioactive iodine was also reported.
A report issued on July 19 by the Nuclear Information and Resource Service (NIRS) claimed the release of radioactive material to be much worse. According to NIRS, the water that leaked into the sea came from the irradiated fuel pool of one of the reactors. Another reactor had been releasing radioactive steam since the earthquake. The Associated Press also reported large amounts of

damage to the plant's infrastructure, with cracks and leaks seemingly everywhere. Liquefaction (formerly solid ground turning to mud) had occurred under parts of KKNPP.

4 *K-431*



Chazhma Bay, near Vladivostok, is home to a naval base that was classified during the Cold War. On August 10, 1985, *K-431*, an Echo-II nuclear submarine, was docked at the base. Leaks in the seal of the upper lid of one of its two reactors were being repaired. Both reactors had been refueled the day before.

A boat passing by in the bay created a large wake, rocking the ship servicing *K-431*. The ship's crane arm tore all of the reactor's control rods free. It wasn't long before a massive steam explosion blew the 12-metric-ton upper lid and all of the fuel assemblies straight out of the reactor compartment and destroyed the pressure hull. The explosion instantly killed 10 people.

A radioactive plume rose 50 meters (160 ft) into the air and drifted to the nearby Dunai Peninsula, leaving a 3.5-kilometer-long (2.2 mi) trace of radioactive fallout. The bay floor and adjacent waterfront were contaminated with cobalt-60. Radiation levels reached 16,000 times normal. A fire started and took four hours to put out. Radioactive material was released from *K-431* for seven hours.

Of the 2,000 people who responded to the accident and decontaminated the sub, 290 received sizable doses of radiation, and 10 suffered acute radiation sickness. The damaged *K-431* was eventually tied up at a nearby submarine base (but not dry-docked). The incident remained classified until 1993.

Later that year, sediments from Chazhma Bay still had 2,000 times more radiation than normal. Certain areas in the bay had radioactivity equivalent to 3,000 chest X-rays per hour in the 1990s. By the 2000s, the Dunai Peninsula still showed radiation levels equal to 30–400 chest X-rays per hour. The bay itself is additionally polluted from use as a scuttling site for old nuclear submarines. Around 30,000 people live near it.

K-431 was finally dismantled for scrap in 2010. The process was closely monitored for radiation spikes.

3 Rocky Flats

The Rocky Flats Plant was located 26 kilometers (16 mi) northwest of downtown Denver. It made plutonium triggers for nuclear weapons. Plutonium isn't a particularly safe substance; it can even spontaneously start to burn with no external ignition source.

On September 11, 1957, a fire broke out in Building 71, a plutonium processing building. Although the area was designed to be fireproof, it was soon ablaze. The entire building was threatened.

The men fighting the blaze knew that they shouldn't use water on a plutonium fire. Doing so could cause a criticality event. The blue flash signaling such a chain reaction would have also heralded the fact that they'd all just received a lethal dose of neutrons. However, the men were desperate and brought in the water.

Luckily, there was no blue flash. Instead, a deafening explosion blew the lead lid off the top of the 46-meter (152 ft) smokestack above, and flames shot 60 meters (200 ft) above its rim. The fire burned for another 13 hours until it was finally extinguished . . . with more water.

Radioactive smoke poured over the Denver area the whole time. It's impossible to know how much plutonium was released, as most of the monitoring equipment that could have measured it was destroyed. The fire also destroyed 620 filters, which hadn't been changed in four years and were full of plutonium and other byproducts. A school 19 kilometers (12 mi) from Rocky Flats had heavy plutonium contamination in its soil. Plutonium was detected as far as 50 kilometers (30 mi) away, and the plume likely traveled farther than that.

Local citizens weren't notified or evacuated, and the fire was kept out of the news. It wasn't until a similar fire on Mother's Day in 1969 that the Department of Energy finally came clean. After that fire, areas near Rocky Flats were found to have concentrations of plutonium greater than Nagasaki. It was also revealed that 5,000 barrels had stood out in the open for 11 years and leaked radioactive waste into the groundwater and soil.

The Rocky Flats area is now a wildlife refuge. Plutonium-239, the most common plutonium isotope, has a half-life of 24,000 years.

2 Tomsk-7

Photo credit: Dmitry Afonin

Tomsk-7, now known as Seversk, is a Siberian city about 3,000 kilometers (2,000 mi) east of Moscow. During the Cold War, it was a so-called "secret city," home to 107,000 people who worked at the Siberian Chemical Combine (SCC), a facility that produced uranium and plutonium for the USSR's nuclear weapons program. The workers' families also lived at Tomsk-7 (not to be confused with the nearby city of Tomsk).

The SCC had a number of nuclear accidents during its operation. The most well-known occurred on April 6, 1993. That day, a nitric acid solution was being introduced into a storage tank called Object 15 in order to separate plutonium from spent nuclear fuel. Object 15 contained approximately 8,700 kilograms (19,200 lb) of uranium and 450 grams of plutonium. Compressed air was required to ensure that the nitric acid and spent fuel mixed properly.

Not enough compressed air was pumped into the tank, probably due to human error. The solutions settled into layers inside the tank instead of mixing. Chemical reactions in the nitric acid layer caused the temperature and pressure inside the tank to rise. Object 15 was built to withstand 12 atmospheres of pressure. It exploded at 18 atmospheres, blowing out the walls on two floors of its building and setting the roof on fire.

The resulting plume of radioactivity contaminated 120 square kilometers (50 mi^2) around the SCC. Radioactive snowfall over the next few days caused some areas to have 100 times more radiation than normal. Soil in the affected area had significantly increased levels of cesium-137 and plutonium for years afterward.

Matters weren't helped by the fact that the SCC area was probably already severely contaminated. Massive amounts of nuclear waste are stored there, and the facility had around 30 major accidents during its operation. The population of Seversk has been continuously exposed to radioactivity.

1 Santa Susana Field Laboratory

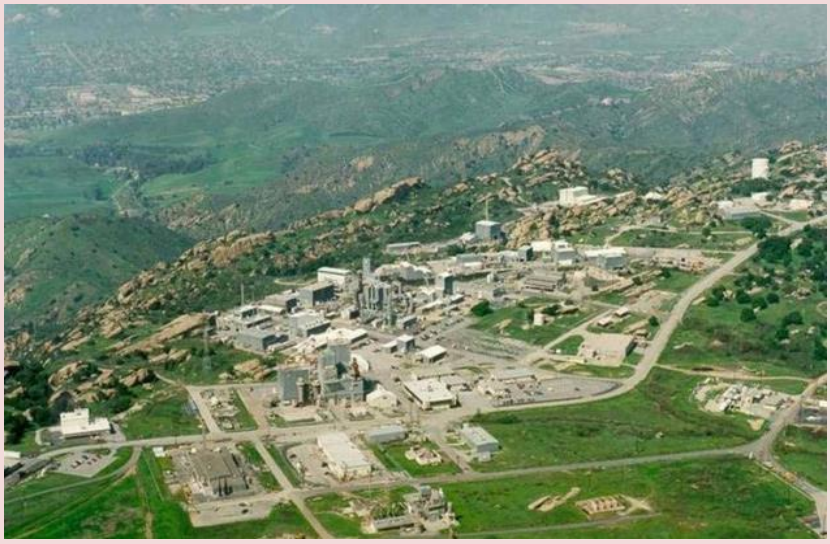


Photo credit: US Department of Energy

The Santa Susana Field Laboratory (SSFL), located near Los Angeles, spans 2,850 acres and was used by private corporations to test rocket engines for NASA. It's contaminated with both toxic chemicals and radiation. Cleaning the place up is incredibly difficult due to the sheer level of pollution, and the situation is exacerbated by the poor condition of many of the complex's structures. Worst off is Area Four, which contained 10 nuclear reactors. The largest reactor, referred to as the Sodium Reactor Experiment, partially melted down on July 13, 1959.

According to a former employee, radiation levels in the building where the meltdown occurred went "clear off the scale." To prevent an explosion that could have been comparable to Chernobyl, radioactive gas had to be vented into the sky. Afterward, workers' attempts to repair the damaged reactor only succeeded in generating more gas. For the next several weeks, a seemingly endless supply of radioactive gas was vented from the building, generally at night. People living nearby in places like Simi Valley, Chatsworth, and Canoga Park were "bombarded" with radiation.

Everyone involved in the incident was sworn to secrecy. Six weeks later, the Atomic Energy Commission reported that a minor incident had occurred and that no radiation was released. The truth wasn't revealed until 1979. Other reactor accidents, also involving the release of radioactive gas, occurred in Area Four during the 1960s.

Radiation from the laboratory is believed to be linked to increased incidences of cancer in nearby communities. One local resident recalls every house on her street having at least one cancer case. In 2007, the CDC found a 60 percent higher rate of some cancers among those living within 3 kilometers (2 mi) of SSFL.

Nuke tally could double by 2020

By Jenny Town

Source: http://www.washingtontimes.com/news/2016/mar/30/north-korea-nuclear-threat-nuke-tally-could-double/

Mar 30 – On March 9, North Korea's state media released photos of Kim Jong-un inspecting a miniaturized nuclear weapon and modern re-entry body. While experts have believed for some time that the North had miniaturization capabilities, the photos put to rest any doubts from skeptics that such capabilities existed, and signaled to the world, once again, that the North's ambitions for weapons of mass destruction (WMD) are both real and a serious, growing threat.

In 2015, the U.S.-Korea Institute at the Johns Hopkins School of Advanced International Studies conducted a yearlong study of North Korea's growing nuclear threat. This study, the North Korea Nuclear Future project, assessed the North's WMD-related capabilities today, and projected low-, mid- and high-level scenarios of where the programs may be by 2020.

The projections, even under the harshest conditions for Pyongyang to maneuver within, estimated that the North could double the size of their nuclear arsenal in five years. Under more optimal conditions (for Pyongyang), that projection increased rapidly — up to 50 nuclear weapons in a midrange scenario and up to 100 in a high-end scenario — along with development projections for the North's delivery systems.

Despite international and unilateral efforts to bolster sanctions against North Korea, the lack of serious diplomatic efforts by the United States or other stakeholders to address Pyongyang's nuclear ambitions have tacitly given Pyongyang the green light to keep developing its WMD. While these ambitions are far from new, the pace of development under Kim Jong-un seems to have accelerated. **In just the past few years**, we have seen major upgrades to the **Sohae Satellite Launching Station (photo above)**, including the building of a taller gantry tower able to handle larger space launch vehicles; construction of more sophisticated assembly systems; and implementation of better concealment facilities, such as covers over the end of the rail spur, and new structures on both the launch pad and engine test stand to provide more cover for launch and test preparations. At North Korea's Punggye-ri nuclear test site, there has been continued excavation of tunnels at the North Portal, where the 2009, 2013 and 2016 tests took place; the beginning of tunnel excavation at a new West Portal; and consistent activity at the main support area, separating the North and South Portals. In addition, North Korea has built a new class of ballistic missile submarine, the GORAE-class, berthed at the Sinpo South Shipyard, and has started testing sea-launched ballistic missiles.

North Korea has also stepped up its fissile material production capacity. In 2013, North Korea restarted its 5 MW reactor for plutonium production, which, if running at full capacity, can produce up to six kilograms of plutonium per year (roughly one bomb's worth); and also doubled the size of its uranium enrichment facility's centrifuge halls.

This year already, the North Koreans have resumed nuclear testing, now claiming to have hydrogen bomb capabilities, and warned of more tests to come. They restarted satellite launches, revealed a miniaturized nuclear weapon design, started wind-tunnel testing of a re-entry vehicle, and have tested solid-

fuel rocket engines.

These developments, while sparking great concern, are not so surprising, given the trajectory North Korea has been on. As its WMD capabilities grow, Pyongyang's nuclear strategy will also evolve. Even in a low-end scenario, doubling its nuclear arsenal and showing some improvement of its delivery systems will still bolster its deterrence capabilities, and continue assured retaliation in response to a nuclear attack by the United States. With larger arsenals, it moves past assured retaliation, and could become emboldened to explore other nuclear options, including tactical nuclear weapons, or could even start to threaten early or first use of nuclear weapons. And here we are today.

The stronger North Korea's WMD capabilities become, the harder it will be to find diplomatic solutions to slow or halt these programs. However, leaving the situation to resolve itself has proven ineffective, time and time again, even with increased pressure through sanctions. As difficult as pursuing a serious, sustained, diplomatic process with North Korea may seem, the threat Pyongyang poses will continue to grow in the meantime.

__Jenny Town__ is assistant director of the US-Korea Institute at the Johns Hopkins School of Advanced International Studies, and managing editor and producer of "38 North," a Web journal on North Korean affairs.

Fact Sheet: Who Has Nuclear Weapons, And How Many Do They Have?

Source: http://www.nbcnews.com/news/world/fact-sheet-who-has-nuclear-weapons-how-many-do-they-n548481

Mar 31 – Global leaders are meeting in Washington on Thursday to unite against the threat of nuclear weapons around the world.

The nuclear security summit, hosted by President Barack Obama, aims to put pressure on North Korea amid concerns over its recent nuclear tests and missile launches.

But many other countries, including the U.S., have known stockpiles of nuclear weapons.

More than two dozen nations have nuclear power. Only nine possess actual nuclear weapons: Russia, the United States, China, India, Israel, France, North Korea, Pakistan and the United Kingdom.

The Ploughshares Fund, a global security foundation, estimates there are more than 15,000 nuclear weapons around the world; the U.S. and Russia possess 93 percent of them. The former Cold War foes keep nearly 2,000 nuclear weapons at the ready for immediate launch against each other, according to the Nuclear Threat Initiative.

While the exact number in each country's arsenal is often a closely guarded secret, some information is publicly available. Here's a breakdown of nuclear arsenals by country, based on data from leading experts in nuclear estimates.

World Nuclear Firepower

Russia

- Total nuclear weapons: 7,300, according to the Federation of American Scientists.
- Number that are operational: 1,790
- Number retired/awaiting dismantlement: 4,490

- Total nuclear tests, approximately: 715, according to the Arms Control Association.
- First test: August 1949
- Most recent test: October 1990

United States

- Total nuclear weapons: 6,970
- Number that are operational: 1,750
- Number retired/awaiting dismantlement: 4,670
- Total nuclear tests, approximately: 1,030
- First test: July 1945
- Most recent test: September 1992

An unarmed Minuteman III intercontinental ballistic missile launches during an operational test at Vandenberg Air Force Base, California, on Feb. 20, 2016. U.S. Air Force via AP, file

China

- Total nuclear weapons: 260
- Number that are operational: 0, according to the Federation of American Scientists. All are in stockpile.
- Number retired/awaiting dismantlement: 260
- Total nuclear tests, approximately: 45
- First test: October 1964
- Most recent test: July 1996

India

- Total nuclear weapons: 110 to 120
- Number that are operational: 0, according to the Federation of American Scientists. All are in stockpile.
- Number retired/awaiting dismantlement: 110 to 120
- Total nuclear tests, approximately: 3
- First test: May 1974
- Most recent test: May 1998

Israel
- Total nuclear weapons: 80
- Number that are operational: 0, according to the Federation of American Scientists. All are in stockpile.
- Number retired/awaiting dismantlement: 80
- Total nuclear tests, approximately: 0. There haven't been any confirmed tests.

France
- Total nuclear weapons: About 300
- Number that are operational: 280
- Number retired/awaiting dismantlement: 10
- Total nuclear tests, approximately: 210
- First test: February 1960
- Most recent test: January 1996

North Korea
- Total nuclear weapons: Unknown. The U.S. said in February it had intelligence indicating the secretive nation could soon have enough plutonium for nuclear weapons and was taking steps toward a long-range missile system, but experts do not believe North Korea currently has the technology to deliver weapons.
- Total nuclear tests, approximately: 4
- First test: October 2006
- Most recent test: January 2016

Pakistan
- Total nuclear weapons: 110 to 130
- Number that are operational: 0
- Number retired/awaiting dismantlement: all 110 to 130
- Total nuclear tests, approximately: 2
- First test: May 28, 1998
- Most recent test: May 30, 1998

United Kingdom
- Total nuclear weapons: 215
- Number that are operational: 120
- Number retired/awaiting dismantlement: 95
- Total nuclear tests, approximately: 45
- First test: October 1952
- Most recent test: November 1991

Is Belgium's nuclear security up to scratch?

By Robert J. Downes and Daniel Salisbury

Source: http://www.homelandsecuritynewswire.com/dr20160401-is-belgium-s-nuclear-security-up-to-scratch

Apr 01 – **Belgium's counter-terrorism efforts are once again being called into question following the recent tragedies in Brussels. The attacks were carried out against soft targets – the public check-in area of Brussels Airport and Maelbeek metro station – but a series of unusual and suspicious occurrences were also reported at nuclear facilities in the country.**

Occurring a week before a major international summit on nuclear security, these events highlight the very real threat to nuclear facilities. For Belgium, this recent episode is one item on a long list of security concerns.

The United States repeatedly has voiced concerns about Belgium's nuclear security arrangements since 2003. That year, Nizar Trabelsi, a Tunisian national and former

professional footballer, planned to bomb the Belgian Kleine-Brogel airbase under the aegis of Al-Qaeda. The airbase, which holds U.S. nuclear weapons, has seen multiple incursions by anti-nuclear activists who have gained access to the site's "protected area," which surrounds hardened weapons storage bunkers.

Yet, Belgium only started using armed guards at its nuclear facilities weeks before the March 2016 attacks.

Beyond incursions, so-called "insider threats" have also cost Belgium dearly. The nation's nuclear industry comprises two ageing power stations first commissioned in the 1970s (Doel and Tihange), and two research facilities, a research reactor facility in Mol, and a radioisotope production facility in Fleurus. In 2014, an unidentified worker sabotaged a turbine at the Doel nuclear power station by draining its coolant. The plant had to be partially shut down, at a loss of €40 million per month.

Based on this history, the Belgian authorities should be primed to take nuclear security especially seriously. But there are serious questions about whether they are.

Islamic State is watching you

Islamic State is believed to have taken possession of radiological materials, including 40kg of uranium compounds in Iraq. This suggests a possible interest in fabricating a radiological dispersal device – or "dirty bomb" – that would spread dangerous radioactive materials over a wide area.

It had been assumed that IS was concentrating this activity in the Middle East. But that all changed in late 2015. A senior nuclear worker at the Mol research facility was found to have been placed under "hostile surveillance" by individuals linked to the Islamic State-sanctioned attacks in Paris. Reports suggested that the terrorist cell may have planned to blackmail or co-opt the worker to gain access to either the facility or radiological materials.

Alongside the 2014 Doel sabotage incident, this raises the specter of an "insider threat". A worker could use their access, authority and knowledge to sabotage a nuclear plant or remove material for malicious purposes.

This concern is furthered by reports of a worker at the Doel plant, who was associated with the radical Salafist organization Sharia4Belgium, joining Al-Qaeda-inspired militants in Syria in late 2012. Following his death in Syria, the Belgian nuclear regulator reported that "several people have … been refused access to a nuclear facility or removed from nuclear sites because they showed signs of extremism".

And in the wake of the Brussels attacks, the authorities have temporarily revoked the security clearances of 11 nuclear workers at Tihange nuclear plant.

Tightening security worldwide

Meanwhile, the fourth and final meeting in a series of international nuclear security summits is taking place in Washington. This brings together high-level decision makers, including heads of state, to try to improve the international nuclear security regime (which has been described as "a rather messy and complicated affair").

While strict processes are in place to prevent the proliferation of nuclear weapons, there are far fewer shared rules on securing nuclear facilities and materials. This summit has aimed to address this imbalance. The first summit was held in 2010, after U.S. president Barack Obama described nuclear terrorism as the "most immediate and extreme threat" to global security.

So far, the summits have seen significant successes. They have led to the removal of highly enriched uranium from 14 jurisdictions and upgrades to security at 32 material storage facilities. Equipment to detect nuclear materials has also been installed at 328 international borders.

But no further summits are planned after the 2016 meeting and no mechanism has been identified to replace the summit process. That means the future progress of nuclear security is uncertain. And as can be seen in Belgium, the threat remains as real as ever.

Robert J. Downes *is MacArthur Fellow in Nuclear Security, King's College London.*

Daniel Salisbury *is Research Associate, King's College London.*

70% of netizens believe nuclear terrorism threat is getting graver

Source http://news.xinhuanet.com/english/2016-04/01/c_135244693.htm

Apr 01 – As world leaders and envoys gather in Washington D.C. for the ongoing Nuclear Security Summit (NSS), Xinhua News Agency posted three polls on Twitter to find out netizens' views on nuclear security, and here is what has been found.

When asked "Is the threat of nuclear terrorism getting graver?", 72 percent of the respondents voted "yes", while only 28 percent voted "no". As of 6:00 p.m. (1000GMT) on April 1, a total of 979 people cast votes.

In the poll with the **question of "Are we inching closer to a world free of nuclear weapons?", only 29 percent voted "yes", while 71 percent voted "no", with a total of 1,022 votes collected.**

On a similar note, Xinhua also asked whether netizens believe in U.S. President Barack Obama' s utopian vision of a nuclear weapons-free world. Out of the 1,062 respondents, 61 percent voted "no", while 39 percent voted "yes."

Such results might come as a surprise to many, but netizens have their reasons to worry, especially considering fear and shock from the Brussels attack still linger.

Last week, synchronized bombings in Brussels killed at least 35 people and injured more than 300 others. Months ago, the carnage in Paris, capital of France, killed 130.

The most disturbing fact is that an unverified report claims terrorists had planned to target a nuclear power plant in Belgium, bringing the prospect of a nuclear attack by terrorist groups into sharp focus.

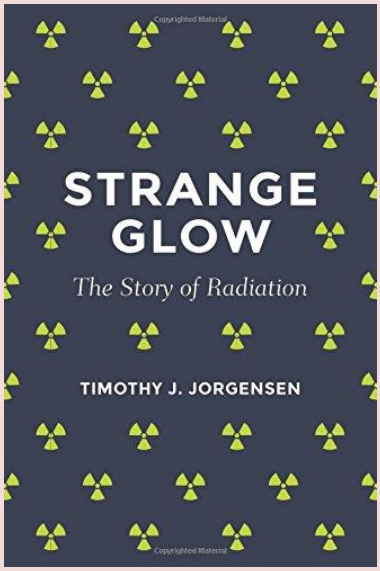
The IS, commanding more recruits, money and expertise than other terrorist groups, has caused widespread alarm, and has now reached far beyond Syria and to the heart of Europe.

How Bad Would A Radiological Terror Attack Be?

By Keturah Hetrick

Source: http://www.defenseone.com/threats/2016/04/how-bad-would-radiological-terror-attack-be/127188/

Apr 01 – When it comes to human health, all nuclear scenarios are not created equal. The Chernobyl disaster caused an estimated 16,000 cases of thyroid cancer, while the Fukushima power plant accident barely produced any. A dizzying number of variables go into understanding the damage that a particular nuclear or radiological device might have. But modeling the effects of such devices has become also become easier, and more public, thanks to the Internet.



It's "no secret" that organizations like Al-Qaeda and ISIS "are interested in securing nuclear materials so they can use them for terrorist attacks," Dr. Timothy Jorgensen, a professor of radiation medicine at Georgetown University and the author of Strange Glow: The Story of Radiation, told an audience at the Center for Strategic International Studies on Monday.

How might we be able to predict the effect of a particular attack? The type and size of bomb, materials used, detonation from the air versus ground, population density, and even wind can help us to predict increases in cancer risk, deaths from a bomb's blast, and the timing of deaths from radiation sickness.

"The distribution of doses within the population determine the survivors," says Jorgensen. "You can predict the type and severity of health consequences by just knowing the doses among individuals."

Our bodies absorb radiation through the course of normal life experiences. For example, we absorb 3.0 millisieverts (a common measurement of the body's radiation absorption, abbreviated as mSv) from a single mammogram. Eating 1,000 bananas adds another 0.1 mSv to our bodies. (Bananas, like all potassium-rich foods, contain very small amounts of radioactive material.)

Of course, our bodies absorb far more radiation if we're near a more-potent source, like an atomic bomb explosion or power plant accident.

At 1,000 mSv, radiation sickness sets in as cells begin to die. Symptoms include spontaneous bleeding, ulcerated organs, and skin that sloughs off. But, you will likely recover, with only a somewhat higher chance of developing cancer later in life.

About half of a population that receives a 5,000-mSv dose will die. This point is known as the Lethal Dose 50 (LD50).

Doses above 10,000 mSv cause gastrointestinal (GI) syndrome, leaving the afflicted with less than two weeks to live. Above 50,000 mSv, brain swelling causes Central Nervous System (CNS) syndrome. Death will come in hours.

Currently, there's no treatment for CNS syndromes. According to Jorgensen, treatment for CNS "wouldn't make much sense" because of GI syndrome's imminence.

In a normal distribution of radiation doses, that leaves a small number of treatable victims.

Unfortunately, our abilities to treat victims within that range haven't improved much. Most deaths from the U.S. bombing of Hiroshima were caused by fires or the detonation's blast, and less than 10 percent of total deaths fell within the treatable range. If the Hiroshima bombing occurred today, we would be able to reduce the number of deaths by only 5 percent, Jorgensen says.

Dirty Bombs

Reports show that last week's Brussels attackers are among many ISIS affiliates pursuing dirty bombs, renewing fears about the group's nuclear ambitions.

Dirty bombs, also known as radiological dispersal devices (RDDs), aren't actually nuclear weapons. Though they distribute a small amount of radioactive material upon detonation, their blast is far deadlier, and most people exposed to the radioactive blast wouldn't receive a lethal dose.

According to a recent report from the Nuclear Threat Initiative, a dirty bomb "would not cause catastrophic levels of death and injury" but "could leave billions of dollars of damage due to the costs of evacuation, relocation, and cleanup," contributing to the weapons' reputation as "weapons of mass disruption."

"Recent reports out of Iraq warn that Islamic State extremists may have already stolen enough material to build a [dirty] bomb that could contaminate major portions of a city and cost billions of dollars in damage," the report states.

Experts agree that terrorists are more likely to use a dirty bomb than other radioactive devices because dirty bombs are less technically complicated to build and require materials that are relatively easy to obtain.

INDs

While experts believe that terrorist groups are more likely to use dirty bombs, uranium-based improvised nuclear devices (INDs) aren't out of the question. But all INDs, which Jorgensen describes as "homemade atomic bomb[s]," are not alike.

Ground detonations and air blasts result in different casualties. Terrorists are more likely to detonate an IND from the ground, rather than dropping it from a plane. This kind of blast would cause a greater amount of fallout, which increases radiation exposure and thus, health risk.

If a terrorist group were to detonate a 15-kiloton nuclear bomb (the size of the Hiroshima bomb, considered a plausible size for a terrorist group to build or obtain), the radius for radiation sickness deaths and the radius for deaths from the blast would be about the same size.

Interestingly, the more energy that an explosion releases, the percentage of people who die from percussive blasts increases, while the percentage who die from radiation sickness decreases. That information helps us to predict deaths from the percussive blast versus deaths from radiation—and to better predict the proportion of the population who might be treatable.

If a 50-kiloton bomb were detonated over a civilian population, radiation sickness wouldn't kill anyone – because anyone

close enough for a lethal dose would already have been killed by the blast.
But energy output and altitude are far from the only variables that help us to forecast a nuclear bomb's health impact.

Enter the Nuke Map, a project from nuclear historian Alex Wellerstein. The interactive map lets you plug in variables to see the outcome of various nuclear bomb scenarios.

For example, a 15-kiloton nuclear bomb (the size of the Hiroshima bomb, considered a plausible size for a terrorist group to obtain) dropped from a plane on downtown Washington, D.C. would leave hundreds of thousands of casualties within city limits. That same bomb set off at ground level would result in fewer immediate casualties—but fallout that extended for miles, due to the region's northeast winds, Jorgensen explained.
And, even at non-lethal doses, radiation exposure introduces myriad concerns: How far away from the detonation site does cancer risk increase? Is it worth the risk to evacuate hospital and nursing home residents? When is it safe for displaced residents to return home?
According to Jorgensen, the best way to answer these questions later is public education now. "People… can't even discuss the topic because they don't know the difference between radiation and radioactivity dose. They need to have at least that much information to be engaged in the process," he says. "We, as public health officials, should do a much better job at bringing this message to the public."

***Keturah Hetrick** is a Washington, D.C.-based journalist. She previously worked at The Futurist magazine and as a private investigator.*

ISIS planning to use drones for radioactive attacks on Western cities

Source: http://www.homelandsecuritynewswire.com/dr20160404-isis-planning-to-use-drones-for-radioactive-attacks-on-western-cities

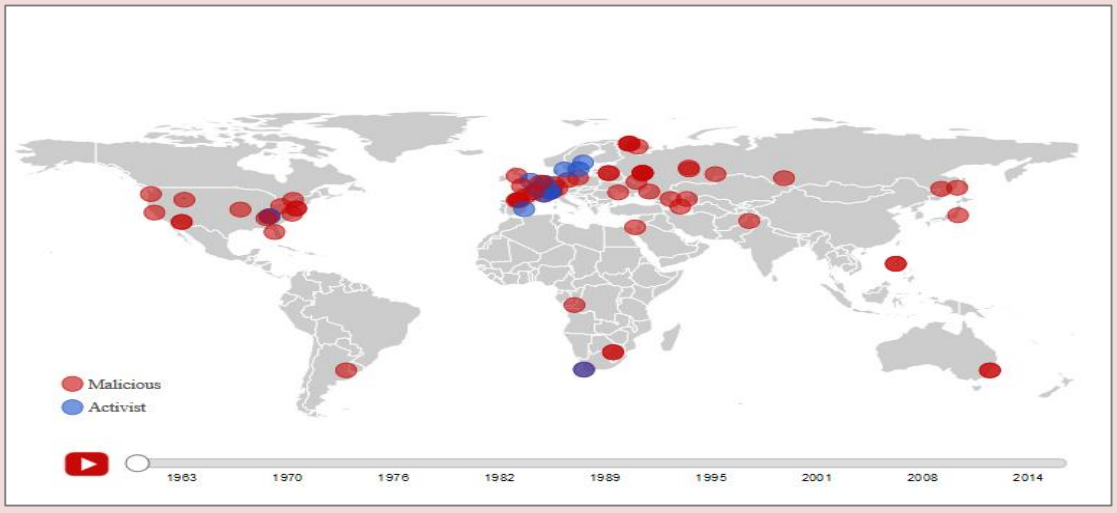
Apr 04 – **Prime Minister David Cameron warned that ISIS terrorists are planning to use drones to spray nuclear material over Western cities in a lethal "dirty bomb" attack.**
Security experts are worried about jihadists buying simple drones, which are widely available, and use them to carry radioactive material into the centers of large cities in attacks which would kill thousands and contaminate large sections of cities, making entire areas uninhabitable for years.
Cameron warned that the dangers of ISIS getting hold of nuclear material was "only too real."
The *Mirror* reports that Cameron on Friday met in Washington, D.C. with world leaders to plan how to prevent – and, if need be, react to – such an attack.
The threat is considered serious, and the world leaders, meeting for the fourth Nuclear Security Summit, were asked to take part in war games to plan how they would respond. Such war games are typically attended by technical and military staff, not political leaders.
The *Mirror* notes that **one scenario, highlighted the danger in remarkable detail. It envisioned radioactive material being taken from a medical facility by "insiders" who then sold it to extremists through the Internet's secretive "dark web."**
Cameron outlined how cabinet mi ministers would hold an emergency meeting of COBRA [Cabinet Office Briefing Rooms, the acronyms used for high-level cabinet meetings on security issues] and order the deployment of counterterrorism police and the U.K. Border Force. A British official said: "We have already seen Daesh [ISIS] trying to look at whether they can they get their hands on low-level crop-using-type drones."
ISIS came into possession of about 90 pounds of low grade uranium from Mosul University after taking over the city in 2014.
There are also fears in Europe about insider risks to nuclear facilities. Belgium has recently revoked the security clearance of eleven employees in the country's two nuclear plants.
Cameron told journalists in Washington, D.C. that concerns over a radioactive attack were real. "So many summits are about dealing with things that have already gone wrong," he said. "This is a summit about something we are trying to prevent.

"The issue of nuclear security and the security of nuclear materials, particularly when it comes to the problems of international terrorism, the concept of terrorists and nuclear materials coming together — which is obviously a very chilling prospect. And something in the light of the Belgian attacks, we know is a threat that is only too real."
"That's the point of being here and that action Britain has taken with America, very much giving a lead on nuclear security, and the security of nuclear sites, transport and materials."
American sources told reporters who covered the summit that U.S. Special Forces have been trained to seize and disable nuclear and dirty bombs.
Cameron announced that Britain would deploy 1,000 more armed police and counterterrorism units to cities outside London to help counter any terrorist attack.
Michael Fallon, the defense Secretary, yesterday announced that more than £40 million will be spent on a new Cyber Security Operations Center. The facility will be dedicated to using "state-of-the-art defensive cyber capabilities" to protect Britain from "malicious actors," Fallon said.
Fallon added: "Britain is a world leader in cyber security but with growing threats this new Operations Center will ensure that our Armed Forces continue to operate securely."

A proposal by the Editor of the Newsletter
Parhaps it is time to change CBRNE to C^2BRNE
Chemical, Cyber Biological Radiological Nuclear Explosives

Nuclear Facilities Attack Database (NuFAD) - interactive

Source: https://www.start.umd.edu/nuclear-facilities-attack-database-nufad



Olympics: UN to provide security against nuclear terrorism at Rio

Source: http://www.channelnewsasia.com/news/sport/olympics-un-to-provide/2665794.html

Apr 05 – The UN atomic agency said on Monday (Apr 4) it will provide Brazil with equipment to help prevent any attempted terrorist attacks with nuclear material at this year's Rio Olympic and Paralympic Games.

The International Atomic Energy Agency said it will loan Brazil selected types of radiation detection devices, including personal radiation detectors, for the Games in August and September.

The Vienna-based IAEA is also prepared to provide and/or facilitate assistance to Brazil "in the event of a nuclear or radiological emergency," it said in a statement.

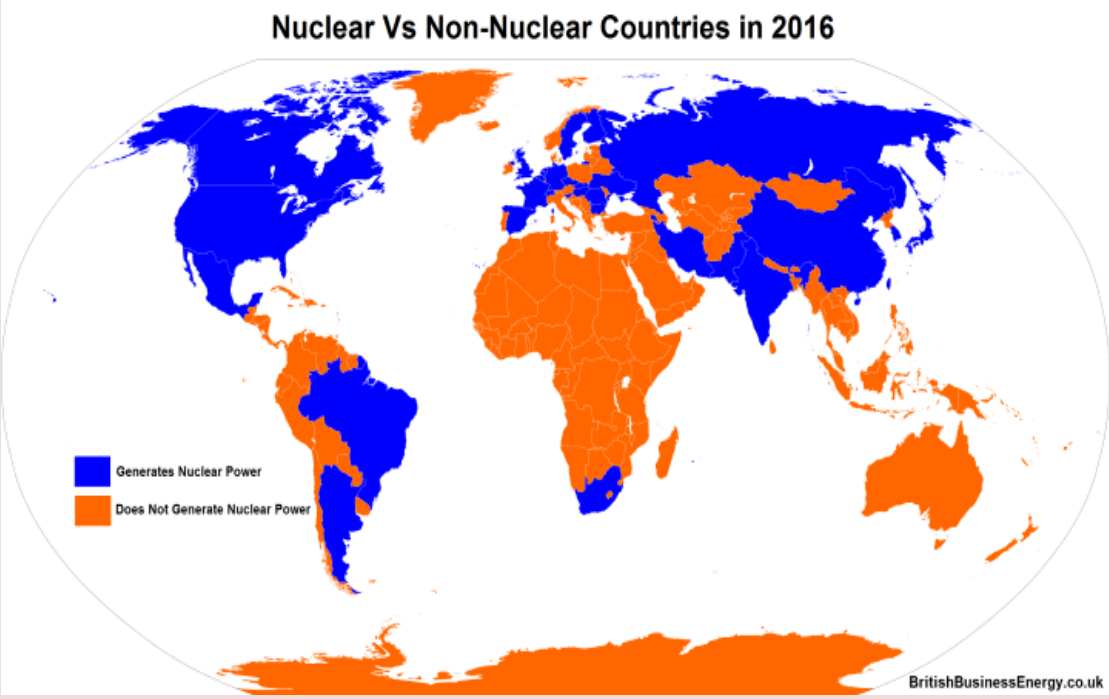
A corresponding agreement was signed Monday in Rio de Janeiro by Renato Machado Cotta, Brazil's nuclear chief, and Khammar Mrabit, director of the IAEA's Division of Nuclear Security.
The IAEA has been involved in previous major sporting events, including the Olympic Games in China in 2008 and the football World Cups in 2006, 2010 and in 2014, which was held in Brazil.
Experts and politicians have long warned of the risks of extremists getting hold of nuclear materials. US President Barack Obama last week hosted a summit on the subject in Washington.

EDITOR'S COMMENT: In fact this is the first time that something concrete CBRN related is published! There is no information on an overall asymmetric threats plan for the coming Olympics and for sure the health sector is not adequately prepared to deal with mass contaminated casualties. Will the military alone would be sufficient to counter the threat? In God we trust…

Chernobyl tourists…

Nuclear Vs Non-Nuclear Powered Countries: 2016 Facts

Source: http://britishbusinessenergy.co.uk/nuclear-vs-non-nuclear/



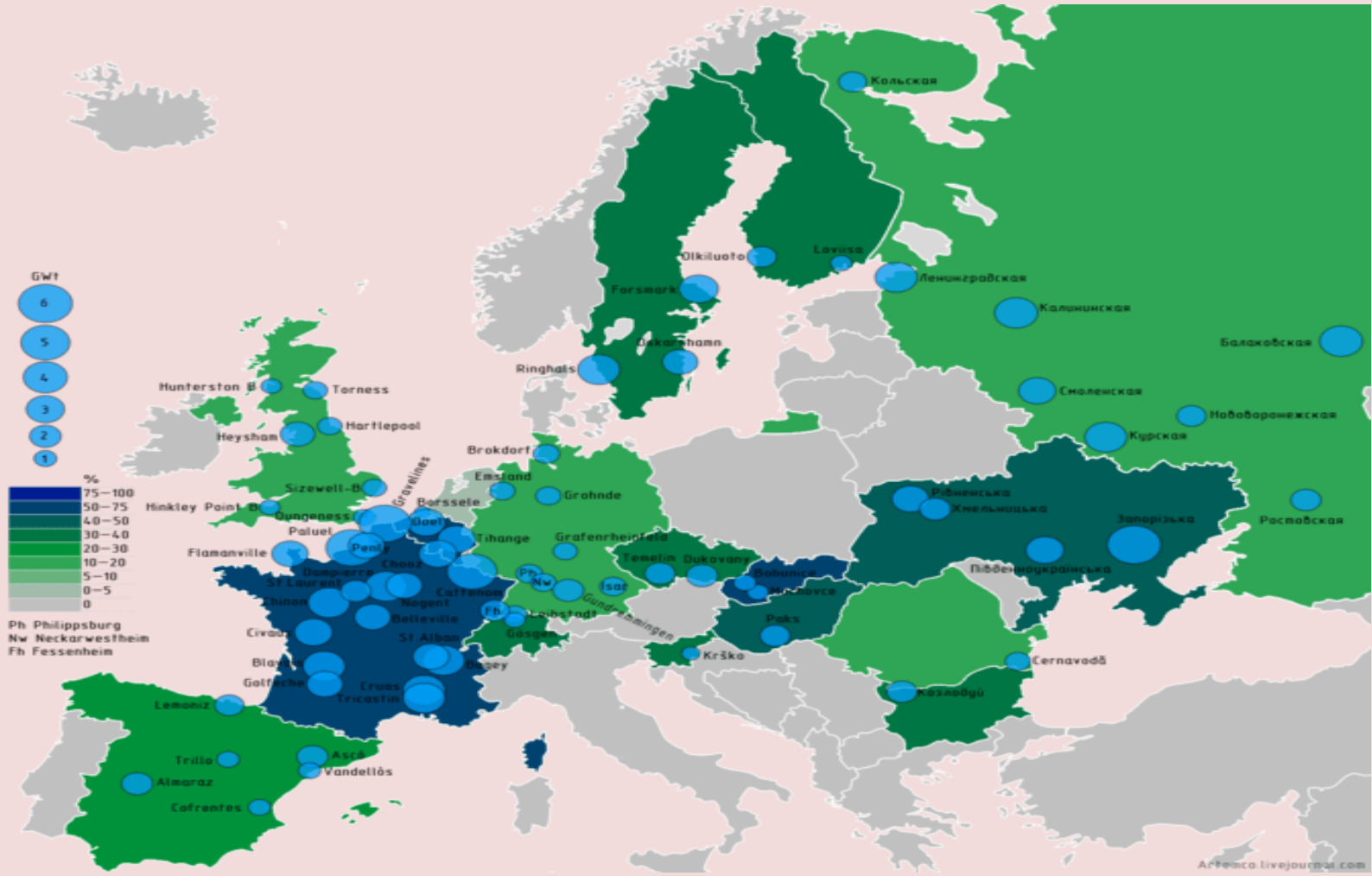
Apr 05 – The map above shows which countries have operating commercial nuclear power stations and which ones do not as of April, 2016. At last count, 31 countries generate at least some of their electricity needs via nuclear power.

Here are 13 interesting facts about these countries and nuclear power:

- **Fact #1:** Only 15.5% of UN Member countries generate nuclear power (30 out of 193).
- **Fact #2:** Taiwan is the only non-UN member to have commercial nuclear power plants.
- **Fact #3:** North Korea is currently the only country known to have nuclear weapons and not have a nuclear power station (***Note:*** *Israel does not have any nuclear power plants either, but it has never confirmed whether or not they have nuclear weapons.)*
- **Fact #4:** In total, 60.3% of the world's population live in countries with nuclear power stations, but these countries only cover cover 45.5% of the earth's land area.
- **Fact #5:** 10.9% of the world's electricity production comes from nuclear.
- **Fact #6:** Italy is the only country to have had operating nuclear power stations and then close them all down, although it imports electricity generated by nuclear power from France.
- **Fact #7:** Slovenia is the smallest country, both by population (2 million) and land area (20,273 km²; 7,827 sq mi), to have nuclear power.
- **Fact #8:** According to the IAEA, The United States has the largest number of nuclear generators (100) and produces the largest total amount of electricity (798,616 GWh) from nuclear (about 19.5% of the their total electricity).
- **Fact #9:** France is the country that is most reliant on nuclear power, which accounts for 76.9% of its total electricity generation.
- **Fact #10:** Antarctica and Australia are the only two continents not have any nuclear power stations, although Africa only has them in South Africa.
- **Fact #11:** Australia is also the largest country by area not to have any nuclear power stations, but it is the world's third largest producer of Uranium.
- **Fact #12:** Indonesia is the most populous (259 million) country not to have nuclear power.
- **Fact #13:** Europe has the largest number of countries that generate nuclear power (18 in total if you include Armenia and Russia), although North America has the largest share of countries (100%) that generate nuclear power.

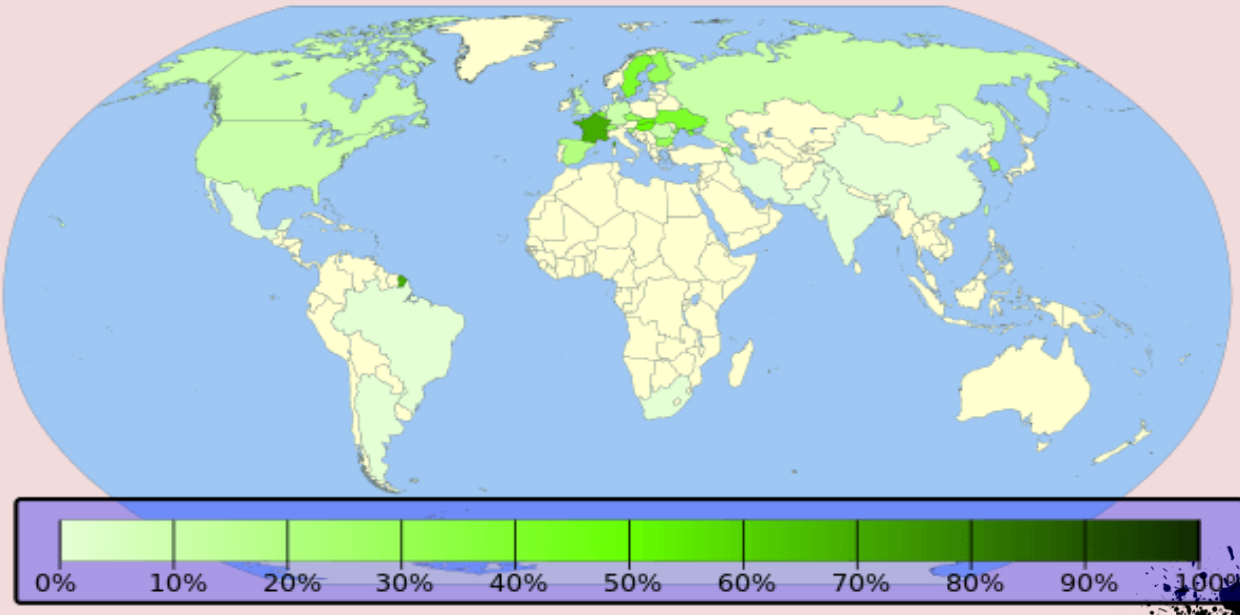
Nuclear Power in Europe

Nuclear Power in Europe map showing power station locations, generating capacity and share of power generated by nuclear.

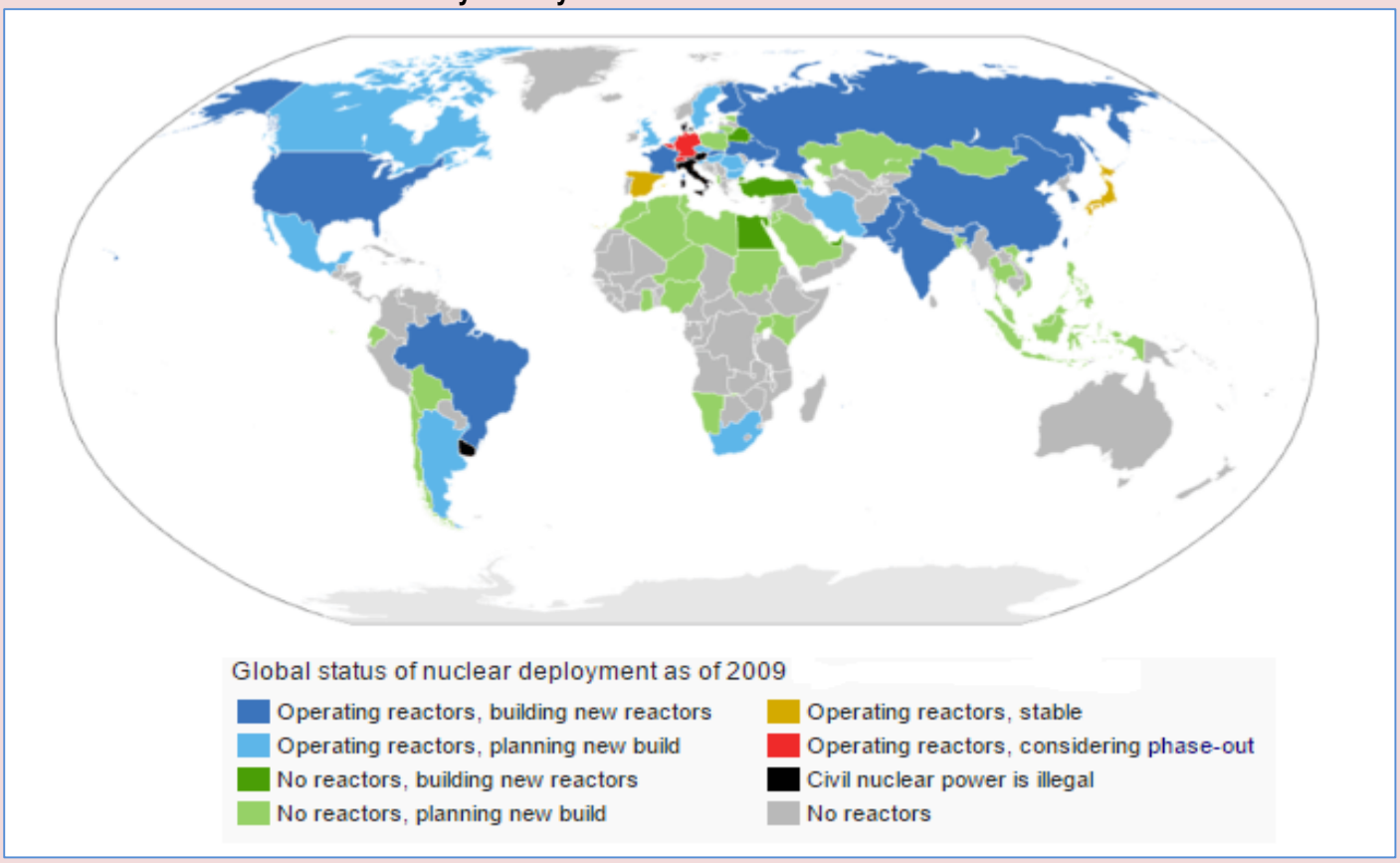


Nuclear Power Share of Total

Map showing nuclear's percentage share of each country's total generating capacity.



Future of Nuclear Power by Country



What is a dirty bomb and how dangerous is it?

By Robert J Downes

Source: http://www.homelandsecuritynewswire.com/dr20160407-what-is-a-dirty-bomb-and-how-dangerous-is-it

Apr 07 – The worrying news that individuals affiliated with the so-called Islamic State have undertaken hostile surveillance at a Belgian nuclear research facility has created growing speculation about the group's nuclear ambitions.

Nuclear weapons and dirty bombs are frequently mentioned in the same breath. However, they are two distinct technologies. Understanding the differences between these weapons and the damage they can cause can ground speculation in reality — and help us work out the most likely route a terrorist organization such as Islamic State may take in the future.

There are two types of actual nuclear weapon — fission and thermonuclear devices. Fission bombs are fueled with fissile material such as uranium and plutonium. When detonated, the atoms in the weapon's core split and release huge amounts of energy — producing a nuclear explosion. Thermonuclear weapons use a fission bomb to ignite special fuel, consisting of light hydrogen isotopes. These nuclei are forced together — undergoing nuclear fusion — releasing an even larger explosion.

There are no indications that a terrorist group has obtained any fissile material to date. If they could it would be possible for them to build a fission device, although this does pose a huge technical challenge. While highly engineered weapons need only a few kilograms of fissile material, a crude terrorist-built design would require far more. Thermonuclear weapons, on the other hand, are too complex for terrorist groups to develop.

An easier option for a terrorist group would be to build a dirty bomb or, technically, a radiological dispersal device. These do not rely on complex nuclear reactions. Instead, conventional explosives are used to disperse radioactive material, contaminating an area with elements

such as radioactive isotopes of cobalt, caesium or americium.

Under the command of Shamil Basayev, a Chechen separatist leader, militants buried a dirty bomb in a Moscow park in 1995. Basayev threatened to turn Moscow into "an eternal desert" unless his demands were met. The weapon was not detonated. The episode was a terrorist publicity stunt — threatening to use unconventional weapons against Russian civilians. But it did show that a dedicated group could build and use a dirty bomb.

How dangerous is a dirty bomb?

Although dirty bombs do not produce catastrophic explosions they can nevertheless be deadly. Radioactive materials produce ionizing radiation which can destroy bodily tissues and create harmful mutations that lead to cancer. The danger posed by radioactive material depends on the means of exposure and type of radiation it produces. Alpha radiation is harmful only if inhaled or ingested, while other types – known as beta and gamma radiation – can penetrate and damage human tissue even if the material is external to the body.

In 1987 two men stole a teletherapy unit from an abandoned cancer clinic in Goiânia, Brazil,

believing its parts might have scrap value. The unit contained a heavily shielded caesium-137 radioactive source which produced high-intensity gamma radiation. When the source was removed from its case, both men received full-body exposure to the penetrating radiation. They worked for several days to remove the caesium, drawn to the fascinating blue glow emanating from an aperture normally used to direct a radiation beam towards malignant tumors.

Experiencing diarrhea and vomiting from their unwitting exposure (which they attributed to food poisoning) the men gave the caesium to their family and friends as gifts. One father gave the glowing material to his daughter who played with it for several hours. She was one of four individuals to succumb to radiation injuries a short time later.

Twenty people developed acute radiation syndrome from the exposure. This is characterized by gastro-intestinal symptoms, immune system disruption, potential loss of consciousness and death. Those who handled the caesium also developed local radiation injuries such as erythema (skin reddening), blisters and ulcers, desquamation (skin shedding) and tissue necrosis (premature death of cells in the tissue).

The event caused widespread panic about contamination in Goiânia. Some 112,000 people (10% of the population) sought help, overwhelming local healthcare services. Decontamination costs ran into tens of millions of dollars, buildings were demolished and contaminated top-soil was removed. Public fears also stoked an unofficial boycott of locally produced goods which dropped in price by 40 percent and tourism collapsed.

Despite the International Atomic Energy Agency calling it "one of the world's worst radiological incidents," only four lives were lost. However, the psychological effect on the population, the protracted clean-up and economic disruption suggest a terrorist dirty bomb can nevertheless have a huge impact. Over the long term, the effects of contamination have been largely social. Public fears of coming in contact with contamination have led to discrimination against survivors. Yet cancer rates in Goiânia have remained comparable with other areas of Brazil.

Tackling the threat

Unlike uranium and plutonium, which are stored in high-security facilities and are extremely hard for terrorists to obtain, there are many radioactive materials with common applications. These include cancer treatment equipment found in hospitals, appliances to irradiate food for preservation and pest control, and smoke alarms.

Such wide availability does present a security challenge, so what can we do about it?

A strong, regulatory regime and effective controls on the sale and

transport of dangerous radioactive sources can certainly mitigate the threat. Alternative technologies can sometimes replace radioactive sources used in medicine. Another option is to install radiation detection equipment at ports and border crossings to identify unauthorized transport of dangerous material.

Dirty bombs are certainly easier for terrorist groups to produce than nuclear weapons. This is the reason for sensible concern, rather than hysterical speculation about Islamic State's recent activities in Belgium and, especially, Iraq and Syria. After all, without an effective government, it is unclear who controls the many radioactive sources in the region.

Robert J Downes *is MacArthur Fellow in Nuclear Security, King's College London.*

Nuclear terrorist threat bigger than you think

By Joe Cirincione

Source: http://edition.cnn.com/2016/04/01/opinions/nuclear-terrorism-threat-cirincione/

Apr 01 – **Nuclear policy experts can seem like Cassandra, constantly prophesizing apocalyptic futures.** In case you haven't noticed, we don't live in a Mad Max world devastated by nuclear war. Terrorists have not blown up New York with a makeshift nuclear bomb. We haven't bankrupted ourselves, despite the trillions of dollars spent on Cold War weapons.

Cassandra's curse, however, was not that she was wrong, but that no one believed her. I don't know a single nuclear expert who thinks that the threat of nuclear terrorism is shrinking. I don't know a single one who thinks that the actions taken by world leaders at this week's Nuclear Security Summit are enough. We are fearful. And you should be, too.

Chills went down a lot of experts' spines last month when we saw the news that the Brussels bombers, the ISIS terrorists who blew up the airport and attacked the metro, were secretly videotaping a Belgian nuclear official. This official worked at a facility that had radiological material that terrorists could use for a "dirty bomb." We do not know if they were filming him or his family, if there was a kidnap plot in motion, or what their exact plans were. But this is not some Hollywood fantasy. This is real. **A nuclear terrorist event may be closer than you think.**

What are the risks? First, that terrorists could steal a complete nuclear weapon, like SPECTRE in the James Bond thriller, "Thunderball." This is hard, but not impossible. The key risk is that the outside terrorists get insider help: For example, a radical jihadist working at a Pakistan weapon storage site. Or the Belgian base just outside Brussels where we still stash a half-dozen nuclear weapons left over from Cold War deployments. Or the Incirlik air base in Turkey where we keep an estimated 50 weapons just 200 miles from the Syrian border.

Second, terrorists could steal the "stuff" of a bomb, highly enriched uranium or plutonium. They cannot make this themselves -- that requires huge, high-tech facilities that only nations can construct. But if they could get 50 or 100 pounds of uranium -- about the size of a bag of sugar -- they could construct a crude Hiroshima-style bomb. ISIS, with its money, territory and global networks, poses the greatest threat to do this that we have ever seen. Such a bomb brought by truck or ship or FedEx to an urban target could kill hundreds of thousands, destroy a city and put the world's economy and politics into shock.

Third, there is the possibility of a dirty bomb. Frankly, many of us are surprised this has not happened already. I spoke to Jon Stewart on his show 15 years ago about the danger. This is not a nuclear explosion unleashed by splitting atoms, but simply a conventional explosive, like dynamite, laced with radioactive material, like cesium or strontium. **A 10-pound satchel of dynamite mixed with less than 2 ounces of cesium (about the size of a pencil eraser) could spew a radioactive cloud over tens of square blocks.** No one would die, unless they were right next to the explosion. But the material would stick to the buildings. Inhaling just a speck would greatly increase your risk of getting cancer. You could go into the buildings, but no one would. There would be mass panic and evacuations, and the bomb would render a port, financial district, or government complex unusable and

uninhabitable for years until scrubbed clean. Economic losses could be in the trillions.

Fourth, terrorists could just attack a nuclear power reactor, fuel storage or other site to trigger a massive radioactive release that could contaminate hundreds or thousands of square miles, like Chernobyl or Fukushima. While nuclear reactors are hardened against outside attack, including by the intentional crash of a medium-sized jet plane, larger planes could destroy them. Or a series of suicide truck bombers. But it might not even take a physical explosion. This week, it was reported the United States and the United Kingdom are to simulate a cyberattack on a nuclear power plant.

Can we prevent these attacks? Yes, by eliminating, reducing and securing all supplies of nuclear materials so that terrorists would find it too difficult to get them. And by reducing and better protecting nuclear reactors and spent nuclear fuel.

Are we doing enough? No. "The capabilities of some terrorist groups, particularly the Islamic State, have grown dramatically," says Harvard scholar and former Bush Administration official William Tobey, "In a net calculation, the risk of nuclear terrorism is higher than it was two years ago."

The United States spends about $35 billion on nuclear weapons every year. This year, we will spend $1.8 billion on all our efforts to stop the spread these weapons and stop nuclear terrorism. You don't have to be a nuclear expert to know something is out of whack here. It is time we put our money where our threats are.

***Joe Cirincione** is the president of Ploughshares Fund, a global security foundation. He is the author of "Nuclear Nightmares: Securing the World Before It Is Too Late," and "Bomb Scare: The History and Future of Nuclear Weapons." He serves on the secretary of state's International Security Advisory Board.*

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

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

Feb 14 – **A team of British scientists are working on designing a form of cement which could safely withstand the harmful**

effects of nuclear waste for thousands of years. The team at the UK's synchrotron science facility, Diamond Light Source, said the project will be vital as Britain looks to expand on its nuclear industry.

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

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

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

Dr Claire Corkhill from the University of Sheffield is using Diamond's unique Long-Duration Experiment (LDE) facility to study the way that cement

reacts with water as it becomes hydrated over a period of hundreds of years. The team at Diamond Light Source now believe following a two-year long experiment that they have discovered new cement material that contains mineral phases known to absorb highly radioactive elements.

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

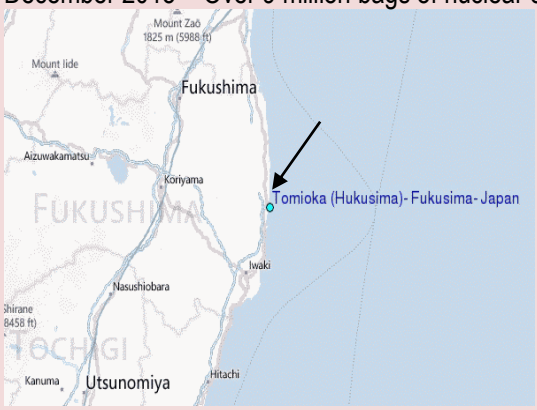
Diamond's Director of Physical Sciences, Trevor Rayment: "Timescales are crucial when it comes to nuclear research. Any facility expected to contain highly radioactive waste will need to remain functional for an extremely long period of time. Until recently, it's been impossible to use synchrotron light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

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

Over 9 million bags of nuclear cleanup waste piled up across Fukushima Pref.

Source: http://mainichi.jp/english/articles/20151210/p2a/00m/0na/020000c

December 2015 – Over 9 million bags of nuclear cleanup waste piled high. The 1-cubic-meter bags are found at some 114,700 interim storage or decontamination sites across Fukushima prefecture. In the town of Tomioka, covered by a nuclear disaster evacuation order, mounds of bags have grown so tall that they obscure the power shovels used to move and stack the waste, the black balls covering every sliver of landscape. The bags of waste are typically stacked four layer high, with a fifth layer of uncontaminated soil laid on top to block radiation. Waterproof sheets are also used to stop rainwater from getting into the bags and becoming contaminated.

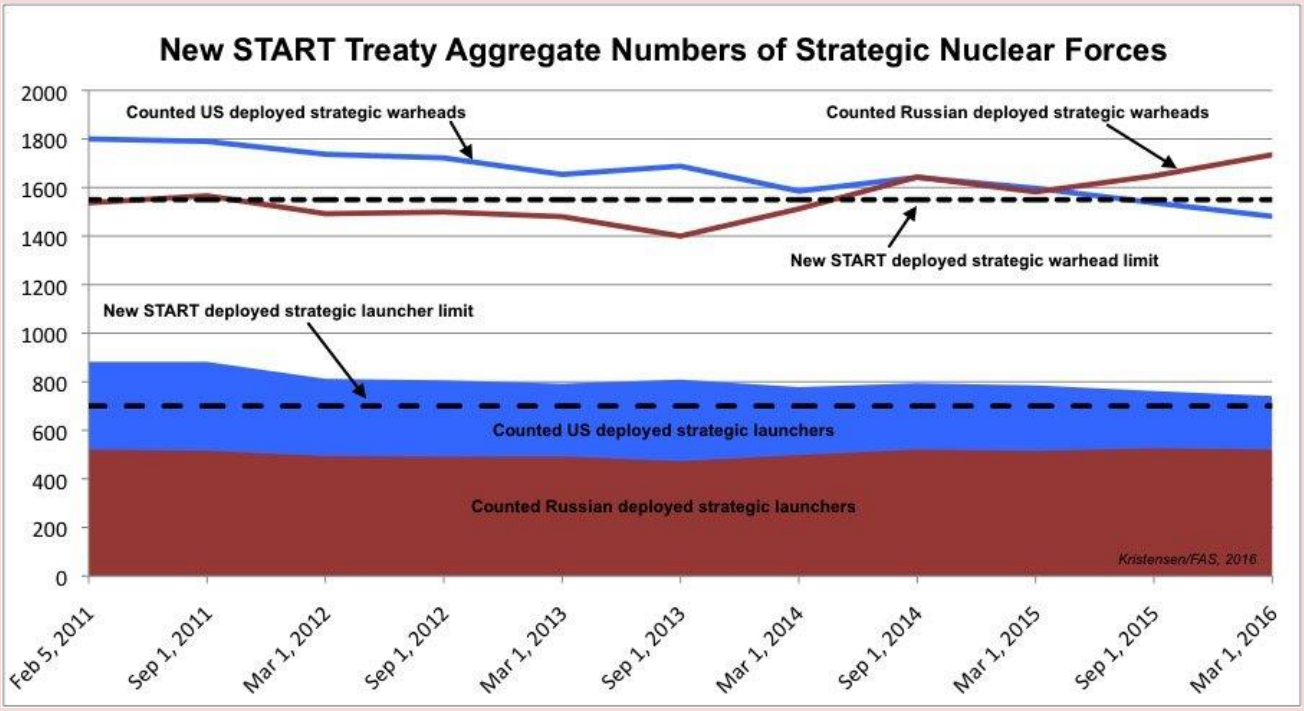


New START Data Shows Russian Increases and US Decreases

Source: http://fas.org/blogs/security/2016/04/new-start-data-shows-russian-increases-and-us-decreases/

[Updated April 3, 2016] Russia continues to increase the number of strategic warheads it deploys on its ballistic missiles counted under the New START Treaty, according to the latest aggregate data released by the US State Department.

The data shows that Russia now has almost 200 strategic warheads *more* deployed than when the New START treaty entered into force in 2011. Compared with the previous count in September 2015, Russia added 87 warheads, and will have to offload 185 warheads before the treaty enters into effect in 2018.
The United States, in contrast, has continued to decrease its deployed warheads and the data shows that the United States currently is counted with 1,481 deployed strategic warheads – 69 warheads below the treaty limit.
The Russian increase is probably mainly caused by the addition of the third Borei-class ballistic missile submarine to the fleet. Other fluctuations in forces affect the count as well. But Russia is nonetheless expected to reach the treaty limit by 2018.



The Russian increase of aggregate warhead numbers is not because of a "build-up" of its strategic forces, as the *Washington Times* recently reported, or because Russia is "doubling their warhead output," as an unnamed US official told the paper. Instead, the temporary increase in counted warheads is caused by fluctuations is the force level caused by Russia's modernization program that is retiring Soviet-era weapons and replacing some of them with new types.

Strategic Launchers

The aggregate data also shows that Russia is now counted as deploying exactly the same number of strategic launchers as when the New START Treaty entered into force in 2011: 521.
But Russia has far fewer deployed strategic launchers than the United States (a difference of 220 launchers) and has been well below the treaty limit since before the treaty was signed. The United States still has to dismantle 41 launchers to reach the treaty limit of 700 deployed strategic launchers.
The United States is counted as having 21 launchers fewer than in September 2015. That reduction involves emptying of some of the ICBM silos (they plan to empty 50) and denuclearizing a few excess B-52 bombers. The navy has also started reducing launchers on each Trident submarine from 24 missile tubes to 20 tubes. Overall, the United States has reduced its

strategic launchers by 141 since 2011, until now mainly by eliminating so-called "phantom" launchers – that is, aircraft that were not actually used for nuclear missions anymore but had equipment onboard that made them accountable.
Again, the United States had many more launchers than Russia when the treaty was signed so it has to reduce more than Russia.

New START Counts Only Fraction of Arsenals
Overall, the New START numbers only count a fraction of the total nuclear warheads that Russia and the United States have in their arsenals. The treaty does not count weapons at bomber bases or central storage, additional ICBM and submarine warheads in storage, or non-strategic nuclear warheads.
Our latest count is that Russia has about 7,300 warheads, of which nearly 4,500 are for strategic and tactical forces. The United States has about 6,970 warheads, of which 4,670 are for strategic and tactical forces.

What does "nuclear terrorism" really mean?

By Elisabeth Eaves
Source: http://thebulletin.org/what-does-nuclear-terrorism-really-mean9309

Apr 07 – There are few scarier pairs of words: "nuclear," evoking the great 20th century fear of atomic annihilation, and "terrorism," the bogeyman of the 21st. Put them together and you've got a frightening specter. Since European authorities revealed that the group behind the November 2015 Paris terrorist attacks was also spying on a senior nuclear official in Belgium, many news sources have reported that the threat of "nuclear terrorism" is upon us.
But what does that actually mean? The news stories don't always say, and sometimes they fail to distinguish among events that would look completely different from one another, if they ever came to pass. In fact, "nuclear terrorism" can refer to several possible occurrences, all of which are best avoided. But if you're the glass-half-full type, you may take some solace in knowing that the most dire scenario is also the least probable.
Here is what nuclear terrorism most likely *won't* look like: A self-styled Islamic State caliph successfully launching a ballistic missile with a nuclear warhead at Washington, incinerating millions of people in a giant mushroom cloud. There are so many technical, financial, military, and logistical barriers that it would be extremely unlikely that even the most dogged, nuclear-obsessed extremist group could make that happen.
But just because nuclear terrorism won't look like a Cold War nightmare come to life doesn't mean we should rest easy. In a March 2016 report, the Harvard Kennedy School's Belfer Center for Science and International Affairs laid out three potential types of "nuclear or radiological terrorism." **One possibility**—the hardest to achieve, but by far the most devastating if it were to occur—is that terrorists will acquire or build and then detonate a nuclear bomb in a major city. **A second possibility** is that they will set off a "dirty bomb," a weapon made of radioactive material attached to conventional explosives, sometimes referred to as a radiological dispersal device or RDD. Executing this scenario would be so easy that many experts are surprised it hasn't happened already. **A third possibility**, which the Belfer Center estimates would fall somewhere between the other two in terms of severity and likelihood, is that terrorists will sabotage a nuclear facility, releasing radioactive material over a wide area.
Least likely: a nuclear weapon. The reason the first scenario is improbable is that it's difficult to steal, buy, or make a nuclear weapon. While there are about 10,000 nuclear warheads in the world, most are heavily guarded and don't lie around fully assembled. To steal one would require the cooperation of more than just one corrupt or coerced person.
Some policy analysts do worry that terrorists might be able to buy an atomic weapon from a nuclear power hostile to Western interests, perhaps North Korea or Pakistan. In 2013, though, political scientists Keir A. Lieber of Georgetown University and Daryl Press of Dartmouth College published one of the few papers to rigorously examine that likelihood and found the fear overblown. As they write, "a

terrorist nuclear strike would not remain anonymous for long and would soon be traced back to the originating state." Few national leaders are crazy or naïve enough to think they wouldn't be found out, or that if they were, there wouldn't be massive repercussions.

As for building an atomic weapon, it's unlikely that terrorists could make anything as sophisticated as the warheads owned by governments, but making a crude nuclear bomb—an improvised nuclear device, or IND—is "potentially within the capabilities of a technically sophisticated terrorist group," according to the Belfer Center report. However, in addition to equipment and know-how, the atom-bomb-seeking terrorist would need—the largest obstacle—some quantity of either plutonium or highly enriched uranium (HEU). **Highly enriched uranium is present in fewer than 25 countries**, according to a new report from the Nuclear Threat Initiative. Even Al Qaeda, which in the 1990s and early 2000s had deep pockets, a centralized command structure, and many scientists in its employ, was not able to acquire material suitable for a nuclear weapon despite its best efforts. There have been reports of attempts to sell nuclear material in countries in the Black Sea area, but none has been successful, as far as has been made publicly known.

Most likely: a dirty bomb. None of this is to suggest that the international community shouldn't worry about the world's nuclear arsenals; we would all be unequivocally safer if there were fewer atomic weapons and less nuclear-weapon-ready material around. But we're far more likely to see the second scenario—a dirty bomb attack—than a nuclear explosion in the near future.

So what will that look like? Nothing like the aftermath of a nuclear weapon attack. As the US Nuclear Regulatory Commission explains, "A dirty bomb is in no way similar to a nuclear weapon." The latter relies on fission or fusion to create an explosion millions of times more powerful than the former. A nuclear bomb could spread radiation over hundreds of square miles, whereas a dirty bomb could only do so over a few square miles. **Dirty bombs have more in common with nuclear medicine than nuclear war.**

A dirty bomb wouldn't immediately kill any more people than an ordinary explosive. It is a weapon ideally suited to terrorism, though, part of the very purpose of which is to sow fear. **In fact, in the perverse psychology of terrorism, a mere claim that a bomb had spread radioactive material would have some of the same effect as a bomb that actually did so.**

That said, getting hold of the sort radioactive material needed to make a dirty bomb isn't difficult; it has occasionally even been stolen by accident. Literally thousands of sites, in more than 100 countries, contain the kind of sources required, which have many uses in agriculture, industry, and medicine. Radioactive isotopes are commonly used, for example, to irradiate blood before transfusions and treat cancer tumors.

One reason governments worry about dirty bombs, even though the stakes are relatively low and none has ever been detonated, is that the materials needed to make them are so obviously in circulation, and apparently in demand. The International Atomic Energy Agency tracks radioactive material that governments discover to have been lost, stolen, or otherwise "outside of regulatory control." The most recent fact sheet from the agency's Incident and Trafficking Database reports **2,734 incidents between 1993 and 2014.** (Only 49 involved HEU or plutonium.) The fact sheet also shows there has been a steady increase in annual incidents of theft and loss since the late 1990s. And because the IAEA fact sheet is based on voluntary reporting by governments reluctant to embarrass themselves or disclose sensitive information, it can be presumed to represent just the tip of the iceberg. The James Martin Center for Nonproliferation Studies, which also tracks incidents, counted **325 instances of radioactive material being outside of regulatory control in 2013 and 2014.**

So what would happen if this stuff gets spewed around a city? The answer depends on many factors. To the untrained eye, the immediate aftermath of a dirty bomb explosion wouldn't look much different than the aftermath of an attack perpetrated with regular explosives, like the Boston Marathon bombing in 2013, the Paris attacks in November 2015, or more recent terrorist bombings in Istanbul, Jakarta, Brussels, and Lahore. Law enforcement authorities would sweep for radioactive material right away, but depending on the isotopes used, the amount of smoke and debris in the air,

and proximity to the blast, a member of the public might, for lack of visual evidence, have no idea that radioactive material was involved until an announcement was made.

Once the public knew the bomb was radioactive, it would be hard to stop fear and chaos from escalating. Authorities would have to decide whether to let people flee, which could reduce their radiation exposure and begin an evacuation, but might also spread radiation through the city and let perpetrators escape.

So many variables would be involved in a possible dirty bomb attack that it's hard to definitively predict an outcome. The IAEA divides radioactive materials into five categories, from Category 1, which is so harmful that exposure for only a few minutes to an unshielded source may be fatal, to Category 5, which poses a relatively low hazard. But Category 5 materials—such as the americium-241 found in lightning detectors or the strontium-90 used in brachytherapy cancer treatment—are more readily available, and if enough are brought together in one place, they can add up to a harmful dose. An early task for first responders would be to figure out what kind of radioactive material was used.

Then there's fear of the big C. Radioactive isotopes are associated with an increase in various cancers, but by how much and over what time period isn't perfectly known. A great deal depends on the concentration to which a person was exposed. Much of what scientists have learned about radiation-caused cancer comes from studying the aftereffects of the 1986 Chernobyl nuclear disaster.

Various cities and government agencies, including the US Department of Homeland Security and the Centers for Disease Control and Prevention, have produced studies and briefings on how to respond to a dirty bomb attack, and many of these focus on the costs of evacuation and decontamination. "A radioactive dirty bomb would not cause catastrophic levels of death and injury," **the Nuclear Threat Initiative report says,** "but depending on its chemistry, form, and location, it could leave billions of dollars of damage due to the costs of evacuation, relocation, and cleanup … Buildings could have to be demolished and the debris removed. Access to a contaminated area could be denied for years as a site is cleaned up well enough to meet even minimum environmental guidelines for protecting the public." Businesses would close, shipping would halt, wages would be lost. This kind of upheaval has earned dirty bombs the moniker "weapons of mass disruption."

It could happen: sabotage. It may be that the Brussels terrorists who spied on the nuclear official were aiming for option three, wreaking havoc by damaging a nuclear power plant. It's hard to say how close they might have come. Belgium experienced a major incident of sabotage at its Doel-4 nuclear power reactor in 2014, when someone opened a valve and allowed lubricant to escape so that the turbine overheated and destroyed itself. No radioactive material was released, but the cost of the damage was estimated at between $100 and $200 million. As authorities investigated, they also happened to discover that a former contractor at the plant had left to fight for terrorists in Syria. (The jihadi contractor wasn't responsible for the valve incident.) Needless to say, Belgium has since tightened security at its nuclear power plants, but at least as of March 2016, security elsewhere remained lax. "Some countries have no armed guards at all at nuclear facilities, relying on offsite response forces some distance away; others have no background checks before allowing employees access to reactor vital areas or nuclear security systems," the Belfer Center report says.

As with a dirty bomb attack, results of an attack on a nuclear facility could vary wildly depending on many factors. The immediate death toll wouldn't necessarily go beyond whatever was caused by the explosive itself. But the fear factor, long-term health effects, and economic consequences could be significant.

Before joining the Bulletin *as columns editor in 2013,* ***Elizabeth Eaves*** *was a columnist at the tablet newspaper The Daily, where she also launched and edited the opinions page. From 2006 to 2010 she worked as a writer and editor at* Forbes *magazine, where in 2008 and 2009 she also wrote a weekly column. She has freelanced widely, including for* Slate, Foreign Policy, Harper's, *the* New York Times, *and the* Washington Post. *In 2006 she was a Robert L. Bartley fellow at the Wall Street Journal. From 1999 to 2000, she worked as a journalist for Reuters in London. Eaves received a B.A. (honors) from the*

Jackson School of International Studies at the University of Washington and a masters degree in international affairs from the School of International and Public Affairs at Columbia University.

New way to clean contaminated groundwater

Source: http://www.homelandsecuritynewswire.com/dr20160415-new-way-to-clean-contaminated-groundwater

Apr 15 – **A team of researchers from Washington University in St. Louis has helped discover a new chemical method to**

immobilize uranium in contaminated groundwater, which could lead to more precise and successful water remediation efforts at former nuclear sites. WUSTL says that researchers in the lab of Daniel Giammar, the Walter E. Browne Professor of Environmental Engineering in the School of Engineering & Applied Science, ran a series of experiments in a laboratory setting using water containing uranium — present in contaminated groundwater at various sites in the United States as a legacy of Cold War-era processing and waste disposal activities associated with nuclear materials production.

Calcium and phosphate work together chemically to immobilize uranium, which is shown to lead to increased cancer risk and liver damage in humans when ingested. Past field studies, including one at the Hanford Site in the state of Washington, focused on an *in situ* solution that injected phosphates directly into contaminated groundwater. Remediation efforts were not fully successful, because the scale of overlap for the calcium, uranium and phosphates was limited.

"A challenge with subsurface remediation is finding the right way to bring the necessary ingredients together in a poorly-mixed system," Giammar said. "In the field-scale test, much of the added phosphate never reached the uranium because it precipitated out near the injection well. The solution is to figure out scenarios where it is possible to send the phosphate to where the uranium is, and other scenarios where the phosphate can be added to a location where the natural groundwater flow will bring the uranium into contact with it."

In three different types of experiments conducted in Giammar's lab, the researchers first determined the exact level of calcium in the water. They were then able to add specific amounts of phosphate that formed calcium phosphate, chemically neutralizing and structurally incorporating the uranium. The exact combination of calcium and added phosphate rendered the uranium inert and trapped it in the groundwater.

WUSTL notes that Giammar's lab will continue this research, with the goal of developing a technique to tailor the location of phosphate injection that would be used in conjunction with the groundwater's existing calcium to remediate the uranium also present.

"The results of this work suggest that there will not be a one-size-fits-all approach to using phosphate to remediate uranium-contaminated groundwater," Giammar said. "With knowledge of the location of the uranium contamination and the composition of the groundwater, we can decide whether to inject phosphate directly into a plume of uranium-contaminated groundwater or to inject phosphate downstream of the uranium to form a calcium phosphate barrier."

— Read more in Vrajesh S. Mehta et al., "Effect of Reaction Pathway on the Extent and Mechanism of Uranium(VI) Immobilization with Calcium and Phosphate," Environmental Science & Technology 50, no. 6 (2 March 2016): 3128.

Paris attacks' mastermind had files on German nuclear waste facility

Source: http://www.homelandsecuritynewswire.com/dr20160415-paris-attacks-mastermind-had-files-on-german-nuclear-waste-facility

Apr 15 – **Salah Abdeslam, the mastermind of the November 2015 terrorist attacks who is now in custody in Belgium, had in his possession documents about a nuclear research center in Germany, the German RedaktionsNetzwerk Deutschland (RND) media group reports.**

The Juelich nuclear center near the Belgium-Germany border is used for the storage of nuclear waste.

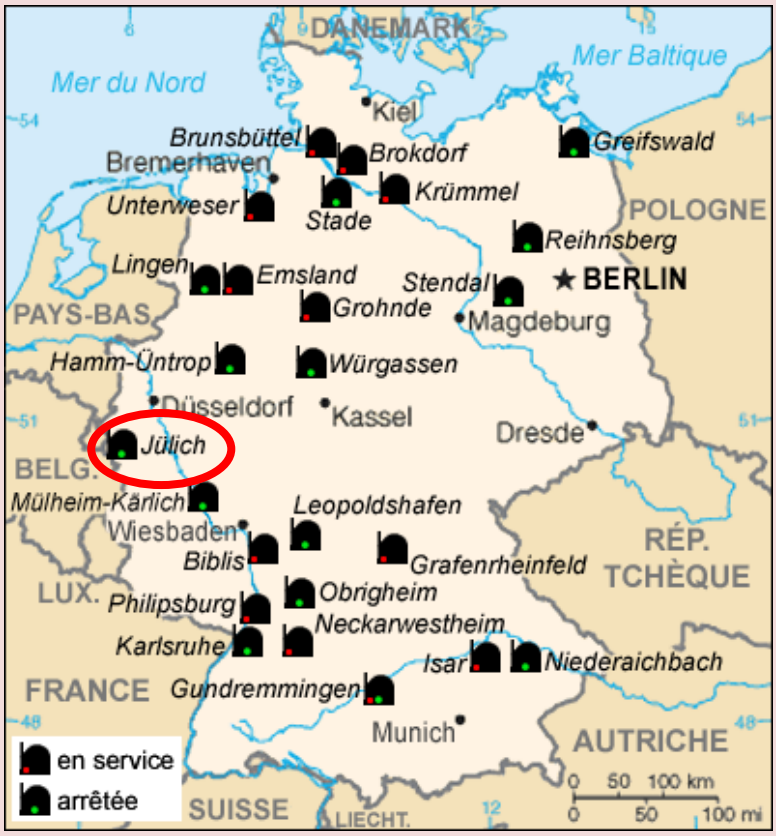
The German media group said there was no indication of any danger and that Juelich was in contact with the German security agencies.

RND cited sources within the parliamentary control committee, whose meetings are held behind closed doors, who said that Hans-Georg Maaßen, the head of Germany's domestic intelligence agency (BfV), told the committee at the end of March that Abdeslam had the documents.

Maaßen told German lawmakers that printouts of articles from the Internet and photos of the Juelich chairman, Wolfgang Marquardt, had been found in Abdeslam's apartment in the Molenbeek area of Brussels.

RND says that several members of the Bundestag and a terrorism expert at the BfV said they knew of this information and that Maaßen had confidentially informed them.

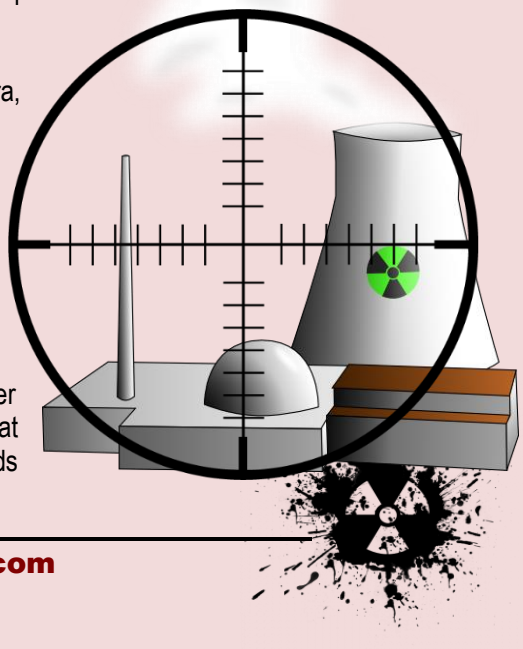
Abdeslam, a Belgian of Moroccan descent, was arrested in Brussels on 18 March.



Nuclear terrorism: How to protect nuclear plants from terrorists

By Allison Macfarlane

Source: http://www.homelandsecuritynewswire.com/dr20160415-how-to-protect-nuclear-plants-from-terrorists



Apr 15 – In the wake of terrorist attacks in Brussels, Paris, Istanbul, Ankara, and elsewhere, nations are rethinking many aspects of domestic security.

Nuclear plants, as experts have long known, are potential targets for terrorists, either for sabotage or efforts to steal nuclear materials.

Currently there are 444 nuclear power plants operating in thirty countries around the world and 243 smaller research reactors, which are used to produce isotopes for medical uses and to train nuclear engineers. The nuclear industry also includes hundreds of plants that enrich uranium and fabricate fuel for reactors. Some of these facilities contain materials terrorists could use to build a nuclear or "dirty" bomb. Alternatively, power plants could be "hijacked" to create an accident of the sort experienced at Chernobyl and Fukushima, sending clouds of radioactivity over hundreds

of miles.

At last month's Nuclear Security Summit in Washington, D.C., representatives from fifty-two countries pledged to continue improving their nuclear security and adopted action plans to work together and through international agencies.

But significant countries like Russia and Pakistan are not participating. And many in Europe are just beginning to consider physical security measures. From my perspective as a former nuclear regulator and now as director of the Center for International Science and Technology Policy at George Washington University, it is clear that nuclear plants are vulnerable to terrorist attacks.

Physical and cyber threats

It is not news that security is weak at many civilian nuclear power and research facilities.

In October 2012, Greenpeace activists entered two nuclear power plants in Sweden by breaking open a gate and scaling fences without being stopped by guards. Four of them hid overnight on a roof at one reactor before surrendering the next morning.

Just this year, Sweden's nuclear regulatory agency adopted a requirement for armed guards and additional security measures at the plants. However, these upgrades do not have to be in place until early 2017.

In 2014 French nuclear plants were plagued by unexplained drone overflights. And Greenpeace activists broke into the Fessenheim nuclear plant near the German border and hung a large banner from the reactor building.

In light of the recent Brussels attacks, reports from Belgium are more alarming. In 2012 two employees at the country's Doel nuclear power station left Belgium to fight in Syria. In 2014 an unidentified saboteur tampered with lubricant in the turbine at the same reactor, causing the plant to shut down for five months. And earlier this year authorities investigating the Paris attacks discovered video surveillance footage of a Belgian nuclear official in the home of one of the Paris suspects.

One has to assume that potential attackers may understand how the sites and materials can be used.

Given the heightened state of alert in Europe, governments should, I believe, immediately increase security at civilian nuclear facilities. They could emulate the United States, where security at nuclear facilities has substantially increased since the September 11, 2001 terrorist attacks.

American role model

U.S. nuclear power plants now are some of the most well-guarded facilities in the world.

The U.S. Nuclear Regulatory Commission (NRC) regulates both safety and security at nuclear power plants. After 9/11, these sites were required to add multiple layers of protection, with the cores of reactors (where the fuel is located) the most highly defended areas.

Up to one-third of the workforce at many U.S. nuclear plants now is security-related. Many nuclear utilities used to hire contract security forces; now guards at many of these plants are employed directly by plant owners and have opportunities to move to other jobs at their sites, increasing employee satisfaction and improving performance.

NRC regulations require U.S. nuclear plants to hold regular drills in which well-trained former military units attack the plants with up-to-date materials and techniques. NRC observers evaluate these exercises, and facility owners face stiff penalties for failure.

The United States has also adopted regulations to ensure cybersecurity at reactors. As new, entirely digital reactors come online, such measures will be more necessary than ever.

The successful 2010 Stuxnet attack, for example, in which a computer worm infiltrated computers at Iranian nuclear facilities and caused machines to malfunction, showed how vulnerable unprotected computer networks can be.

Improving security worldwide

There are no global standards for physical protection at civilian nuclear facilities. Each country adopts its own laws and regulations dictating what nuclear site owners are required to do to protect plants from attack.

As a result, measures at plants can vary widely, with some countries depending on the local police force for protection and leaving guards unarmed. Often the level of security depends on cultural norms and attitudes, but the recent attacks in

Europe suggest a rapid adjustment is needed.
Here are steps that, in my view, all countries can take to make nuclear plants more secure.
One priority is to provide enough funds to the International Atomic Energy Agency (IAEA), which has recently elevated its physical security section to assist member countries looking for ways to protect their nuclear plants more effectively. Since 2010 the agency has trained more than 10,000 people in nuclear security, including police and border guards. It also tracks illicit trafficking and other activities involving nuclear material, and has recorded nearly 3,000 such events since 1995.
Countries that have nuclear power plants or research reactors understandably tend not to spotlight the challenges of protecting these sites. But we know from instances like the ones cited above that they exist. In many countries nuclear regulatory agencies oversee safety but not security. Each of these nations needs to empower an independent regulator to enforce new requirements and inspect security at nuclear sites. Most importantly, security forces at nuclear facilities should be required to practice attack scenarios regularly under the gaze of independent observers.
Countries such as the United States that already have solid physical security requirements for nuclear facilities can help.
Nuclear regulators from all countries meet regularly and could easily share information and train their counterparts on plant physical security. In December 2012, for example, the U.S. NRC organized the first-ever International Regulators Conference on Nuclear Security. No other government has offered to head up a follow-on meeting since then.
And countries with existing reactors aren't the only problem. At least sixty countries have expressed a desire to acquire nuclear power. The United Arab Emirates is in the process of constructing four reactors. Turkey and Vietnam have made deals with the Russian manufacturer, Rosatom, in which construction, financing, operation, even waste disposal, will be handled solely by the Russians. Many of these "emergent" countries do not regularly attend Convention on Nuclear Safety peer review meetings at the International Atomic Energy Agency. Without a security regime in place, how can we expect them to do any better than the existing plants?
To prevent an attack at a nuclear site, governments must take security at nuclear sites seriously now, not a year from now.
In light of the current terrorist threat and with four Nuclear Security Summits completed, countries with nuclear plants need to up their game with regards to physical security at nuclear power facilities before it's too late.

__Allison Macfarlane__ is Professor of Public Policy and International Affairs, George Washington University.

Nuclear Power in the United Arab Emirates

(Updated April 2016)
Source: http://www.world-nuclear.org/information-library/country-profiles/countries-t-z/united-arab-emirates.aspx

- **The UAE is embarking upon a nuclear power program in close consultation with the International Atomic Energy Agency, and with huge public support.**
- **It accepted a $20 billion bid from a South Korean consortium to build four commercial nuclear power reactors, total 5.6 GWe, by 2020 at Barakah.**
- **All four units are now under construction. The first is more than 85% complete and is expected on line in 2017.**

Barakah power plant

In April 2010 ENEC lodged licence applications and an environmental assessment for its preferred site at Barakah (formerly 'Braka'), on the coast 53 km west of Ruwais and 300 km west of Abu Dhabi city – a little closer to Qatar than to the capital. The applications were assessed by the Federal Authority of Nuclear Regulation (FANR). This assessment, with environmental management plan, was considered by Abu Dhabi's Environmental Agency and approval was given in July 2012.

The site evaluation process for the four reactors considered ten potential sites and was based on guidance from FANR as well as the US Electric Power Research Institute, the US Nuclear Regulatory Commission, and the IAEA. The Gulf seawater at Barakah is about 35°C, which will give less thermal efficiency than the Shin-Kori 3&4 reference units, where the sea is about 27°C, so larger heat exchangers and condensers are required.

UAE nuclear power reactors under construction and planned

	Type	MWe gross	Construction start	Start up
Barakah 1	APR-1400	1400	July 2012	5/2017
Barakah 2	APR-1400	1400	May 2013	2018
Barakah 3	APR-1400	1400	Sept 2014	2019
Barakah 4	APR-1400	1400	Sept 2015	2020
Total		5600 MWe		

1345 MWe each net

Fuel Cycle

By August 2012 ENEC had awarded six contracts related to the supply of natural uranium concentrates, conversion and enrichment services individually, and the purchase of some enriched uranium product. A spread of suppliers is involved for each stage of the front-end fuel cycle. The company estimates the contracts are worth some $3 billion and will enable the Barakah plant to generate up to 450 billion kilowatt-hours of electricity over a 15-year period from 2017.

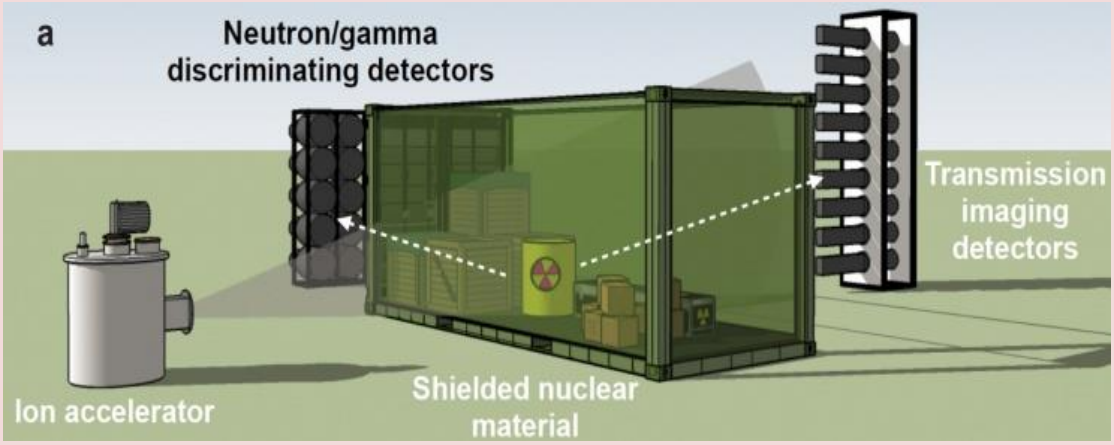
The contracts involve Canada-based Uranium One, UK-based Rio Tinto, France's Areva and Russia's Techsnabexport (Tenex) for supply of uranium concentrates. For conversion services, contracts utilise the USA's Converdyn, Tenex and Areva. Enrichment will be by Europe-based Urenco, Areva and Tenex. Areva said that its contract involved supply of enriched uranium worth some $500 million, and Tenex claimed to have secured half of the supply. ENEC "expects to return to the market at various times to take

advantage of favorable market conditions and to strengthen its security of supply position."
The enriched uranium will be supplied to Kepco Nuclear Fuels – part of the prime contractor consortium led by Korea Electric Power Corporation (Kepco) – which will manufacture the fuel assemblies.

Public Opinion
A total of 82% of people surveyed by market research company TNS in December 2012 (N=750) were in favour of nuclear power, compared with 66% in 2011, and 89% also supported a plant being built in their emirates, up from 67% in 2011, before Barakah construction started. The 2012 poll also found that awareness of nuclear energy had increased, 89% of residents now felt that peaceful nuclear energy is "extremely important, very important or important" for the UAE, and 55% viewed it as a main source of power generation, second to oil. **The high support was attributed to public engagement as plans developed.** The survey saw a decline in concerns related to overall safety of nuclear power plants, which TNS attributed to efforts spearheaded by the national government, ENEC and other nuclear industry bodies in the UAE. However, some work remained to be done to reassure the public about nuclear waste disposal, the company said.

Improving detection of concealed nuclear materials

Source: http://www.homelandsecuritynewswire.com/dr20160420-improving-detection-of-concealed-nuclear-materials



Schematic shows how a fan-like beam of gamma particles created by an ion accelerator would pass through a shielded radioactive material inside a cargo container, and be measured on the other side with Cherenkov quartz detectors. (Courtesy Anna Erickson)

Apr 20 – Researchers have demonstrated proof of concept for a novel low-energy nuclear reaction imaging technique designed to detect the presence of "special nuclear materials" — weapons-grade uranium and plutonium — in cargo containers arriving at U.S. ports. The method relies on a combination of neutrons and high-energy photons to detect shielded radioactive materials inside the containers.
The technique can simultaneously measure the suspected material's density and atomic number using mono-energetic gamma ray imaging, while confirming the presence of special nuclear materials by observing their unique delayed neutron emission signature. The mono-energetic nature of the novel radiation source could result in a lower radiation dose as compared to conventionally employed methods. As a result, the technique could increase the detection performance while avoiding harm to electronics and other cargo that may be sensitive to radiation.
If the technique can be scaled up and proven under real inspection conditions, it could significantly improve the ability to prevent the smuggling of dangerous nuclear materials and their potential diversion to terrorist groups.
The research, supported the National Science Foundation and the Department of Homeland Security, was reported 18 April in the *Nature* journal *Scientific Reports*. Georgia Tech reports that scientists from the Georgia Institute of Technology, the University of Michigan, and the

Pennsylvania State University conducted this research, which is believed to be the first successful effort to identify and image uranium using this approach.

"Once heavy shielding is placed around weapons-grade uranium or plutonium, detecting them passively using radiation detectors surrounding a 40-foot cargo container is very difficult," said Anna Erickson, an assistant professor in Georgia Tech's George W. Woodruff School of Mechanical Engineering. "One way to deal with this challenge is to induce the emission of an intense, penetrating radiation signal in the material, which requires an external source of radiation."

The technique begins with an ion accelerator producing deuterons, heavy isotopes of hydrogen. The deuterons impinge on a target composed of boron, which produces both neutrons and high-energy photons. The resulting particles are focused into a fan shaped beam that could be used to scan the cargo container.

The transmission of high-energy photons can be used to image materials inside the cargo container, while both the photons and neutrons excite the special nuclear material – which then emits gamma rays and neutrons that can be detected outside the container. Transmission imaging detectors located in the line of sight of the interrogating fan beam of photons create the image of the cargo.

"The gamma rays of different energies interact with the material in very different ways, and how the signals are attenuated will be a very good indicator of what the atomic number of the hidden material is, and its potential density," Erickson explained. "We can observe the characteristics of transmission of these particles to understand what we are looking at."

When the neutrons interact with fissile materials, they initiate a fission reaction, generating both prompt and delayed neutrons that can be detected despite the shielding. The neutrons do not prompt a time-delayed reaction with non-fissionable materials such as lead, providing an indicator that materials of potential use for development of nuclear weapons are inside the shielding.

"If you have something benign, but heavy — like tungsten, for instance — versus something heavy and shielded like uranium, we can tell from the signatures of the neutrons," Erickson said. "We can see the signature of special nuclear materials very clearly in the form of delayed neutrons. This happens only if there are special nuclear materials present."

Earlier efforts at active detection of radioactive materials used X-rays to image the cargo containers, but that technique had difficulty with the heavy shielding and could harm the cargo if the radiation dose was high, Erickson said. Because it uses discrete energies of the photons and neutrons, the new technique minimizes the amount of energy entering the container.

Researchers at Georgia Tech — led by Erickson — and at University of Michigan and Penn State University — led by Igor Jovanovic, professor of nuclear engineering and radiological sciences — demonstrated that the technique works in a laboratory setting by detecting uranium plates and rods.

Georgia Tech notes that in testing conducted in collaboration with the Massachusetts Institute of Technology at the Bates Linear Accelerator Center, the researchers used a fan-like pattern of particles created by an ion accelerator and emitted at 4.4 and 15.1 MeV. The particles passed through a shielded radioactive material, and were measured on the other side with Cherenkov quartz detectors connected to photomultiplier tubes.

"This provided proof that the physics works, and that we can use these particles to actually distinguish among various materials, including special nuclear materials," Jovanovic said. The technique has not yet been tested under the real-world conditions of a steel cargo container, but such demonstration may take place in the near future.

Beyond the potential homeland security uses, the technology could also find application in materials science, medical imaging, low-energy nuclear physics and industrial imaging.

— Read more in Paul Rose et al., "Uncovering Special Nuclear Materials by Low-energy Nuclear Reaction Imaging," Scientific Reports 6, Article number: 24388 (18 April 2016).

90 potential suicide bombers 'roaming' EU, French Interior Ministry report reveals

Source:https://www.rt.com/news/336456-france-terror-report-bombing/

Mar 22 – **The 55-page testimony, which was produced exclusively for the French Interior Ministry and was seen by the New York Times, shows the scale of planning that went into the November 13 Paris terror attacks, including precise encryption, top level document forgers and even sending bomb makers from Syria to Europe.**

The documents included interviews with both officials and witnesses and showed how Islamic State (IS, formerly ISIS/ISIL) has evolved into being able to carry out terror attacks on such a grand scale.

The report shows that the bombs used by the terrorists were simple to make, but very effective. They found traces of the same explosives used at each of the sites in Paris which were attacked by suicide bombers.

The bomb maker who made the explosives had used triacetone triperoxide, or TATP, which can be made from everyday products such as bleach or nail polish remover – items which could be purchased without raising suspicion. However, the person putting the explosives together certainly knew what he or she was doing.

"Their ingredients, when combined, are highly unstable and can explode easily if mishandled," said Peter Bergen, the director of the National Securities Studies Program at the New America Foundation, according to the New York Times.

"To make an effective TATP bomb requires real training, which suggests a relatively skilled bomb-maker was involved in the Paris plot, since the terrorists detonated several bombs. It also suggests that there was some kind of bomb factory that, as yet, appears to be undiscovered, because putting together such bombs requires some kind of dedicated space," he added.

The report also states that a lack of border controls allowed the terrorists to move freely around Europe without arousing suspicion, while the inability of international governments to share intelligence also made it easier for the jihadists to avoid detection.

(U//FOUO) Crude TATP (left) and pure TATP (right).

(U//FOUO) Key Identifiers

- Crystals or powder
- Sugar-like appearance
- Colorless or white
- Solids settled at bottom of container
- Additives can alter the physical appearance and color
- Fruity smell, like acetone but gentler
- Old TATP smells very acrid, like bad vinegar
- Evaporates in an open container
- If stored in a closed jar, glass may look frosted
- May be stored in a refrigerator or freezer

(U) Chemical Precursors

- **Acetone**: nail polish remover, paint remover
- **Strong Acid**: sulfuric, nitric, hydrochloric
- **Hydrogen peroxide** disinfectant, bleaching agent

(U//FOUO) Improvised filtration set-up

(U//FOUO) Improvised cooling set-up.

(U) Lab Equipment

Glassware — Distillers
Mixers — Ice Bath
Filters

"We don't share information," former head of French intelligence Alain Chouet told the New York Times. *"We even didn't agree on the translations of people's names that are in Arabic or Cyrillic, so if someone comes into Europe through Estonia or Denmark, maybe that's not how we register them in France or Spain."*

The documents released by French police also showed that the attackers did their utmost to keep themselves digitally hidden from the authorities. Police found numerous unused cell phones still in their packaging. There were also discarded phones which showed a number of calls had been made between Paris and Belgium – suggesting that the attackers had support from further afield.

It was also revealed following interviews with hostages at the Bataclan Theater that the terrorists had also seized cell phones from those being kept against their will in order to access the internet, without leaving any data trails that the authorities could later trace.

Discarded phones that belonged to the terrorists also revealed detailed maps of the theater's layout, suggesting that they had meticulously planned their operation.

One of the hostages noticed that a terrorist was using a laptop computer. However, when he turned it on, all she could see was lines of text on the screen.

"It was bizarre — he was looking at a bunch of lines, like lines of code. There was no image, no internet," she said, according to the New York Times.

Following the November 13 attacks, police tried to piece together the movements of the attackers, and the authorities hope the arrest of Salah Abdeslam in Brussels on Friday will provide them with further clues.

IS Claims Suicide Bombing on Stadium in Iraq That Killed 29

Source: http://abcnews.go.com/International/wireStory/suicide-bomber-hits-stadium-iraqi-city-killing-29-37932751

Mar 25 – **A suicide bomber blew himself up in a soccer stadium south of the Iraqi capital on Friday, killing 29 people and wounding 60, security officials said, as the military announced new gains on the ground against the Islamic State group.**

The bombing took place during a match in the small stadium in the city of Iskanderiyah, 30 miles (50 kilometers) from Baghdad, the officials said. Medical officials confirmed the death toll. The officials spoke on condition of anonymity because they were not authorized to talk to the press.

The Islamic State group claimed responsibility for the attack via a statement posted online, SITE intelligence group, a monitoring organization, reported.

IS has been waging a campaign of suicide bombings in and around the capital as Iraqi forces and their allies battle the militants in the north and west of the country.

The bombing came as Iraqi military spokesman Yahya Rusoul announced that Iraqi troops and Sunni tribal fighters recaptured the town of Kubeisa in western Anbar province from the Islamic State group. A day earlier, IS fighters were pushed out of a string of villages in Iraq's northern Nineveh province under cover of heavy coalition airstrikes.

The Mayor of the city was among the dead of the suicide attack.

In Pakistan, Taliban's Easter bombing targets, kills scores of Christians

Source: http://edition.cnn.com/2016/03/27/asia/pakistan-lahore-deadly-blast/index.html

Mar 28 – **A splinter group of the Pakistani Taliban has claimed responsibility for a deadly attack on Easter Sunday, saying it intentionally targeted Christians.**

The suicide blast in the eastern Pakistan city of Lahore killed 70 people, a local government spokesman told CNN.

More than 341 others were injured, according to Punjab government spokesperson Jehangir Awan.

The explosion ripped through the heart of Lahore on Sunday evening, at a time when many families were at the city's Gulshan Iqbal Park to celebrate the Easter holiday. Many women and children were among the victims.

Ehsanullah Ehsan, a spokesman for the splinter group of the Pakistani Taliban known as Jamat-ul-Ahrar vowed such attacks would continue.

Pakistani Prime Minister Muhammad Nawaz Sharif strongly condemned the blast. Sharif was born in Lahore and enjoys strong support there.

Blasphemy law protests erupt

Protests erupted again Sunday, almost a month after a former bodyguard who assassinated a moderate politician was executed. Mumtaz Qadri, was hanged in a Rawalpindi prison February 29, five years after being found guilty of shooting and killing Punjab Gov. Salman Taseer.

The governor had spoken out against the blasphemy law that makes insulting Islam a crime punishable by death.

As many as 10,000 demonstrators gathered in the capital, Islamabad, Friday, praising Qadri and demanding changes to Pakistan's laws, including the adoption of Sharia law, according to local media reports.

International condemnation

Indian Prime Minister Narendra Modi, who has worked to thaw the icy relations between the two neighbors, called Sharif on Sunday to express his grief over the bombing.

The Indian leader expressed solidarity with Pakistan, the Pakistani state-run news agency reported.

"Modi said coward terrorists had targeted females and kids which was highly condemnable and regrettable," according to the state-run agency, the Associated Press of Pakistan.

The United States and Australian governments also condemned the attack.

"This cowardly act in what has long been a scenic and placid park has killed dozens of innocent civilians and left scores injured," National Security Council spokesman Ned Price said in a statement.

Australian Foreign Minister Julie Bishop echoed the sentiment.

"As Christians worldwide celebrate Easter, a shocking terrorist attack in Lahore, Pakistan, reminds us that terrorism is a global scourge," she said Monday.

"The Australian Government condemns this horrific act that has killed dozens of civilians, including children, and expresses our condolences to the people of Pakistan and its government at this time."

History of violence

In March last year, suicide bombers attacked a Christian community, also in Lahore, setting off two blasts that killed at least 14 people and wounded dozens more, officials said.

The Pakistani Taliban claimed responsibility for that attack too and warned of more to come.

The explosions, which struck the Nishtar Colony area in the city of Lahore, wounded at least 78 people, Dr. Muhammed Saeed Sohbin, medical superintendent at Lahore General Hospital, said then.

In 2013, suicide bombers struck a church in the northwestern city of Peshawar, killing more than 80 people.

EDITOR'S COMMENT: It was a 20kg bomb with metal spheres inside and the suicide bomber was 20-22 yrs old. And all that for what? To eliminate infidels? To win his share in the world of virgins? To prove that religious fanatism is a disease? To facilitate the Chaliphate's dominance over the planet? He is dead. His victims are dead. And the world keeps on turning despite his sick efforts and of those behind him! So sad…

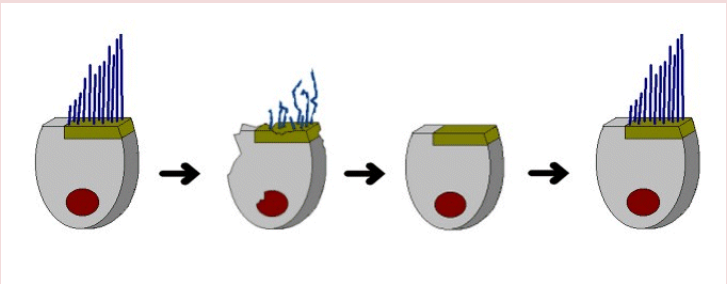
Subtler Harm From Bombs: Some Victims Lose Hearing

Source: http://www.nytimes.com/2013/04/25/us/boston-bomb-victims-hidden-injury-hearing-loss.html

April 24, 2013 – Acoustic trauma of this sort can rupture the delicate eardrum, and hearing experts at several hospitals in Boston said on Wednesday that torn eardrums accounted for most of the hearing loss they have seen among those near the explosions.

In most of these cases, the eardrum will heal in a few weeks or months. If not, a tear can be repaired with an outpatient surgical reconstruction called a tympanoplasty, which can restore normal hearing.

But proximity to an explosion also can cause "sensorineural" hearing loss: damage to **hair cells** (photo) in the inner ear, which is potentially permanent, said Dr. Daniel Lee, an ear surgeon at Brigham and Women's Hospital in Boston. Hair cells cannot be regenerated.

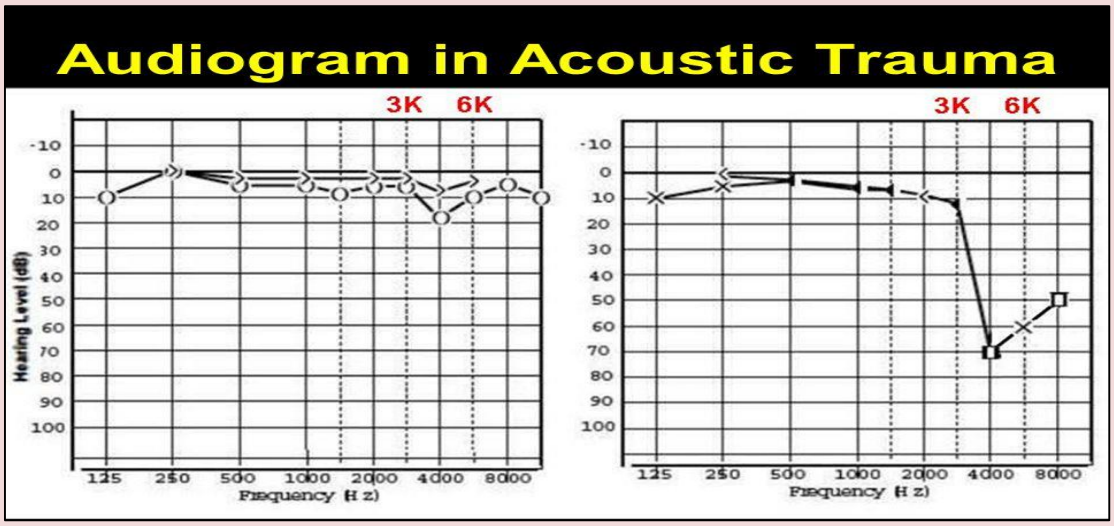


"We're generally seeing patients who have a conductive hearing loss associated with traumatic eardrum perforation," he said. "Some of the patients may develop a progressive sensorineural hearing loss in the future."

At present, most of the patients with sensorineural damage have suffered only mild to moderate hearing loss. There is great variability in the hearing loss experienced by

people exposed to acoustic trauma, based on things like which way they were facing or what was between them and the explosion.

Nick Yanni, 32, a student at Bunker Hill Community College, and his wife, Lee Ann Yanni, 31, a physical therapist, were 10 feet from the first bomb when it went off. Ms. Yanni said she immediately lost hearing in her left ear, but at the time was far more worried about her broken left fibula.



At the emergency room at Tufts Medical Center, she struggled to answer doctors' muffled questions about her leg.

Mr. Yanni discovered at the E.R. that he could not hear in either ear and tried to read lips. An hour or two later, his ears became painfully sensitive to background noise, so he put in earplugs. By nightfall, his hearing had returned.

"We were standing right next to each other," Ms. Yanni said. "His hearing loss turned out to be temporary, and mine is lasting."

After three operations for her leg fracture in five days, she was discharged on Monday. "I know I can function even if my hearing isn't perfect, but I'd like to get it back," Ms. Yanni said.

Within 24 hours of the bombings, Beth Israel Deaconess Medical Center in Boston began auditory evaluations of bombing victims after several mentioned that voices sounded as if they were underwater or that their own voices seemed louder.

Dr. Selena E. Heman-Ackah, medical director of otology, neurotology and audiology at Beth Israel Deaconess, has evaluated roughly 20 patients with hearing loss in wake of bombings. All but two suffered perforations of the eardrums, she said.

Given the loudness of the explosions, Dr. Heman-Ackah said she expected to see more patients with nerve-related hearing loss. She believes that the eardrum perforations might have been protective against the more permanent neural loss.

The night of the bombings, Dr. Alicia M. Quesnel, an ear specialist at the Massachusetts Eye and Ear Infirmary, began doing consultations with some patients injured by bomb blasts, once they had been stabilized, using a tuning fork to gauge the type of auditory loss.

If patients can hear the tuning fork touching their skull, the hearing loss is probably conductive — related to a torn eardrum or damage to the tiny bones behind it. But if they can hear a tuning fork held in front of the ear better, or cannot hear either one, Dr. Quesnel said, "you worry about inner ear hearing loss that's neural."

"Most of what we are seeing is conductive hearing loss," she said. "It will either heal on its own, or down the line they won't end up with a huge hearing loss because it can be fixed."

Dr. Jonathon Sillman, an ear specialist at Tufts Medical Center, has evaluated about 10 bombing victims for hearing injuries. All were given audiograms as soon as they could sit in a wheelchair in a soundproof booth. "One of the most striking things about this experience is how variable the injuries were," Dr. Sillman said.

One patient was standing next to a person who lost her legs, he said, yet "her only injury is one perforated eardrum with no neural hearing loss." He suspects the person who lost her limbs must have shielded his patient from the energy of the blast.

Terrorist group that planned to bomb UAE malls given life in prison

Source: http://www.thenational.ae/uae/courts/terrorist-group-that-planned-to-bomb-uae-malls-given-life-in-prison

Mar 27 – **The founder of a terrorist group that planned to bomb malls and hotels has been sent to jail for life, along with 10 other members.**

Khalid Abdulla Kalantar considered himself a caliph and preached extremist ideology at Al Manara Mosque in Dubai.

Kalantar focused on young social outcasts with criminal records, to recruit them to his group, Shabab Al Manara.

The group had an arsenal including Kalashnikov assault rifles, hand grenades and landmines hidden in the desert.

Kalantar was one of 41 men on trial at the Federal Supreme Court for involvement in the group. They included four of his sons – Abdullah and Othman who were given life sentences, and Abdulrahman and Mohammed who were given 10 years.

Fifty-seven family members attended the sentencing in the capital on Sunday amid tight security. A wife of one of the men jailed for life collapsed and had to be helped by paramedics.

During interrogation, the members said they were influenced by watching films and lectures by the late Al Qaeda leader Osama bin Laden.

Prosecutors said all confessed to joining Shabab Al Manara and intending to use terrorism to oust the Government, but only two pleaded guilty in court.

In sentencing, Judge Mohammed Al Jarrah Al Tunaiji said: "Terrorism is one of the gravest of crimes. It uses religion as a pretext to achieve its goals.

"It doesn't believe in national or human values and does not abide by laws or agreements. Countries are working collectively to eradicate terror through laws and agreements.

"This case is one of the most important that the Federal Supreme Court has dealt with and it has taken months, but the court was able to establish who founded, who joined and who participated in the group."

Judge Al Tunaiji ordered that the weapons be destroyed.

The other eight jailed for life: Mohammed Al Bloushi, Kalantar's Emirati second in command; Ahmed Yousuf, who holds a Comoros Islands passport; Iranian Abdulaziz Ahmed Ismail; and Emiratis Abdulrahman Mohammed Al Marzouqi, Abdulrahman Hussain Al Marzouqi and Mohamed Abdullatif Al Zaraooni. Emiratis Mansour Ali Al Shahari and Mohamed Abdullatif Al Zarooni were sentenced in their absence.

The whereabouts of the two is unknown.

Jailed for 10 years, along with Kalantar's sons, were Emiratis Jassim Al Bulooshi, Ibrahim Belshalat, Mohammed Al Raeesi, Khalil Al Shemaili, Hassan Bellaith, Saeed Sumbakh,

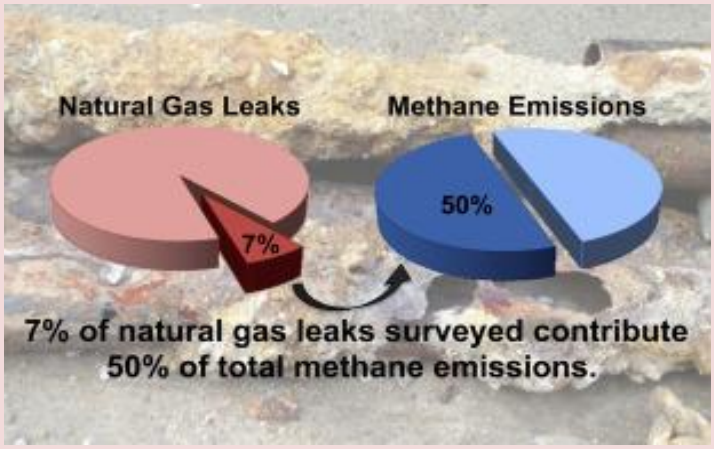
Naser Al Afifi, Ahmed Al Hammadi and Ali Al Bloushi, and Iranian Khalid Qashmi and Ezz Al Dein Makhlouta from Syria.
Emiratis Ghanim Al Marri and Assem Al Naqbi were given 15-year jail sentences for fighting in international terrorist organisations.
Mohamed Ahli, Nayef Al Mulla, Eissa Al Bloushi, Ahmed Al Ahmed, Ali Al Bloushi and Mansour Al Naqbi, all Emiratis, were jailed for three years.
Their compatriots Abed Al Shaer and Omar Al Janahi were jailed for five years.
Ahmed Al Bloushi, Abdulrahman Belshalat, Ali Al Bloushi, Jumaa Al Bloushi, Suhail Al Bloushi, Abdullatif Al Ahmed and Saleh Al Bloushi, all Emiratis, were acquitted of all charges.

The UAE established its anti-terror laws in 2004.

Clearer view of risky leaks from gas mains in Boston

Source: http://www.homelandsecuritynewswire.com/dr20160329-clearer-view-of-risky-leaks-from-gas-mains-in-boston

Mar 29 – **Precise measurements of leaks from natural gas pipelines across metropolitan Boston have demonstrated that almost a sixth of the leaks qualified as potentially explosive, and that a handful of leaks emitted half of the total gas lost.**
The findings by Boston University researchers differ significantly from results gathered by gas companies and other monitoring groups, and highlight the risks that these "fugitive" gas emissions pose both for safety and the environment, says Margaret Hendrick, a Ph.D. candidate in BU's Department of Earth & Environment.



BU reports that Hendrick is lead author on a paper published today in *Environmental Pollution*, which emphasizes the need to develop standardized ways to detect leaks and prioritize their repair.
Natural gas is considered a relatively clean fossil fuel, but a substantial amount of the gas is lost in production and distribution. In addition to the safety risks, methane (the main component of natural gas) is a major contributor to atmospheric warming.
Gas pipelines may date back as early as the mid-nineteenth century in east coast cities such as Boston. About a third of the installed pipelines use leak-prone materials such as cast iron, wrought iron or unprotected steel. There are thousands of gas leaks in these cities, but how the sizes of these leaks vary in an urban area "was a big black box until this project," Hendrick says.
She and her colleagues looked at emissions from cast iron pipelines at 100 sites in greater Boston where leaks had been detected in the air along roadways. The researchers painstakingly analyzed the release of methane inside custom-built chambers created with plastic buckets and the lids from child sandboxes. "To fully ascertain the safety hazards of leaks really does require us to get out on the ground with instrumentation," Hendrick explains.
This was the first survey that performed detailed measurements of loss from pipelines on this urban scale, says Professor of Earth and Environment Nathan Phillips, Hendrick's advisor and senior author on the paper.
Risk of explosion does not necessarily correlate with the amount of methane leaking, because the local environment around the leak also plays a part. "Even a very small leak can be a great safety concern," says Hendrick, who notes that a 2014 gas explosion in Dorchester injured twelve people. **There were 113 gas distribution pipeline incidents, with 18 fatalities, in the United States that year.**

The seven "super-emitter" leaks that released half the methane in the study also raise warning signs for climate change. Methane accounts for about one tenth of U.S. greenhouse gas emissions. **On average over a 20-year period, a methane molecule released into the atmosphere traps about eighty-six times as much heat as does a carbon dioxide molecule,** Phillips points out.

"We know we have a problem with aging natural gas infrastructure, but we need a better understanding of how big the problem is and the best ways to solve it," Hendrick says.

One major issue is a lack of agreement on the number of gas leaks. For instance, Phillips led a 2013 survey on all Boston city roads that found 3,356 gas leaks. The most recent estimate from an annual report filed by National Grid with the Massachusetts Department of Public Utilities (DPU), which regulates natural gas in the state, is about half that number.

Massachusetts categorizes gas leaks by risk, with potentially explosive leaks given a Grade 1 classification. The National Grid annual report cited a total of 36 Grade 1 leaks — but the BU fieldwork, identifying 15 out of 100 leaks as Grade 1, suggests that that figure may be low.

Even if all parties agree on how to assess gas leaks and prioritize their repair, fixing them will not be inexpensive, and the cost is borne by gas customers.

"We're stuck in this conundrum where if we were to retrofit this infrastructure quickly, there would be huge rate increases, and families might not be able to pay their utility bills," Hendrick says. "But it isn't if these old pipes will start leaking, it's when."

Bills now before the Massachusetts legislature may help to better address these challenges. In the meantime, the BU researchers encourage the public to stay watchful for any gas leaks. "People may become habituated to the smell of a gas leak, but if you smell one you should call it in to your local gas company," says Phillips.

While the first priority in dealing with leaks is to assure public safety, it's also critical to consider the climate implications, Hendrick emphasizes. Her paper proposes a leak classification scheme that includes both safety and climate risks.

"We are consuming more natural gas than ever before in the United States," she notes. "We need research to try to characterize fugitive methane emissions across the entire natural gas system."

That need is highlighted by the recent environmental disaster as natural gas escaped from storage in Porter Ranch, California — the worst such leak in U.S. history. "We're starting to realize that unless the entire natural gas system is better regulated, the carbon footprint may be just as bad for natural gas as it is for coal and oil," Hendrick says.

— Read more in Margaret F. Hendrick et al., "Fugitive methane emissions from leak-prone natural gas distribution infrastructure in urban environments," Environmental Pollution, 213 (June 2016): 710–16.

How to Detect Explosive Devices at Airports?

Source: http://www.cbrneportal.com/how-to-detect-explosive-devices-at-airports/

Mar 28 – More than ever before, the current situation and the climate in which we live in calls for important measures to protect the general public from threats coming from mischievous individuals such as extremist factions' members and other terrorist groups' adherents.

Being a hub for low cost airlines such as Ryanair and Jetairfly, the Brussels South Charleroi Airport welcomes almost 7 millions passengers each year.

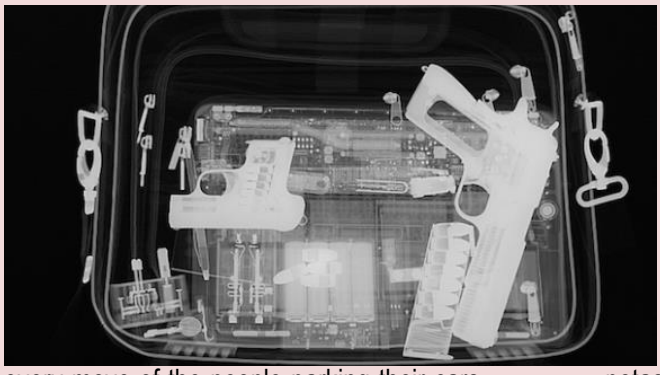
With thousands of people walking the halls of this buzzing public place, a premium security operation has to be put in place in order to ensure the safety of all these passengers and the 3,500 employees that work for the different airlines and the various restaurants, shops, and boutiques located all over the terminal.

That being said, who could be more qualified to talk to us about the security tactics and processes put in place to ensure the security of all these people, then Security Operations Chief, Abdel El Gharib?

My colleague, Greg and I seized the first occasion we got to interview the man in charge of the whole operation, and drove from our offices located in Welkenraedt to

Gosselies, Charleroi (46 km south of Brussels) to get a glimpse at the security measures implemented at the BSC Airport.

A quick ride later, Greg and I arrived in front of the BSC's terminal ready to start our examination. From the start, we could already see the extent of the operation. Indeed dozens of CCTV's were already in action observing the every move of the people parking their cars…. Mr. El Gharib's team already knew we had arrived for the interview.



Following a brief chitchat in front of the Check-in counters, Mr. El Gharib welcomed us inside the "control room", and we got to see behind the scene of the all Security Operation put in place to monitor the entire terminal.

Once inside, Mr. El Gharib proceeded to explain the process that takes place every time a suspect package or object is left unattended in the Airport itself, the parking lots, garages or at the bus and taxi stops.

According to Abdel El Gharib, a team of qualified operators and security agents are observing and assessing the entire facility thanks to HD cameras and by walking the site 24/7**.** If a suspect package is spotted, a security perimeter is set up instantly. The item is, therefore isolated and nobody is allowed to touch the object. From then on, the investigation begins…

You could believe that evacuation of the airport undergoes instantly, followed by the arrival of the EOD (Explosive Ordnance Disposal) or bomb squad teams… but this would actually results in a massive panic and involved important financial impacts.

Once the perimeter is set-up, the fact-finding process begins. First of all, the videotapes recorded during the day are scrupulously examined in order to identify the person responsible for abandoning the suspect objet.

Secondly, the first explosive test is carried out by a member of the Airport' security team with the help of a "sniffer"**,** which is basically what its name suggests: a device that "smells" the suspect object, and not unlike a dog, detects presence of explosive compounds.

Just by absorbing a very small quantity of the bag or object's composition, the machine, which is using Ion-mobility Spectrometry (IMS), is able to tell you whether that particular object has been in contact with explosives. You might have seen that particular technology before if you have been asked to swab your hands against a piece of paper before entering a high-protected building like an embassy or a government facility.

Unfortunately, this kind of test can easily produce false results… indeed, these "sniffers" are set up to detect common compounds such as glycerin and potassium nitrate, that are used in every-day life products, such as hand sanitizers and food additives.

Therefore, if the test reveals to be positive, then, a second test is carried out… by a dog! Machines are good; but dogs have a sense of smell that is 10,000 times better than the ones of humans. Moreover, these detection dogs have been trained for years to detect even the slightest trace of explosive, which makes them incredible defensive weapons against terrorism.

If the dog test is also positive, the situation becomes critical and more drastic measures ought to be taken.

But before calling the bomb squad in, the security team needs to make sure that a life-threatening device is actually inside the given object.

At that stage, it is time to bring out the big guns, a portable x-ray detection system, that allows the security team of the Brussels South Charleroi Airport to inspect inside the package without ever having to open it up – since doing so could trigger the explosion.

Since x-rays are ionizing radiations, a bigger security parameter is determined.

Once this is done, one of the six operators that counts the BSC Airport, easily obtain a clear and precise image of the interior of the object in just a few seconds, thanks to the **FLATSCAN** Technology – developed by the x-ray expert and Belgo-American company, Teledyne ICM.

▶ You can read the rest of this interesting article at source's URL.

Turkey – Six Police Officers Killed In Car Bombing

Source: http://news.sky.com/story/1670483/six-police-officers-killed-in-car-bombing

Mar 31 – Six police officers have been killed in a car bombing near a bus terminal in the Turkish city of Diyarbakir.

Another 20 people were wounded, including civilians, in what is a mainly Kurdish city in southeast Turkey.

The bomb detonated as a special forces bus passed, according to state-run media.

It damaged cars and shattered almost all the windows of a nearby high-rise.

At least six ambulances deployed to collect casualties and security forces rushed to seal off the area.

The city has suffered renewed violence since a ceasefire between the outlawed Kurdistan Workers Party (PKK) and the government collapsed last July.

A PKK offshoot has claimed two car bomb attacks this year in the capital Ankara - including one on a military bus that killed 29.

There has been no immediate claim of responsibility following the Diyarbakir blast.

CIA left explosive material on Loudoun school bus after training exercise

Source: https://www.washingtonpost.com/local/public-safety/cia-left-explosive-material-on-loudoun-school-bus-after-training-exercise/2016/03/31/428f9824-f78d-11e5-a3ce-f06b5ba21f33_story.html

Mar 31 – **The CIA left "explosive training material" under the hood of a Loudoun County school bus after a training exercise last week, a bus that was used to ferry elementary and high school students to and from school on Monday and Tuesday with the material still sitting in the engine compartment**, according to the CIA and Loudoun County officials.

The Loudoun County Sheriff's Office and the CIA said in statements Thursday that the explosive material was left behind after a training exercise at Briar

Woods High School during spring break. The CIA said it was a training scenario for explosives-detecting dogs.

CIA officials said in a statement that the material "did not pose a danger to passengers on the bus," which was used on March 28 and 29. Authorities held a joint training program at Briar Woods from March 21 to 24.

Loudoun schools spokesman Wayde Byard said the CIA indicated the nature of the material but asked the school system not to disclose it. Byard described it as a **"putty-type" material designed for use on the battlefield and which requires a special detonator; such putty, or plastic, explosives — including the well-known C-4 — are used in demolition and are considered stable.**

Byard said law enforcement agencies use school facilities on occasion to conduct realistic training exercises, including active-shooter drills.

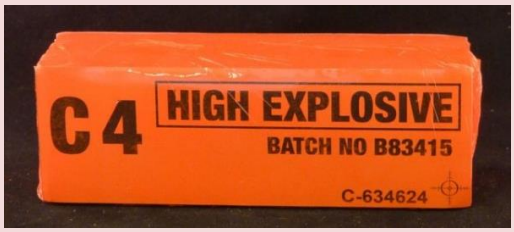
As part of last week's training exercise, CIA trainers placed explosive material into the engine compartment of a school bus on Thursday to test a dog's ability to sniff it out. They also placed the material in parts of the school. Byard said the dog successfully found the material in the engine compartment, but some of the material fell deeper inside the compartment and became wedged beneath the hoses.

He said school bus drivers check under the hoods of their buses before they take them out on the road, but the package was wedged too far deep inside the engine compartment and was the same color as the hoses, so it could not easily be seen.

The bus shuttled students to and from school for two days with the explosive material under the hood, making eight runs totaling 145 miles and carrying 26 students attending Rock Ridge High School, Buffalo Trail Elementary School and Pinebrook Elementary School.

The bus was taken to a school system facility on Wednesday for routine maintenance. Byard said the county's buses are regularly taken off-line to check their spark plugs, hoses and to rotate tires. It was during a routine inspection that a technician discovered the explosive material.

The school system immediately notified the county sheriff's office and the fire marshal, who removed it. The CIA also helped remove the material.



"The training materials used in the exercises are incredibly stable and according to the CIA and Loudoun County explosive experts the students on the bus were not in any danger from the training material," according to a Sheriff's Office statement.

Officials said they checked all other buses at the school as a precaution.

School officials on Thursday met with the CIA, Loudoun County Sheriff's Office, the fire marshal and county administrators and determined that all law enforcement training exercises at schools would be suspended until stronger protocols are established.

"We're all very upset by what happened, but we're going to review everything that did happen," Byard said. "Obviously we're concerned. The CIA really expressed its deep concern and regret today, and it was sincere."

CIA officials acknowledged the error in a statement and confirmed that an agency canine unit ran a training exercise with local agencies last week in the county. Agency officials said they were notified by Loudoun officials Wednesday and coordinated with them to recover the material.

The intelligence service said that both CIA and Loudoun County

experts said the explosive material did not pose a danger to passengers on the bus. The agency statement said they would take "immediate steps to strengthen inventory and control procedures in its K-9 program" and that they will investigate the canine training program.
The CIA said in the statement that the agency accounted for all training explosives after performing a full inventory Thursday.

How IEDs Work

By Craig Freudenrich, Ph.D.
Source: http://science.howstuffworks.com/ied1.htm

A neighborhood in Iraq reverberates with a deafening explosion. A military convoy has been hit by a roadside bomb. The explosion has left a crater in its wake, ripped apart vehicles and injured the soldiers riding within them. In a nearby marketplace, a suicide bomber blows himself up, maiming and killing scores of nearby civilians. These violent scenes have played out repeatedly in Iraq and Afghanistan since combat operations began there in the early 21st century.

It wasn't always this way. In the beginning of the Iraq war, U.S. soldiers were injured mainly from gunfire, mortars and grenades. The injuries are wrought now by a different source. The preferred weapon of insurgents and terrorists has become an **improvised explosive device**, or **IED**. You might call it a homemade bomb or a booby trap. Whatever you call it, an IED is relatively simple to make, easily hidden and very destructive.
Soldiers, civilians, as well as paramilitary and terrorist groups, have been building and detonating homemade bombs for years.

- During the Vietnam War, the Viet Cong hid IEDs in soda cans because they observed that U.S. soldiers liked to kick empty cans while marching along the roads [source: GlobalSecurity.org].
- The Irish Republican Army used them in the 1960s and 1970s during its struggles with the British in Northern Ireland.
- In 1996, Eric Rudolph made a pipe bomb (IED) and set if off in Atlanta's Centennial Olympic Park during the Summer Olympics. One person died and more than 100 people were injured in the attack.

You could fill volumes with all the IED attacks that have occurred within the last decade. That's because IEDs can be an effective strategy when facing a superior or more technological military force. Guerilla fighters, rebels and terrorists employ the weapons mainly to harass the military and to terrorize civilians and governments. Their use shows no signs of abating.
In fact, roadside bombs, which are typically IEDs, have reigned as the No. 1 killer of U.S. troops in Iraq, although the number of IED casualties dropped substantially in August 2008 [source: McMichael]. In Afghanistan, however, IED attacks are up 50 percent in 2008 [source: NPR]. No wonder the U.S. military is actively researching countermeasures.
This article will explore the destructive world of IEDs -- how they're made and detonated, why they're so prevalent, how they injure people and how to protect people from them.

Anatomy of an IED

Before we pick apart an IED, a refresher on more conventional bombs might be handy.

- **Landmines** are planted within a designated area (a minefield) and are intended to bring down entering soldiers or vehicles.
- Soldiers throw **hand grenades** over a short range

to clear an area of enemy personnel.

- **Rocket-propelled grenades**, or just RPGs, are launched over a larger range and can rid a target area of enemy personnel or destroy enemy vehicles.
- **Bombs** are dropped from planes, are self-contained and controlled to devastate anything within a specific area.

A cordless phone is a popular remote trigger for an IED since it may allow a signal to be transmitted up to a mile.

Such bombs are commercially made. Armies purchase these weapons from defense contractors for military and training operations, although other individuals can obtain them through the thriving black market for weapons.

In contrast, IEDs are homemade with five basic parts:

1. A power supply, often provided by car batteries or alkaline flashlight batteries
2. A trigger, switch or some other direct or indirect means of setting the device off, such as a radio signal, trip wire, timer or firing button that someone presses. A common form of remote trigger is a cell phone, cordless phone, radio or garage door opener activated by someone who is watching [source: GlobalSecurity.org].
3. A detonator, a small explosive charge that sets off the main charge. Detonators are usually electrical, like those used for explosions in construction.
4. A main charge, the primary explosive that's the big guns behind the blast. Unexploded landmines fit the bill.
5. A container to hold everything together. The container may be designed to force the blast in a specific direction.

Additional components packed in the device may include projectiles for shrapnel, such as ball bearings, nails and stones, as well as hazardous, toxic or fire-starting chemicals. IEDs may also be used as the explosive part of a biological or radioactive dirty bomb.

Let's look at how these parts work together:

1. The power source supplies electricity to the trigger or switch and to the detonator.
2. The trigger activates the detonator and initiates the explosion sequence. The trigger may sense the target, be activated by the target, be a timed trigger or be operated remotely.
3. The detonator explodes, thereby providing energy for the main explosive.
4. The main charge explodes, producing a high-pressure shock wave or blast wave, and may propel shrapnel, toxic chemicals or fire-starting chemicals.

Here's the distressing part: IEDs are relatively simple to make with a little research, time and training. After all, how hard is it to get batteries, cell phones and radios? Detonators and explosives such as C-4, Semtex and dynamite can be found at construction sites and oil rigs. They also may be stolen, purchased legally or cooked up at home or in a makeshift lab. Terrorist groups have been known to post recipes on their Web sites.

Once made, people tend to use one of three methods for delivering their weapon. Often they'll conceal the device in a package that may be in plain sight, hidden or buried. Insurgents have even hidden IEDs in animal carcasses alongside military convoy routes. They may also place the IED in a vehicle's trunk (**vehicle-borne IED** or **VBIED**). A driver may park the vehicle alongside a convoy route. A remote watcher can then detonate the VBIED from a safe distance. The last delivery method relies on a suicide bomber. The suicide bomber may drive a VBIED into the target area and explode it or strap the device on his or her body, walk into the intended target area and explode it. What happens when an IED explodes?

Bryan Anderson, a U.S. Army military policeman, lost three limbs after an IED exploded near his Humvee in Iraq in October 2005. Scott Olson/Getty Images

IED Impacts

Aside from how it's made, an IED is like any other bomb -- it explodes.

Before you can understand the impact of an IED, it helps to know what's happening during that fateful moment.

1. When the primary charge explodes, gases heat up and expand rapidly outward under pressure.
2. The expansion creates shock waves or blast waves. The waves travel outward at about 1,600 feet per second (488 meters per second) over hundreds of yards or more depending upon the amount of explosive.
3. The explosion fragments the container and sends pieces of shrapnel at high speeds outward. If the IED also contained other fragments such as ball bearings, nuts, bolts and pellets, then they also would be thrown outward.
4. The heat from the explosion causes fire.
5. The heat and fires from the explosion can cause secondary fires.
6. The blast wave leaves a partial vacuum, which causes air to rush back in under high pressure. The inrushing air also pulls in debris and shrapnel.

So, an IED explosion causes damage to vehicles and property primarily through the blast wave, heat and fires.

In contrast, casualties within the blast radius can stem from many causes. The explosion can release shrapnel or create debris from secondary impacts such as flying glass from broken windows. This debris can penetrate the body in many places, leading to lacerations, bleeding, broken bones and loss of limbs. Second, the heat from the blast causes fires; both the heat and the fires themselves can cause severe burns. Finally, the pressure in a blast wave can be on the order of 1,000 times atmospheric pressure. This intense pressure can rupture your eardrums and slam your brain against the inside of your skull, which leads to concussion, blindness, deafness and swelling of the brain. In addition, many air-filled tissues and organs such as the lungs and bowels can be perforated by the pressure changes.

The type and extent of the injury depends on the person's location relative to the IED. A person in the primary blast radius can be hit by pressure changes, heat and shrapnel. Most likely, this person will die. Outside the primary blast radius, a person is most likely to be injured by shrapnel. The person may survive depending on how many injuries the shrapnel causes and where they're located. If shrapnel tears a hole in a major artery, then that person can bleed to death.

Civilian casualties are often high in IED attacks because these people are unprotected. Initial injuries to U.S. soldiers from IED attacks were caused mainly by shrapnel. However, the use of Kevlar body armor and helmets has greatly reduced shrapnel injuries. While these types of injuries have fallen, military surgeons have reported increases in traumatic brain injuries caused by the blast effects

Defeating and Detecting IEDs

Insurgents and terrorists don't just go make a bomb and use it. IED attacks are the result of coordinated enemy activities such as financing, obtaining supplies, making IEDs, and planting and detonating them. So defeating these devices must involve a combined strategy of understanding and observing the enemy. Soldiers and personnel have to be trained to be aware of the enemy's behaviors, to look for indicators of IEDs in their patrol areas and to use technology to dispose or disable them. The U.S. Army's IED defeat strategy includes the following measures:

- Collecting data about enemy activities that might indicate upcoming IED attacks. This could be anything from observing suspicious activities of people within the combat area to tracing or disrupting the movements of supplies and money.
- Detecting the IEDs themselves
- Disposing of or disabling the detected IED
- Protecting military personnel and civilians from a detected IED

Training soldiers to be keen observers in combat operations is important. For example, a U.S. Marine spotter near Habbaniyah, Iraq, noticed a man who was videotaping a nearby patrol of assault vehicles. The man had a high-powered rifle in his car next to him. After a sniper shot the man, soldiers discovered a cache of IED materials and munitions in the car.

Likewise, soldiers or other personnel should be trained to be suspicious of unattended packages along a road, fence, building or even a trash pile. IEDs are easy to hide. Simulating more IED attacks during military training will help soldiers to detect and deal with these attacks before encountering them in combat.

Besides training soldiers, some new technologies are capable of

detecting, disrupting or disabling IEDs. These technologies are designed to place a "bubble" of protection around troops operating in combat situations. For example, many combat vehicles are now equipped with radio frequency jamming devices, which disrupt the cell phone signals often used to trigger IEDs.

Another device called a **NIRF**, which stands for neutralizing improvised explosive devices with radio frequency, emits a high frequency radio pulse that deactivates IED electronics within a short area. Microwave-pulsing devices also can be used to "fry" the electronics of IEDs. Another device called LIBS (laser-induced breakdown spectroscopy) uses lasers to detect IED explosives within a 100-foot (30-meter) radius.

Alternatively, you might not need a soldier to deal with a suspected IED at all. The military is exploring using robots and drones to protect people from IEDs. Aerial drones may be able to detect IEDs or suspicious activities without exposing troops, while robots can search areas for the suspected devices or handle shady looking packages without involving soldiers.

What about protecting soldiers during an attack if the detection methods fail? Kevlar body armor has shielded soldiers from the shrapnel released in an IED explosion. In addition, armored vehicles have been redesigned with the blast impacts of an IED in mind. These vehicles are called **Mine Resistant Ambush Protected** (**MRAP**) **vehicles** (photo). Essentially, the usual flat undercarriage of a vehicle is changed to a **V-shaped undercarriage, which diverts the blast waves from an explosion underneath around the vehicle rather than into it.** Because IED attacks are a favored strategy in modern war, the U.S. Department of Defense continues research aimed at IED countermeasures.

Craig Freudenrich, Ph.D., *is a freelance science writer and former senior editor at HowStuffWorks. He earned a B.A. in biology from West Virginia University and a Ph.D. in physiology from the University of Pittsburgh School of Medicine before completing eight years of postdoctoral research at Duke University Medical Center.*

Pot grinder that looked like a grenade closed Bellingham's airport temporarily

Source: http://kgmi.com/news/007700-pot-grinder-that-looked-like-a-grenade-closed-bellinghams-airport-temporarily/

Apr 10 – **A marijuana grinder that looked like a grenade triggered a bomb squad response Saturday morning at the Bellingham International Airport,** according to a spokesperson.

Marie Duckworth with the airport says the grinder was found at the security checkpoint. "Out of an abundance of caution, we called in the experts," said Duckworth. The security area was evacuated and all flights were held during the investigation.

Once the Bellingham Police Department bomb squad arrived on scene, Duckworth said it didn't take them long to realize it was not an explosive, but rather a tool used to grind marijuana buds.

HAZMAT Unit arrives at the airport

The suspicious object

"I really want this to be a teachable moment," said Duckworth. She says the safety and security of passengers is their highest priority, and that's why they called in the bomb squad.
Flights were held for a little over an hour, but service at the airport returned to normal by afternoon.

Sex bomb: Mass evacuation sparked by 'suspicious buzzing' at gambling hall in Germany found to have been caused by vibrating penis ring

Source: http://www.dailymail.co.uk/news/article-3526399/Sex-bomb-Mass-evacuation-sparked-suspicious-buzzing-gambling-hall-Germany-caused-vibrating-penis-ring.html

Apr 06 – German police called to the scene of a suspected bomb could breathe a sigh of relief when the feared explosive device turned out to be a sex toy.

Police evacuated a gambling hall in Halberstadt, some 85miles south-east of Hanover, Saxony-Anhalt, after reports of a humming noise in a bin.
A bomb squad was called in, but officers were soon able to declare it a false alarm, after discovering that the buzzing was a penis ring.
Police were called to the gambling hall in Halberstadt after a member of staff reported hearing suspicious vibrations echoing from a metal garbage bin in the men's toilet, police said.
More than 90 people were evacuated from the business and nearby premises, and a nearby street was closed off.
Three explosives experts of the Office of Criminal Investigation in the state of Saxony-Anhalt were called in to defuse the 'bomb'. However, when the bomb squad examined the bin, they found that the explosive device was in fact a battery-powered vibrating penis ring.

Imaging drones to spot signs of explosive chemicals leaking from landmines

Source: http://www.gizmag.com/drones-landmines-bristol/42732/

.

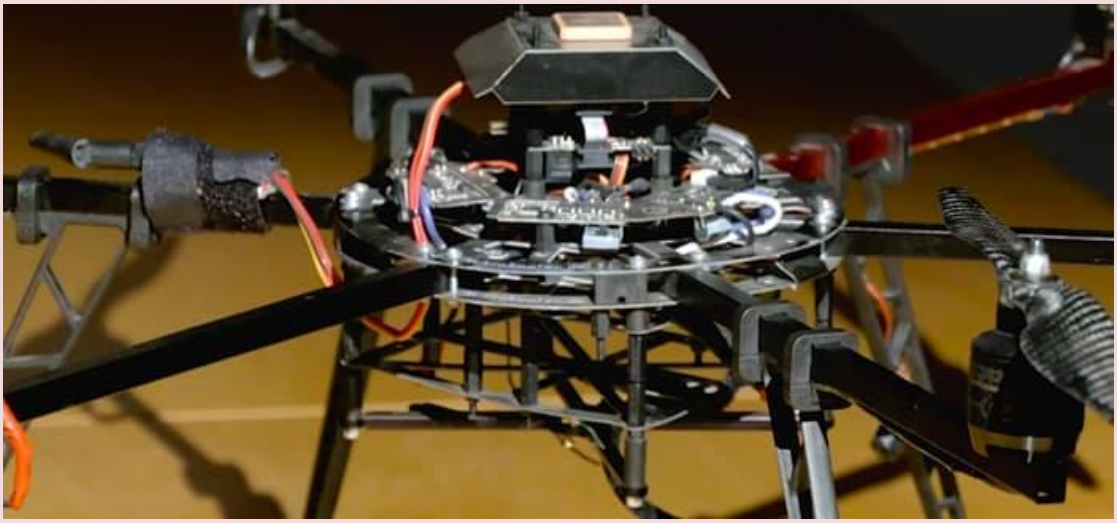
Apr 10 – **Care estimates there are some 110 million landmines buried around the world, with more than 70 people killed or injured each day by these deadly devices. Locating and disabling landmines is not only a meticulous and time-intensive task, but an incredibly dangerous one as well.** Working to help keep humans out of harm's way, British scientists are developing drones with advanced imaging technology to more effectively map and speed up the clearing of affected areas.

Flying a drone over a football stadium would normally incite all kinds of outrage from protective managers determined to safeguard their secret tactics. But last week at Old Trafford, the home of global footballing giant Manchester United, an unmanned aircraft was given free rein as researchers demonstrated the potential of an airborne approach to landmine detection.

Funded by Manchester United legend Sir Bobby Charlton, the Find A Better Way charity has been working since 2011 to advance technologies that will enable safer and more efficient clearance of landmines. Its latest push in this area involves teaming up with scientists at the University of Bristol to deploy drones that can quickly identify landmines buried in the ground.

The Old Trafford flight saw the drone snap only high-res images to clearly show the terrain and objects on the ground, but this is only the first step. If the team's hyperspectral imaging drones come along as hoped, they will be able to perform flyovers and gather images at various wavelengths, or colors, of light, which could indicate explosive chemicals seeping from landmines into the surrounding foliage.

"Living plants have a very distinctive reflection in the near infrared spectrum, just beyond human vision, which makes it possible to tell how healthy they are," explains Dr John Day from the University of Bristol. "Chemicals in landmines leak out and are often absorbed by plants, causing abnormalities. Looking for these changes might be a way of discovering the whereabouts of mines."



The researchers estimate that removing the landmines scattered across the globe using current technologies would cost around US$30 billion and take more than 1,000 years. They plan to significantly cut these numbers by fitting drones with hyperspectral imaging technology to quickly identify where mines are buried.

"Flying over the Manchester United pitch will demonstrate that we can map a football pitch-sized area of land in two hours or less," said John Fardoulis, project researcher from Bristol University. "Clearing a minefield that size can currently take months, and the maps our drones will generate should help deminers focus on the places where mines are most likely to be found. This will speed the process up and make the demining significantly safer."

The researchers also note that infrared imaging can expose unexploded and camouflaged mines that would otherwise go undetected.

The Bristol team isn't the only group turning to drones to combat landmines. Last year at the $1 million Drones For Good competition, Spanish company CATUAV was selected as a finalist for a drone fitted with optical sensors to scan war-affected regions of Bosnia and Herzegovina for landmines buried during the 1990s.

The British research effort kicked off in January 2016 and will last two years. The team is developing the technologies to work with commercially available drones, with a view to making the devices affordable and accessible in developing countries.

▶ **You can hear from some of the researchers involved in the video (click on source's URL).**

Sikh temple: Three people injured in explosion during festival in Essen

Source: http://www.independent.co.uk/news/world/europe/sikh-temple-three-people-injured-in-explosion-at-wedding-in-germany-city-of-essen-a6987681.html

Apr 17 - **German police have revealed that three people have been injured in what was apparently deliberate explosion at a Sikh temple in the western city of Essen.** The attack happened as a celebration was being celebrated at the temple, or gurdwara.

A spokesman for Essen police told the *Associated Press* that a masked person was reported to have fled the scene shortly after the blast at 7pm.

Spokesman Lars Lindemann said the explosion was "quite violent", blowing out several windows. One of the injured was said to be in a serious condition.

Local media subsequently said that three people had been arrested and were being questioned in connection with the incident.

Sikh groups said the incident took place as people were celebrating the Sikh festival of Vaisakhi. Celebrations taking place inside the gurdwara and children's classes were also taking place.

Mr Lindemann said the police were working on the assumption that the explosion was caused deliberately but that there are no indications it was a terrorist incident. **He says the temple had hosted a wedding earlier in the day and those injured are believed to have been among the guests.**

Inspectors smuggle bomb parts through Cologne airport

Source: http://www.thelocal.de/20160418/authorities-smuggle-weapons-bomb-parts-through-cologne-airport

Apr 18 – **EU authorities have managed to smuggle dangerous weaponry through Cologne-Bonn airport, raising concerns about the effectiveness of security controls there.**

During so-called "open tests" conducted in February, nine of the 12 banned objects which EU authorities tried to smuggle through airport security were not found, the Rheinische Post reported on Monday.

In undercover testing meanwhile they were able to to smuggle six of twelve weapons or bomb parts through the x-ray units without the security personnel noticing.

The results were seen by public broadcaster WDR but are considered highly secret and will not be published.

Kötter Aviation, the company responsible for the security checks at the airport, said in a statement on Friday that its employees passed 98 percent of tests conducted by the German federal police.

"In this respect were are surprised at the results of the tests conducted by the EU inspectors at Cologne-Bonn airport," said managing director Klaus Wedekind.

Wedekind said he had taken immediate action in light of the test results to further train his employees but states that success in tests carried out by the police showed "the very high performance of our employees."

German airports don't have a spotless record when it comes to scrutiny from the EU over security arrangements.

In May 2015 the European Commission started legal proceedings against Germany for not adequately checking security measures at its airports. In July, the interior ministry conceded that "quality control checks weren't carried out to the necessary extent or with the necessary regularity." At the end of 2014, meanwhile, EU inspectors found gaps in security procedures at several airports including Frankfurt, the country's largest air hub.

Authorities were able to successfully smuggle dangerous objects through security on half their attempts at that time, and cited poor levels of training among security personnel as the principal cause.

Carnegie Mellon Tor Attack Confirmed

Source: http://i-hls.com/2016/03/carnegie-mellon-tor-attack-confirmed/

Mar 17 – **Despite repeated denials by the US government, a federal judge has now confirmed that Carnegie Mellon University (CMU) was commissioned by the government to break the encryption of the ultra-secure Tor network**.

Tor, the so-called "onion router," is a privacy network that hitches a ride over the regular internet. Like an onion, each layer is opaque to the other. Connect to an entry node to the network, and the darknet is laid out before you. There, a range of users roam, from privacy-aware law-abiding citizens, to the seedy underbelly of society. The drugs marketplace Silk Road found its home there until it was shut down, and child pornography is spread through sordid sites on the network.

But, journalists and activists under oppressive regimes find unmonitored means of communications through the network, and even the US International Broadcasting Bureau (think Voice of America and Radio Free Europe) supports the development of the network.

Details of the operation are murky, but a few things are clear. It was not the FBI who approached CMU as was long suspected, but an agency under the Department of Defence umbrella. This points, in all likelihood, to either National Security Agency (NSA) or the whacky kooks at the Defense Advanced Research Projects Agency (DARPA).

A large number of entrance and exit nodes were operated on the network by CMU's Software Engineering Institute (SEI), the purpose of which was demasking and deanonymising the network and its users. The attack relied on a number of vulnerabilities in the software, and could potentially unmask new servers within a fortnight. **This led to the arrest of Brian Farrell, the operator behind Silk Road 2.0.** It is through his case that details of the cooperation have emerged. Most details of the case are still under wraps, and it is unclear if they will be released.

The Tor Project told *Motherboard* that "The Software Engineering Institute ("SEI") of Carnegie Mellon University (CMU) compromised the network in early 2014 by operating relays and tampering with user traffic. That vulnerability, like all other vulnerabilities, was patched as soon as we learned about it. The Tor network remains the best way for users to protect their privacy and security when communicating online."

Belgium's nuclear plants face threat of cyber-attack

Source: http://m.news24.com/news24/World/News/belgiums-nuclear-plants-face-threat-of-cyber-attack-

Mar 26 – **Belgium's network of nuclear power plants and other major infrastructure face the threat of a cyber-attack over the next five years,** the European Union's counter-terror chief said in an interview published on Saturday.

"I would not be surprised if there was an attempt in the next five years to use the Internet to commit an attack," Gilles de Kerchove told daily La Libre Belgique.

"It would take the form of entering the SCADA (Supervisory Control and Data Acquisition), which is the nerve centre of a nuclear power plant, a dam, air traffic control centre or railroad switching station," he added.

His concerns come as Belgium is on high alert following Tuesday's suicide bombings at Brussels airport and aboard a metro train that killed 31 people and injured some 300.

Belgium's neighbours have raised concerns over the country's creaking nuclear plants for some time, after a series of problems ranging from leaks to cracks and an unsolved sabotage incident.
Doel 1, the country's oldest reactor, was originally shuttered in February 2015 under a law calling for the country's gradual phasing out of nuclear power, but the government then restarted it under an extension deal.
According to reports, a security guard at a Belgian nuclear power plant was murdered on Thursday and his access badge stolen. Officials were not immediately available to comment.
These reports follow the discovery by investigators last year of surveillance footage of a Belgian nuclear plant official in the flat of a suspect linked to the Brussels and Paris attacks.

EDITOR'S COMMENT: Indeed the cyber threat is much more valid than an aerial attack against a nuclear power plant or steel material for a RDD or RED. So what are we going to do about this? NOW!

Syria-Linked Hacking Group Gains Access to Water Plant

Source: https://www.clarionproject.org/news/syria-linked-hacking-group-gain-access-water-plant

Mar 29 – **A "hacktivist group with ties to Syria" has hacked into the control system of a water treatment facility and altered the ratio of the chemicals in the water,** according to technology news site *The Register.*

The hackers "managed to manipulate the system to alter the amount of chemicals that went into the water supply and thus handicap water treatment and production capabilities so that the recovery time to replenish water supplies increased" according to an investigation conducted by forensic experts working for Verizon Security Solutions.
Staff was able to quickly identify and reverse the changes and at no point did the water become poisonous.
No motive for the attack has been confirmed and the location of the plant, owned by Kemuri Water Systems, has not been revealed.

Jihadists have attempted to hack water plants before. In 2002 federal officials arrested two Al-Qaeda suspects who planned to poison water supplies in the US. In 2003 an Al-Qaeda spokesman threatened to poison water supplies in Western cities.
An accomplice of Khalid Sheikh Mohammed, the mastermind of 9/11, admitted to plotting with him to poison water reservoirs in America. More recently in 2015 the Islamic State are believed to have plotted to poison water supplies in Kosovo, leading to security services cutting off the water supply of the capital city Pristina.

FBI cracks terrorists' iPhone without Apple's help

Source: http://www.homelandsecuritynewswire.com/dr20160329-fbi-cracks-terrorists-iphone-without-apples-help

Mar 29 – The Justice Department on Monday asked a court to withdraw the government's request that the court order Apple to help the FBI gain access to the encrypted iPhone used by the San Bernardino terrorists. The Justice Department filed the request after the FBI had successfully accessed data stored on an encrypted iPhone.
The FBI wanted the court to compel Apple to relax the 10-attempt limit, which is part of the encryption system which comes with the device. If there are more than ten attempts to guess the password, the phone locks forever and all the data on it is wiped out. The FBI argued that its computers, using brute-force, would be able to break the phone's password, but that it would take more than ten attempts.

The court initially agreed with the government, but Apple appealed the decision.

On Monday eight days ago, the Justice Department had asked the court to delay its ruling because the FBI had been approached by a third party, which offered an alternative method for opening the iPhone.

The *New York Times* reports that in Monday's two-page court filing, the Justice Department said the government "no longer requires" Apple's assistance and asked a federal magistrate in Riverside, California to withdraw the order to force Apple to assist.

In its own argument before the court, Apple argued the government request would create a "back door" to the company's devices which could be abused by hackers and governments agencies.

Eileen Decker, a federal prosecutor in Los Angeles, said on Monday that the government's request to Apple was part of a "solemn commitment" to the victims.

She said: "Although this step in the investigation is now complete, we will continue to explore every lead, and seek any appropriate legal process, to ensure our investigation collects all of the evidence related to this terrorist attack."

The *Times* notes that the government's withdrawal of its request does not put an end to the issue but instead raises new questions, including questions about the strength of security in Apple devices. Apple, for its part, may now demand that the government disclose the method the FBI used to open the device so the company could fix the vulnerability in its encryption method. Lawyers for Apple have already put the government on notice that the company would want to know the procedure used to break the phone's encryption – but the government may decide to classify the method.

"From a legal standpoint, what happened in the San Bernardino case doesn't mean the fight is over," Esha Bhandari, a staff lawyer at the American Civil Liberties Union, told the *Times*. She notes that the government generally goes through a process before it decides whether to disclose information about certain vulnerabilities so that manufacturers can patch them.

"I would hope they would give that information to Apple so that it can patch any weaknesses," she said, "but if the government classifies the tool, that suggests it may not."

Melanie Newman, a spokeswoman for the Justice Department, also indicated that the broader battle over access to digital data from devices was not over.

"It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties, or through the court system when cooperation fails," Newman said. "We will continue to pursue all available options for this mission, including seeking the cooperation of manufacturers and relying upon the creativity of both the public and private sectors."

Cryptography experts urged the government to share its information with Apple. "Courts should be skeptical going forward when the government claims it has no other option besides compelling a device maker's assistance," Riana Pfefferkorn, a cryptography fellow at the Stanford Center for Internet and Society, told the *Times*.

"Now that the F.B.I. has accessed this iPhone, it should disclose the method for doing so to Apple," she added. **"Apple ought to have the chance to fix that security issue, which likely affects many other iPhones."**

Hacking Hospitals And Holding Hostages: Cybersecurity In 2016

Source: http://www.forbes.com/sites/kalevleetaru/2016/03/29/hacking-hospitals-and-holding-hostages-cybersecurity-in-2016/#778ed2003e2e

Mar 30 – **Yesterday morning MedStar Health became just the latest organization to suffer the damage of a cyberattack in what early reports suggest may be yet another ransomware attack.** Unlike traditional cyberattacks designed to exfiltrate records, delete data or physically damage computing systems, ransomware attacks appear to be on the rise due to the ease in which such extortion translates directly to money in the pockets of cyber criminals. If MedStar's cyberattack turns out to be ransomware, it would join at least three other

medical institutions breached in just the last few weeks. Combined with the anonymity of bitcoin and the rise of targeted attacks focused on soft targets like hospitals, 2016 is shaping up to be a bountiful year in the extortion business.

While the underlying technology has been around for several decades, ransomware has enjoyed a renaissance of sorts with the confluence of improved targeting, the all-digital workplace and bitcoin to provide secure anonymized funds transfer. Modern ransomware attacks increasingly target small business, local government and medical institutions due to their historically poor cyber posture. Medical facilities in particular are proving to be a target-rich environment in that they are all too often a hodgepodge of outdated systems and rushed employees with little cyber training. Hospitals can ill-afford the downtime of restoring from backups or shutting down their systems for extended periods of time and so may be viewed in the eyes of cyber criminals as more likely to pay up without a fight.

The Hollywood image of a hospital held hostage by hackers burst into national headlines last month when Hollywood Presbyterian Medical Center announced it had been infected by ransomware and elected to pay the ransom in order to restore access to its files. The dystopian nightmare of an entire city being held hostage has even become reality as municipalities are finding their outdated IT infrastructure a severe liability.

As ransomware tactics have evolved, attacks have shifted from high-volume blind targeting to carefully orchestrated breaches in which the attackers sometimes burrow into a victim's network for months in order to infect the furthest corners of the network and encrypt or corrupt backup files, making payment the only way to get back the missing data.

In the physical world, law enforcement acts as a deterrence to a group of criminals raiding a hospital and holding its workers and patients hostage and will respond quickly and in force to end any hostage situations that do occur. In the cyber domain, however, law enforcement is largely absent, unable to offer any meaningful deterrence or protection. **When a cyber hostage situation does occur, all police can do is conduct a postmortem at best.** Even if a victim is able to definitively identify its attackers, they are frequently based outside of law enforcement jurisdiction and the legal rights of a company to launch its own cyber operations to forcibly end an attack and recover its data are murky at best.

Even banks are no longer safe in the cyber world. While robbing the New York Federal Reserve is usually limited to Hollywood blockbusters the Bangladesh Central Bank learned last month that bank robbers today are increasingly using computers instead of guns when hackers transferred more than 100 million dollars out of its accounts at the Federal Reserve. An Austrian aerospace company similarly lost 54 million dollars this past January when hackers got ahold of login credentials for its corporate treasury management system. Government itself, including its most senior intelligence and national security officials are no better off when a single phishing email can redirect their home phone service and personal email accounts.

Today such ransomware attacks are largely the work of criminal actors looking for a quick payoff, but the underlying techniques are already part of military planning for state-sponsored cyberwarfare. Russia showcased the civilian targeting of modern hybrid operations in its attack on Ukraine's power grid, which included software designed to physically destroy computer equipment. Even the US has been designing crippling cyberattack plans targeting the civilian sector. In case its nuclear negotiations with Iran failed, the US was prepared to shut down

the country's power grid and communications networks.

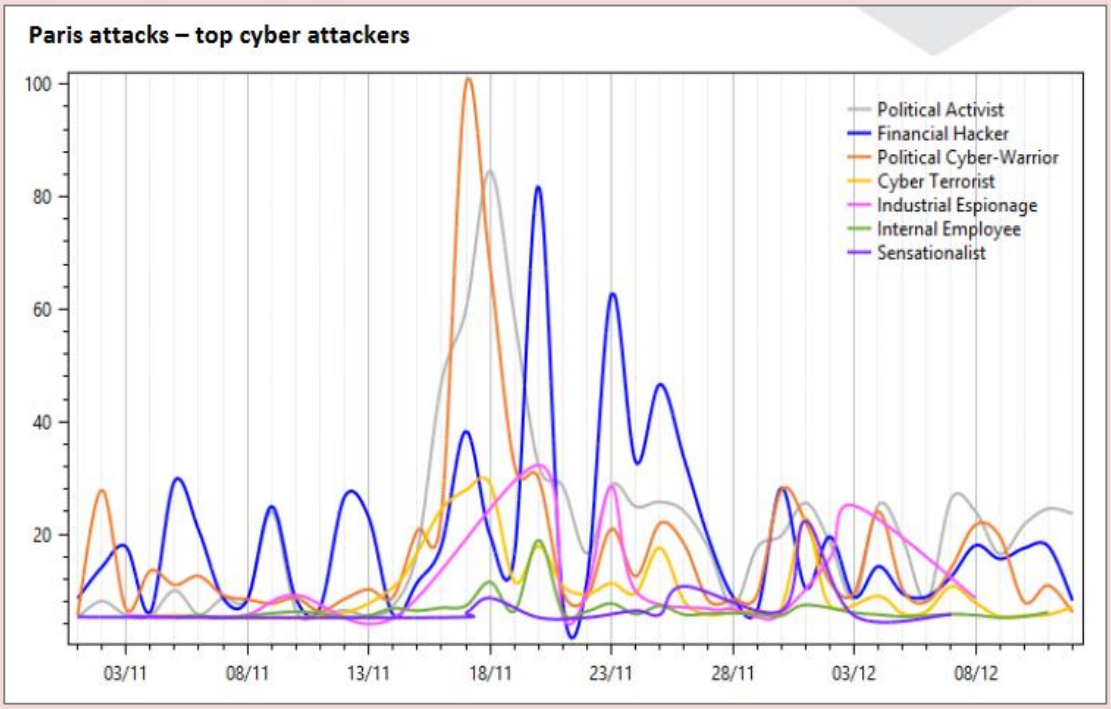
Imagine a future "first strike" cyberattack in which a nation burrowed its way deeply into the industrial and commercial networks of another state and deployed ransomware across its entire private sector, flipping a single switch to hold the entire country for ransom. **Such a nightmare scenario is unfortunately far closer than anyone might think.**

Researchers Claim Correlation Between Terror Attacks, Cyber-Activity

Source: http://mobile.eweek.com/security/researchers-claim-correlation-between-terror-attacks-cyber-activity.html

Mar 31 – **An Israeli security research company Cytegic claims there are predictable cycles of cyber-attacks just before and after major terrorist atrocity, such as the March 22 bombings in Brussels.**

The links between cyber-warfare and terrorism are well-established. Terrorist organizations such as ISIS have been attacking targets they perceive as unfriendly nearly since their inception.



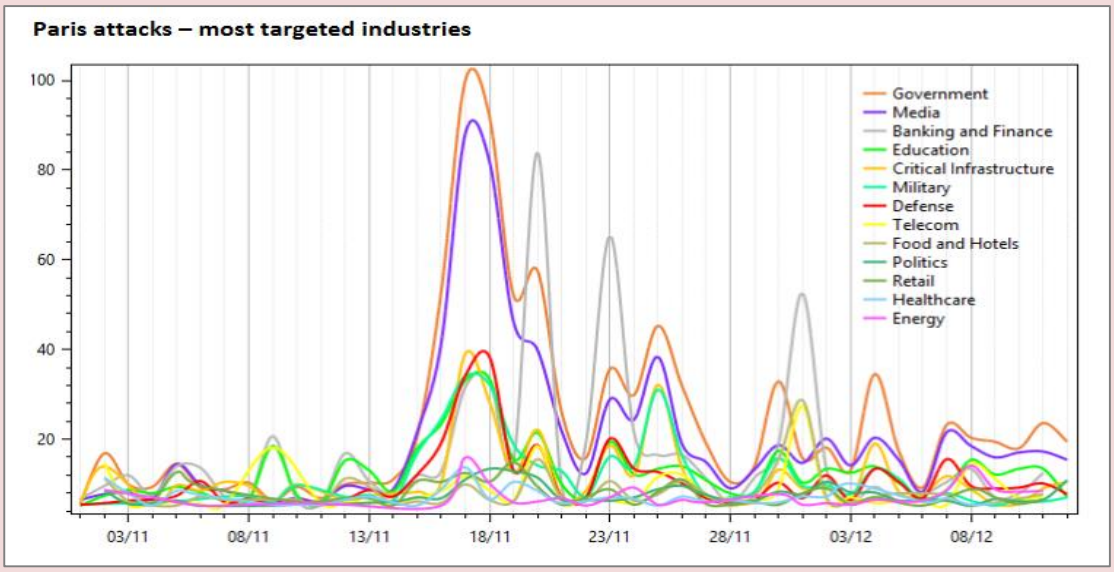
Now, researchers at Cytegic report that they have discovered a link between terrorist attacks, such as the deadly attacks on the Brussels airport and metro system on March 22, and cyber-terror activities immediately before and after those attacks.

According to the activity graphs in its March 23 report on the link between the terrorist attacks in Paris last November and the related cyber-terrorist activity, cyber-attacks increase dramatically shortly after the attacks took place.

Those attacks were aimed in large part against government and media activities on the Internet, and took the form of denial-of-service (DoS) attacks, defacements, phishing attacks including email social engineering and malware injection. Financial service organizations and critical infrastructure were also high on the target list, but not as high as the first two.

Perhaps most surprising of all, there appears to be a reduction in activity immediately preceding the terrorist attacks in both Paris and Brussels. This "quiet period" isn't a cessation of all cyber-terrorist activity, but rather a reduction in intensity. Some attackers seem to continue at their normal level, while others, who are identified by Cytegic as being cyber-terrorists, show a significant decrease until the attacks take place.

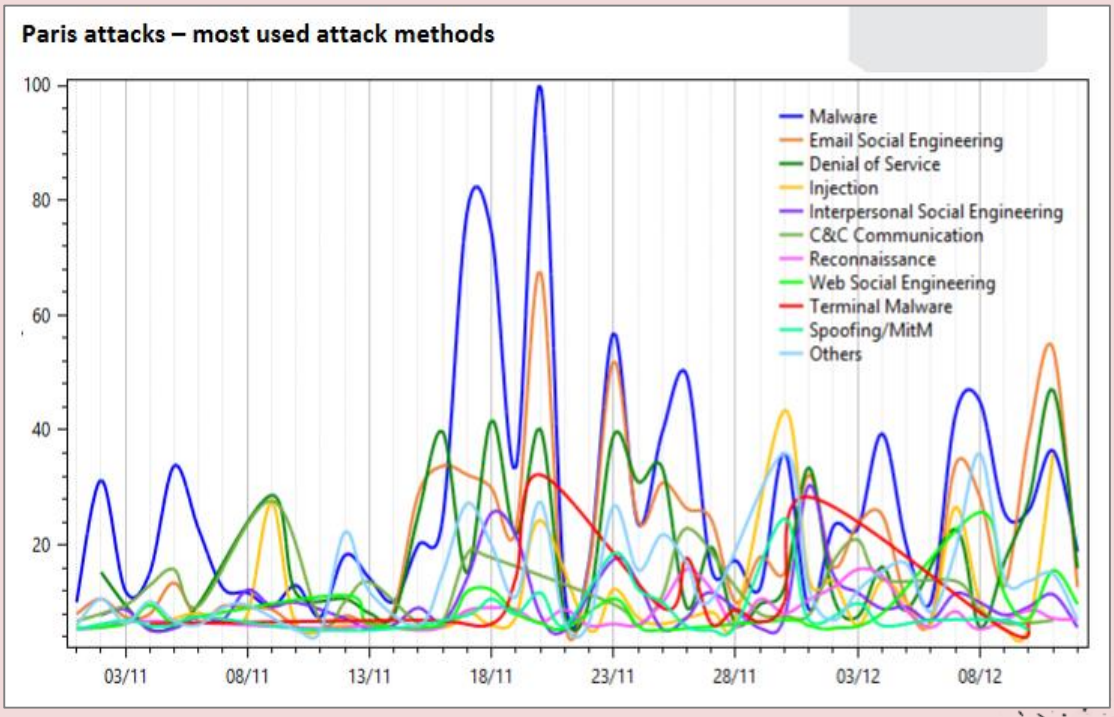
It's worth noting that cyber-attackers are comprised of several types. There are the attackers that are directly sponsored by the terrorist organizations; there are sympathizers and activists that may be inspired by the terrorists, but don't work directly for them; and then there are cyber-attackers who are unrelated to terrorist organizations.



After a terrorist attack, the cyber-attack activity picks up markedly. Within a day or so after an attack the cyber-terrorists ratchet up their activity, but so do government-sponsored attackers who are fighting the terrorists, and independent groups such as Anonymous, which have begun fighting the terrorists on their own.

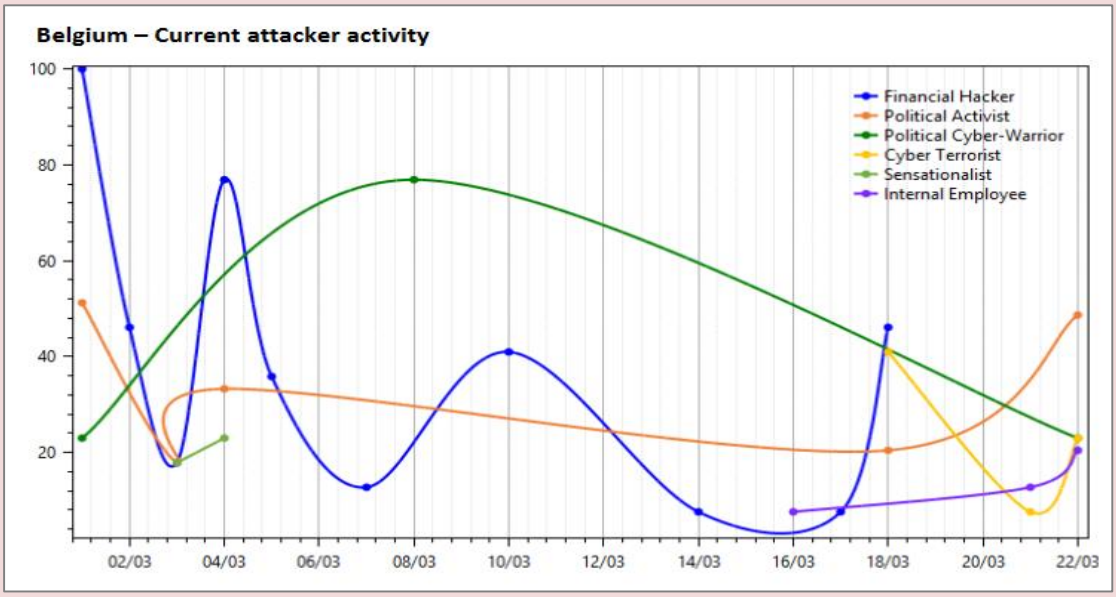
The activity both by and against the terrorist organizations continues for a period of about three weeks, according to the Cytegic study, after which it returns to whatever passes as normal these days.

Cytegic CEO and co-founder Shay Zandani told *eWEEK* that his researchers gather their information from public sources plus a number of sources on the Dark Web. The data that they gather is processed by what Zandani calls a thesaurus engine to reveal the specific patterns in the attacks. The engine



analyzes key words in the data to determine how the attacks are taking place and who is carrying out the attack.

"We think that if one can isolate specific geopolitical data and industry sectors for specific information, one can identify a pattern of behavior," Zandani said. By discerning a pattern of behavior, he said it's possible to proactively protect against the attacks.



When compared against the attack methods, he said it would be possible to determine what steps to take following a major terrorist attack.

Zandani said that organizations can work with their ISPs to prepare for an expected distributed-denial-of-service attack, and to take steps to prevent defacement of their Web presence. He also suggests that this would be a good time to reinforce training on how to combat phishing and other social engineering attacks.

Organizations should also harden their security incident management rules and prepare their security operations center in advance of the expected increase in activity.

Anti-ISIS activities carried out by military and intelligence services and by Anonymous will also have some limited effect on other organizations, but mostly because of potential network congestion if they launch a DoS attack against ISIS or an affiliated group.

Unfortunately, the level of cyber-attack activity immediately before and after a terrorist attack can tell you only so much. The reduction just before an attack does not appear to be location-specific, so predicting a terrorist attack on the basis of such activity is unlikely. In addition, Zandani said that there are similar patterns before and after other major activities, such as the NFL Super Bowl held in February and perhaps before and after major elections.

Perhaps the best lesson that can come out of the preparation for a cyber-attack is that it will demonstrate whether your organization is actually prepared to effectively manage such an event. "It shows where you need to invest more resources," Zandani said.

He also noted that companies can use the changes in cyber-activity to fine tune their security alerts and responses since they know that there may be a predictable increase for a three-week period after an attack.

Right now most of the change in activity seems to be focused on Europe because that's where the increase in ISIS-sponsored terrorist attacks is taking place. But Zandani said that such activity is a good reason to start beefing up your defenses wherever your organization operates. For example, he noted that investing in improved logging systems would provide better alerts when a cyber-attack does take place.

While there's nothing most organizations can do in response to the terror attacks if they weren't directly affected, there's a lot they can do to prevent or mitigate the cyber-attacks that may follow.

The day or two gap between the terror attack and when the related cyber-campaign starts ramping up is enough for most organizations to make sure their defenses are in place.

As tragic as those terrorist attacks may be, there's no need to sit still for a crippling follow-up cyber-attack if you can prevent it by taking advantage of the warning that the attacks provide.

Personal details of 50 million Turkish citizens leaked online, hackers claim

Source: http://www.telegraph.co.uk/news/2016/04/04/personal-details-of-50-million-turkish-citizens-leaked-online-ha/

Apr 04 – **Hackers claim to have accessed the personal details of nearly 50 million Turkish citizens and posted them online in a massive security breach that could seriously embarrass the country's government.**

If confirmed, it would be one of the biggest public leaks of personal data ever seen, experts said - effectively putting two-thirds of the country's population at risk of fraud and identity theft. AP reported on Monday that it had partially verified the leak as authentic.

Personal information including national identity numbers, addresses, dates of birth and names of parents were all posted online in a downloadable 6.6 GB file.

The data was accompanied by an online statement headlined Turkish Citizenship Database that made some taunting stabs at Turkey's ruling establishment and its Islamist-rooted Justice and Development Party (AKP) government.

"Who would have imagined that backwards ideologies, cronyism and rising religious extremism in Turkey would lead to a crumbling and vulnerable technical infrastructure?," it read.

Significantly, the details included those of Recep Tayyip Erdogan, Turkey's authoritarian president, at whom the leak appeared to be partially targeted, judging by some highly politicised comments on the accompanying statement.

Under the heading Lessons for Turkey, the poster wrote: "Do something about Erdogan. He is destroying your country beyond recognition."

The leak also purported to disclose the details of Ahmet Davutoglu, the Turkish prime minister, and Abdullah Gul, Mr Erdogan's predecessor as president.

Other "lessons", offered in bullet points. made mockingly dismissive references to the Turkish authorities' internet security procedures. They stated: "Bit shifting isn't encryption; Index your database. We had to fix your sloppy DB work; Putting a hardcoded password on the UI [user interface] hardly does anything for security."

The message also addressed Donald Trump, the Republican frontrunner in the American presidential election, in terms that suggested the hackers were United States citizens. "We really shouldn't elect Trump, that guy sounds like he knows even less about running a country than Erdogan does," it read under a final section headlined Lesson For The US.

The site appeared to be hosted by an Icelandic group specialising in divulging leaks, using servers in Romania, AP reported.

Hackers have a track record of targeting Turkey. One hacking episode by the group Anonymous saw 17.8 GB of material from the national police database released online in February.

Jacob Applebaum, an American computer security specialist and hacker based in Berlin, said the latest leak could constitute a major breach for the Turkish authorities.

"If this is really what it claims, I think it is one of the largest security/PII breaches since the #OPM hack," he wrote on Twitter, referring to last year's hacking of the United States Office of Personnel Management database, which is thought to have compromised the records of 18 million people.

UK and US to simulate cyber-attack on nuclear plants to test resilience

Source: http://www.theguardian.com/uk-news/2016/mar/31/uk-us-simulate-cyber-attack-nuclear-plants-test-resilience

Mar 31 – Britain and the US will stage a war-game later this year, simulating a cyber attack on a nuclear power plant, to test the readiness of the government and utility firms.

As David Cameron prepares to fly to Washington to attend a nuclear security summit, convened by Barack Obama, government sources said the two countries plan to cooperate on exploring the resilience of nuclear infrastructure to a terrorist attack.

Government sources said the exercise was not triggered by any credible intelligence about the threat of such an attack, but that it was "prudent planning," adding: "It gives us the ability to test these systems, and make sure that we learn any lessons."

The approach will echo a similar exercise last year, which tested how the major banks could withstand a cyber-security attack.

Nuclear research site in Dounreay, currently housing most of the waste material to be exchanged with the US. Photograph: Murdo MacLeod for the Guardian

Separately, Cameron is also set to announce an exchange deal with the US, which will see the UK ship 700kg (110st) of nuclear waste, most of it currently stored at Dounreay, in Scotland, to be processed in America.

In return, the US will send supplies of a different type of uranium to Euratom, the European nuclear agency, to be turned into medical isotopes, that can then be used in diagnosing and treating cancer across Europe.

Government sources described the swap as a "landmark deal," adding: "it's a win-win: we get rid of waste, and we get back something that helps us to fight cancer".

They said by working together in this way, Washington, London and Brussels hope to set an example to other states of the innovative measures that may need to be taken to deal with nuclear waste products in future.

"It's an opportunity for the UK, the US and Europe who show how countries can work together to deal with nuclear waste. It's an opportunity for us to show some leadership to the rest of the world", the source said.

The nuclear security summit, the fourth and final one held during Obama's presidency, is aimed at enhancing the safety of domestic nuclear systems — something the US president first discussed in a speech in Prague in 2009, and which he sees as part of his legacy.

Since the first summit in Washington in 2010, the states attending have agreed to reduce their stockpiles of potentially dangerous highly enriched uranium – the by-product of nuclear power generation – and strengthened the role of watchdog the International Atomic Energy Agency (IAEA).

Over that time, 14 countries have committed to removing nuclear materials from their territory altogether, and many others have pledged to step up security and tackle nuclear smuggling, by stepping up checks at ports, for example.

But in a statement setting out its hopes for this week's meeting, the White House said there was more to do. "We all need to do more together to enhance nuclear security performance, to dissuade and apprehend nuclear traffickers, to eliminate excess nuclear weapons and material, to avoid production of materials we cannot use, to make sure our facilities can repel the full range of threats we have already seen in our neighbourhoods, to share experiences and best practices, and to do so in ways that are visible to friends, neighbours, and rivals – and thereby provide assurance that we are effectively executing our sovereign responsibility," it said.

During the summit, the UK will offer to share its expertise on tackling cyber-crime with other countries. Japan, Korea, Turkey and Argentina have already said they would like to cooperate with the UK on this.

Cameron will also commit to spend £10bn this year to fund the world of agencies including the IAEA, on improving the security of civil nuclear infrastructure worldwide.

Over lunch on Friday, the world leaders will discuss "scenario-planning" for protecting their nuclear facilities, and preventing volatile nuclear materials falling into the wrong hands.

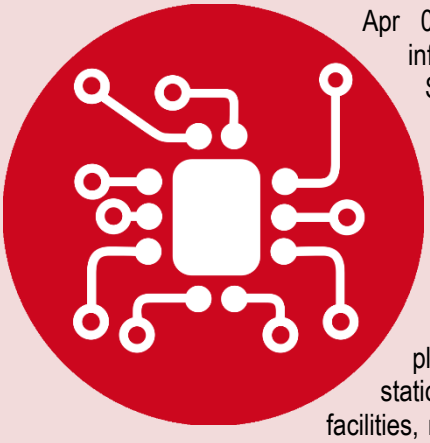
While the main focus is civil security, he will also receive an update on progress in implementing the Iran nuclear deal, which was signed in January, and aimed at preventing Tehran acquiring nuclear weapons, in exchange for the lifting of punitive sanctions.

While in Washington, Cameron will also hold a series of bilateral meetings with other world leaders. However, the government sources said he would not be meeting with potential candidates for the US presidency.

Four Dangerous Myths about Infrastructure Cybersecurity

By Mike Baker

Source: http://www.hstoday.us/single-article/special-four-dangerous-myths-about-infrastructure-cybersecurity/d188461055c71fd8f39bf09ed28ad324.html



Apr 06 – Is your transport infrastructure truly secure? Successful cyberattacks against **Supervisory Control and Data Acquisition (SCADA)** and other process control systems at airports, nuclear and petroleum production plants, power generation stations, water treatment facilities, mass-transit systems and other critical infrastructure systems have increased significantly.

SCADA networks contain computers and applications that perform key functions in providing essential services and commodities to all Americans. Given the sensitive nature of what they protect, SCADA and Distributed Control Systems (DCS) are attractive targets for hackers and terrorists.

Even though cybersecurity has vaulted to the forefront of concerns for many businesses, fewer than a third say they're prepared to meet an attack, according to an industry report from consulting firm Black and Veatch titled "2014 Strategic Directions: US." Furthermore, only 32 percent of electric utilities surveyed for the report had integrated security systems with the "proper segmentation, monitoring and redundancies."

In 2013, a hacker compromised a US Army database that held sensitive information about vulnerabilities in US dams. In 2014, it was reported that Nuclear Regulatory Commission (NRC) computers within the past three years were successfully hacked by foreigners twice, as well as by an unidentifiable individual, according to an internal investigation.

Mass-transit systems and airports, not airplanes, are extremely vulnerable points of attacks.

Countering the increasingly dangerous cyber threats to the nation's critical infrastructure will, however, require breaking down a number of growing misconceptions about SCADA systems, which can create a false sense of security.

Myth: Most SCADA systems are not connected to the Internet, so they're secure

The average system has eleven direct connections to the Internet. Those connections may include intranets, direct Internet connection, wireless and dial-up modems and Internet of Things (IoT) devices. This kind of patchy security and lack of 24/7 monitoring can lead to potential disaster.

As an example, the Davis-Besse nuclear power plant's process computers and safety display systems were infected via a contractor T1 line, which took the plant's safety monitoring capability offline for five hours. In another example, a water treatment plant in Harrisburg, PA was hacked remotely over an infected employee laptop. The cybercriminal used the worker's remote access to install malware and spyware.

Even if your SCADA network is completely walled off from the Internet by utilizing private physical network links or satellite technology, it's still vulnerable.

Myth: Firewalls are all you need

Many organizations believe that firewalls are the equivalent of an impenetrable force field. Shields up. We're safe. Wrong!

Firewalls offer some protection, but they can be easily hacked. In spite of record spending on firewalls, anti-virus software, malware detectors, and the widget of the day, organizations keep getting hacked because the focus is in the wrong place.

Organizations expose themselves to cyberattack when they use technology as a crutch. The crutch of believing that buying more hardware and software equates to safer infrastructure could be a fatal mistake. Departments and organizations need to realize that it is the quality of the cybersecurity personnel, at the end of the day, that will help identify and eliminate potential threats before they are executed. All the best technology in the world will fail if the human element is ignored.

Myth: SCADA is obscure technology and hackers do not get it

SCADA cybercrime has become very lucrative. In fact, cybersecurity has vaulted to the forefront of concerns for US electric utilities this year, yet fewer than a third say they're prepared to meet the growing threat of an attack. The Wall Street Journal reported in March 2015 that if only nine of the country's 55,000 electrical substations went down – whether from mechanical issues or malicious attack – the nation would experience a coast-to-coast blackout. One month later, sniper fire knocked out a substation in San Jose, California. The very definition of a hacker means that vulnerabilities can and will be found.

Myth: Our facility is not a target, we're too remote

Research by the Kaspersky Lab has shown that computers running SCADA software encounter the same malware afflicting business systems, which include Trojans, viruses, malware/ransomware, worms, and other exploits that target vulnerabilities in the Windows operating system. In the cybersecurity world, physical location and distance are irrelevant to state and non-state malicious actors.

SCADA: An emerging security market

To successfully defend against SCADA attacks, organizations must utilize a more thorough and systematic approach for identifying "normal" behavior and placing safeguards around sensitive PAC (Protected Access Credentials) and other hardware and software components. Organizations need a complete solution that does not adhere to the outdated belief that just physically isolating systems and buying technology will make a facility safe.

The role for managed security services in the control systems segment is really no different than any other market – the task and goal are the same, but many companies lack the time or personnel to operate a Security Operations Center (SOC). Most organizations running control systems have limited expertise and the resource bandwidth to deal with the complexities of security and compliance. Security is a multifaceted approach; proactive security is more complex and requires vigilant oversight.

Managed security services providers (MSPs) with the ability to monitor, manage and protect control systems fill that cybersecurity gap. MSPs focus solely on their side of the coin, security and monitoring. This allows organizations to focus their employees on the things that

matter most to them, running the business.
An MSP who employs both technology and an intelligent human network of on-site personnel can monitor and act as a full operations team. Technology, if deployed correctly, is a force multiplier for intelligent human beings. An MSP adopts teams that are trained to be security aware in all areas, from older hacking techniques that are making a comeback to recognizing the behaviors of a zero-day attack. Understanding how attacks occur allow MSPs to proactively fight against malicious behavior in any facility.
MSPs can also help customers with compliance. In the Industrial Control Systems field, for example, the North American Electric Reliability Corp.'s Critical Infrastructure Protection (NERC CIP) standard is a key requirement. The huge regulatory burdens by the NERC, which maintains a set of cybersecurity standards for Critical Infrastructure Protection (CIP), can be daunting. Partnering with an MSP allows organizations to have an additional oversight to ensure they are following the most current security policies required by their governing body.
Technology is only as good as the people who use it and is merely a tool in the fight against cybercrime; as are the misconceptions about infrastructure SCADA systems and their vulnerability for attack. This is a future trend that must be recognized if organizations hope to safeguard critical infrastructure. It is a war that must be fought daily, but one that can be won.

***Mike Baker** is founder and Principal at Mosaic451, a bespoke cybersecurity service provider and consultancy with specific expertise in building, operating and defending some of the most highly-secure networks in North America.*

Want To See AnonGhost Attacks In Real-Time?

Source: http://i-hls.com/2016/04/want-to-see-anonghost-attacks-in-real-time/

Today is April 7th, which is the day the hacking group AnonGhost declared it will launch continuous attacks against the state of Israel: OPIsrael 2016.
In the past few days a list of potential targets has been published, and although these attacks are not perceived as posing any significant threat, it is advised to stay alert and make sure that security is at its maximum. The list of targets can be seen here. Targets vary from governmental and financial to academic institutes.

▶ **You can see the attacks in real-time at:** http://threatmap.fortiguard.com/

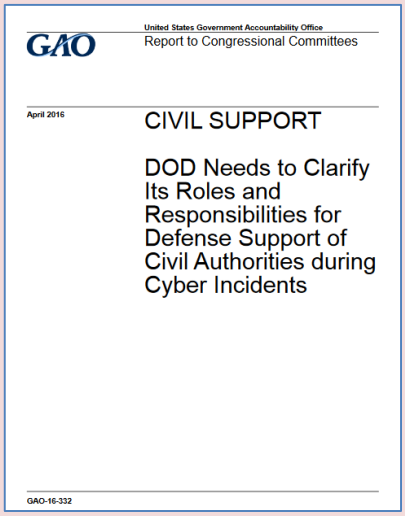
Throughout the morning Anonymous declared several attacks on Israel, although Israeli sources deny that any such attack took place. According to the hacking organization, at least 55 websites were attacked so far, including the ministry of economy, the IDF website, ministry of foreign affairs, and others. Israeli sources, on the other hand, claim that no

such attacks were detected, that all the websites are operational and that these are false reports.
Either way, it seems that the operation itself has not yet commenced. We advise both commercial and private sectors to stay alert and tuned.
Major General Rami Efrati, former head of the national cyber bureau said in an interview last night that the hackers are already trying to attack but that "there is no need to panic."
"They intend to take down sites which are no well-protected. So all we have to do is use anti-virus, use a password and stay alert – don't answer any e-mail, and be prepared for a situation where if a site is down and it is the end of the world, then see … how to put it back up again. But most important is not get into any hysteria, there's no reason," he explained.
So – don't panic, but stay alert.

DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents

GAO-16-332: Published: Apr 4, 2016. Publicly Released: Apr 4, 2016.
Source: http://www.gao.gov/products/GAO-16-332

The Department of Defense (DOD) has developed overarching guidance about how it is to support civil authorities as part of its Defense Support of Civil Authorities (DSCA) mission, but DOD's guidance does not clearly define its roles and responsibilities for cyber incidents. Specifically, DOD has developed and issued key DSCA guidance—such as DOD Directive 3025.18, *Defense Support of Civil Authorities*—that provides guidance for the execution and oversight of DSCA. However, DOD guidance does not clarify the roles and responsibilities of key DOD entities—such as DOD components, the supported command, and the dual-status commander—that may be called upon to support a cyber incident. Specifically:


United States Government Accountability Office
Report to Congressional Committees
April 2016
CIVIL SUPPORT
DOD Needs to Clarify Its Roles and Responsibilities for Defense Support of Civil Authorities during Cyber Incidents
GAO-16-332

- **DOD components:** DOD Directive 3025.18 identifies the specific responsibilities of DOD officials who oversee DOD components responsible for various elements of DSCA, such as the Assistant Secretary of Defense for Health Affairs for health or medical-related support, but does not specify the responsibilities of DOD components (such as the Assistant Secretary of Defense for Homeland Defense and Global Security) in supporting civil authorities for cyber incidents.
- **Supported command:** Various guidance documents are inconsistent on which combatant command would be designated the supported command and have primary responsibility for supporting civil authorities during a cyber incident. U.S. Northern Command's DSCA response concept plan states that U.S. Northern Command would be the supported command for a DSCA mission that may include cyber domain incidents and activities. However, other guidance directs and DOD officials stated that a different command, U.S. Cyber Command, would be responsible for supporting civil authorities in a cyber incident.
- **Dual-status commander:** Key DSCA guidance documents do not identify the role of the dual-status commander—that is, the commander who has authority over federal military and National Guard forces—in supporting civil authorities during a cyber incident. According to U.S. Northern Command officials, in a recent cyber exercise there was a lack of unity of effort among the DOD and National Guard forces that were responding to the emergency but were not under the control of the dual-status commander.

DOD officials acknowledged the limitations of current guidance to direct the department's efforts in supporting civil authorities in a cyber incident and discussed with GAO the need for clarified guidance on roles and responsibilities. DOD officials stated that the department had not yet determined the approach it would take to support a civil authority in a cyber incident and, as of January 2016, DOD had not begun efforts to issue or update guidance and did not have an estimate on when the guidance will be finalized. Until DOD clarifies the roles and responsibilities of its key entities for cyber incidents, there would continue to be uncertainty about which DOD component or command should be providing support to civil authorities in the event of a major cyber incident.

Why GAO Did This Study

Cyber threats to U.S. national and economic security are increasing in frequency, scale, sophistication, and severity of impact. DOD's 2013 *Strategy for Homeland Defense and Defense Support of Civil Authorities* states that DOD must be prepared to support civil authorities in all domains — including cyberspace — and recognizes that the department plays a crucial role in supporting a national effort to confront cyber threats to critical infrastructure.

House Report 114-102 included a provision that GAO assess DOD's plans for providing support to civil authorities related to a domestic cyber incident. This report assesses the extent to which DOD has developed guidance that clearly defines the roles and responsibilities for providing support to civil authorities in response to a cyber incident.

GAO reviewed DOD DSCA guidance, policies, and plans; and met with relevant DOD, National Guard Bureau, and Department of Homeland Security officials.

What GAO Recommends

GAO recommends that DOD issue or update guidance that clarifies DOD roles and responsibilities to support civil authorities in a domestic cyber incident. DOD concurred with the recommendation and stated that the department will issue or update guidance.

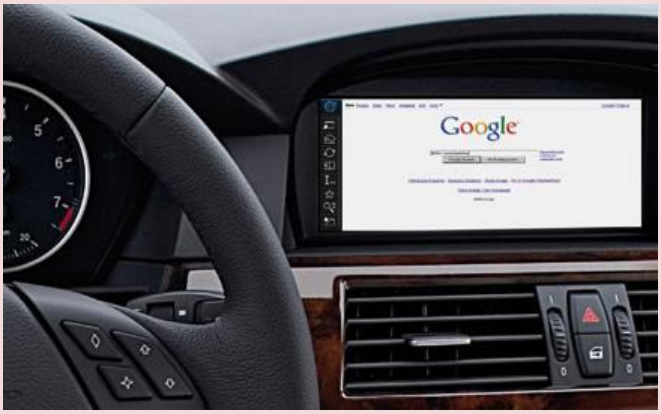
▶ **Read the report at**: http://www.gao.gov/assets/680/676322.pdf

Feds: Let's Try to Build a Terrorist-Proof Car

Source: http://www.emergencymgmt.com/safety/Feds-Lets-build-a-terrorist-proof-car-or-at-least-try.html

Apr 13 – In its quest to build connected and self-driving cars, the automotive industry is facing a daunting task that national security experts say is a must: Design a car that's terrorist-proof — or at least try.

With **220 million Internet connected cars expected to be on the roads within five years**, a national security expert visited Detroit Tuesday and urged automakers to be mindful of the growing cyber-security threats posed by terrorists, information crooks and spies who could potentially try to hack into wired vehicles and cause mayhem of all sorts.



While there are no known cases of terrorists hacking a connected car, the Department of Justice official stressed that automakers need to try to stay one step ahead of any potential hackers and ask: "'What are the bad buys thinking? We've seen them be creative before," said Assistant Attorney General for National Security John Carlin, who met with auto executives and law enforcement personnel at Cobo Center at a presentation titled, "Emerging National Security Cyber Threats and Their Implications for the C-Suite."

During his speech, Carlin reminded the audience about last year's intentional hacking of a sports utility vehicle by security researchers, who hijacked a Jeep Cherokee over the Internet. They managed to turn the steering wheel, disable the brakes and shut down the engine -- among other things -- triggering the eventual recall of nearly 1.5 million vehicles.

"It doesn't take much imagination to see how similar vulnerabilities could be used against us by our adversaries to bring about horrific results," Carlin said.

Carlin spoke on national security cyber threats and economic espionage at the opening management program of the SAE 2016 World Congress. He addressed the growing threat posed by sophisticated computer intrusions to the transportation sector and the economy at large, as well as the role the government and private sector must play in protecting companies before, during and after a serious hack.

In a sit-down interview with reporters, Carlin stressed that his reason for visiting Detroit was not to raise panic or stir fear, but to encourage automakers to assess the security risks associated with connected cars before anything bad happens.

"It's better in every respect to think of the risk on the front end," Carlin said, later adding: "We can't play catch up ... Assume the worst."

Concerns about cybersecurity in the automotive industry began to emerge several years ago. In 2014, a group of automakers and suppliers led by Delphi, Battelle, the Alliance of Automobile Manufacturers and the Association of Global Automakers banded together to formed a coalition to study cyber security issues.

Last year, two car hacking reports vaulted automotive cyber security into national headlines: In February, "60 Minutes" demonstrated how a car could be hacked as Lesley Stahl was driving the vehicle. In June, Wired Magazine published a story detailing how two researchers took control of a Jeep Cherokee.

But both events took place under a highly controlled environments and were orchestrated by hackers who had spent a lot of time targeting a specific vehicle. **To date, there haven't been any documented cases of real-world, malicious car hacking.**

Still, both reports elevated public concerns and set off alarm bells within the automotive industry, cyber security experts said today at an Automotive Press Association event.

Carlin noted how the auto industry has taken technology to a whole new level, making cars that can be opened by fingerprints, driven by themselves and shut down through the push of a button from anywhere. Connected cars in particular will soon hit the market by storm.

Carlin cited one estimate that shows by 2020, 75 percent of new cars shipped will have Internet connectivity. There could be 220 million so-called connected cars on the road by then, each with more than 200 sensors. These cars will allow drivers to stream music, look up movie times, get real-time updates about traffic and weather conditions, he said.

But there's more, Carlin said, noting that by 2022, driverless cars will be able to navigate crowded city streets; By 2025, the driverless car market will be worth $42 billion.

"You can easily see how the auto industry makes for a valuable target for hackers of all stripes. You have valuable information and infrastructure that they want," Carlin said.

In recent years, the country has witnesses a number of computer hacking incidents involving foreign spies, organized crime and terrorists.

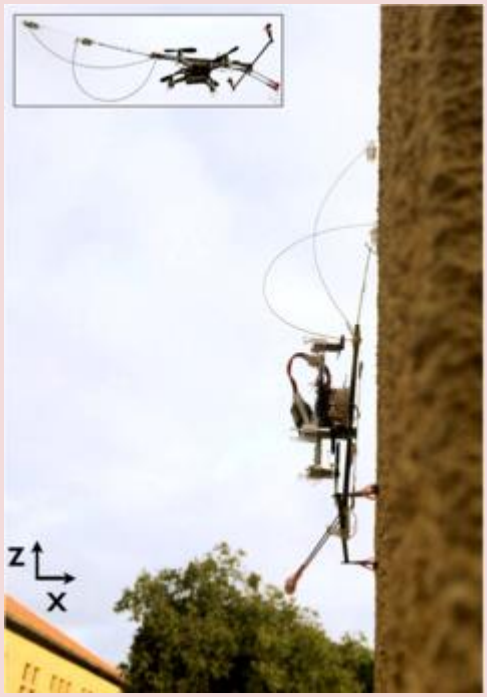
For example, in a 2014 attack on Sony, what was believed to be North Korean-sponsored hackers damaged company computer systems, compromised valuable information, and released corporate data and intellectual property.

Most recently, seven hackers affiliated with the Islamic Revolutionary Guard Corps were indicted last month for alleged hacking-attacks against the financial sector, costing tens of millions of dollars in remediation costs and locking hundreds of thousands of customers out of their accounts. One of the defendants also allegedly hacked into the computer system of the Bowman Dam in New York, which allowed him to obtain information regarding the status and operation of the dam.

"Every sector of the economy is a target – infrastructure, financial institutions, entertainment, agriculture, energy and yes, the auto industry," Carlin said.

SCAMP, The Robot That Flies, Climbs Walls Like An Insect

Source:http://i-hls.com/2016/03/watch-scamp-the-robot-that-flies-climbs-walls-like-an-insect/



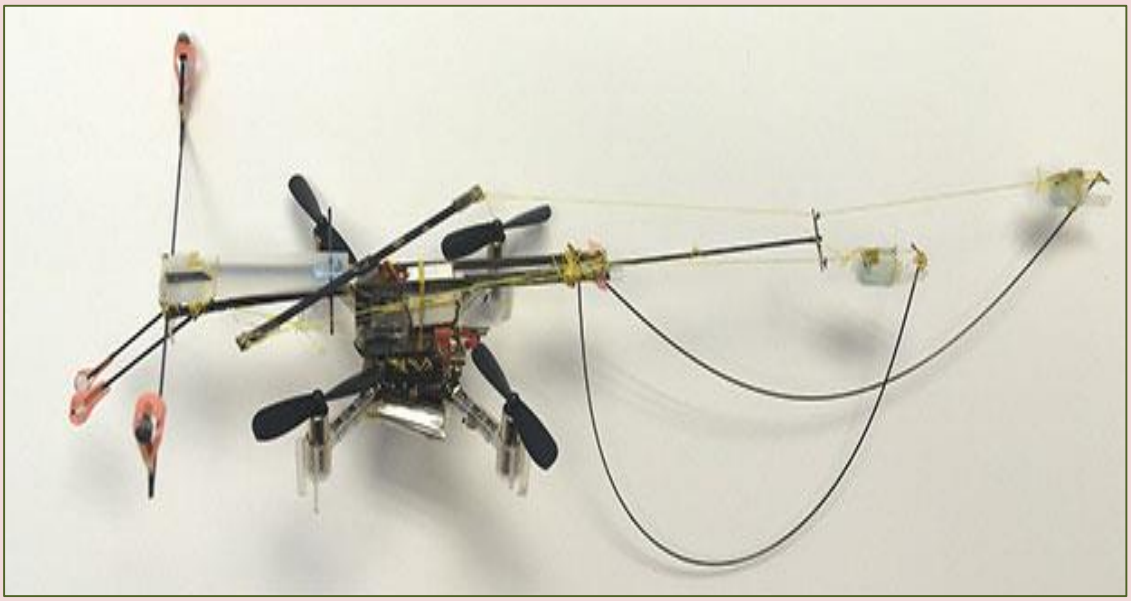
Mar 21 – Meet SCAMP, the Stanford Climbing and Aerial Maneuvering Platform, a robot that can fly, land on vertical walls, and then scamper up them. SCAMP flies using quadrotors and climbs up walls with spiny feet, and was built at Stanford's Biomimetics and Dextrous Manipulation Lab.

"Quadrotors have limited endurance because of restrictions on battery capacity and the physics of small-scale flight, but perching can allow them to operate for hours or even days, gathering data or performing communication tasks while stationary," says project lead PhD candidate Morgan Pope.

Perching is usually difficult for robots, Pope says. But this robot has a unique advantage in that it can use its climbing abilities to reposition itself if it lands improperly.

SCAMP is based on multi-years' work on climbing robots performed at the lab. They first began looking at feet coated with adhesive, but settled on spined feet that work on the same principle as those of an insect. Spined feet have the advantage of being lightweight and low-power – both important qualities for a flying machine.

The feet are not the only similarity this robot shares with insects. The feet are attached to long legs that



are based on those of creatures like stick insects or daddy-long-legs. This particular design (long, thin, and low-weight) allows SCAMP to take fewer steps and conserve energy.

To top it all off, SCAMP features a pretty long tail. It approaches walls tail-first. When contact is made, it is detected by accelerometers, and the robot then knows to pivot around its tail until it's oriented properly to the wall.

Pope says that they "see SCAMP as the starting place for an entire family of perching and climbing robots of varying scales and attachment strategies. The lessons we learned from SCAMP should allow us to tackle new surfaces, new environments, and different quadrotor platforms with new sensing and communication abilities."

Drones For Search And Rescue

http://i-hls.com/2016/03/drones-for-search-and-rescue/

Mar 17 – All around the world, search and rescue team respond to many thousands of calls annually.They search for lost travellers, hikers, and holidaymakers in mountain areas, marshes, bogs, coasts, and out at sea. These operations can be resource and time consuming, taking many hours and the combined effort of scores of trained professionals and volunteers. Well, search and rescue is about to become a bit more hi-tech and a lot more efficient.

Unmanned aerial vehicles (UAVs) can play a vital role in such operations and supplement the work performed by rescue teams. UAVs are small, relatively inexpensive, and can be deployed in large numbers. This makes them ideally suited for this type of mission. Researchers from the Dalle Molle Institute for Artificial Intelligence and the University of Zurich are about to realise this dream. They have developed artificial intelligence (AI) algorithms that enables small quadcopters to autonomously navigate around forests, to recognise and follow trails and paths.

"While drones flying at high altitudes are already being used commercially, drones cannot yet fly autonomously in complex environments, such as dense forests. In these environments, any little error may result in a crash, and robots need a powerful brain in order to make sense of the complex world around them," says Prof. Davide Scaramuzza from the University of Zurich.

Through a pair of small cameras, like the ones in most smartphones, the UAV observes its environment. AI interprets the images, specifically seeking man made paths in them. When it finds one, the UAV is steered in the appropriate direction.

To make accomplishing this hard task possible (after all, trails can be hard to find even for a human), the researchers set Deep Neural Network (DNN) algorithms at it. DNNs are part of a branch of AI called machine learning. They learn to solve problems by solving "training example," similar to how brains learn. To give their AI enough example, the researchers hiked for hours along several different trains in the Swiss Alps, taking more than 20,000 photos along the way with cameras attached to a helmet.

The DNN worked. When presented with a new, untested trail it was able to identify the correct direction in 85 percent of cases. That's better than humans, who only choose correctly 82 percent of the time. There is still work to do before this solution becomes a reality. Technological challenges need to be overcome. But soon enough, this work could end up saving lives.

The public's response when nobody turned up to this autistic 6-year-old's birthday was incredible

Source: http://metro.co.uk/2015/02/21/the-publics-response-when-nobody-turned-up-to-this-autistic-6-year-olds-birthday-was-incredible-5073081/#ixzz44C0KPzfD

Feb 21 – **When not one person from six-year-old Glenn Buratti's class showed up to his birthday party, he was heartbroken.**

Glenn's mother, Ashlee, sent invites to all 16 children in her son's form and despite no RSVPs from parents, she still hoped that at least one of Glenn's classmates would show.

But they didn't – and when Mrs Buratti broke the news to her son, who is autistic, she said the look on his face 'killed her inside.'

Devastated for her son, she took to Facebook, venting on the local Osceola Rants, Raves & Reviews List.

'I know this might be something silly to rant about, but my heart is breaking for my son,' she posted.

'We invited his whole class (16 kids) over for his 6th birthday party today. Not one kid came.'

The response of the good people of Osceola, Florida, blew her mind.

Responses poured in. Locals asked if they could stop by to wish Glenn a happy birthday and drop him a gift. Within a few hours, 15 children and 25 adults had turned up, reports the Osceola News-Gazette.

One woman brought Glenn a brand new bike, while another came and took pictures of the family, when he then gave to them.

The Osceola County Sheriff's Office sent the force helicopter to fly over the party, while officers pooled their money to buy gifts for the six-year-old.

A few days later, the town's fire department stopped by to pay Glenn a visit, wishing him a belated happy birthday and letting him climb up on the fire truck.

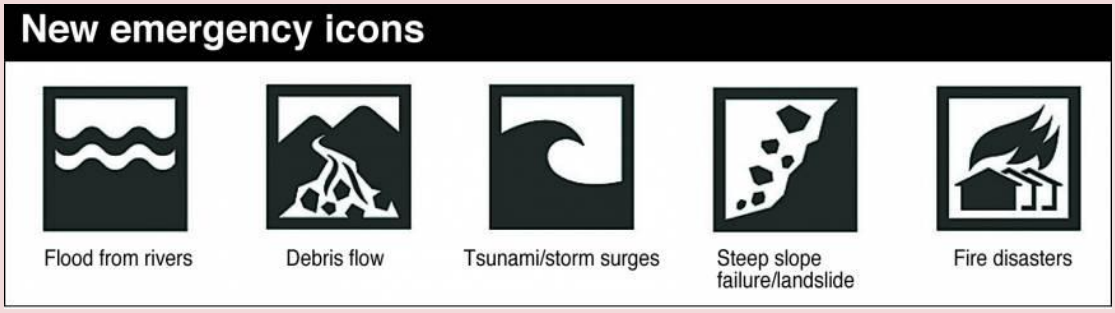
A week since the party, Mrs Buratti told WKMG that she still hadn't heard from any of Glenn's classmates' parents – but she didn't mind.

'The amazingness of everybody coming together for someone that they didn't even know, a kid that didn't have anybody come to his birthday party – it warmed my heart,' she said.

EDITOR'S COMMENT: Congrats First Responders!

Japan Enlists New Emergency Icon System

Source: http://www.emergencymgmt.com/disaster/Japan-Enlists-New-Emergency-Icon-System.html



Mar 25 – **The government has urged prefectures and municipalities to put five redesigned emergency icons into use to guard against tsunami, floods, landslides and other disasters.**

The standardized icons were designed to be easily universally understood as Japan prepares for an influx of foreign tourists for the 2020 Tokyo Olympics, officials at the Cabinet Office said Wednesday.

The icons indicate emergency shelters and evacuation areas for five types of disasters — tsunami, floods, debris flows (such as from mudslides), fires and landslides or slope failures.

Any given sign will bear the five icons, with circles and Xs denoting their functions.

For example, if an evacuation center bears a tsunami/storm surge icon with a circle under it and a landslide icon with an X underneath, it is safe from tsunami but not particularly designed to withstand landslides.

All areas are urged to use the five icons when erecting or replacing emergency signs, but there is no deadline, the officials said.
The government did not create an icon for earthquakes because evacuation takes place only after one has struck — mainly to avoid subsequent disasters like tsunami, fires and landslides.
The Ministry of Economy, Trade and Industry plans to submit the five emergency icons to the International Organization for Standardization so other countries can adopt them.

One Concern: Applying Artificial Intelligence to Emergency Management

By Jason Shueh
Source: http://www.emergencymgmt.com/disaster/One-Concern-Applying-Artificial-Intelligence-Emergency-Management.html

Buildings crumbled after the 2014 Napa Valley, Calif., earthquake, an incident that prompted Stanford Alumni and entrepreneur Ahmad Wani to co-found the disaster response and artificial intelligence company One Concern. *Flickr/James Gunn*

Mar 26 – Ahmad Wani remembers Oct. 8, 2005. It was the day when at 8:50 a.m. Pakistan Standard Time, a magnitude 7.6 earthquake struck his home in Kashmir killing more than 70,000 people and displacing another 4 million. He recalls the devastation clearly, the homes left in shambles, the shortages of food and water, the many lives torn asunder in the course of seconds.
"Having been one of the lucky few who lived through the disaster, I could see rescue authorities going around trying their best to rescue people," Wani said. "However, the scale of the disaster was so large that they couldn't identify who needed to be rescued first, and what the priorities for rescue were."
First responders were burdened by a lack of proper tools to coordinate efforts and clear blocked roadways to extricate victims. The aftermath's resulting pandemonium — and subsequent national and international earthquakes that followed — led Wani, along with his fellow Stanford University alumni Nicole Hu and Timothy Frank, to create One Concern. **The startup aspires to be one of the first to use artificial intelligence to save lives through analytical disaster assessment and calculated damage estimates.** Wani said that with the platform,

emergency operations centers (EOCs) can receive instant recommendations on response priorities and other insights to dispatch resources effectively.

One Concern's efforts to pioneer machine learning services for state and local agencies has earned it a spot in *Government Technology's* GovTech100, a list of noteworthy companies to watch in the public-sector IT market.

Wani, who serves as One Concern's CEO, elaborated on his startup's origins and how the company is progressing after its recent beta launch.

Government Technology: What led to the idea and ultimate conception of One Concern?

One Concern CEO Ahmad Wani: The combination of the right people, the right background and a unifying problem. I am from Kashmir, a region prone to earthquakes and floods. When I was 17 years old, in 2005, 70,000 people lost their lives in an earthquake in my hometown. This event compelled me to study engineering and specifically in 2005, start performing earthquake engineering research. Then, in 2014, a combination of two events on different sides of the world inspired the creation of One Concern.

In 2014, during a break from graduate school at Stanford, I was visiting my parents in Kashmir when a large flood engulfed the state. Eighty percent of Kashmir went under water within minutes! Most people were on their rooftops for up to seven days without food and water, waiting for rescue. Thousands of people lost their lives ... most of the rescue was random, and response priorities were ad hoc. I was quick to assume that the problem of situational awareness was probably restricted to the developing world.

Thereafter, upon my return to the Bay Area, I discovered that a natural disaster had struck in California, in Napa County, while I was away. A magnitude 6.0 earthquake on Aug. 24, 2014, in Napa had driven thousands of 911 calls, and overwhelmed the authorities who carried out the rescue effort on a first-come, first-served basis. Power and communication lines were not fully restored for weeks. In fact, most of the badly damaged regions did not even have connections to a phone network and couldn't call in for help — which has been seen in nearly all of the previous earthquakes.

Napa was just a magnitude 6.0 earthquake, which caused minor or no damage in most regions. I seemed to imagine the situation in a magnitude 7.0 earthquake (nearly 10 times larger than a magnitude 6.0) or a magnitude 8.0 (nearly 100 times larger), for which there is significant probability of occurrence in California. Not just Napa, but 25 other counties could be very badly hit and out of network. I recognized at that point there would be a huge need for situational awareness, for driving rescue and relief operations.

It was clear that difficulties in the chaos following a natural disaster were not limited to the developing world. It is a worldwide issue and it affects all regions vulnerable to any kind of natural disaster. Not only rescue, but the importance of reconnaissance and recovery also became apparent.

These two events crystallized for me the opportunity to solve the problem of post-disaster reconnaissance and rescue through artificial intelligence given the community scale and highly nonlinear nature of the problem. First up was earthquakes, as I was studying earthquake engineering at Stanford. I partnered with Nicole Hu and Timothy Frank, who were both driven to solve this problem based on their unique previous experiences. Nicole, at the time a computer science grad student, had worked for large companies in data science and Web security, but she was looking for a real-world problem that could really make a positive impact on people's lives. Timothy, a major in the U.S. Air Force and a Ph.D. candidate in structural engineering, had several years of experience in emergency management and disaster response. He was well aware of the current tools and processes in addition to the challenges and pain points that those in the emergency response community face. Like Nicole and me, Timothy was also driven by the impact this project could have on saving lives and strengthening communities.

A combined class project between the Machine Learning and Performance Based Earthquake Engineering courses at Stanford was undertaken. Results of the project were compared with historical records.

The goal was to see if damage to homes could be predicted on a community scale for the Napa earthquake. Results showed that

our machine learning model accurately predicted structural damage to homes on a scale of 1-to-4 with significant accuracy.

At the public presentation for the machine learning course, a venture capitalist — who turned out to be our first investor and trusted adviser and mentor — Mar Hershenson of Pejman Mar Ventures, stopped by to chat. She said if we were interested in starting a company, to let her know. Then, Stanford Machine Learning Professor Andrew Ng, famous for his pioneering roles with the Google Brain project and Coursera, stopped by to see our project. He immediately saw a need for it in the real world, and offered his support and advice to start a company, and to develop the class project into something more robust. It didn't take the three of us long to commit to taking the project forward and see if we can make a difference to communities all over California, the U.S. and the world.

Government Technology: How did One Concern select the data sources that are analyzed to create damage estimates post-disaster?

Wani: Our team of skilled and experienced domain experts in the fields of earthquake engineering and flood modeling have carefully selected our data sources. We are becoming a repository for organized geospatial data in the process.

***Government Technology:* What actionable intelligence does One Concern provide its users and how does it do it?**

Wani: Our vision is to change the way society plans for, responds to and recovers from all types of natural disasters. Currently we provide critical situational awareness in the minutes and hours following an earthquake. Our core product is a Web platform called "Seismic Concern" that alerts you when an earthquake may have affected your jurisdiction, and displays a color-coded map of the likely structural damage. This saves time in reconnaissance and allows emergency operations centers to allocate their limited resources to rescue and recovery. It gets all the stakeholders a common operating picture and not only facilitates response prioritization, but also recovery operations such as material staging and shelter management. Apart from the map, the platform furnishes key insights like the elderly population in a particular block that is badly damaged, or the number of kids in a school which could be hit. This helps in instant situational awareness and assigning response priorities to the places that need the most help. For instance, an elementary school wouldn't be prioritized if an earthquake struck at midnight, but if it hit at 10 a.m. on a schoolday, it might jump to the top of the response priority list.

Moreover, going to the phone network being jammed or lines being down, most people who have the worst damage cannot call 911. Seismic Concern is built on geographically distributed servers and redundant systems, which means our site will be up during an emergency when the emergency operations center needs it most.

Compiling an Initial Damage Estimate (IDE) is critical for emergency operation centers to request financial aid from state level and federal authorities. Initially done using a wind-shield tour, wherein emergency managers carry out a quick reconnaissance survey of the area, street by street, it took around two months of time after the [2014] Napa earthquake to complete the process of requesting financial aid. "Seismic Concern" would provide a scientific basis to an IDE, an incident commander would be able to identify and quantify extent of damage to his jurisdiction with a significant amount of accuracy in minutes, thus saving a lot of time, and promising high precision.

We use state-of-the-art machine learning algorithms and stochastic modeling on derived features, and proprietary models to do this for the people we serve, which as of now are exclusively local governments.

Apart from the live response platform, One Concern also offers a training module, which works on the same artificial intelligence and stochastic modeling back end of Seismic Concern combined with state of art geophysical and seismological research. This technological breakthrough will enable emergency operations centers to train on scenarios based on actual simulations to get a real sense of the situation. The platform would provide damage from simulated earthquakes for emergency response drills before a disaster strikes. This can aid in personnel readiness and plans development, thereby making a community more resilient.

We view the Seismic Concern Training module as democratizing the information in our platform, and allowing local agencies to

inform, train and empower the public how to respond to predictive disaster scenarios. The training module is a powerful tool for public policy makers and emergency operation centers in their interactions with the public at large.

Government Technology: **How is One Concern working to develop its platform through its recent beta launch?**

Wani: We are receiving feedback from our beta partners that will allow us to improve the user experience, as well as add functionality to support the needs of the community. What we provide should change the way emergency managers do business. It should be easy to use, simple to understand, and facilitate action that will save time, money and lives. We won't stop until that mission is achieved.

Government Technology: **What user input did you gather from cities and first responders to create the analytic and predictive analytics tools**

Wani: We interviewed dozens of experts in the emergency management community from all over the U.S. and beyond. We learned the foremost problem immediately following a disaster is situational awareness. All stakeholders need rapid, accurate information about the situation in a format easy to see and use. I'm sure we'll be making modifications and additions to our platform, but from some initial feedback, we hit the nail on the head with the foremost problem. We learned about how the emergency operations centers operate, how first responders and 911 call centers do their heroic jobs, how a diverse team of professionals work behind the scenes to coordinate response and recovery, how levels of emergency managers (e.g., city, county, state, federal) relate and report to each other to share resources and receive aid. The business of being ready and able to respond to anything at any time is a huge industry that spans the globe. The people we are working with are an invaluable resource to help us develop our platform. We expect our product to be one of their most valuable resources in their time of crisis. We empower heroes with the actionable information they need to save lives.

Government Technology: **How would you describe One Concern's current development as a startup? For example, are you in the seed stage, reaching out to angel investors, or preparing for a round of Series A venture capital?**

Wani: We raised a seed round in the fall of 2015, grew our team, and deployed and refined the product. Based on feedback from our partners, we then built our training module. We'd like to reach out to any city or county who may be interested in being an early adopter of this revolutionary technology.

***Jason Shueh** is a staff writer for* Government Technology *and* Emergency Management *magazines. His articles and writing have covered numerous subjects, from minute happenings to massive trends. Born in the San Francisco Bay Area, Shueh grew up in the east bay and Napa Valley, where his family is based.*

Protecting firefighters from harm

Source: http://www.homelandsecuritynewswire.com/dr20160329-protecting-firefighters-from-harm

Mar 29 – **If there is anything common among the 1.1 million firefighters — both career and volunteer — serving in the United States, it is that at any moment, they may be required to put their lives on the line to protect people and property from disaster.** But who helps protect these dedicated public servants from the on-the-job dangers they face? One group making the effort is the National Fallen Firefighters Foundation (NFFF), whose **Everyone Goes Home program** champions a set of sixteen life safety initiatives designed to reduce the number of preventable firefighter line-of-duty injuries and fatalities.

Recently, the National Institute of Standards and Technology (NIST) teamed with the NFFF to host a symposium at which more than 100 representatives of the fire service and fire research communities identified and prioritized firefighter health and safety issues, and then created a guide for addressing them through scientific study and technology development. NIST says that the new National Fire Service Research Agenda is now available for individuals and organizations that conduct and support projects that meet the "Everyone Goes Home" goals.

"Fifty-four recommendations were developed with input from the nation's most highly trained and informed subject matter experts, who through education and experience, understand what must be accomplished to keep firefighters safe, fit, healthy, and effective," said Dennis Compton, former fire chief for the city of Mesa, Ariz., and chairman of the NFFF Board of Directors.

For simplicity, each of the recommendations approved for the research agenda were grouped into one of three themes:

- Data collection and data analysis projects — those focusing on developing new foundations of research or expanding existing data/research;
- Problem or program analysis and evaluation projects — those assessing and improving existing efforts related to firefighter safety; and
- Research to practice projects — those related to translating research findings into operational resources.

Once grouped, the recommendations were then assigned a high, medium or low priority rating so that those with the greatest impact on firefighter survivability would be addressed first. The recommendations also were categorized by the issues they addressed, such as data gathering, economic impact of lifesaving measures, emergency response procedures, occupational diseases due to line-of-duty exposures, personnel protective equipment, and fighting wildland fires.

NIST notes that NIST, NFFF, and the other collaborators on the latest National Fire Service Research Agenda (previous versions were published in 2005 and 2011) are currently educating members of the fire service and fire research communities about the guide and urging them to use its recommendations in prioritizing research goals, designing studies that address the highest impact areas, and strengthening funding proposals to get the resources needed.

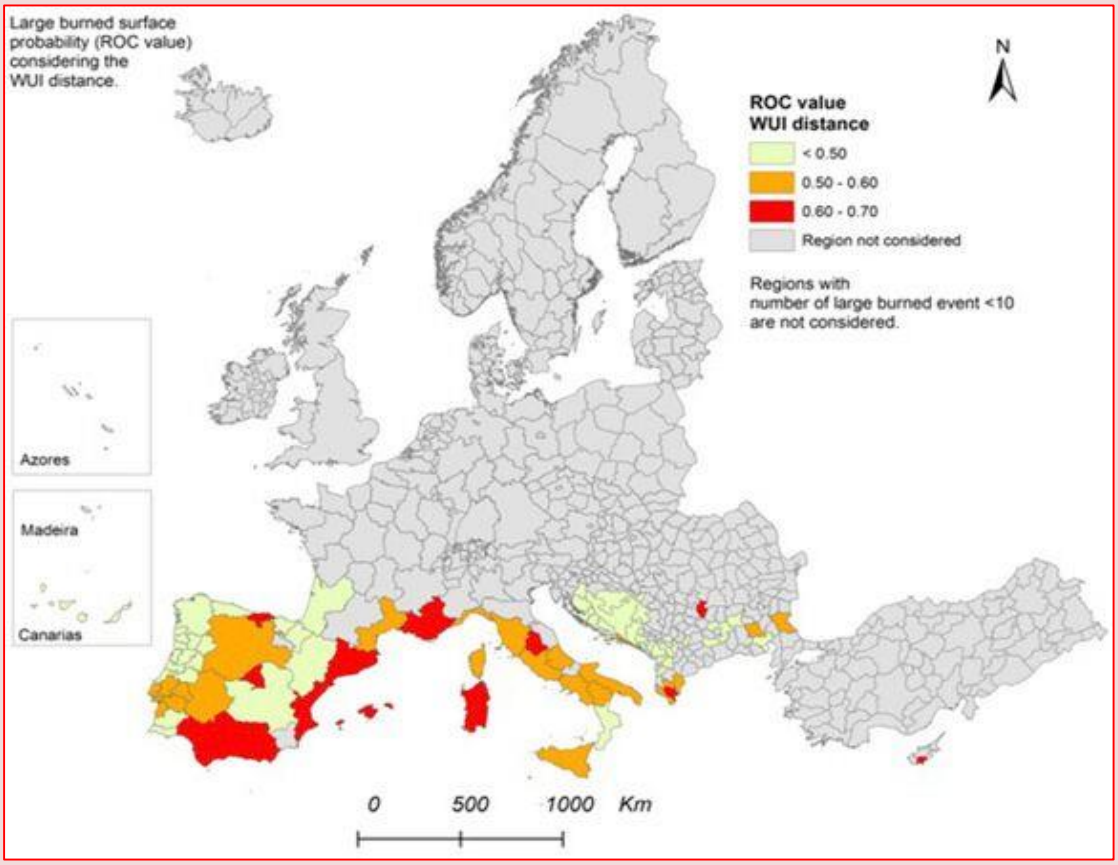
▶ **More information is available on the Everyone Goes Home Web site.**

Wildfire map shows European countries most at risk of catastrophic fire damage

Source: http://www.homelandsecuritynewswire.com/dr20160331-wildfire-map-shows-european-countries-most-at-risk-of-catastrophic-fire-damage

Mar 31 – **Cities and tourist areas such as Catalonia, Madrid, and Valencia are among those most at risk of catastrophic damage from wildfires in Europe, according to research led by the University of Leicester.**

An international research team has put together a map using satellite data that details the countries in Europe with the highest likelihood of experiencing wildfire damage — with large fires occurring more frequently near "Wildland-Urban Interface" WUI areas in the countries of Albania, Bulgaria, Cyprus, France, Italy, and Spain.



The map is published in the *Journal of Environmental Management* and is the first European-scale map of wildland/urban areas.

U Leicester reports that for the first time, the researchers set out to map the extent of wildland areas around cities all over Europe to find out where they create a risk for large wildfires threatening people.

Using satellite maps of land cover and of the extent of large fires, they used statistics to find areas where large fires have happened more frequently and where wildland areas are close enough to cities to make them vulnerable.

The distance from the nearest wildland/urban areas explained the occurrence of large fires in many regions across Southern Europe, where fires are the biggest problem.

Professor Heiko Balzter, Director of the Centre for Landscape and Climate Research at the University of Leicester, said: "In the regions we have identified as high-risk, local authorities need to prioritize fire risk control and develop better forest fire risk management strategies.

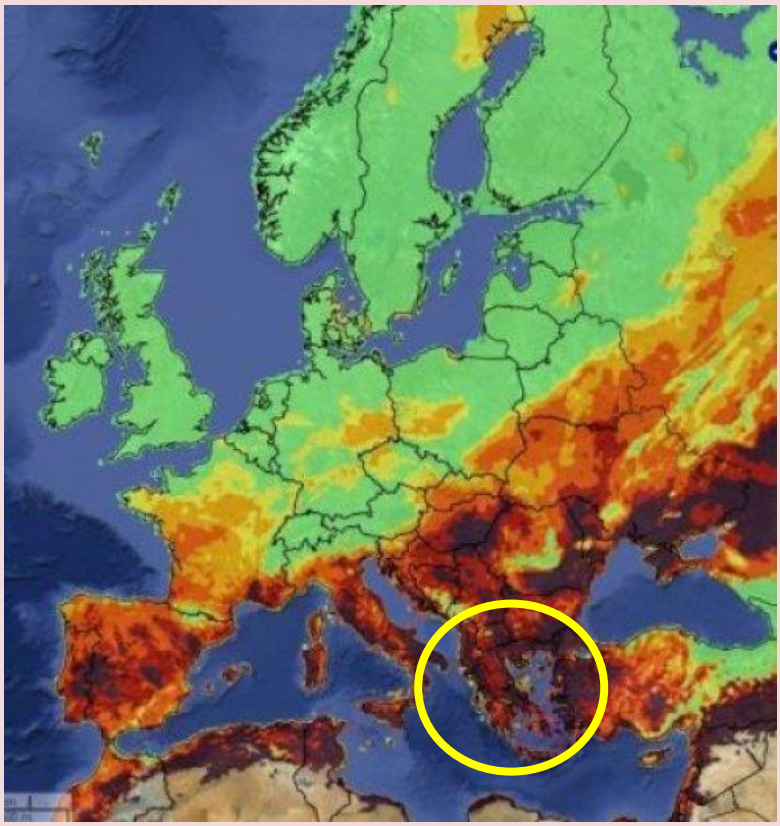
"This study was exciting, especially when we had our Eureka moment as it became clear that were onto something. We did not know what to expect when we started this work. To map the extent of wildland/urban areas all across Europe was already quite new. But to find that we can use that map to predict fire risk was a real breakthrough."

The overall study area covered the entire European Union, including the non-member states of Switzerland, Norway, Iceland, Montenegro, the Former Yugoslav Republic of Macedonia, Turkey, Bosnia, and Herzegovina Kosovo.

WUI mapping and the cross-national scale statistical analysis between WUI distance and large forest fires were performed for the whole study area.

Amongst the included countries, forest fires are strongly concentrated in the Mediterranean countries.

Dr. Beth Cole from the University of Leicester's Centre for Landscape and Climate Research, a co-author of the study, added: "A European wide approach to mapping the interface of wildland and urban areas has really allowed us to see the relationship between land cover and fire risk at a continental scale. This opens up a great opportunity for land management practices to reduce the risk of costly and dangerous wildfires in these populated areas."



In many regions of Europe the rapid changes in the global economy have led to dramatic changes in land use.

Many farmers have given up production and shrubs encroach on abandoned land and these changes have altered the landscapes around many large cities, particularly in the Mediterranean.

Where such wildland areas meet the city boundaries, wildfires are a serious risk. This is especially the case in Southern Europe where summers can be hot and dry.

Such conditions lead to sometimes catastrophic wildfires resulting in the loss of human lives and damage to property.

Wildland areas around cities are landscapes where urban land use makes people and properties very vulnerable to disasters and at the same time woody plants act as fuel for massive fires.

With the recent extreme weather in Europe such fires have been called 'mega-fires' by researchers.

They can be self-fanning, some have fire tornadoes throwing embers high up into the air and spreading themselves across vast landscape very quickly. They are notoriously difficult to extinguish and are feared by many fire-fighters.

The study, which is supported by the Natural Environment Research Council (NERC), was carried out by the University of Leicester's Centre for Landscape and Climate Research and National Centre for Earth Observation, the University of Cassino and Southern Lazio, and the European Commission's Joint Research Centre in Ispra, both in Italy.

Dr. Sirio Modugno, researcher from the University of Cassino and Southern Lazio, lead author of the study and an Honorary Visiting Fellow at the Centre for Landscape and Climate Research of the University of Leicester, said: "The land cover use well reflects the interaction between human activity and the surrounding environment. The increase of wildland urban interface areas, with the associated forest fire risk, could be interpreted like an intrusion of the urban model in the wild areas. The rural abandonment, the touristic pressure and the urban

sprawl have determined an increase of contact between urban and wildland areas.
"This study highlights the importance of the geographic data availability. The presence of a homogeneous and standardized European database supports the environmental analysis. The use of digital cartography and the viable production of thematic maps opens several possibilities not only to the scientific research sector but to territorial operators involved in planning actions too".

Dr. Paquale Borrelli from the European Commission's Joint Research Centre in Ispra, added: "Wise land management can provide a valuable ecosystem service of fire risk reduction that is currently not explicitly included in ecosystem service valuations. The results reemphasize the importance of including this ecosystem service in landscape valuations to account for the significant landscape function of reducing the risk of catastrophic large fires."

— Read more in Sirio Modugno et al., "Mapping regional patterns of large forest fires in Wildland Urban Interface areas in Europe," Journal of Environmental Management 172 (1 May 2016): 112–26.

EDITOR'S COMMENT: It is a pity that Greece is not included in this study! Why?

The App That Is About to Save Lives

Source: http://i-hls.com/2016/03/the-israeli-app-that-is-about-to-save-lives/

Mar 31 – About two years ago, in 2014, Amir Elichai was walking along the beach when he was mugged by a group of people. Amir immediately called an emergenency number to report – and was "investigated" on the phone with hard and complex questions to the point where he wished he hadn't called at all.

Following this incident, Amir came up with the idea to make emergency response procesdures more efficient by using existing technologies and capabilties that every one of us has. After some research, Amir found out that the world of emergency response has been stuck with the same technologies, capabilities and procedures for a very long time.

Amir took his idea to Brig.Gen. Pinchas Buchris, the father of a classmate, who got excited over the idea. He brought Lital Leshem to the project – and there they took off. Development, marketing and seeking funds.

In a similar process simultaenously, Alex Dizengof, a computer science graduate from Bar Ilan University, has developed along with prof. Gal Kaminka a smartphone-based ability to locate someone inside a structure (as GPS is only effective outside). Alex turned to Amir in order to use the latter's background in raising funds for companies, and instead received an offer from his to join efforts and cooperate.

At the start of 2015 tthe three founders arrived to showcase the company to Ehud Barak, the former Prime Minister of Israel, who was greatly impressed and invested about 1.5 million dollars in the firm – from his own money. Today the company employees fourteen people, eight of them are developers. The company is now closing a first substantial fund raising round.

Reporty is a system which is based on end-devices (smartphones)' application and a connection to emergency call centers. The app (for both iPhone and Android) provides the ability to communicate fast to emergency centers, without having to rely on the available communications platform (cellular, Wi-Fi). Once contact with the center is made, a video call is established and important personal details are transferred (caller ID, exact geographic location, whereabouts inside a building, chat call and more).

A system which isn't being used everyday, will probably not operate properly during emergency. For that reason, Reporty added everyday options to the application: Features such as Reporteam – a connection of five close contacts to receive an automatic report during emergencies (which also contributes to the app's virality), the ability to send instant messages with different icons, SpotMe – a request from a friend or family member "to watch over" the user along a certain route or a given time phrame, to make sure the user has arrived home safely.

On the emergency center's end, a Reporty station can be installed which stand-alone, through which operators can see emergency calls, or alternatively integrated with the center's command and control system, so that all the information from the App, arriving in real-time, enters automatically into the operator's emergency system. Such integration has already taken place with Israel's emergency medical services (MDA).

Reporty's official launch was about a week ago, and already more then 22,000 Israeli users downloaded the application. On Saturday the first life was saved, when a Reporty user walked around a shopping center and saw suddenly a mother and her child, the mother holding the baby and screaming that he is suffocating – the baby was already turning blue and convulting. The app was turned on, the operator saw the baby live and instructed those present how to treat him and save his life.

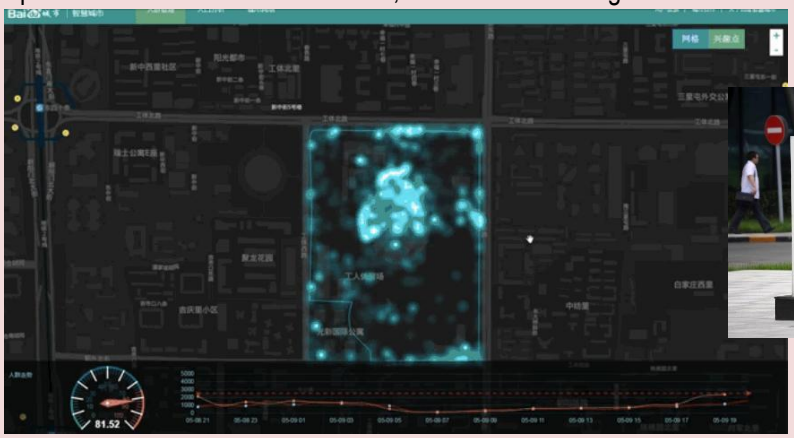
Reporty's vision is to become a global standard in the field of emergency response – in order to help save human lives.

According to Lital Leshem, co-founder and VP business development, in about three years the company sees itself operating offices in Asia, US, and Europe, with over a million users around the world.

China's Baidu Creates AI To Warn of Crowd Stampedes

Source: http://i-hls.com/2016/04/69053/

Apr 02 – In New Year's Eve of 2015, thousands in Shanghai came to the Bund where a light show was to take place to mark the New Year. A dangerously dense crowd formed, and at a viewing platform overlooking the river, confusion and a lack of crowd control led to panic and eventually stampede. Within minutes, 36 people had been killed and another 49 had been injured in the crush.



This might a memorable one, but it is by no means the only stampede in China's collective memory. The number of people cause masses in the country to be, well, massive. In order

to tackle this issue, Baidu (China's largest research engine)'s Big Data Lab has offered a solution: data-**crunching predictive A.I.**

A paper presenting the system describes how it uses Baidu Maps data to predict areas where dangerous crowds could be forming, and warn both users and authorities in advance. Baidu researchers figured that areas with spiking Baidu Map queries from users at nearby locations might be places where crowds are likely to form in the near future, as many consult the digital map before choosing a route on their way to somewhere. They studied mapping data from a number of high-density crowd events, including the 2014 stampede, and found that this was indeed the case. The team devised a method to crunch Baidu's mapping query data in real time and output a warning if the number of queries on a single area from nearby locations crossed a specific threshold. Then, a machine learning system was implemented to help crunch historical data and make accurate predictions about future danger areas.

Although the system hasn't been implemented anywhere yet, real-world implementation is the ultimate goal. "We believe the successful deployment of our method can bring many benefits to our society," the paper concludes.

Drone attack during Little League World Series is scenario for mass casualty exercise

By John Beauge

Source: http://www.pennlive.com/news/2016/04/drone_attack_during_little_lea.html

Apr 14 – **An annual exercise for emergency responders in the Williamsport area scheduled for next week be based on a scenario that seems out of a science fiction movie: a drone attack during the Little League World Series.**

The mock attack Thursday will be based on a scenario in which drones disperse a chemical agent over a crowded stadium, followed by more drones dropping explosive devices as fans rush to the exits.

The exercise will be conducted on vacant land adjacent to the Williamsport Medical Center between 8 a.m. and noon. Nothing is planned to occur at the Little League complex in South Williamsport.

The drill will include use of a command center and two drones to provide a touch of realism.

Santa's sleigh won't be the only thing in the skies this holiday season. Be sure to check in with

the FAA about the laws relating to your new unmanned aircraft system.

Vital signs of "patients" will be checked at the scene just like a real emergency, said the health system's emergency preparedness coordinator, Jim Slotterback said.

"It's really neat to work with so many agencies," he said. He estimates more than 300 people, including the National Guard, will be involved in some aspect of the exercise.

"It helps we are getting the chance to work with all the players at Little League," said South Williamsport Police Chief Robert Hetner, who helps coordinate world series security.

"It gives us the chance to tweet some things and get ready for another year," he said. The world series this year is Aug. 18-28.

The health system has a de-contamination center that has never been tested, hence the decision to include a hazardous materials component in the drill, said the system's emergency preparedness coordinator, Jim Slotterback.

By training together, everyone will be more comfortable should something happen, said FBI agent Juan A. Grajales Jr. who is in charge of the Williamsport office.

"It makes us more efficient," he said. "We try to catch any gaps that are identified." Given the importance of the series, "we want to cover all bases," he said.

"It's all about safety. The more we practice together, the better off we all are."

Planning for the exercise began last year during the world series, Slotterback said. An early idea was for a crop dusting plane to disperse a chemical agent over the crowd, he said.

A drone attack entered the picture after he said he learned about someone in New England strapping a gun to drone and discharging the weapon in the air.

*Williamsport native **John Beauge** obtained a bachelor's degree in journalism from Penn State and a master's from Northwestern University. He was photo editor of the Daily Collegian his senior year at Penn State. He worked for the Williamsport Sun-Gazette from 1963 to 1983, rising to the position of city editor. He has been a correspondent for the Harrisburg Patriot-News since 1983.*

1.4 billion people face severe natural disaster risks in South Asia

Source: http://www.homelandsecuritynewswire.com/dr20160328-1-4-billion-people-face-severe-natural-disaster-risks-in-south-asia

Mar 28 – **New data has revealed that 1.4 billion people in South Asia, 81 percent of the region's population, are acutely exposed to at least one type of natural hazard and live in areas considered to have insufficient resources to cope with and rebound from an extreme event.**

The research, released by risk analysis and research company Verisk Maplecroft, highlights a lack of resilience to hazards across the region, especially in India, Pakistan, and Bangladesh. According to the Bath, United Kingdom-based company, these governments have struggled to translate record levels of economic growth into improved resilience against natural hazards, leaving investors open to disruption to economic outputs, risks to business continuity and threats to human capital.

Verisk Maplecroft says that to reach its conclusions, it assessed **the risks posed by eleven types of natural hazards, including tropical cyclones, floods, winter storms, earthquakes, wildfires, and tsunamis in twenty new risk indices covering 198 countries.** The research forms part of its annual Environmental Risk Dataset, which has been developed to help companies identify risks to their assets, personnel and supply chains.

India lags behind U.S., China, and Japan in capacity to mitigate natural disasters

The populations of ten countries, including India (ranked 1st), China (2), Bangladesh (3), Indonesia (4), Philippines (5), U.S.(6), Japan (7), Nigeria (8), Brazil (9), and Pakistan (10) are identified by Verisk Maplecroft as facing the greatest exposure to natural hazards in its Natural Hazards Population Exposure Index.

Crucially though, South Asian nations lag behind the world's leading economies when it comes to mitigating the worst impacts of natural hazards. The company's Natural Hazards Vulnerability Index, which assesses a country's ability to prepare for, respond to, and recover from a natural hazard event, rates Japan (183) and the United States (173) as "low risk," and China (126) "medium risk." In comparison, the weaker

institutional capacity, financial resources and infrastructure of Bangladesh (37), Pakistan (43), and India (49) mean they are rated "high risk," leaving companies and populations there under greater threat if a significant event strikes.

The data identifies flooding as one of the most substantial risks to communities and business in South Asia. In India alone, 113 million people, or 9 percent of the population, are acutely exposed to flood hazard, with a further seventy-six million exposed in Bangladesh and ten million in Pakistan. Indeed, heavy monsoon rain in November-December 2015 sparked record flooding in South India, which cost the country upwards of $3 billion and displaced more than 100,000 people.

In its city-level analysis, Verisk Maplecroft flags the populations of three South Asian cities among the ten most exposed globally. These include the major garment producer Dhaka in Bangladesh (ranked 5th most exposed) and the rapidly growing tech hubs of Kolkata (6) and Delhi (9) in India. Manila, Philippines (1), Tokyo, Japan (2), Jakarta, Indonesia (3), Dongguan, China (4), Osaka, Japan (7), Mexico City, Mexico (8), and Sao Paolo, Brazil (10) complete the list.

Resilience to natural hazards lowest in Africa and South Asia

"This data highlights the scale of the task facing governments and business in mitigating the threats to populations and workforces from natural hazards in these high risk regions," states Dr. James Allan, Director of Environment at Verisk Maplecroft. "With overseas investment pouring into the emerging Asian markets, companies have an increasing responsibility to understand their exposure and work with governments to build resilience."

According to Verisk Maplecroft, poor governance, weak infrastructure, and high levels of poverty and corruption amplify the economic and humanitarian losses associated with significant natural hazards events. In the Natural Hazards Vulnerability Index, Africa hosts eight out of the nine most vulnerable countries, with South Sudan (1), Burundi (2), Afghanistan (3), Eritrea (4), Chad (5) Niger (6), Sudan (7), Mali (8), and DR Congo (9) all are considered "extreme risk."

Outside of Africa, South Asia is the most vulnerable region. Despite progress in recent years, rapid economic growth is yet to translate into the development of resilience at the community level, including bolstering healthcare and education provision. Additionally, the capacity of these countries' building stocks to withstand hazards is typically inadequate. This was evident during the April 2015 earthquake in Nepal (31), where a lack of institutional capacity and poor infrastructure contributed to a death toll of more than 9,000 people and left many communities isolated for days afterwards.

Water problems in Asia's future?

By Peter Dizikes

Source: http://www.homelandsecuritynewswire.com/dr20160331-water-problems-in-asia-s-future

Mar 31 – **Economic and population growth on top of climate change could lead to serious water shortages across a broad swath of Asia by the year 2050, a newly published study by MIT scientists has found.**

The study deploys detailed modeling to produce what the researchers believe is a full range of scenarios involving water availability and use in the future. In the paper, the scientists conclude there is a "high risk of severe water stress" in much of an area that is home to roughly half the world's population.

Having run a large number of simulations of future scenarios, the researchers find that the median amounts of projected growth and climate change in the next thirty-five years in Asia would lead to about one billion more people becoming "water-stressed" compared to today.

And while climate change is expected to have serious effects on the water supply in many parts of the world, the study underscores the extent to which industrial expansion and population growth may by themselves exacerbate water-access problems.

"It's not just a climate change issue," says Adam Schlosser, a senior research scientist and deputy director at MIT's Joint Program on the Science and Policy of Global Change and a co-author of the study. **"We simply cannot ignore that economic and population**

growth in society can have a very strong influence on our demand for resources and how we manage them. And climate, on top of that, can lead to substantial magnifications to those stresses."

The paper, "Projections of Water Stress Based on an Ensemble of Socioeconomic Growth and Climate Change Scenarios: A Case Study in Asia," was published in the journal *PLOS One*. The lead author is Charles Fant, a researcher at the Joint Program. The other co-authors are Schlosser; Xiang Gao and Kenneth Strzepek, who are also researchers at the Joint Program; and John Reilly, a co-director of the Joint Program who is a senior lecturer at the MIT Sloan School of Management.

Teasing out human and environmental factors

To conduct the study, the scientists built upon an existing model developed previously at MIT, the Integrated Global Systems Model (IGSM), which contains probabilistic projections of population growth, economic expansion, climate, and carbon emissions from human activity. They then linked the IGSM model to detailed models of water use for a large portion of Asia encompassing China, India, and many smaller nations.

The scientists then ran an extensive series of repeated projections using varying conditions. In what they call the "Just Growth" scenario, they held climate conditions constant and evaluated the effects of economic and population growth on the water supply. In an alternate "Just Climate" scenario, the scientists held growth constant and evaluated climate-change effects alone. And in a "Climate and Growth" scenario, they studied the impact of rising economic activity, growing populations, and climate change.

Approaching it this way gave the researchers a "unique ability to tease out the human [economic] and environmental" factors leading to water shortages and to assess their relative significance, Schlosser says.

This kind of modeling also allowed the group to assess some of the particular factors that affect the different countries in the region to varying extents.

"For China, it looks like industrial growth [has the greatest impact] as people get wealthier," says Fant. "In India, population growth has a huge effect. It varies by region."

The researchers also emphasize that evaluating the future of any area's water supply is not as simple as adding the effects of economic growth and climate change, and it depends on the networked water supply into and out of that area. The model uses a network of water basins, and as Schlosser notes, "What happens upstream affects downstream basins." If climate change lowers the amount of rainfall near upstream basins while the population grows everywhere, then basins farther away from the initial water shortage would be affected more acutely.

Future research directions

Other scholars who have examined the work say it makes a valuable contribution to the field. "They're looking at a really important issue for the world," says Channing Arndt, an agricultural economist at the United Nations' World Institute for Development Economics Research, who thinks that the basic finding of the study "makes sense."

Arndt also believes that the ambitious scope of the study, and the way it evaluates the effects of climate change as well as economic and population growth, is a worthwhile approach. "Doing it in this integrated way is the right way to go about it," he adds.

The research team is continuing to work on related projects, including one on the effects of mitigation on water shortages. While those studies are not finished, the researchers say that changing water-use practices can have significant effects.

"We are assessing the extent to which climate mitigation and adaptation practices — such as more efficient irrigation technologies — can reduce the future risk of nations under high water stress," Schlosser says. "Our preliminary findings indicate strong cases for effective actions and measures to reduce risk."

The researchers say they will continue to look at ways of fine-tuning their modeling in order to refine their likelihood estimates of significant water shortages in the future.

"The emphasis in this work was to consider the whole range of plausible outcomes," Schlosser says. "We consider this an important step in our ability to identify the sources of changing risk and large-scale solutions to risk reduction."

— Read more in Charles Fant et al., "Projections of Water Stress Based on an Ensemble of Socioeconomic Growth and Climate Change Scenarios: A Case Study in Asia," is being published today in the journal PLOS One (30 March 2016).

Selected Articles: Poverty and Social Inequality

By Global Research News

The Winds of a New Economic Recession Gather Force in the United States

By Ariel Noyola Rodríguez, April 01 2016

…inflation has not increased in any significant way and unemployment has been chronic in more than 30 states of the American Union, with this, the dangers of deflation persist and with this a new recession.

Housing Crisis, Bankruptcies, Schools, Water: Michigan Struggles Expose Failure of Ruling Class Policies

By Abayomi Azikiwe, March 30 2016

Members of the Moratorium NOW! Coalition and other community-based organizations held a demonstration outside the Wayne County Treasurer's Office on March 23 demanding a moratorium on the scheduled 30,000 tax foreclosures set for March 31.

Poverty and Social Inequality in Canada: The Debate on Basic Income and Guaranteed Annual Income (GAI)

By John Clarke, April 01 2016

Both the Trudeau Liberals in Ottawa and the Wynne Government at Queen's Park in Toronto have been making noises of late on the subject of Basic Income.

French Workers, Youth Defy State of Emergency to Protest Austerity Policies

By Anthony Torres, April 01 2016

Masses of workers and youth, 1.2 million according to union sources and 390,000 according to police, protested Thursday across France against the labour law reform of Labour Minister Myriam El Khomri.

Expensive Weapons of Mass Destruction: As Saudi and Allies Bombard Yemen, US Clocks up $33 Billion Arms Sales in Eleven Months

By Felicity Arbuthnot, April 01 2016

The latest jaw dropper, as Saudi Arabia continues to bombard Yemen with US and UK armaments, dropped by US and UK-made aircraft, is sales worth $33 Billion in just eleven months to the Gulf Cooperation Council (GCC) according to Defense News.

Starvation is only one crop breeding cycle away

Source: http://www.homelandsecuritynewswire.com/dr20160401-starvation-is-only-one-crop-breeding-cycle-away

Apt 01 – **In the race against world hunger, we are running out of time. By 2050, the global population will have grown and urbanized so much that we will need to produce 87 percent more of the four primary food crops – rice, wheat, soy, and maize – than we do today.**

At the same time, the climate is projected to change over the next thirty years, with warmer temperatures and more carbon dioxide (CO_2) in the atmosphere. Crop plants can adapt to change through evolution, but at a much slower rate than the changes we are causing in the atmosphere. Furthermore, the land available for growing crop plants is unlikely to expand to accommodate the predicted rise in demand. In fact, land suited to food crop production is being lost on a global scale.

"We have to start increasing production now, faster than we ever have. Any innovation we make today won't be ready to go

into farmers' fields for at least twenty years, because we'll need time for testing, product development, and approval by government agencies. On that basis, 2050 is not so far off. That's why we say we're one crop breeding cycle away from starvation," says University of Illinois crop scientist Stephen P. Long.

U of I reports thatresearchers at the University of Illinois, along with their large, multi-institution team, say a solution lies in genetically engineering photosynthetic mechanisms to take advantage of the projected rise in global temperatures and CO2, and to achieve much higher yields on the same amount of land.

"The rate of photosynthesis in crops like soy and rice is determined by two factors," Long explains. "One is the enzyme which traps the CO2: we call that rubisco. Under lower atmospheric CO2 levels and at high temperatures, rubisco can make a mistake and use oxygen instead of CO2. When it uses oxygen, it actually ends up releasing CO2 back into the atmosphere."

Under higher levels of CO2, such as those projected for future climates, rubisco becomes much more efficient and photosynthesis rates naturally increase as it makes fewer mistakes. The carbon fixed by rubisco is eventually turned into carbohydrates that the plant can use as an energy source for producing grains, fruits, and vegetative structures.

However, rising temperatures are projected to accompany increased CO2. Unfortunately, rubisco's increased efficiency under high CO2 begins to break down in hot climates. This is why project partners are looking to improve rubisco so that it will operate efficiently in both high temperature and high CO2 conditions.

"Our partners are looking at a wide range of rubiscos from different organisms to see whether they can find one that will make fewer of these mistakes in hot climates," Long says.

But the team is not stopping at improving rubisco.

Long adds, "The second factor that can limit photosynthesis is the rate at which everything else in the leaf regenerates the CO2-acceptor molecule, known as RuBP. As we go to higher CO2 levels, instead of being limited by rubisco, we're limited by this regeneration step. We're looking at ways to manipulate the speed of that regeneration."

The researchers developed mathematical models that showed how, by altering the way nitrogen is divided between parts of the photosynthetic apparatus, more carbohydrate could be made under conditions of higher temperature and CO2 without the crop requiring more nitrogen fertilizer.

The models were then taken for a test-run in the field. Using genetic engineering methods, the team tried to speed up the regeneration of RuBP in tobacco plants while subjecting them to high-CO2 environments. The proof of concept worked: photosynthesis rates and yield increased.

The group's next step will include tests on staple food crops in controlled environments and in field trials. Long stresses that this potential solution won't be ready for commercial roll-out for many years, but they won't give up.

"In the face of the extraordinary challenges ahead, we simply do not have the luxury to rule out the use of any technology that may hold promise to improve crop performance," he notes.

— Read more in Johannes Kromdijk, Stephen P. Long, "One crop breeding cycle from starvation? How engineering crop photosynthesis for rising CO2 and temperature could be one important route to alleviation," Proceedings of the Royal Society B (9 March 2016).

ICM ANNUAL CRISIS REPORT

NEWS COVERAGE OF BUSINESS CRISES IN 2015

Issued March 2016

Source:http://crisisconsultant.com/wp-content/uploads/2014/11/ICM-Annual-Crisis-Report-for-2015.Issued_March22.2016.pdf

Once again in 2015, many of the oldest and most trusted organizations in the world found them-selves in crisis. The **Institute for Crisis Management** tracked a total of 212,115 crisis stories in the news in 2015, a six percent decrease from the previous year. The crises in the news were no less alarming than 2014, however. Perhaps more so.

Most Crisis-Prone Industries in 2015

- Food
- Energy
- Automotive Manufacturing
- Transportation
- Banking, Insurance & Financial Services
- Education
- Government Agencies
- Pharmaceuticals
- Health Care
- Retail

ICM DEFINITION of a BUSINESS CRISIS

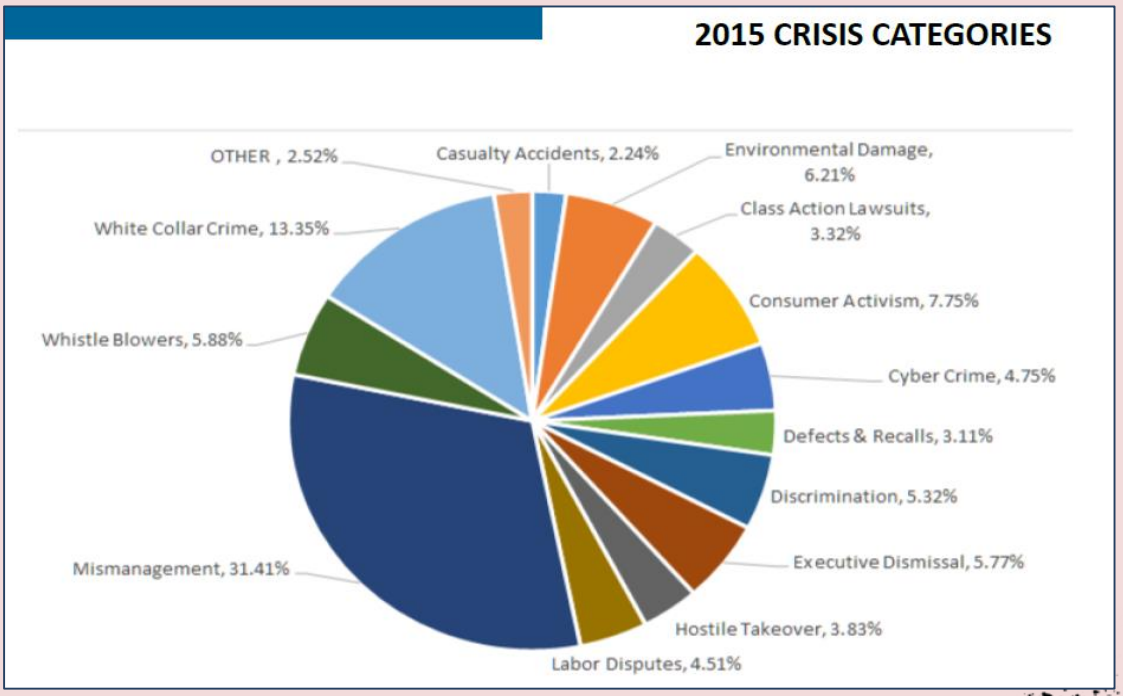
Any issue, problem or disruption which triggers negative stakeholder reactions that impact the organization's business and financial strength

TYPES OF BUSINESS CRISES

Sudden Perceptual Smoldering Bizarre

Cyber-crime and data breaches at industry stal-warts like Hyatt, Hilton and Starwood, Jeep, T-Mobile, Experian, Scottrade and others continue to challenge hundreds of organizations of all kinds. In the US alone, 781 breaches were reported. And for every breach that was reported, there are surely dozens more that we nev-er heard about.

FedEx captured head-lines when the company was indicted in federal court with allegations it knowingly shipped illegal prescription drugs from two online pharmacies. Money laundering charg-es later were added, alleg-ing the online pharmacies paid their FedEx bill with money obtained illegally. UPS settled similar charges in 2014, paying $40 million in fines. Brazil's state-run oil firm Petrobras stayed in the news throughout the year amid a widening corruption scandal.



▶ **Read the full report at source's URL.**