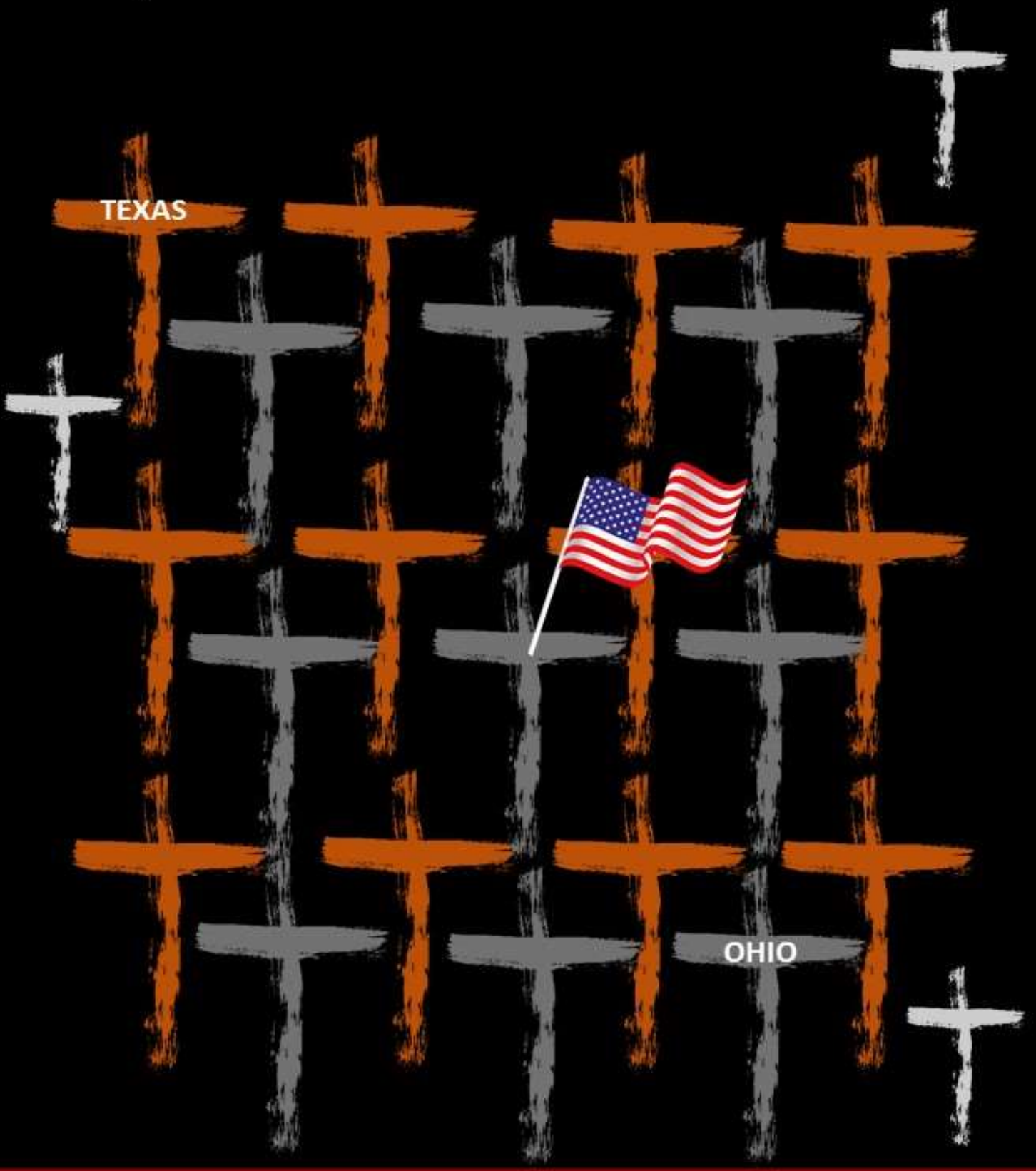
2 CBRNE DIARY

Dedicated to Global First Responders

August 2019



www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

DIRTY R-NEWS

Turkey's Akkuyu nuclear plant facing numerous safety concerns - Birgün

Source: https://ahvalnews.com/akkuyu/turkeys-akkuyu-nuclear-plant-facing-numerous-safety-concerns-birgun

July 22 – Top-level officials working at Turkey's Akkuyu Nuclear Power Plant construction project say a series of problems, including lack of design adaptation and a shortage of competent engineers on site, are posing serious safety concerns, left-wing Birgün newspaper reported.

Located in Turkey's Mediterranean coastal town of Mersin, Turkey's first nuclear power plant Akkuyu is a

joint Russian-Turkish project with Russian energy company Rosatom as the majority stakeholder. President Recep Tayyip Erdoğan and his Russian counterpart Vladimir Putin kicked off the construction of the plant on Apr. 3 amid concerns about the potentially destructive ecological consequences of the plant.

The project hit a snag in May when fissures discovered in the foundations, according to pro-government outlet HaberTürk. New concrete was laid only for more cracks to be discovered.

The problem of the cracks, discovered by Turkey's Atomic Energy Authority (TAEK), have since been fixed, however the foundation of the plant remains a problem.
The design of the plant was created with Russian landscape and weather in mind and is in need of revision to be adapted to Turkey's warm climate, officials told Birgün.
"For example, sloping in the mountains should be conducted in a more horizontal fashion, but it has been done vertically to minimise costs and this is resulting the boulders continually rolling down the hills," one official said.
The ground the plant is being built on, which according to a geology engineer, who spoke on condition of anonymity, is filled with gaps and cannot support the plant.
"Technically speaking, you can construct a structure over any kind of surface. However, the structure at hand is not a copy-paste matter, it must be revised according to the present surface. None of this is happening because the engineers of the project are not competent," the engineer said, pointing to gaps that may lead to condensation, among other problems.
The project is run entirely on the "past experiences" contractors, one official said. "They are acting as though a building is being constructed instead of a nuclear reactor. And even during the process of constructing a building, a much more serious plan of action is followed."
The cooling of the plant is to take place through the waters of the Mediterranean Sea.
The warm water to be released into the sea after the cooling process, a chemical engineer who spoke to left-wing Birgün daily said, will lead to increased temperatures in the water, which in turn affects marine life.
"Chlorine is placed in the water to avoid mussels etc. from sticking to the pipes used to draw the water. And then this water, which now naturally has chlorine in it, is released into the sea," the official said. "Imagine the damage this can create in the sea, which is filled with living organisms."

460,000 Premature Deaths: The Horror That Was Nuclear Weapons Testing

Source: http://www.homelandsecuritynewswire.com/dr20190729-460-000-premature-deaths-the-horror-that-was-nuclear-weapons-testing

July 29 – For a brief fraction of a second on an early March morning in 1954, the United States summoned a second sun into existence above Bikini Atoll. This was the Castle Bravo thermonuclear test, one of several dozen nuclear detonations the United States carried out in the Marshall Islands during the Cold War. At 15 million tons of TNT—one *thousand* times more powerful than the bomb that destroyed Hiroshima—it was the largest explosion ever set off by Americans.

Zack Brown and Alex Spire write in the *National Interest* that it was also the dirtiest, as a new study published this month shows. Researchers from Columbia University, analyzing soil samples from , Researchers from Columbia University, analyzing soil samples from several Marshall Island atolls, discovered widespread radioactivity. Bikini Island itself was declared unsafe for human habitation, while the three other atolls had significant radionuclide concentrations—mainly americium, cesium, and plutonium. In some cases, the level of radioactivity—more than sixty years since the last mushroom cloud loomed over Bikini's azure lagoon—exceeded that found at Chernobyl or Fukushima.
Brown and Spire note that American nuclear testing didn't just occur in the middle of the Pacific. Throughout the Cold War, the United States detonated *hundreds* of atomic

bombs in Nevada at a test site just northwest of Las Vegas. Many of these tests were above-ground, exposing the continental United States to the same radioactive fallout that fell over those remote atolls.
As with the Marshall Islands, the radiological effects of this testing were widespread—and immense. A 2017 study from the University of Arizona suggested that the fallout generated by the Nevada nuclear explosions exposed millions of Americans to its lethal radiation. The study suggested that fallout from the Nevada nuclear testing could have led to between 340,000 and 460,000 premature deaths, mostly Americans and mainly through cancer.

The Threat of an Electromagnetic Attack

Source: http://www.homelandsecuritynewswire.com/dr20190729-the-threat-of-an-electromagnetic-attack

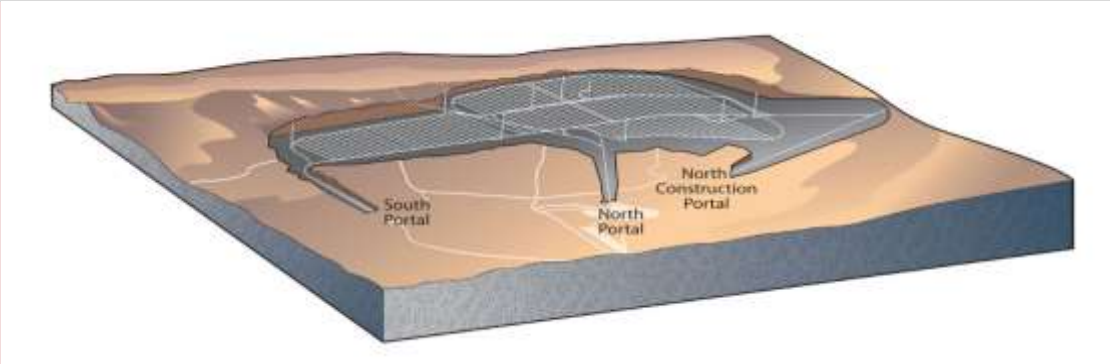
July 29 – When much of Venezuela was plunged into darkness after a massive blackout this week, President Nicolás Maduro blamed the power outage on an "electromagnetic attack" carried out by the U.S.

The claim was met with skepticism. Blackouts are a regrettably frequent part of life in Venezuela, where the electric grid has fallen into serious disrepair.
Nevertheless, AP writes, Maduro's claim has raised questions over what exactly is an electromagnetic attack, how likely is it to occur and what impact could it have.
In the 1962, during the Cold War, the U.S. detonated a nuclear weapon above the atmosphere over the Pacific Ocean, and the experiment — known as Starfish Prime — knocked out power to traffic lights and telecommunications in parts of Honolulu, illuminating the sky and even leading hotels to host viewing parties, according to news reports.
Russia conducted a series of "high-altitude nuclear bursts" in 1961 and 1962 to test electromagnetic pulse impacts over Kazakhstan and destroyed that country's electrical grid, according to testimony to Congress from the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

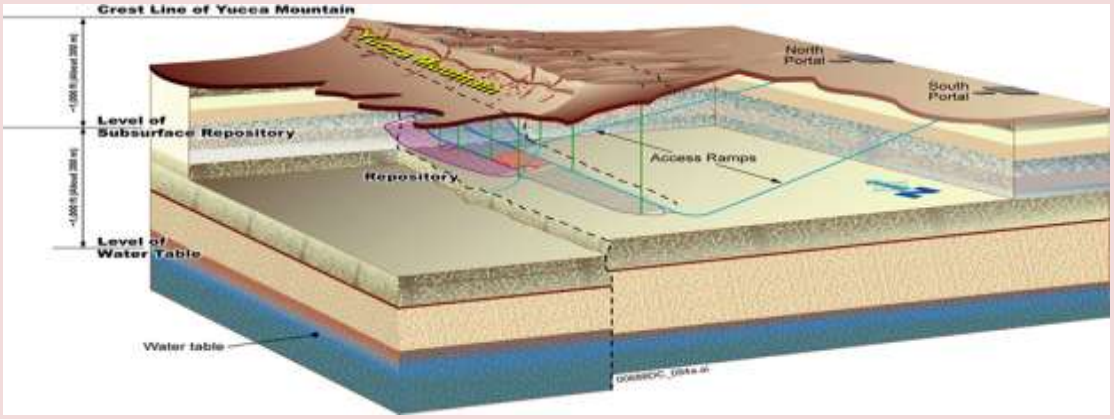
Truth and Fearmongering: Yucca Mountain Nuclear Waste Repository

Source: http://www.homelandsecuritynewswire.com/dr20190729-truth-and-fearmongering-yucca-mountain-nuclear-waste-repository

July 29 – Last month, Alex Berezow wrote an op-ed for *USA Today* about Yucca Mountain. The argument he made, in a nutshell, is that the nuclear waste storage facility that has already been built is safe and should be opened for business. However, because Nevadans are (improperly) worried about the safety of the Yucca facility, he suggested that the federal government offer to pay each of the state's citizens $500 each year (for 10 years) as "rent." This provides financial compensation for the risk of hosting the site, even though the risk is exceedingly small.



In a post on the website of the American Council on Science and Health, Berezow writes in the usual counterargument is, "F*** you." Nevada Congresswoman Susie Lee also weighed in. While her counterargument is at least civil, Berezow argues that it spreads disinformation about geology and public health.



He says that an absolutely excellent, must-read article by physicist Dr. Richard Muller explains the science behind nuclear waste disposal. We routinely say that nuclear waste needs to be secure for about 10,000 years. This is because, by then, most of the radioactivity has decayed away. But in reality, after merely

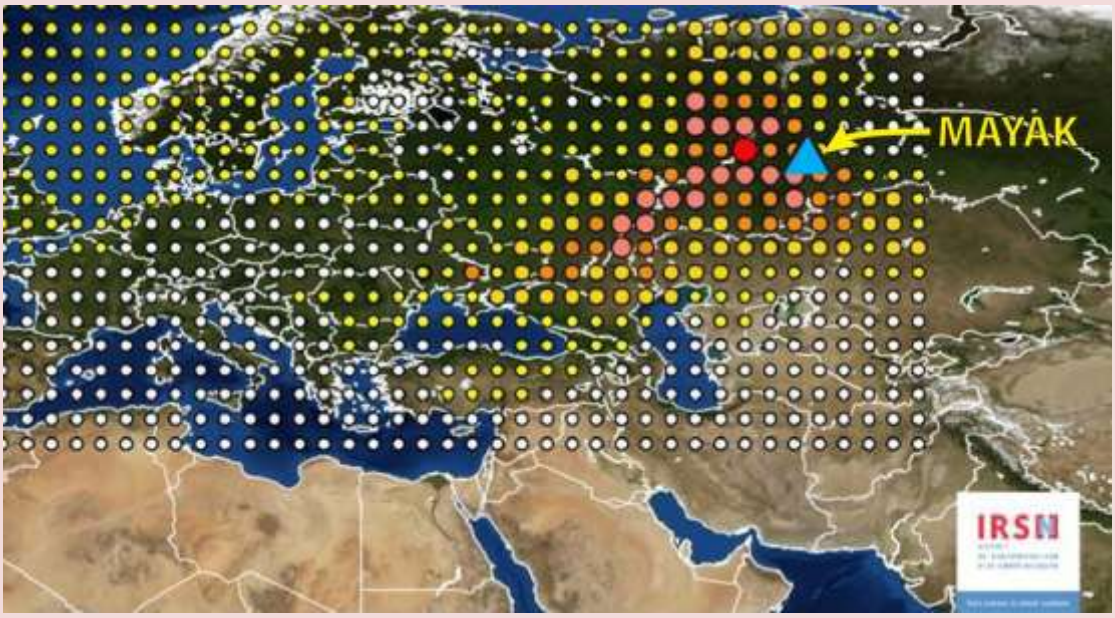
300 years, the level of radioactivity has declined by roughly 90 percent. So, the question is not, "Can we guarantee that Yucca is eternally secure forever and ever amen?" but "Can we ensure that Yucca is safe for about 300 years?" And that answer is yes.
Here is the excerpt from Muller's article:

Colorado, where much of the uranium is obtained, is a geologically active region, full of faults and fissures and mountains rising out of the prairie, and its surface rock contains about a billion tons of uranium. The radioactivity in this uranium is 20 times greater than the legal limit for Yucca Mountain, and it will take more than 13 billion years—not just a few hundred—for the radioactivity to drop by a factor of 10. Yet water that runs through, around, and over this radioactive rock is the source of the Colorado River, which is used for drinking water in much of the West, including Los Angeles and San Diego. And unlike the glass pellets that store the waste in Yucca Mountain, most of the uranium in the Colorado ground is water-soluble. Here is the absurd-sounding conclusion: *if the Yucca Mountain facility were at full capacity and all the waste leaked out of its glass containment immediately and managed to reach groundwater, the danger would still be 20 times less than that currently posed by natural uranium leaching into the Colorado River* (emphasis added).

Mysterious Radiation Cloud Over Europe Traced to Secret Russian Nuclear Accident

Source: https://www.livescience.com/66050-radiation-cloud-secret-russian-nuclear-accident.html

July 29 – A vast cloud of nuclear radiation that spread over continental Europe in 2017 has been traced to an unacknowledged nuclear accident in southern Russia, according to an international team of scientists.



The experts say the cloud of radiation detected over Europe in late September 2017 could only have been caused by a nuclear fuel-reprocessing accident at the Mayak Production Association, a nuclear facility in the Chelyabinsk region of the Ural Mountains in Russia, sometime between noon on Sept. 26 and noon on Sept. 27.

Russia confirmed that a cloud of nuclear radiation was detected over the Urals at the time, but the country never acknowledged any responsibility for a radiation leak, nor has it ever admitted that a nuclear accident took place at Mayak in 2017. [Top 10 Greatest Explosions Ever]

The lead author of the new research, nuclear chemist Georg Steinhauser of Leibniz University in Hanover, Germany, said that more than 1,300 atmospheric measurements from around the world showed that between 250 and 400 terabecquerels of radioactive ruthenium-106 had been released during that time.

In early October 2017, several European countries detected elevated levels of ruthenium-106 above the continent. Based on concentration levels, the likely source of contamination was located around the Ural Mountains. *Credit: ISRN*

Ruthenium-106 is a radioactive isotope of ruthenium, meaning that it has a different number of neutrons in its nucleus than the naturally occurring element has. The isotope can be produced as a byproduct during nuclear fission of uranium-235 atoms.
Although the resulting cloud of nuclear radiation was diluted enough that it caused no harm to people beneath it, the total radioactivity was between 30 and 100 times the level of radiation released after the Fukushima accident in Japan in 2011, Steinhauser told Live Science.
The research was published today (July 29) in the journal Proceedings of the National Academy of Sciences.

Ruthenium release
The cloud of radiation in September 2017 was detected in central and eastern Europe, Asia, the Arabian Peninsula and even the Caribbean.

Only radioactive ruthenium-106 — a byproduct of nuclear fission, with a half-life of 374 days — was detected in the cloud — Steinhauser said.
During the reprocessing of nuclear fuel — when radioactive plutonium and uranium are separated from spent nuclear fuel from nuclear power reactors — ruthenium-106 is typically separated out and placed into long-term storage with other radioactive waste byproducts, he said.
That meant that any massive release of ruthenium could only come from an accident during nuclear fuel reprocessing; and the Mayak facility was one of only a few places in the world that carries out that sort of reprocessing, he said.
Advanced meteorological studies made as part of this new research showed that the radiation cloud could only have come from the Mayak facility in Russia. "They have done a very thorough analysis and they have pinned down Mayak — there is no doubt about it," he said.
The accident came a little more than 60 years since a nuclear accident at Mayak in 1957 caused one of the largest releases of radiation in the region's history, second only to the 1986 explosion and fire at the Chernobyl nuclear power plant, which is now in the Ukraine. [Chernobyl Nuclear Disaster 25 Years Later (Infographic)]

In the 1957 accident, known as the Kyshtym disaster after a nearby town, a tank of liquid nuclear waste at the Mayak facility exploded, spreading radioactive particles over the site and causing a radioactive plume of smoke that stretched for hundreds of miles.

Nuclear accident

The study showed that the 2017 accident at Mayak was unlikely to have been caused by a relatively simple release of radioactive gas, Steinhauser said. Rather, a fire, or even an explosion, might have exposed workers at the plant to harmful levels of

Russia has not acknowledged that any accident occurred at the Mayak facility, maybe because plutonium is made there for thermonuclear weapons. However, Russia had established a commission to investigate the radioactive cloud, Steinhauser said.

The Russian commission ruled that there was not enough evidence to determine if a nuclear accident was responsible for the cloud. But Steinhauser and his team hope it may look again at this decision in the light of the new research.

"They came to the conclusion that they need more data," he said. "And so we feel like, okay, now you can have all of our data — but we would like to see yours as well."

Any information from Russia about an accident at the Mayak facility would help scientists refine their research, instead of having to rely only on measurements of radioactivity from around the world, Steinhauser said.

The international team of scientists involved are keenly interested in learning more about its causes. "When everybody else is concerned, we are almost cheering for joy, because we have something to measure," he said. "But it is our responsibility to learn from this accident. This is not about blaming Russia, but it is about learning our lessons," he said.

Improving Security of Nuclear Materials Transportation

Source: http://www.homelandsecuritynewswire.com/dr20190731-improving-security-of-nuclear-materials-transportation

July 31 – Nuclear power plants can withstand most inclement weather and do not emit harmful greenhouse gases. However, trafficking of the nuclear materials to furnish them with fuel remains a serious issue as security technology continues to be developed.

Two physicists working out of the University of Florida and Pacific Northwest National Laboratory, Paul Johns and Juan Nino, conducted research to enhance global nuclear security by improving radiation detectors. According to them, improving radiation detectors requires the identification of better sensor materials and the development of smarter algorithms to process detector signals. They discuss their work in this week's *Journal of Applied Physics*, from AIP Publishing.

"The end users of radiation detectors don't necessarily have a background in physics that allows them to make decisions based on the signals that come in," Johns said. "The algorithms used to energy-stabilize and identify radioactive isotopes from a gamma ray spectrum are therefore key to making detectors useful and reliable. When sensors can

provide better signal resolution, algorithms are able to more accurately inform users about the radiation sources in their environment."
Currently, no single radiation detector is perfect for every application. With size, signal resolution, weight, and cost all being factors, designing the ideal detector has proved to be a major challenge.
AIP says that Johns and Nino examined a list of potential compounds for room temperature semiconductor detectors, which don't need to cool a sensor down to cryogenic temperatures for them to function properly, and identified several prime candidates. When choosing between compounds, the authors considered the cost, practicality and efficiency of each.
After assessing a diverse list of more than 60 candidates for alternative semiconductor compounds, the authors concluded that hybrid organic-inorganic perovskite — a mineral consisting mainly of calcium titanate — has the strongest potential among emerging compounds. Hybrid perovskites can be easily synthesized and grown via solution over the course of only several hours to a couple of days as opposed to the weeks or months that it takes to produce conventional sensors. Their cost efficiency, yield and output rate lead the authors to believe that if their stability can be improved, these compounds will be at the forefront of room temperature semiconductor detector research.

Security challenge
Equipping law enforcement and first responders with the best possible radiation detectors is key to detecting, identifying and, ultimately, prohibiting radioactive threats," said Johns.
To prevent nuclear terrorism and the acquisition and use of weapons of mass destruction, radiation sensors must continue to be updated. Johns and Nino look forward to enhancing global security through improvements to room temperature semiconductor compounds.

5 Unknown Nuclear Disasters: Chernobyl Is Far from the Only One

Source: https://interestingengineering.com/5-unknown-nuclear-disasters-chernobyl-is-far-from-the-only-one

Aug 01 – The recent miniseries "Chernobyl" has scared the daylights out of everyone, but Chernobyl is far from the world's only nuclear disaster. Here are some others that are also worth knowing.

The Kyshtym Disaster

In September 1957, **Ozyorsk, Russia** was a closed city, built around the Mayak plant which produced plutonium for both nuclear weapons and fuel.
After scrambling to build the **Mayak plant** between 1945 and 1948, all six of its reactors initially dumped high-level radioactive waste directly into Lake Kyzyltash. When it became

contaminated, they moved on to dumping into Lake Karachay, which also became contaminated.
In 1953, workers built a storage facility for liquid nuclear waste, but that waste was being heated by residual decay heat from the nuclear reaction. The coolers around one of the tanks failed, and on September 29, 1957, that tank exploded with the force of between 70 to 100 tons of TNT.
While there were no immediate casualties, the explosion released an estimated 20 MCi (800 PBq) of radioactivity into the air. A plume containing 2 MCi (80 PBq) of radionuclides, primarily caesium-137 and strontium-90, moved toward the northeast and contaminated an area of more than 52,000 square kilometers (20,000 sq miles).

Map of the East Urals Radioactive Trace (EURT). *Source: Jan Rieke/Wikimedia Commons*

At least 270,000 people lived in that area, which is referred to as the **East-Ural Radioactive Trace** (EURT).
In an attempt to maintain secrecy, no evacuation was ordered, but a week later, on October 6, 1957, 10,000 people were removed from their homes.
Estimates of the death toll caused by the accident go from 200 to more than 8,000, depending on the study. A 2001 work stated that the accident caused 66 diagnosed cases of chronic radiation syndrome.
Amazingly, it wasn't until 18 years later, in 1976, that the full scope of the disaster was disclosed by **Zhores Medvedev** in the publication the *New Scientist*.
In 1968, the Soviet government disguised the EURT area by creating **East Ural Nature Reserve**, with access allowed to only authorized personnel. Documents describing the disaster were only declassified in 1989.
On the International Nuclear Event Scale (INES), Kyshtym is rated a 6, making it the third-most serious nuclear accident behind only the **Fukushima Daiichi nuclear disaster** and the **Chernobyl disaster**, which are both Level 7.

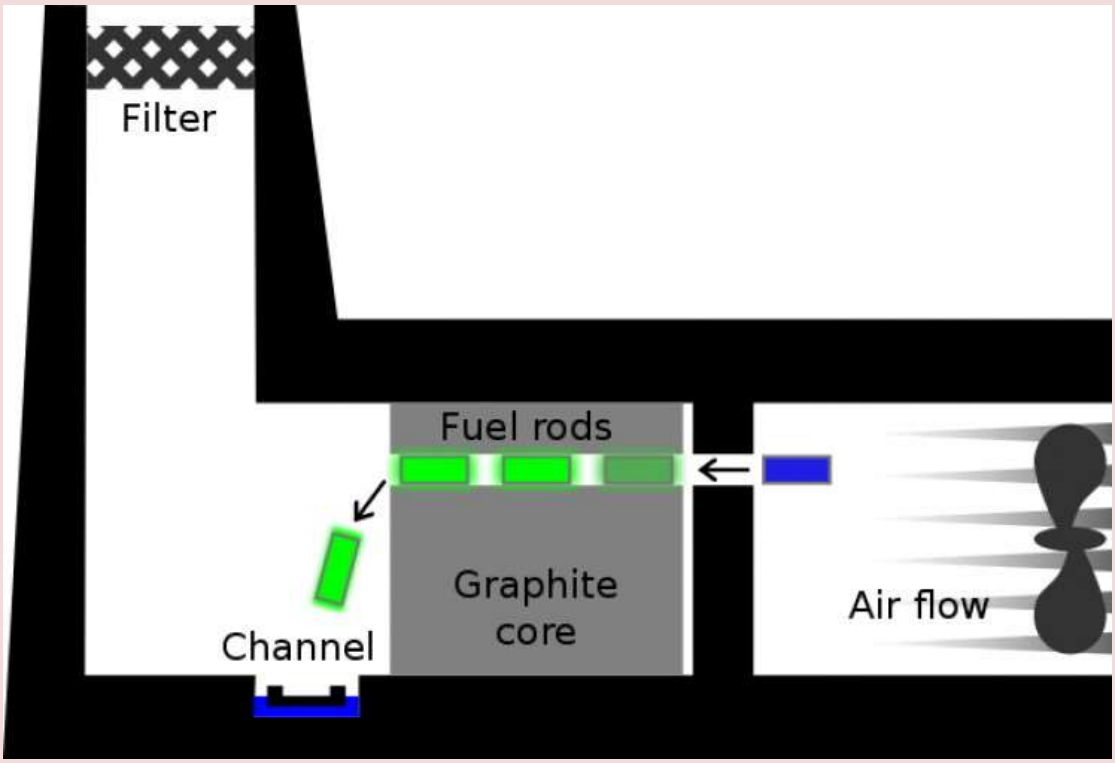
The Windscale Fire

Less than two weeks after Kyshtym, a fire broke out in Unit 1 of the two reactors at the **Windscale** facility located in what is now known as Sellafield, Cumbria UK.
The two reactors were created because of Britain's need for an atomic weapon following World War II. Determining that a uranium enrichment plant would cost ten times as much to

produce the same number of atomic bombs as a nuclear reactor, the decision was made to build a nuclear reactor that would produce plutonium.

Windscale reactors. *Source: Chris Eaton/Wikimedia Commons*

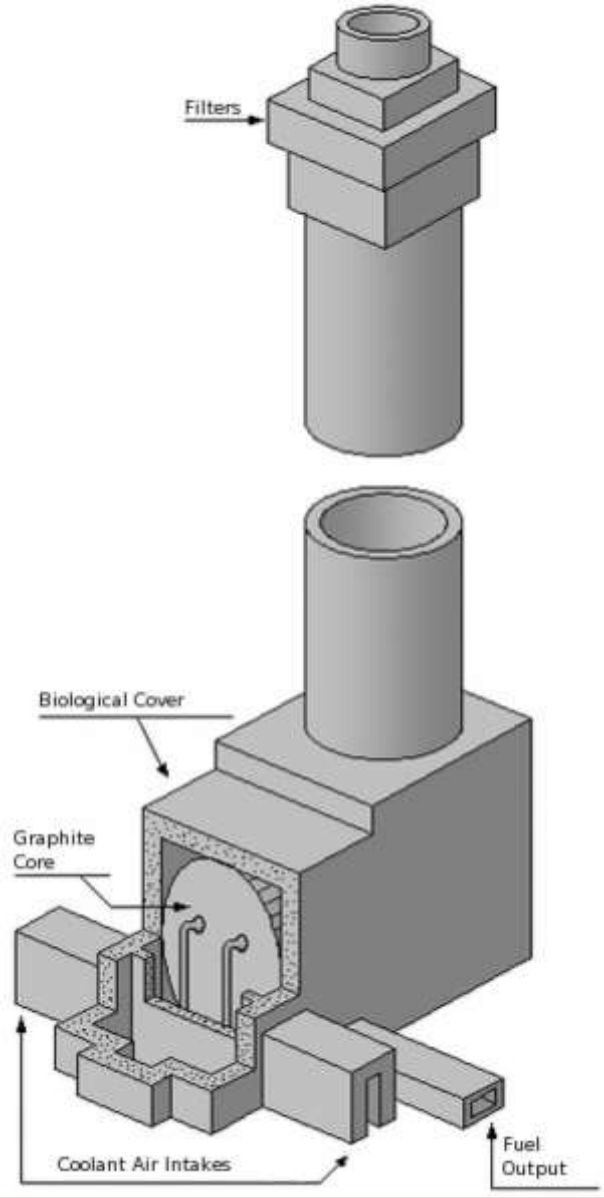
The cores of the reactors were comprised of a large block of graphite, with horizontal channels drilled through it for the fuel cartridges. Each cartridge consisted of a 12-inch-long (30 centimeters) uranium rod encased in aluminum.



Windscale reactor diagram. *Source: HereToHelp/Wikimedia Common*

The reactor was cooled by convection through a 400-foot (120 m) tall chimney. When **Winston Churchill** committed the UK to create a hydrogen bomb, the fuel loads at Windscale were modified to produce *tritium*, but this also meant that the core became hotter.

On the morning of October 10, 1957, the core began to uncontrollably heat, eventually reaching 400 degrees C. Cooling fans were brought in to increase the airflow, but just worsened the problem. It was then that operators realized that the core was on fire.



Windscale reactor diagram. *Source: Argentum at pl/Wikimedia Commons*

Workers tried dousing the core first in carbon dioxide, then in water, but both proved ineffective. What finally worked was cutting off air to the reactor building, which starved the fire.
The fire caused the release of radioactive radionuclides across the UK and Europe, including an estimated 740 terabecquerels (20,000 curies) of iodine-131, 22 TBq (594 curies) of caesium-137 and 12,000 TBq (324,000 curies) of xenon-133.
By comparison, the 1986 Chernobyl explosion released far more, and the **Three Mile Island** accident in 1979 in the U.S. released 25 times more xenon-135 than Windscale, but less iodine, caesium, and strontium. The atmospheric release of xenon-133 by the Fukushima Daiichi nuclear disaster was similar to that released at Chernobyl, and thus, high above what the Windscale fire released.
There were no evacuations of the surrounding area, but it has been estimated that the incident caused 240 additional cancer cases. For a month after the accident, milk coming from 500 square kilometers (190 sq mi) of the nearby countryside was destroyed.
The reactor tank has remained sealed since the accident and still contains about 15 tons of uranium fuel. The reactor core is still slightly warm due to continuing nuclear reactions. It is not scheduled for final decommissioning until 2037. On the International Nuclear Event Scale, Windscale ranks at level 5.

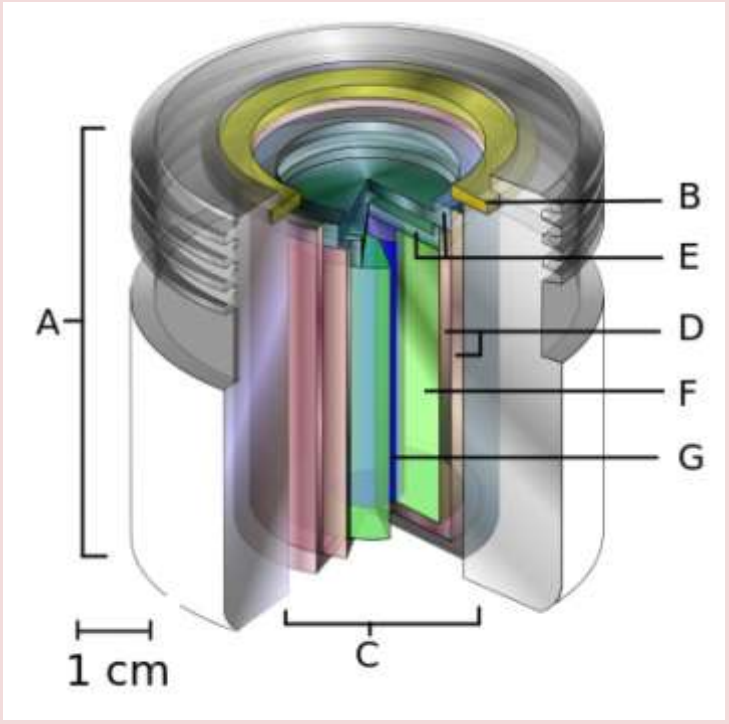
Soviet Submarine K-19

K-19 was one of what the Soviets called their Project 658-class submarines, while NATO called them Hotel-class. They were the first generation of nuclear submarines equipped with nuclear ballistic missiles.
Commissioned on April 30, 1961, K-19 was snake bit from the start. On its initial voyage, on July 4, 1961, it was conducting exercises off the coast of Greenland when suddenly, pressure in the reactor's cooling system dropped to zero due to a leak.
The emergency SCRAM system immediately inserted the control rods, but due to decay heat, the reactor's temperature rose to 800 degrees C (1,470 degrees F). The accident released steam containing fission products throughout the ship through the ventilation system.
The captain ordered the ship's engineering crew to fabricate a new cooling system, but this required them to work within the radioactive area. The jury-rigged cooling water system prevented a complete meltdown of the reactor core.
American warships nearby had picked up K-19's distress call and offered to help, but K-19's captain, fearful of giving away Soviet military secrets, refused. Instead, K-19 sailed to meet up with a diesel-powered Soviet submarine. The accident had irradiated K-19's entire crew, as well as the ship and some of her ballistic missiles.
Within a month, all eight members of the ship's engineering crew died of radiation exposure. They are **Boris Korchilov**, **Boris Ryzhikov**, **Yuriy Ordochkin**, **Evgeny Kashenkov**, **Semyon Penkov**, **Nicolai Savkin**, **Valery Charitonov**, and **Yuriy Povstyev**.

Within the next two years, 15 other sailors died of radiation-related illnesses.
Towed into port, K-19 contaminated a 700 meter (2,300 feet) wide area, and the repair crews who worked on her. Eventually, the Soviet Navy dumped the damaged reactor into the Kara Sea.
The 2002 movie *K-19: the Windowmaker,* which starred Harrison Ford and Liam Neeson, is based on the K-19 disaster.

The Goiânia Accident

In the 1980s, the Instituto Goiano de Radioterapia (IGR) was a private radiotherapy hospital in Goiânia, Brazil. When it moved to a new facility in 1985, a caesium-137-based therapy unit was left behind. The caesium-137 was encased in a shielding canister made of lead and steel.



Goiania capsule Source: *KDS444/Wikimedia Commons*

A. an international standard source holder (usually lead),
B. a retaining ring, and
C. a teletherapy "source" composed of
D. two nested stainless steel canisters welded to two
E. stainless steel lids surrounding an
F. internal shield (usually uranium metal or a tungsten alloy) that protects a
G. cylinder of radioactive source material, often but not always cobalt-60. The diameter of the "source" is 30mm.

Legal wrangling prevented the canister from being removed from the facility, and the court posted a security guard to protect the equipment. Unfortunately, that guard was nowhere to be found on September 13, 1987, when two men, **Roberto dos Santos Alves** and **Wagner Mota Pereira**, entered the facility and made off with the equipment, placing it in a wheelbarrow and taking it to Alves's house.
There, they began dismantling the equipment, and both immediately began to vomit. The next day, Pereira noticed a burn on his hand that required the amputation of several fingers.
Alves soldiered on, piercing the canister with a screwdriver. He noticed the blue light of **Cherenkov radiation**. Alves's arm ulcerated and had to be amputated, but before that, he sold the items to a scrapyard owned by **Devair Alves Ferreira**.
Fascinated by the blue glow being emitted, Ferreira carried the items into his house, and over the next three days, he invited his friends and family in to observe the blue glow.
Ferreira's brother brought some of the caesium to his house where he sprinkled it onto a floor. There, his six-year-old daughter, **Leide das Neves Ferreira**, sat down and ate a sandwich.
Eventually, Ferreira's wife took the caesium to a hospital, and news of the radioactive leak was broadcast on local media. 250 people were found to be contaminated by radiation, with 129 people having internal contamination.
Four people would die of radiation sickness including six-year-old Leide, Ferreira's wife **Gabriela**, 37, and two employees of Ferreira, **Israel Baptista dos Santos**, 22, and **Admilson Alves de Souza**, 18.
The Goiânia accident spread significant radioactive contamination throughout the Aeroporto, Central, and Ferroviários districts of Goiânia. Contaminated areas included Alves's house, Devair Ferreira's scrapyard which had extremely high levels of radiation, and his brother Ivo's house.
The "NATO Science for Peace and Security Series" bizarrely found radioactive contamination on:
* Three buses
* 42 houses

* Fourteen cars
* Five pigs
* 50,000 rolls of toilet paper.

The Goiânia accident ranks as a number 5 on the International Nuclear and Radiological Event Scale. A 1990 film about the disaster won several awards at the 1990 Festival de Brasília film festival, and a 1994 episode of the TV series "Star Trek: The Next Generation," "Thine Own Self," was inspired by the Goiânia accident.

Chalk River Ontario, Canada Incident

On December 12, 1952, there was a power excursion and partial loss of coolant in the NRX reactor at the **Chalk River nuclear laboratories**. Because of mechanical problems, the control rods couldn't be lowered into the core, and the fuel rods overheated, resulting in a meltdown of the core.

Just like at Chernobyl, hydrogen gas caused an explosion that blew off the multi-ton reactor vessel seal. Also like at Chernobyl, 4,500 tons of radioactive water was found in the basement of the Chalk River reactor building.

Chalk River nuclear power plant. *Source: Padraic Ryan/Wikimedia Commons*

During the accident, 10,000 curies or 370 TBq of radioactive material was released into the atmosphere. Future U.S. president **Jimmy Carter**, then a U.S. Navy officer, led a team of 13 U.S. Navy volunteers who helped in the cleanup of this disaster.

On the International Nuclear Event Scale, Chalk River is a 5, along with Goiânia, Three Mile Island, and Windscale.

New radiation detector updates will help improve nuclear security

Source: https://www.earth.com/news/radiation-detector-updates-nuclear-security/

Aug 02 – Paul Johns and Juan Nino, from the University of Florida and Pacific Northwest National Laboratory, researched new ways to enhance global nuclear security by improving radiation detectors with the aim being to enhance the safety of trafficking of nuclear materials.

In their study, published in the *Journal of Applied Physics*, Johns and Nino believe that identification of better sensor materials, as well as the development of smarter algorithms to process detector signals, are needed to improve radiation detectors.

"The end users of radiation detectors don't necessarily have a background in physics that allows them to make decisions based on the signals that come in," Johns said.

"The algorithms used to energy-stabilize and identify radioactive isotopes from a gamma ray

spectrum are therefore key to making detectors useful and reliable."
"When sensors can provide better signal resolution," he continued, "algorithms are able to more accurately inform users about the radiation sources in their environment."
Designing the perfect radiation detector is no easy feat. Specific size, signal resolution, weight, and cost are all factors in designing each detector. Johns and Nino chose a compound for a room temperature semiconductor detector, which doesn't need to cool sensors down to cryogenic temperatures to function. They considered cost, practicality, and efficiency of each possible compound before narrowing down their search.
Johns and Nino chose hybrid organic-inorganic perovskite — a mineral consisting mainly of calcium titanate — which they say has the strongest potential among other emerging compounds. Hybrid perovskites can be synthesized and grown via solution over several hours to a couple of days, compared to conventional sensors that take weeks or months to grow.
Furthermore, once their stability is improved, their cost efficiency, yield, and output rate will put these compounds at the forefront of room temperature semiconductor detector research.
Radiation sensors must be updated to avoid nuclear terrorism and acquisition and use of weapons of mass destruction.
"Preventing radioactive materials from being used for harmful purposes is a global nuclear security challenge," Johns said. "Equipping law enforcement and first responders with the best possible radiation detectors is key to detecting, identifying and, ultimately, prohibiting radioactive threats."

2018 Global Incidents and Trafficking Database Identifies 150+ Incidents Involving Nuclear and Radioactive Materials

Source: https://media.nti.org/documents/global_incidents_trafficking_2018.pdf

On July 2019,, NTI released the annual Global Incidents and Trafficking Database , produced exclusively for NTI by the James Martin Center for Nonproliferation Studies (CNS). In 2018 alone, CNS recorded 156 incidents in 23 countries where nuclear and other radioactive materials were found outside of regulatory control. Among them: the loss of 1g of weapons-gram plutonium from a university in the United States. The report includes interactive maps and visualizations that show the entire database at a glance, illustrate incidents of concern, and highlight efforts to secure dangerous materials.

The 2018 database has 156 incidents. Trends remain consistent with the data collected between 2013 and 2017.

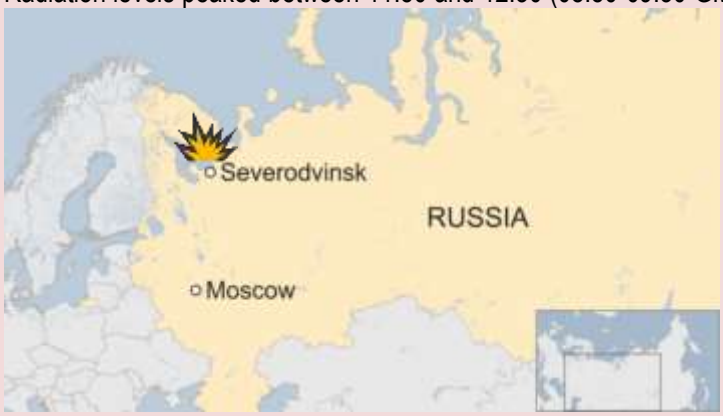
- 58 losses were recorded, constituting 37% of all incidents.
- 45 thefts were recorded, constituting 29% of all incidents.
- 64 incidents occurred during transport, constituting 41% of all incidents

'Brief radiation spike' after rocket engine blast in northern Russia

Source: https://www.bbc.com/news/world-europe-49275577

Aug 08 – A rocket engine explosion on a naval test range in northern Russia has killed two people and injured six, the defence ministry told Russian media.
The victims of the explosion in Arkhangelsk region were civilian specialists while military and civilian personnel are among the injured.
The ministry said radiation levels were normal but the city of Severodvinsk registered a "brief spike" in levels.
An area of the White Sea nearby has reportedly been closed for a month.
But the deputy head of Archangelsk port, Sergei Kozub, told the BBC the closure was planned before the accident.

Radiation levels peaked between 11:50 and 12:30 (08:50-09:30 GMT) before falling and normalising by 14:00, the city administration in Severodvinsk said on its website, without reporting how significant the spike had been.



It is unclear what could have caused radiation levels to rise.

Local people were reportedly urged to take precautions against radiation. No increase in ambulance call-outs was recorded, the administration added.

A woman in Severodvinsk named only Alina told Russian news site lenta.ru: "I work in the hospital where they're bringing the injured.

"They advise everyone to close their windows and drink iodine, 44 drops per glass of water."

Children in local kindergartens were taken indoors after reports of the blast and parents were advised not to take them outside in the evening, other residents were quoted as saying.

What do we know about the explosion?

The defence ministry did not say officially where or when the blast occurred but unofficial sources say it happened near the village of Nyonoksa, where a navy missile test range is located.

Nyonoksa is about 47km (29 miles) west of Severodvinsk, which has a population of nearly 200,000 and is 1,260km from the Russian capital, Moscow.

"During testing of a liquid jet engine an explosion and combustion of the product occurred," the ministry said in a statement.

"There have been no harmful chemicals released into the atmosphere, the radiation levels are normal."

Emergency aircraft were used to airlift the injured. They included defence ministry officials and developer company representatives, who "had injuries of varying severity", the statement added.

There had been earlier reports of a fire at a military facility near Nyonoksa. Telegram-based media outlet Mash said radiation levels in the village were three times higher than normal.

Nyonoksa carries out tests for virtually every missile system used by the Russian navy, including sea-launched intercontinental ballistic missiles, cruise missiles and anti-aircraft missiles.

It is the second accident involving Russia's military this week.

On Monday, one person was killed and eight others were injured in a blaze at an ammunition dump in Siberia.

Flying munitions damaged a school and a kindergarten in the area. More than 9,500 people were evacuated.

An investigation is under way into the cause of the incident.

Russian village evacuation as rocket blast sparks radiation fears

Source: https://www.aljazeera.com/news/europe/2019/08/russian-village-evacuation-rocket-blast-sparks-radiation-fears-190813132704410.html

Aug 13 – Russian authorities have advised residents of a village to leave while clear-up work is being carried out nearby following a mysterious rocket engine accident last week that caused a temporary spike in radiation, according to a report.

Russia's Rosatom nuclear agency said five of its staff were killed in the August 8 blast at a naval facility that tests ballistic missiles used by nuclear submarines. At least three people were injured.

The workers were providing support for the "isotope power source" of a missile and were thrown into the water from the testing platform in the White Sea by the force of the explosion.

On Tuesday, Interfax news agency cited local officials as saying they had received a notification about clear-up work being carried out by military authorities.
"In this regard, residents of Nyonoksa were asked to leave the territory of the village from August 14."
Rosgidromet, the weather monitoring service, said on Tuesday its sensors in Severodvinsk - located about 30km from the test site - registered radiation exceeding background levels by "four to 16 times" on the day of the blast.
The service said the levels were higher at six out of eight of its stations in Severodvinsk and returned to normal after 2.5 hours.
One of the sensors registered a level of 1.78 microsieverts per hour, well above the local average but far below dangerous levels.

Thousands of people attend the burial of five Russian nuclear engineers killed by an explosion [Russian State Atomic Energy Corporation ROSATOM via AP]

The blast caused panic, with residents rushing to buy iodide, which can help limit the damage from exposure to radiation.
Following the explosion, Russian authorities also closed part of Dvina Bay on the White Sea to shipping for a month, in what could be an attempt to prevent outsiders from seeing an operation to recover the missile debris.
Rosatom's mention of a "nuclear isotope power source" led some Russian media to conclude it was the Burevestnik (Petrel), a nuclear-powered cruise missile first revealed by Russian President Vladimir Putin in March 2018 during his state of the nation address along with other doomsday weapons.
Some experts have also linked the blast to the 9M730 Burevestnik nuclear-powered cruise missile, known by NATO as SSC-X-9 Skyfall.
Kremlin spokesman Dmitry Peskov on Tuesday did not confirm that the accident was linked to the Burevestnik project.
Peskov added, however, that Russian research and development in the sphere of nuclear-powered missiles "significantly surpass the level reached by other countries and are rather unique".
Lawrence Korb, a former US assistant secretary of defence who has worked with Russia on nuclear issues and arms control, said the so-called Skyfall weapon is considered a "fantasy" by most experts in the United States as "it's a very dangerous thing".
"It sounds great in theory but as we've seen with this accident, it's much easier said than done and the chances of having accidents are great because you have a nuclear weapon with nuclear fuel so that's a very dangerous thing," Korb told Al Jazeera.

"The US tried this back in the 1960s and 1970s but they gave up because they recognised it just wouldn't work and wasn't needed and was very dangerous."

Confusion

Al Jazeera's Step Vaessen, reporting from Moscow on Tuesday, said information had only begun emerging five days after the blast, adding that this had created a lot of confusion and prompted the emergence of conspiracy theories.

"Soon after news came out that [residents] were ordered to leave this village within the next 24 hours, other authorities in the region have said that that was complete nonsense, that there has never been an order to evacuate," Vaessen said.

"What we've been seeing in the last five days is that news and reports from different authorities are contradicting each other so we don't really know exactly what's going on."

Local authorities in Severodvinsk last week initially published information about the spike in radiation, but later deleted it and a local official said that radiation levels were not above the norm.

Vaessen added that the medics who treated the victims of the blast were being sent to a Moscow hospital for testing.

"It's also not clear what kind of tests are going to be done but it's happening right now. According to a report, it will take three days before the results become known," Vaessen said.

US President Donald Trump on Monday weighed in on the blast on Twitter, saying the US "is learning much from the failed missile explosion" and claimed that Washington has "similar, though more advanced, technology".

The US and the Soviet Union pondered nuclear-powered missiles in the 1960s, but they abandoned those projects as too unstable and dangerous.

Emirati students complete nuclear energy internship in South Korea

Source: https://www.thenational.ae/uae/emirati-students-complete-nuclear-energy-internship-in-south-korea-1.896390

Aug 09 – **A future career in the nuclear industry could be in store for ten Emirati students enrolled in an eight-week internship in South Korea.**

The program mixed science and culture to introduce Khalifa University undergraduates to life in the country and experience of key organizations in the nuclear industry.

During their time in South Korea, the students developed their capabilities in understanding nuclear energy as well as science, technology, engineering and maths (STEM), reported state news agency Wam on Friday.
Organized by the Emirates Nuclear Energy Corporation (ENEC), the internship is a partnership with the International Nuclear Graduate School, KINGS, a subsidiary of the Korea Electric Power Corporation, (KEPCO).
Students completed intensive training on nuclear energy systems and also received an introduction to Korean culture.
They took part in a series of nuclear energy familiarization courses and training at a variety of research facilities, nuclear energy plants and institutions around South Korea.
Now in its second edition, the internship aims to nurture students' academic knowledge while providing them with experience they can carry forward into a future career in the nuclear industry.
By 2050, the UAE aims to have 6 per cent of its power driven by nuclear energy.
A $25 billion contract was awarded to South Korea in 2009 to build the first nuclear power plant in the Arab world.
Four APR-1400 nuclear reactors will be used at the Barakah Nuclear Energy Plant in Al Dhafra, 280 km west of Abu Dhabi.
The student internship is the result of ENEC and its subsidiary Nawah Energy Company's commitment to developing UAE National capabilities in nuclear energy and STEM subjects.
which include undergraduate, postgraduate and vocational courses spanning every aspect of the nuclear energy industry.

After a nuclear bomb detonation

Ambulances to nowhere

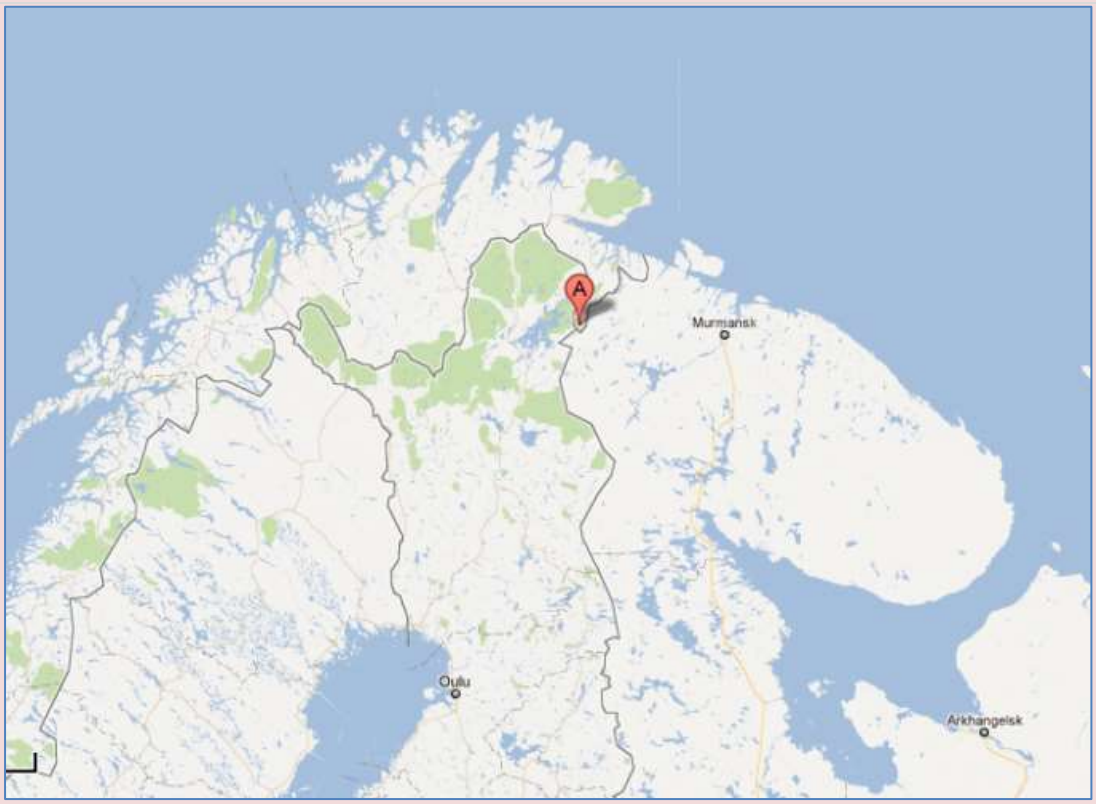
The explosion would also destroy much of the city's ability to respond. Hospitals would be leveled, doctors and nurses killed and wounded, ambulances destroyed. (In Hiroshima, 42 of 45 hospitals were destroyed or severely damaged, and 270 of 300 doctors were killed.) Resources that survived outside the zone of destruction would be utterly overwhelmed. Hospitals have no ability to cope with tens or hundreds of thousands of terribly burned and injured people all at once; the United States, for example, has 1,760 burn beds in hospitals nationwide, of which a third are available on any given day.

Do we have a plan for this?

Norway detects radioactive iodine by Russian border days after blast

Source: https://www.reuters.com/article/us-russia-blast-norway/norway-detects-radioactive-iodine-by-russian-border-days-after-blast-idUSKCN1V510N

Aug 15 – Norway's nuclear safety authority is analyzing tiny amounts of radioactive iodine detected in the air in northern Norway in the days after a deadly explosion during a rocket engine test over the border in Russia.
Russia's state nuclear agency, Rosatom, said on Saturday that five people killed in the blast were its staff members, and the accident involved "isotope power sources", giving further details.
Norway's radiation and nuclear safety authority DSA said it had detected the radioactive iodine at its air filter station in Svanhovd, which is by the Russian border. A river separates the two countries.



The samples were collected in the period Aug. 9-12, while the accident in the Arkhangelsk region of northern Russia occurred on Aug. 8, it said.

"At present it is not possible to determine if the last iodine detection is linked to the accident in Arkhangelsk last week. DSA continues more frequent sampling and analysis," DSA said.

Such radiation measurements are not unusual in Norway, as its monitoring stations detect radioactive iodine about six to eight times a year and the source is usually unknown.

Russia's state weather service said on Tuesday that radiation levels in the city of Severodvinsk had spiked by up to 16 times last Thursday, while medics who treated victims of the accident have been sent to Moscow for a medical examination, the TASS news agency reported.

Remotely Monitoring Nuclear Reactors with Antineutrino Detection

Source: http://www.homelandsecuritynewswire.com/dr20190815-remotely-monitoring-nuclear-reactors-with-antineutrino-detection

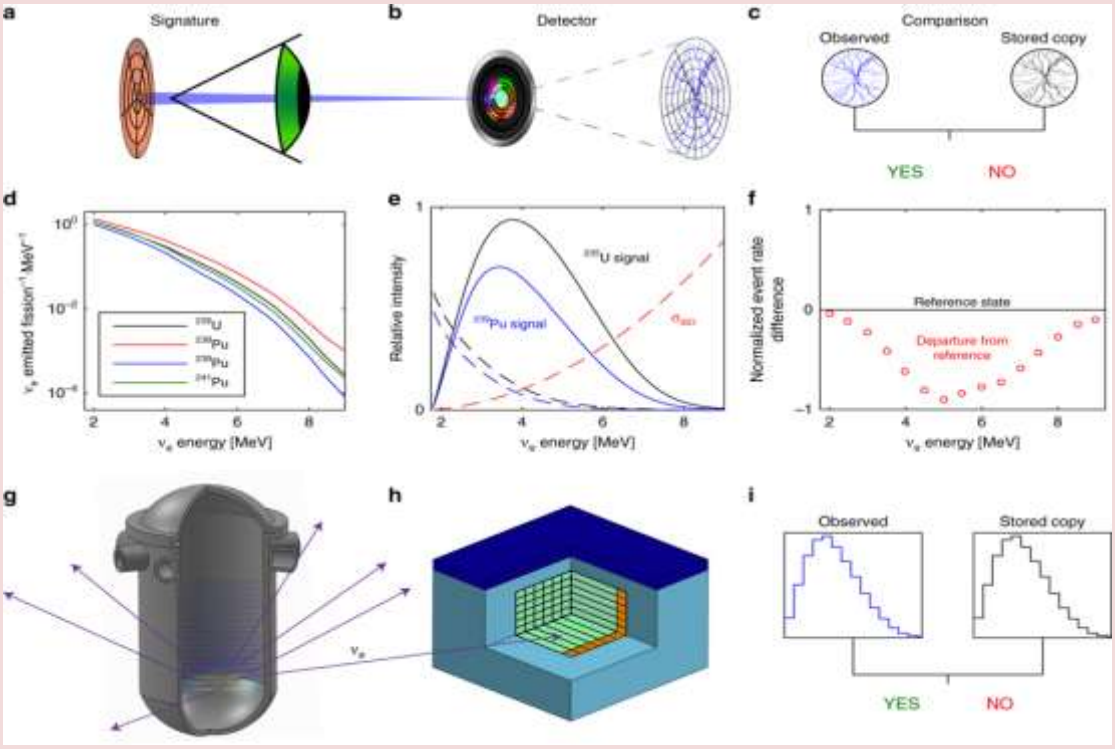
Aug 15 – Technology to measure the flow of subatomic particles known as antineutrinos from nuclear reactors could allow continuous remote monitoring designed to detect fueling changes that might indicate the diversion of nuclear materials. The monitoring could be done from outside the reactor vessel, and the technology may be sensitive enough to detect substitution of a single fuel assembly.

The technique, which could be used with existing pressurized water reactors as well as future designs expected to require less frequent refueling, could supplement other monitoring techniques, including the presence of human inspectors. The potential utility of the above-ground antineutrino monitoring technique for current and future reactors was confirmed through extensive simulations done by researchers at the Georgia Institute of Technology.

"Antineutrino detectors offer a solution for continuous, real-time verification of what is going on within a nuclear reactor without actually having to be in the reactor core," said Anna Erickson, associate professor in Georgia Tech's George W. Woodruff School of Mechanical Engineering. "You cannot shield antineutrinos, so if the state running a reactor decides to use it for nefarious purposes, they can't prevent us from seeing that there was a change in reactor operations."

The research, reported August 6 in the journal *Nature Communications*, was partially supported by a grant from the Nuclear Regulatory Commission (NRC). The research

evaluated two types of reactors, and antineutrino detection technology based on a PROSPECT detector currently deployed at Oak Ridge National Laboratory's High Flux Isotope Reactor (HFIR).
Georgie Tech notes that antineutrinos are elementary subatomic particles with an infinitesimally small mass and no electrical charge. They are capable of passing through shielding around a nuclear reactor core, where they are produced as part of the nuclear fission process. The flux of antineutrinos produced in a nuclear reactor depends on the type of fission materials and the power level at which the reactor is operated.



Principle of reactor operation verification with antineutrino monitors. The process for verifying reactor inventory integrity with antineutrinos bears similarities to biometric scans such as retinal identity verification. In retinal scans, an infrared beam traverses a person's retina (**a**) and the blood vessels, distinguishable by their higher light absorption (**b**) relative to other tissue, are mapped. The mapping is extracted and compared to a copy stored in a database (**c**), and if the two match, the person's identity is verified. Similarly, a nuclear reactor (**g**) continuously emits antineutrinos which vary in flux and spectrum with the particular fuel isotopes undergoing fission (**d**). Some interact in a nearby detector (**h**) via inverse beta decay (**e**). The measured signal is compared to a reference copy stored in a database for the relevant reactor, initial fuel, and burnup (**f**); a sufficiently matching signal indicates that the core inventory has not been covertly altered. If the antineutrino flux of a perturbed reactor is sufficiently different from expected, a diversion can be concluded to have taken place (**i**)

"Traditional nuclear reactors slowly build up plutonium 239 in their cores as a consequence of uranium 238 absorption of neutrons, shifting the fission reaction from uranium 235 to plutonium 239 during the fuel cycle. We can see that in the signature of antineutrino emission changes over time," Erickson said. "If the fuel is changed by a rogue nation attempting to divert plutonium for weapons by replacing fuel assemblies, we should be able to see that with a detector capable of measuring even small changes in the signatures."
The antineutrino signature of the fuel can be as unique as a retinal scan, and how the signature changes over time can be predicted using simulations, she said. "We could then verify that what we see with the antineutrino detector matches what we would expect to see."
In the research, Erickson and recent Ph.D. graduates Christopher Stewart and Abdalla Abou-Jaoude used high-fidelity computer simulations to assess the capabilities of near-field antineutrino detectors that would be located near – but not inside – reactor containment vessels. Among the challenges is distinguishing between particles generated by fission and those from natural background.

"We would measure the energy, position and timing to determine whether a detection was an antineutrino from the reactor or something else," she said. "Antineutrinos are difficult to detect and we cannot do that directly. These particles have a very small chance of interacting with a hydrogen nucleus, so we rely on those protons to convert the antineutrinos into positrons and neutrons."

Nuclear reactors now used for power generation must be refueled on a regular basis, and that operation provides an opportunity for human inspection, but future generations of nuclear reactors may operate for as long as 30 years without refueling. The simulation showed that sodium-cooled reactors could also be monitored using antineutrino detectors, though their signatures will be different from those of the current generation of pressurized water reactors.

Among the challenges ahead is reducing the size of the antineutrino detectors to make them portable enough to fit into a vehicle that could be driven past a nuclear reactor. Researchers also want to improve the directionality of the detectors to keep them focused on emissions from the reactor core to boost their ability to detect even small changes.

The detection principle is similar in concept to that of retinal scans used for identity verification. In retinal scans, an infrared beam traverses a person's retina and the blood vessels, which are distinguishable by their higher light absorption relative to other tissue. This mapping information is then extracted and compared to a retinal scan taken earlier and stored in a database. If the two match, the person's identity can be verified.

Similarly, a nuclear reactor continuously emits antineutrinos that vary in flux and spectrum with the particular fuel isotopes undergoing fission. Some antineutrinos interact in a nearby detector via inverse beta decay. The signal measured by that detector is compared to a reference copy stored in a database for the relevant reactor, initial fuel and burnup; a signal that sufficiently matches the reference copy would indicate that the core inventory has not been covertly altered. However, if the antineutrino flux of a perturbed reactor is sufficiently different from what would be expected, that could indicate that a diversion has taken place.

The emission rates of antineutrino particles at different energies vary with operating lifetime as reactors shift from burning uranium to plutonium. The signal from a pressurized water reactor consists of a repeated 18-month operating cycle with a three-month refueling interval, while signal from an ultra-long cycle fast reactor (UCFR) would represent continuous operation, excluding maintenance interruptions.

Preventing the proliferation of special nuclear materials suitable for weapons is a long-term concern of researchers from many different agencies and organizations, Erickson said.

"It goes all the way from mining of nuclear material to disposition of nuclear material, and at every step of that process, we have to be concerned about who's handling it and whether it might get into the wrong hands," she explained. "The picture is more complicated because we don't want to prevent the use of nuclear materials for power generation because nuclear is a big contributor to non-carbon energy."

The paper shows the feasibility of the technique and should encourage the continued development of detector technologies, Erickson said.

"One of the highlights of the research is a detailed analysis of assembly-level diversion that is critical to our understanding of the limitations on antineutrino detectors and the potential implications for policy that could be implemented," she said. "I think the paper will encourage people to look into future systems in more detail."

Russia's Nclear Propulsion Experiment a Cause for Worry

Source: http://www.homelandsecuritynewswire.com/dr20190813-russias-nclear-propulsion-experiment-a-cause-for-worry

Aug 13 – In March last year President Vladimir Putin first announced his country's new nuclear-powered cruise missile. He accompanied his speech with an animated video showing the guided-missile flying over oceans, avoiding air defense systems, circumnavigating Cape Horn, and then hitting a target on Hawaii. RT, Russia's government-funded propaganda broadcaster, referred to the new weapons system as 9M730 Burevestnik in a YouTube clip.

As was the case with the Soviet Union, Russia's propaganda stories and films often exaggerated and embellished the truth, so analysts were wondering whether the animated video presented by Putin and RT referred to an actual missile, named Skyfall by NATO.

The BBC reports that last week, a powerful explosion occurred at a Russian military facility in the Arkhangelsk region, according to the country's state-controlled nuclear energy corporation Rosatom. Russia news agencies reported that five researchers were killed when an accident occurred **testing "a liquid propulsion system involving isotopes."** Another Rosatom engineer suffered serious burns.

The Russia version of events raised more questions than it answered, since most isotopes are radioactive and not typically used as fuel for liquid-propelled rockets.

Following the explosion at the test site, Russia's state weather agency, Roshydromet, said on Tuesday that it believed radiation levels had risen by four to 16 times in the area. Greenpeace said radiation levels rose by 20 times. Both of these figures mean that radiation had been released during the Arkhangelsk accident.

Rockets propelled by liquid fuel do not emit any radiation, however, so it is likely that the missile system tested in Arkhangelsk was powered by a hybrid propulsion system, consisting of both conventional and nuclear propulsion component.

Putin has insisted that the new cruise missile was successfully tested in 2017, but there is no independent evidence to support his claim. In late March 2019, CNBC 2019 cited anonymous U.S. intelligence sources who said Russia's new cruise missiles had been tested five times since February 2018, but crashed each time. CNBC also said the missile had never flown further than 22 miles.

Time notes that if the Burevestnik weapon exists, it would be the world's first intercontinental cruise missile. This would make it strategically superior to Intercontinental Ballistic Missiles (ICBMs), which follow a set flight pattern after being launched, allowing a ballistic missile defense system, at least in theory, to intercept them.

In reality, however, ICBMs cannot be intercepted, especially if a large number of them is launched simultaneously. After the missiles release their warheads, accompanied by hundreds or even thousands of decoys, interception is impossible.
A nuclear-powered rocket engine does not use energy generated by combustion to propel a missile forward. The propulsion instead relies on heat generated by an ongoing nuclear fission. Since the end of the Second World War, both the United States and the Soviet Union have experimented, unsuccessfully, with nuclear-powered aircraft- and carrier-carried rockets.
Both superpowers successfully built planes with nuclear reactors on board, but the reactors were never connected to the engines, and the planes relied on conventional jet engines. The reactors on board were meant to test whether the crew could be effectively shielded from the radiation emitted by the nuclear reactors.
Experts note that radiation leakage is one of the major risks associated with nuclear-power missiles. A rocket does not have a crew which might be at risk of contamination, but as the explosion last Tuesday shows, the crash of, or an accident related to, such a nuclear-powered missile could have serious consequences for the neighboring communities.
There is a chance military leaders and engineers would accept such nuclear collateral damage could occur in an allied country in case of a nuclear war.
There is another danger: If a nuclear-powered cruise missile carries a conventional warhead to its target, an accident occurring with these missiles may turn what was meant to be a non-nuclear attack into a nuclear one, even if the explosion and radiation dispersion would be smaller relative to a "real" nuclear attack.
The Archangelsk accident, though, may offer evidence that nuclear propulsion technology is dangerous in peacetime – and dangerous for the population at home.

EDITOR'S COMMENT: Just wondering if the missile was of American or French or British origin the comments and worries should be the same? Because lately, what is Russian is bad and what is Western is justified…

White Supremacists Want a Dirty Bomb

Source: https://foreignpolicy.com/2019/08/16/white-supremacists-want-a-nuclear-weapon/

Aug 16 – On Dec. 9, 2008, police raided the home of the millionaire James Cummings in Belfast, Maine. Cummings was an abusive husband, and he had been shot in the head by his wife, but that wasn't what still disturbs investigators to this day. At Cummings's home, police obtained radiological material and literature on constructing a dirty bomb. Cummings had collected the radioactive isotope thorium-232 and depleted uranium, the latter of which he bought online, along with the materials necessary to build a conventional explosive. Angered by the election of Barack Obama as U.S. president, Cummings had compiled the materials he deemed necessary to build a dirty bomb just 42 days before the inauguration.
At the scene, investigators found literature on how to create different types of radiological dispersal devices (RDDs), colloquially referred to as dirty bombs, using the radioactive isotopes cesium-137, cobalt-60, and strontium-90 and an application for the U.S. Nationalist Socialist Movement, a neo-Nazi organization. Cummings had ties to white nationalist groups, he revered Adolf Hitler, and, according to workers who spent time in his home, he was a collector of Nazi memorabilia.
More than a decade later, on Aug. 3, 2019, a gunman posted an anti-immigrant, white nationalist manifesto on a far right forum, walked into a Walmart on the East side of El Paso, Texas and opened fire with a semi-automatic rifle, killing 22 people.. There is no longer any question of whether the country is facing the rise of domestic white supremacist terrorists. The question is how far they will go.
While the United States has been focused on the trafficking of nuclear and radiological materials abroad, experts at the Nuclear Threat Initiative (NTI) have argued that the threat of dangerous radiological materials being used in America's own backyard is "just as serious."
With a wide variety of civilian uses, including in the medical, industrial, and research fields, radiological materials rated by the International Atomic Energy Agency (IAEA) as Category

1 threats—such as cesium-137, cobalt-60, and strontium-90—are left relatively unguarded. These materials could be used to contaminate a major U.S. city with devastating consequences.

That is what makes these devices so attractive to modern terrorist organizations. The Islamic State declared its intent to get its hands on a nuclear device in its propaganda magazine *Dabiq*. Al Qaeda trained the domestic terrorist José Padilla in Egypt and Afghanistan and then sent him back to the United States to detonate a dirty bomb.

The budding nationalist white supremacist terrorist movement in the United States is no different. Consider the case of the "All-American Nazis." Four neo-Nazi roommates lived together until one of them converted to Islam and shot two others for disrespecting his religion. The double homicide shed light on an organization called Atomwaffen (German for "nuclear weapons"). Devon Arthurs, the convert to Islam, described Atomwaffen as a terrorist group that had 60-70 members nationwide and planned bombing attacks on synagogues and nuclear plants. Brandon Russell, the roommate who wasn't home at the time of the argument, had been collecting thorium since the 10th grade. These are not isolated incidents; in 2004 and 2013, the FBI arrested two white supremacists interested in acquiring and detonating a dirty bomb.

Moreover, these are not "lone wolves." They are part of an extremist network bound by white supremacist ideology, far-right hate, and online indoctrination. And there is no shortage of evidence that they want to acquire their own radioactive weapons.

When it comes to public knowledge about dirty bombs, there are a lot of misconceptions. An RDD does not have to be a bomb; it could be a radiological material in a crop duster or any other tool that can disperse the material. Positioned correctly, even wind itself could disperse a radiological material like cesium-137, which is a powder in its most common form.

No one has ever succeeded in detonating a dirty bomb, but Andrew Bieniawski, a former vice president for material security and minimization at NTI, said the United States has "thousands and thousands" of radiological sources that could be used in one. The delivery system of an RDD is essentially arbitrary: "Getting the material is the most difficult step in the process," he said.

"We're concerned about cesium because it is located in open environments and not behind guns, gates, and guards like nuclear material," said Ioanna M. Iliopulos, a senior consultant at NTI. "Most medical and research centers have 2 to 4 gram-sized quantities of cesium chloride, which could create a lot of havoc if stolen and dispersed in a major metropolitan area."

Russian Nuclear-Monitoring Stations' Silence Fuel Fears over Extent of Deadly Blast

Source: http://www.homelandsecuritynewswire.com/dr20190820-russian-nuclearmonitoring-stations-silence-fuel-fears-over-extent-of-deadly-blast

Aug 20 – Officials at the Vienna-based Comprehensive Nuclear-Test-Ban Treaty Organization (CTBTO) say that two nuclear monitoring stations in Russia have resumed operations after mysteriously halting the transmission of data.

The CTBTO did not comment on August 20 on the other two stations which it previously said had gone silent in the aftermath of an explosion at a Russian naval test site that killed at least five people and caused a temporary spike in radiation levels.

Russia operates a total of six monitoring stations that scan for so-called radionuclide particles wafting through the air.

Silence at several of the stations raised fears that Moscow was hiding the extent of the blast.

"RN stations RUP 56 (Peleduy) and RUP 57 (Bilibino) have resumed operations in Russia & are currently backfilling data," Lassina Zerbo, executive secretary of the CTBTO, said in a message on Twitter.
"Excellent cooperation & support from our Russian station operators under 'The Provisional Operation Status of the IMS,'" he added, referring to the International Monitoring System that collects and monitors data worldwide on radiation in the atmosphere.
Kremlin spokesman Dmitry Peskov told reporters on August 20 that while Russian President Vladimir Putin receives information "about everything," the monitoring stations were "outside our purview."
"As for the operation of the stations, frankly, I don't know who they report to. It is easier for you [journalists] to find who they report to and request information directly as to why some data is or is not being transmitted," Peskov said.
"But, so you understand, the head of state is receiving complete updates about what is going on out there," he added.
The August 8 explosion near Nyonoksa, the village where a military testing site is located on the White Sea, sent intelligence analysts from Washington to Brussels to Oslo scrambling to figure out what happened.
In the days after the mishap, civilian and military authorities gave conflicting information as to what exactly occurred, how many casualties there were, and where the recorded spike in radiation came from and whether it was dangerous.
Monitoring stations in the nearby shipbuilding port of Severodvinsk recorded the brief spike in radiation levels in the hours after the explosion, but Russian officials have emphasized that there was no danger to public health.
Monitors in Norway, hundreds of kilometers to the northwest, detected a small increase in airborne radioactive iodine in the days that followed, but they have not linked it to the Nyonoksa explosion.
Several analysts have suggested that the item involved in the explosion may have been a nuclear-powered cruise missile dubbed the Burevestnik in Russian, which President Vladimir Putin boasted was under development last year.
Speaking at an August 19 meeting with French President Emmanuel Macron, Putin said there was no risk of increased radiation levels because of the incident, adding that all of those injured and killed in the blast would receive state awards.
U.S. President Donald Trump has added to the speculation by posting a Tweet stating outright it was the Burevestnik, known by NATO analysts under the name Skyfall.
Other analysts said it might not be a nuclear-propelled, super-fast cruise missile, but a "radioisotope thermoelectric generator" used to generate power for a missile and its components.

Key Takeaways from the Fukushima Disaster

Source: http://www.homelandsecuritynewswire.com/dr20190820-key-takeaways-from-the-fukushima-disaster

Aug 20 – In March and April of 2011 the Fukushima Nuclear Power Plant disaster resulted in what was the largest ever accidental release of radioactive material into the ocean. Zofia Baumann, assistant professor of marine sciences at the University of Connecticut, has researched the impacts of the disaster on marine ecosystems in the Pacific Ocean, and has authored a section of a chapter in the forthcoming book *Environmental Contamination from the Fukushima Nuclear Disaster*, detailing the findings of her research. She discussed her research with *UConn Today*'s Elaina Hancock, sharing some unexpectedly good news in the wake of the disaster.

Elaina Hancock: What are some of the impacts of the Fukushima disaster that you have found?

Zofia Baumann: The Fukushima disaster was complex, radioactivity was deposited into the atmosphere, on the land, but much of it was dispersed into the ocean, which was actually seen as a blessing in disguise.
Even though the levels of radiation in the area and in the marine organisms were elevated, they were actually not a threat to the ecosystem or to human consumers in most cases.
Through our research we found that due to the massive currents present in the ocean, this radioactivity deposited into the ocean was quickly dispersed. The most problematic marine

organisms were those found in the harbor near the plant, but the levels of radioactivity in that area reduce exponentially as one moves away from the area. The radioactivity levels are rarely a cause for concern.

Hancock: Can you tell us about how you tracked the radioactivity?

Baumann: Fukushima delivered artificially made radionuclides, ones that are not found in nature. We tracked Cesium 134 and 137 that were made through the process of creating energy at the nuclear power plant.

While certainly the amount of radioactivity dumped into the ocean, atmosphere, and onto the land was to the point where we could detect the radiation, for most marine organisms it wasn't because levels were dangerously high, it was because our equipment was really, really good.

However, in terms of health impacts associated with the consumption of fish, the levels were negligible.

Our tools are great, and we are able to detect chemicals at an extremely low concentration, but just because we detect radioactivity, it doesn't mean it is dangerous.

Hancock: Are there possible long-term effects resulting from the disaster?

Baumann: When you talk about radioactivity, people get nervous. We worked with researchers who are experts in the levels of risk of radioactivity, called dosimetry, who can calculate the dose to a human and to animals. We concluded the dose received by people consuming contaminated tuna at the levels found in Japan and elsewhere are so low, that from a statistical point of view, we were unable to calculate any risk because those levels are extremely low.

One very positive outcome from the research on the disaster was with Pacific bluefin tunas which are heavily overfished. Based on findings from our research the Japanese government created new regulations to provide more protection for these fish. So, the cool thing is that we were able to use the pollution disaster to learn something that we would not have been able to learn otherwise.

Hancock: Was the Fukushima disaster an example where dilution really was a solution to pollution?

Baumann: Absolutely, this is one situation where 'dilution is the solution to pollution'. To illustrate this, a good comparison is between Fukushima and Chernobyl. Chernobyl polluted the Black, Baltic, and other in-land seas and the dilutions of the radioactive materials was not significant compared to the massive currents that continuously flush the Atlantic or Pacific oceans. The strong ocean currents worked to disperse the radiation quickly.

Of course, prevention of spills is the most important solution.

Hancock: Can this research be applied to other types of environmental contaminants?

Baumann: Yes, but again, it is important to understand the contaminant and the situation. Where is the source of the contaminant? Is it organic or not? Is it soluble in the water or not? Some of these contaminants can be considered global pollutants, meaning they get deposited into the atmosphere and distributed globally. Eventually the contaminants will come back down to Earth in the form of rain for example.

Some contaminants will also stay more local. For instance, in Connecticut, mercury is a persistent contaminant in the Danbury area. Danbury was once world-famous for hat making and mercury nitrate was used in the process. Mercury is still slowly released into the rivers in the area, and eventually to Long Island Sound.

Hancock: What would you consider to be some key takeaways from your research into this disaster?

Baumann: We are living in a radioactive world. For example, potassium is everywhere. It is in the soil, it is in concrete, which is in our building walls, it is in the food — wherever we are, there is potassium and a small fraction of that is radioactive potassium. There are also other naturally occurring radioactive isotopes that have been on planet Earth long before life occurred.

Radioactivity is really scary when you are talking about nuclear weapons, clearly that is a very troubling situation, but we must ensure we are not comparing apples with oranges.

It is important to be well informed and I encourage everyone to learn more about environmental contaminants, their activities, and chemistry. We do not have a 'planet b' and we should be as knowledgeable about environmental issues as possible.

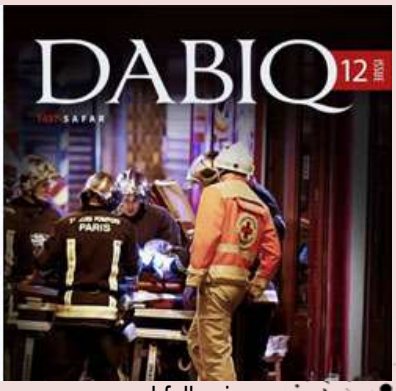

ICI International
CBRNE INSTITUTE
CBRNE-Terrorism Newsletter
W M O D
C2BRNE DIARY
EXPLOSIVE NEWS

Source: https://www.france24.com/en/video/20190717-inside-kabul-school-explosive-detection-dogs

At a facility in Kabul, Afghanistan canine conscripts are training for a life or death mission: learning how to sniff out explosives in a country where blasts from mines and homemade bombs kill and wound hundreds a year.
Around 200 dogs train at a time at the Mine Detection Centre (MDC) in the Afghan capital, starting when they are just pups.
They are put through their paces around obstacle courses and are taught to correctly identify target smells from a conveyor belt of identical canisters during an intense two-year course.
Once qualified, they are a vital part of the team for Afghanistan's bomb and mine detection squads.
"Dogs are protectors and a good friend for me, and always one step ahead of me in dangerous places," says Zainuddin Quraishi, chief trainer at the MDC.
The facility opened in 1989 and has now trained more than 1,100 dogs, which are now a common site at checkpoints, government buildings and other high-security sites around Kabul.
At least 1,432 people were killed or wounded in Afghanistan by mines or other explosive devices across Afghanistan in 2018, according to figures from Afghanistan's Directorate of Mine Action Coordination.

British Airways Cancels All Cairo Flights

Source: https://www.euronews.com/2019/07/21/british-airways-cancels-all-flights-to-cairo-due-to-security-precautions



July 22 – British Airways had canceled all flight service to and from Cairo, Egypt due to unspecified security concerns. This was followed by the Foreign and Commonwealth Office issuing a travel warning for Egypt citing a "*heightened risk of terrorism against aviation.*" Lufthansa later followed the British Airways move, but flights from both airlines have now resumed following

reviews of security protocols and procedures. Few details have been provided about the specific threat prompting the flight cancellations.
The airline's concerns are not unwarranted. Readers are reminded that on October 31st, 2015, Metrojet Flight 9268 flying from Sharm El Sheikh International Airport in Egypt to Saint Petersburg, Russia was destroyed by a bomb above the northern Sinai, killing all 224 passengers and crew who were on board. Shortly after the crash, the Islamic State's Sinai Branch claimed responsibility for the incident in a written statement and on video, both of which were distributed globally via social media. The group also published photographs of what it said was the bomb in their online magazine known as Dabiq. That device was contained within a can of Schweppes Gold pineapple soda.

Fake improvised explosive devices slip through regional airport security

Source: https://www.9news.com.au/national/airport-security-test/57c07311-3285-4e7b-b625-ad10bfac93b9

Aug 01 – Serious security deficiencies have been uncovered at Townsville Airport, with fake bombs passing through screening undetected.
In April this year aviation inspectors, with Home Affairs, conducted what is known as red teaming tests.
Two fake improvised explosive devices passed through without being spotted by staff. Last month another device slipped through without anyone noticing.
Terrorism expert Neil Fergus says the breaches are a serious concern.
"It's a key regional airport and anything that indicates an IED can get through the aviation logistics chain should cause us great concern."
Security at Townsville airport is controlled by ISS Australia which touts itself as a world leader of airport security services. In a statement the company said it understood »the extremely important responsibility of providing safe airports and would continue to work with authorities to meet the highest levels of compliance".

Townsville airport boss Kevin Gill also issued a statement confirming an "independent audit" had been ordered into ISS systems "following some testing issues".
Dr John Coyne is a security specialist with Australian Strategic Policy institute. He takes some comfort in the fact the tests uncovered a weakness.
"When it comes down to threat, the sorts of people who do us harm, whether they are criminals or terrorists, are themselves always innovating. They are trying to find new ways to defeat our security systems so it's important these tests happen."
An Australian Border Force spokesperson told 9News that Home Affairs would not comment on the outcome of individual tests but said they were communicated to airports, and used to identify if additional training or other measures were required.
The Federal Government has previously announced it will spend $50 million to upgrade security at regional airports.

Filling the Gaps in the Detection of Homemade Explosive Devices

By Jenny Stone and Katherine Kendrick
Source: https://www.hstoday.us/subject-matter-areas/terrorism-study/filling-the-gaps-in-the-detection-of-homemade-explosive-devices/

Aug 20 – The threat of terrorism and the use of explosives in attacks on our homeland continues to evolve. The focus has shifted from large, well-funded, and international organized groups with considerable access and resources to smaller, domestic, less-sophisticated groups and lone wolves making bombs in their garages. Policy and technology in the U.S. were developed and targeted toward events like the World Trade Center bombing in 1993, when an al-Qaeda-backed group set off a 1,300-pound bomb made of sophisticated nitrate-based explosives, aimed at taking down both towers. The goal of this attack was to maximize casualties and disrupt the U.S. economy. Twenty years later, two self-radicalized brothers, not connected to a major terrorist group, set off homemade bombs at the finish line of the Boston Marathon. The potential for death and injury was significantly less than a WTC attack, but the effect on Americans' sense of safety was the same. Protocols and procedures exist and are deployed to detect and protect against the former type of attack, but a significant gap exists in the detection and protection against a less-sophisticated, homemade attack.
Solid counter-IED (C-IED) programs include a combination of tactical and strategic methods to detect and protect from an IED event, including specially trained canines, robots, awareness campaigns, training, and other technologies. An integral part of C-IED is technological detection systems that identify the presence of explosive compounds. There are numerous systems on the market that provide sensitive, portable, and reliable detection results, such as Smiths Detection's IONSCAN 600, which can detect and identify both explosives and narcotics. L3HARRIS' B220 HT Desktop Trace Detector optimizes sampling hands for explosives, simplifying detection in high-traffic environments. These devices and others like them have high success rates when detecting commercial and industrial explosive material, like C-4 and dynamite.
Today, thanks in part to regulation, commercial and industrial explosive materials are not easy to procure and our adversaries have adapted accordingly, using commercially available Explosive Precursor Chemicals (EPCs) and household items, to develop less sophisticated, but equally threatening Home Made Explosives (HMEs) for use in Improvised Explosive Devices (IEDs). Lone wolves and smaller, less-organized groups are able to use materials like fertilizer, paint remover, car batteries, and airbag initiators to create pipe bombs, pressure cooker bombs, and suicide vests that can be easily concealed under clothing or in an everyday item like a backpack. Based on the wide availability of EPCs used to manufacture HMEs, coupled with the technical instruction found on social media, it is far more likely that HMEs would be used in an attack versus commercial or military explosives. In response to the much more significant threat of HMEs, the advancement of better detection technology is a focused and ongoing effort.
There are a number of U.S. government programs, including the Bomb Making Materials Awareness Program (BMAP) that acknowledge this shift in threat. These programs focus on building an informed community and hinge on the community's ability to recognize the

behavior of an adversary and the types of materials that may commonly be used to create HMEs. While these important human-element steps are being taken, the technological capability gap leaves significant risk unmitigated. An informal survey conducted at this year's National Homeland Security Conference revealed many government officials were unaware that their existing technology was incapable of identifying certain elements of an HME.

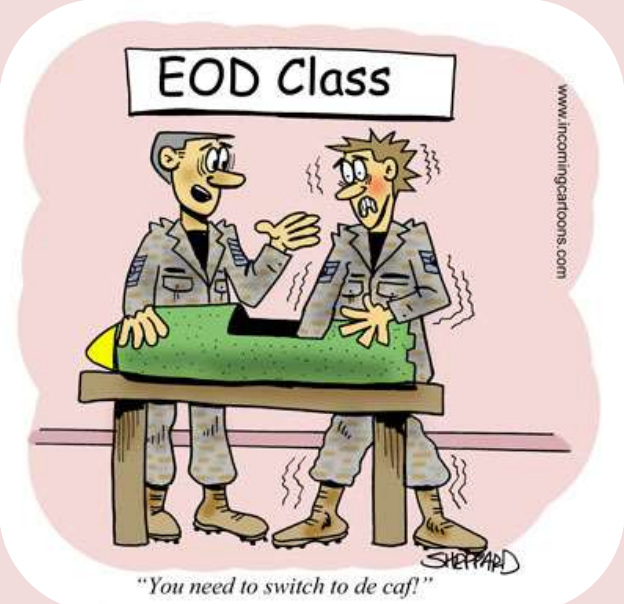
"HMEs are the next major threat for 'soft targets' and transportation modalities," said Mo McGowan, retired Transportation Security Administration Assistant Administrator and Senior Advisor for GTSC commented. "State and federal government agencies and those portions of the private sector responsible for security of these venues should be making every effort to identify multiple ways to mitigate and disrupt attacks from this threat, including the ability to detect the devices or their components."

Companies are beginning to emerge on the market with innovative solutions to address this disparity in C-IED. TechLink's improved colorimetric explosive detection kit detects HMEs using "dry chemistry." This process presents a color change associated with a type of explosion and is ready in under a minute. GreyScan, an Australian-based company, has developed an automated and rapid detection machine that allows users to detect inorganic explosive materials such as chlorates, perchlorates, nitrates – elements found in household items like fertilizer.

Adversaries have evolved over time and our attentions have shifted with the perceived threats and risks. Our policies and technology are continuously updated to match the adversary evolution. At this moment, it is imperative that our attention stay focused on HME detection and protection and ensure security professionals have the tools to defeat this threat.

Jenny Stone *is the Founder and President of Partner Forces. She and her team have worked side-by-side with the Department of Homeland Security (DHS) for more than 16 years supporting federal and state and local critical infrastructure and cyber protection initiatives and building preparedness capabilities targeted at manmade and natural disasters. Jenny is a recognized expert in infrastructure protection and the homeland security doctrine, regulations, and partnership framework-built post 9/11 to manage the risk and threats to our country. Jenny holds a bachelor's degree in English and Economics from Washington and Lee University, as well as a master's degree in Security Studies from Georgetown University.*

Katherine Kendrick is *a Consultant at Partner Forces LLC with over six year of experience managing interagency efforts at the Department of Homeland Security and for state and local clients. She specializes in the analysis of cyber and physical risks to infrastructure, systems, and regions. Katherine has a BA in International Relations from Virginia Tech and a Graduate Certificate in Applied Cybersecurity from George Mason University.*



IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

CYBER NEWS

Hacking Connected Cars to Gridlock Whole Cities

Source: http://www.homelandsecuritynewswire.com/dr20190730-hacking-connected-cars-to-gridlock-whole-cities

July 30 – In the year 2026, at rush hour, your self-driving car abruptly shuts down right where it blocks traffic. You climb out to see gridlock down every street in view, then a news alert on your watch tells you that hackers have paralyzed all Manhattan traffic by randomly stranding internet-connected cars.

Flashback to July 2019, the dawn of autonomous vehicles and other connected cars, and physicists at the Georgia Institute of Technology and Multiscale Systems, Inc. have applied physics in a new study to simulate what it would take for future hackers to wreak exactly this widespread havoc by randomly stranding these cars. Georgia Tech says that the researchers want to expand the current discussion on automotive cybersecurity, which mainly focuses on hacks that could crash one car or run over one pedestrian, to include potential mass mayhem.

They warn that even with increasingly tighter cyber defenses, the amount of data breached has soared in the past four years, but objects becoming hackable can convert the rising cyber threat into a potential physical menace.

"Unlike most of the data breaches we hear about, hacked cars have physical consequences," said Peter Yunker, who co-led the study and is an assistant professor in Georgia Tech's School of Physics.

It may not be that hard for state, terroristic, or mischievous actors to commandeer parts of the internet of things, including cars.

"With cars, one of the worrying things is that currently there is effectively one central computing system, and a lot runs through it. You don't necessarily have separate systems to run your car and run your satellite radio. If you can get into one, you may be able to get into the other," said Jesse Silverberg of Multiscale Systems, Inc., who co-led the study with Yunker

Freezing Traffic Solid

In simulations of hacking internet-connected cars, the researchers froze traffic in Manhattan nearly solid, and it would not even take that to wreak havoc. Here are their results, and the numbers are conservative for reasons mentioned below.

"Randomly stalling 20 percent of cars during rush hour would mean total traffic freeze. At 20 percent, the city has been broken up into small islands, where you may be able to inch around a few blocks, but no one would be able to move across town," said David Yanni, a graduate research assistant in Junker's lab.

Not all cars on the road would have to be connected, just enough for hackers to stall 20 percent of all cars on the road. For example, if 40 percent of all cars on the road were connected, hacking half would suffice.

Hacking 10 percent of all cars at rush hour would debilitate traffic enough to prevent emergency vehicles from expediently cutting through traffic that is inching along citywide. The same thing would happen with a 20 percent hack during intermediate daytime traffic.

The researchers' results appear in the journal *Physical Review E* on July 20, 2019. The study is not embargoed.

It could Take Less

For the city to be safe, hacking damage would have to be below that. In other cities, things could be worse.

"Manhattan has a nice grid, and that makes traffic more efficient. Looking at cities without large grids like Atlanta, Boston, or Los Angeles, and we think hackers could do worse harm because a grid makes you more robust with redundancies to get to the same places down many different routes," Yunker said.

The researchers left out factors that would likely worsen hacking damage, thus a real-world hack may require stalling even fewer cars to shut down Manhattan.

"I want to emphasize that we only considered static situations – if roads are blocked or not blocked. In many cases, blocked roads spill over traffic into other roads, which we also did not include. If we were to factor in these other things, the number of cars you'd have to stall would likely drop down significantly," Yunker said.

The researchers also did not factor in ensuing public panic nor car occupants becoming pedestrians that would further block streets or cause accidents. Nor did they consider hacks that would target cars at locations that maximize trouble.
They also stress that they are not cybersecurity experts, nor are they saying anything about the likelihood of someone carrying out such a hack. They simply want to give security experts a calculable idea of the scale of a hack that would shut a city down.
The researchers do have some general ideas of how to reduce the potential damage.
"Split up the digital network influencing the cars to make it impossible to access too many cars through one network," said lead author Skanka Vivek, a postdoctoral researcher in Yunker's lab. "If you could also make sure that cars next to each other can't be hacked at the same time that would decrease the risk of them blocking off traffic together."

Traffic Jams as Physics

Yunker researches in soft matter physics, which looks at how constituent parts – in this case, connected cars – act as one whole physical phenomenon. The research team analyzed the movements of cars on streets with varying numbers of lanes, including how they get around stalled vehicles and found they could apply a physics approach to what they observed.
"Whether traffic is halted or not can be explained by classic percolation theory used in many different fields of physics and mathematics," Yunker said.
Percolation theory is often used in materials science to determine if a desirable quality like a specific rigidity will spread throughout a material to make the final product uniformly stable. In this case, stalled cars spread to make formerly flowing streets rigid and stuck.
The shut streets would be only those in which hacked cars have cut off all lanes or in which they have become hindrances that other cars can't maneuver around and do not include streets where hacked cars still allow traffic flow.
The researchers chose Manhattan for their simulations because a lot of data was available on that city's traffic patterns.

US issues hacking security alert for small planes

Source: https://techxplore.com/news/2019-07-issuing-hacking-small-planes.html

July 30 – The Department of Homeland Security issued a security alert Tuesday for small planes, warning that modern flight systems are vulnerable to hacking if someone manages to gain physical access to the aircraft.
An alert from the DHS critical infrastructure computer emergency response team recommends that plane owners ensure they restrict unauthorized physical access to their aircraft until the industry develops safeguards to address the issue, which was discovered by a Boston-based cybersecurity company and reported to the federal government.
Most airports have security in place to restrict unauthorized access and there is no evidence that anyone has exploited the vulnerability. But a DHS official told The Associated Press that the agency independently confirmed the security flaw with outside partners and a national research laboratory, and decided it was necessary to issue the warning.
The cybersecurity firm, Rapid7, found that an attacker could potentially disrupt electronic messages transmitted across a small plane's network, for example by attaching a small device to its wiring, that would affect aircraft systems.
Engine readings, compass data, altitude and other readings "could all be manipulated to provide false measurements to the pilot," according to the DHS alert.

The warning reflects the fact that aircraft systems are increasingly reliant on networked communications systems, much like modern cars. The auto industry has already taken steps to address similar concerns after researchers exposed vulnerabilities.

The Rapid7 report focused only on small aircraft because their systems are easier for researchers to acquire. Large aircraft frequently use more complex systems and must meet additional security requirements. The DHS alert does not apply to older small planes with mechanical control systems.

But Patrick Kiley, Rapid7's lead researcher on the issue, said an attacker could exploit the vulnerability with access to a plane or by bypassing airport security.

In this July 15, 2018 photo, the New Orleans Lakefront Airport air traffic control tower is seen in front of a sunset and a rain cloud over Lake Pontchartrain, in New Orleans. The Department of Homeland Security plans to issue a security alert Tuesday for small planes, warning that modern flight systems are vulnerable to hacking if someone manages to gain physical access to the aircraft. A DHS alert recommends that plane owners ensure they restrict unauthorized physical access to their aircraft until the industry develops safeguards to address the issue, which was discovered by Boston-based cybersecurity company, Rapid7, and reported to the federal government. (AP Photo/Gerald Herbert)

"Someone with five minutes and a set of lock picks can gain access (or) there's easily access through the engine compartment," Kiley said.

Jeffrey Troy, president of the Aviation Information Sharing and Analysis Center, an industry organization for cybersecurity information, said there is a need to improve the security in networked operating systems but emphasized that the hack depends on bypassing physical security controls mandated by law.

With access, "you have hundreds of possibilities to disrupt any system or part of an aircraft," Troy said.

The Federal Aviation Administration said in a statement that a scenario where someone has unrestricted physical access is unlikely, but the report is also "an important reminder to remain vigilant" about physical and cybersecurity aircraft procedures.

Aviation cybersecurity has been an issue of growing concern around the world.

In March, the U.S. Department of Transportation's inspector general found that the FAA had "not completed a comprehensive, strategy policy framework to identify and mitigate cybersecurity risks." The FAA agreed and said it would look to have a plan in place by the end of September.

The UN's body for aviation proposed its first strategy for securing civil aviation from hackers that's expected to go before the General Assembly in September, said Pete Cooper, an ex-Royal Air Force fast jet pilot and cyber operations officer who advises the aviation industry.

The vulnerability disclosure report is the product of nearly two years of work by Rapid7. After their researchers assessed the flaw, the company alerted DHS. Tuesday's DHS alert recommends manufacturers review how they implement these open electronics systems known as "the CAN bus" to limit a hacker's ability to perform such an attack.

In this June 7, 2017 photo, the Red River is seen in this aerial photo from a private plane near Shreveport, La. The Department of Homeland Security plans to issue a security alert Tuesday for small planes, warning that modern flight systems are vulnerable to hacking if someone manages to gain physical access to the aircraft. A DHS alert recommends that plane owners ensure they restrict unauthorized physical access to their aircraft until the industry develops safeguards to address the issue, which was discovered by Boston-based cybersecurity company, Rapid7, and reported to the federal government. (AP Photo/Gerald Herbert)

The CAN bus functions like a small plane's central nervous system. Targeting it could allow an attacker to stealthily hijack a pilot's instrument readings or even take control of the plane, according to the Rapid7 report obtained by The AP.

"CAN bus is completely insecure," said Chris King, a cybersecurity expert who has worked on vulnerability analysis of large-scale systems. "It was never designed to be in an adversarial environment, (so there's) no validation" that what the system is being told to do is coming from a legitimate source.

Only a few years ago, most auto manufacturers used the open CAN bus system in their cars. But after researchers publicly demonstrated how they could be hacked, auto manufacturers added on layers of security, like putting critical functions on separate networks that are harder to access externally.

The disclosure highlights issues in the automotive and aviation industries about whether a software vulnerability should be treated like a safety defect—with its potential for costly manufacturer recalls and implied liability—and what responsibility manufacturers should have in ensuring their products are hardened against such attacks. The vulnerability also highlights the reality that it's becoming increasingly difficult to separate cybersecurity from security overall.

"A lot of aviation folks don't see the overlap between information security, cybersecurity, of an aircraft, and safety," said Beau Woods, a cyber safety innovation fellow with the Atlantic Council, a Washington think tank. "They see them as distinct things."

The CAN bus networking scheme was developed in the 1980s and is extremely popular for use in boats, drones, spacecraft, planes and cars—all areas where there's more noise interference and it's advantageous to have less wiring. It's actually increasingly used in airplanes today due to the ease and cost of implementation, Kiley said.

Given that airplanes have a longer manufacturing cycle, "what we're trying to do is get out ahead of this." The report didn't name the vendors Rapid7 tested, but the company alerted them over a year ago, the report states.

Facebook Isn't Responsible as Terrorist Platform, Court Says

Source: http://www.homelandsecuritynewswire.com/dr20190801-facebook-isn-t-responsible-as-terrorist-platform-court-says

Aug 01 – Facebook Inc. doesn't have to face a lawsuit by victims of Hamas attacks and their relatives who claimed that the social network unlawfully assisted the terror group, a federal appeals court ruled.

In a 66-page ruling issued Wednesday, a divided court upheld a judge's decision to throw out the case, saying an interactive computer service is not the publisher of third-party information when it uses tools that are designed to match content with consumer interests.

"Facebook does not edit (or suggest edits) for the content that its users — including Hamas — publish," the Second Circuit Court of Appeals said, noting that the company only requires users to provide basic information and therefore acts as a "neutral intermediary."

Chris Dolmetsch writes in *Bloomberg* that the lawsuit was among several around the U.S. testing whether victims of terrorist attacks and their families can hold social-media companies to account for allowing violent extremists to use their platforms to recruit followers. The terrorism victims attempted for the first time to argue that social-media companies could be held liable under the U.S. Anti-Terrorism Act.

North Korea Launched Cyberattacks Against Nigeria To Raise Money For Weapons Of Mass Destruction

Source: http://saharareporters.com/2019/08/14/north-korea-launched-cyberattacks-against-nigeria-raise-money-weapons-mass-destruction

Aug 14 – UN experts say they are investigating at least 35 instances in 17 countries of North Koreans using cyberattacks to illegally raise money for weapons of mass destruction programs, and they are calling for sanctions against ships providing gasoline and diesel to the country.

Last week, The Associated Press quoted a summary of a report from the experts which said that North Korea illegally acquired as much as $2 billion from its increasingly sophisticated cyber activities against financial institutions and cryptocurrency exchanges.

The lengthier version of the report, recently seen by the AP, revealed that neighbouring South Korea was hardest-hit, the victim of 10 North Korean cyberattacks, followed by India with three attacks, and Bangladesh and Chile with two each.

Thirteen countries suffered one attack — Costa Rica, Gambia, Guatemala, Kuwait, Liberia, Malaysia, Malta, Nigeria, Poland, Slovenia, South Africa, Tunisia, and Vietnam, it said.

The experts said they were investigating the reported attacks as attempted violations of UN sanctions, which the panel monitors.
The report cited three main ways that North Korean cyber hackers operate.
One is attacks through the Society for Worldwide Interbank Financial Telecommunication or SWIFT system used to transfer money between banks, "with bank employee computers and infrastructure accessed to send fraudulent messages and destroy evidence".
The other two are, theft of cryptocurrency "through attacks on both exchanges and users", and "mining of cryptocurrency as a source of funds for a professional branch of the military".
Experts stressed that implementing these increasingly sophisticated attacks "is low risk and high yield", often requiring just a laptop computer and access to the internet.
The report to the Security Council gave details on some of the North Korean cyberattacks as well as the country's successful efforts to evade sanctions on coal exports in addition to imports of refined petroleum products and luxury items including Mercedes Benz S-600 cars.

A cyberattack could wreak destruction comparable to a nuclear weapon

By Jeremy Straub
Source: https://www.pri.org/stories/2019-08-16/cyberattack-could-wreak-destruction-comparable-nuclear-weapon

Aug 16 – People around the world may be worried about nuclear tensions rising, but I think they're missing the fact that a major cyberattack could be just as damaging — and hackers are already laying the groundwork.
With the US and Russia pulling out of a key nuclear weapons pact — and beginning to develop new nuclear weapons – plus Iran tensions and North Korea again test-launching missiles, the global threat to civilization is high. Some fear a new nuclear arms race.
That threat is serious — but another could be as serious, and is less visible to the public. So far, most of the well-known hacking incidents, even those with foreign government backing, have done little more than steal data. Unfortunately, there are signs that hackers have placed malicious software inside US power and water systems, where it's lying in wait, ready to be triggered. The US military has also reportedly penetrated the computers that control Russian electrical systems.

Many intrusions already
As someone who studies cybersecurity and information warfare, I'm concerned that a cyberattack with widespread impact, an intrusion in one area that spreads to others or a combination of lots of smaller attacks, could cause significant damage, including mass injury and death rivaling the death toll of a nuclear weapon.
Unlike a nuclear weapon, which would vaporize people within 100 feet and kill almost everyone within a half-mile, the death toll from most cyberattacks would be slower. People might die from a lack of food, power or gas for heat or from car crashes resulting from a corrupted traffic light system. This could happen over a wide area, resulting in mass injury and even deaths.
This might sound alarmist, but look at what has been happening in recent years, in the US and around the world.
In early 2016, hackers took control of a US treatment plant for drinking water, and changed the chemical mixture used to purify the water. If changes had been made — and gone unnoticed — this could have led to poisonings, an unusable water supply and a lack of water.
In 2016 and 2017, hackers shut down major sections of the power grid in Ukraine. This attack was milder than it could have been, as no equipment was destroyed during it, despite the ability to do so. Officials think it was designed to send a message. In 2018, unknown cybercriminals gained access throughout the United Kingdom's electricity system; in 2019 a similar incursion may have penetrated the US grid.
In August 2017, a Saudi Arabian petrochemical plant was hit by hackers who tried to blow up equipment by taking control of the same types of electronics used in industrial facilities of

all kinds throughout the world. Just a few months later, hackers shut down monitoring systems for oil and gas pipelines across the US. This primarily caused logistical problems — but it showed how an insecure contractor's systems could potentially cause problems for primary ones.
The FBI has even warned that hackers are targeting nuclear facilities. A compromised nuclear facility could result in the discharge of radioactive material, chemicals or even possibly a reactor meltdown. A cyberattack could cause an event similar to the incident in Chernobyl. That explosion, caused by inadvertent error, resulted in 50 deaths and evacuation of 120,000 and has left parts of the region uninhabitable for thousands of years into the future.

A power grid monitor device is displayed at cyber-security conference. Credit: David Becker/Reuters

Mutual assured destruction

My concern is not intended to downplay the devastating and immediate effects of a nuclear attack. Rather, it's to point out that some of the international protections against nuclear conflicts don't exist for cyberattacks. For instance, the idea of "mutual assured destruction" suggests that no country should launch a nuclear weapon at another nuclear-armed nation: The launch would likely be detected, and the target nation would launch its own weapons in response, destroying both nations.
Cyber-attackers have fewer inhibitions. For one thing, it's much easier to disguise the source of a digital incursion than it is to hide where a missile blasted off from. Further, cyberwarfare can start small, targeting even a single phone or laptop. Larger attacks might target businesses, such as banks or hotels, or a government agency. But those aren't enough to escalate a conflict to the nuclear scale.

Nuclear grade cyberattacks

There are three basic scenarios for how a nuclear grade cyberattack might develop. It could start modestly, with one country's intelligence service stealing, deleting or compromising another nation's military data. Successive rounds of retaliation could expand the scope of the attacks and the severity of the damage to civilian life.
In another situation, a nation or a terrorist organization could unleash a massively destructive cyberattack – targeting several electricity utilities, water treatment facilities or industrial plants at once, or in combination with each other to compound the damage.

Perhaps the most concerning possibility, though, is that it might happen by mistake. On several occasions, human and mechanical errors very nearly destroyed the world during the Cold War; something analogous could happen in the software and hardware of the digital realm.

A cyber-attack wouldn't be launched from a nuclear operator's console, like the one shown here from the decommissioned Oscar Zero site, but rather through cyberspace. A human might not even be required. Credit: Jeremy Straub

Defending against disaster

Just as there is no way to completely protect against a nuclear attack, there are only ways to make devastating cyberattacks less likely.

The first is that governments, businesses and regular people need to secure their systems to prevent outside intruders from finding their way in, and then exploiting their connections and access to dive deeper.

Critical systems, like those at public utilities, transportation companies and firms that use hazardous chemicals, need to be much more secure. One analysis found that only about one-fifth of companies that use computers to control industrial machinery in the US even monitor their equipment to detect potential attacks — and that in 40% of the attacks they did catch, the intruder had been accessing the system for more than a year. Another survey found that nearly three-quarters of energy companies had experienced some sort of network intrusion in the previous year.

Industrial control rooms like this often contain vulnerable computer systems. Credit: Ben Job/Reuters

But all those systems can't be protected without skilled cybersecurity staffs to handle the work. At present, nearly a quarter of all cybersecurity jobs in the US are vacant, with more positions opening up than there are people to fill them. One recruiter has expressed concern that even some of the jobs that are filled are held by people who aren't qualified to do them. The solution is more training and education, to teach people the skills they need to do cybersecurity work, and to keep existing workers up to date on the latest threats and defense strategies.

If the world is to hold off major cyberattacks — including some with the potential to be as damaging as a nuclear strike — it will be up to each person, each company, each government agency to work on its own and together to secure the vital systems on which people's lives depend.

***Jeremy Straub** is an Assistant Professor of Computer Science at North Dakota State University.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

Warning Over Terrorist Attacks Using Drones Given by EU Security Chief

By Zak Doffman Contributor

Source: https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones/#5c91ee9e7ae4

Aug 04 – **"Drones are becoming more and more powerful and smarter," EU Security Commissioner Julian King** warned this weekend, "which makes them more and more attractive for legitimate use, but also for hostile acts."

This is not new news—the threat from a drone attack on a crowded space in the West has been focusing security minds for some time now. And the real fear from a drone attack is that a

chemical or biological payload could be delivered into the midst of a crowded space with relative ease. The challenge with such attacks has always been delivery. A drone takes that challenge away.

According to Germany's *de Welt*—which published King's comments—in December last year, France's Anti-Terrorism Unit (UCLAT) issued a "secret report" for the country's Special Committee on Terrorism. The report warned of "a possible terrorist attack on a football stadium by means of an unmanned drone that could be equipped with biological warfare agents."

I have reported before on terrorist use of drones in the Middle East to mount attacks—countless Islamic State raids on the Iraqi frontline, recent Houthi attacks on Saudi targets and the Iranian-backed Islamic Jihad sharing video online of an attempted drone attack on Israeli tanks on the Gaza border. I said at the time, that security agencies will overlook the specifics of such attacks, and will focus instead on the implied threat that a larger or more ominous payload would represent to targets in the West.

That terrorist threat has now become more front of mind, with the vulnerability of aircraft and crowded spaces to such devices highlighted as particular causes for concern. With this in mind, King said that he will "support EU member states to build networks for sharing information, increase engagement at the international level, and provide funding for projects that address the threat of drones—both for the threat as it appears today and how it will look in the future."

Last year, at a closed meeting with one of the U.K.'s leading soccer clubs, the stadium's security director told the room "there are two things that terrify us: a large vehicle driven at speed at thousands of fans as they head home after a match, and, of course, drones." The

meeting room overlooked a stadium where 50,000 plus people gather 25 plus times a year, the threat from drones did not require elaboration.

FBI Director Christopher Wray told a Senate Homeland Security Committee last year that the terrorist threat from drones is escalating—such devices "will be used to facilitate an attack in the U.S. against a vulnerable target, such as a mass gathering," he warned. A year earlier Wray had told senators that "we do know that terrorist organizations have an interest in using drones. We've seen that overseas already… the expectation is that it's coming here. They are relatively easy to acquire, relatively easy to operate, and quite difficult to disrupt and to monitor."

Islamic State propaganda posters have already depicted a drone attack on the Eiffel Tower in Paris and New York City, and former U.S. Secretary of Homeland Security, Kirstjen Nielsen has warned that the threat from drones "is outpacing our ability to respond… terrorist groups such as the Islamic State aspire to use armed drones against our homeland and US interests overseas… We have already worked with our partners to stop terrorist plots that could have involved drone technology."

Remember, IS operatives have extensive drone experience from the Middle East. As U.K. police counter-terror lead Neil Basu pointed out, drones "have been used on the battlefield and what's used on the battlefield will eventually be adapted to be used on domestic soil."

The relative ease of availability and execution to mount a drone attack terrifies security agencies worldwide, and the context is that payload risk. The amount of explosive that can be carried by a commercial drone remains somewhat limited. A targeted attack on a high-profile location or an aeroplane in-flight would be possible but challenging to execute. In a crowded space it would generate headlines but limited damage. But a rudimentary attack using a non-explosive payload into an unprotected public space...

King's latest comments echo a similar warning in Europe from U.K. Defence Secretary Ben Wallace, who said last year that "terrorists continue to explore new ways to kill us on our streets: chemical and biological weapons are marching in closer. They have developed and worked on a better arsenal. We have to be prepared for the day that might come to our streets here."

GammaEx project: A solution for CBRN remote sensing using Unmanned Aerial Vehicles in maritime environments

By Mario Monteiro Marques, Rodolfo Santos Carapau, Alexandre Valério Rodrigues et al.

Source:https://www.academia.edu/36921997/GammaEx_project_A_solution_for_CBRN_remote_sensing_using_Unmanned_Aerial_Vehicles_in_maritime_environments?email_work_card=view-paper

Nowadays Chemical, Biological, Radiological and Nuclear (CBRN) agents are real threats, and they can be released from intentional and non-intentional sources. Intentional sources include weapons of mass destruction, and they can inflict serious amount of damage. CBRN non-intentional sources can go from disease outbreaks or even incidents, such as a nuclear accident. The interest for unmanned vehicles is growing more and more, either in military or civilian applications. In this scenario, they can be applied, especially Unmanned Aerial Vehicles (UAVs). The response to CBRN releases should follow several steps, such as reconnaissance of the affected area, detection of the agent, sampling, decontamination, victim screening, medical evacuation, identification of the type of agent and medical treatment. Therefore, UAVs can be an important asset in this scenario, as they bring many advantages, such as the access to inhospitable or inaccessible spaces, incorporation of sensors that can be used to identify the

agent, and many other factors that increase the speed of the task, reducing at the same time the risk to personnel. In this paper, an UAV system is presented to fulfill the requirements of this issue, including the vehicle, sensors and control station. This system was tested and the validation tests are also represented. It proved to be an asset in CBRN releases, either intentional or non-intentional.

The use of UAVs as CBRN detection platforms

By Stephen Johnson
CBRNe World I Spring 2010
Source: https://www.academia.edu/4999304/The_use_of_UAVs_as_CBRN_detection_platforms

Unmanned Aerial Vehicles in CBRN environment: Sensors review and concepts of operations

By Júlio Gouveia-Carvalho and Mário Marques
International Symposium "Mine Action 2015"
27 to 30 April 2015, Beograd, Croatia
Source:https://www.academia.edu/21524442/Unmanned_Aerial_Vehicles_in_CBRN_environment_Sensors_review_and_concepts_of_operations

Recent crisis like the use of chemical warfare agents in Syria and the Fukushima accident, presents a need for new technologies, which may lead to the deployment of unmanned aerial vehicles (UAV) to detect chemical, biological, radiological and nuclear (CBRN) threats in the future. Unmanned aircrafts are an ideal choice when operations are required in environments that would be hostile to a manned aircraft or its crew. Airborne sampling or observation missions related to CBRN threats would be ideally suited to unmanned aircrafts. Sensors can be fitted to a range of types, from a small man-portable system for local tactical use, to large aircraft-sized systems for global monitoring. This review aims to describe some trends on CBRN sensors and integration on UAV platforms and also to identify concepts of operations involving the use of UAV in a CBRN scenario. From the technical perspective the biggest challenge is to combine the avionic flight system of the UAV, the sensor systems and the wireless communication link while guaranteeing the absence of any mutual interference. Another issue that is addressed is related to the need for decontamination of the platforms after an operation in a "*hot zone*". Modular approach with disposable components or the use of low cost systems could be a solution where smaller systems can be disposed in a safe area once data has been gathered rather than having to recover to an airfield where it would have to be decontaminated, or risk contaminating personnel and other equipment. The knowledge of CBRN sensor technologies, future trends and concepts of operations are some of the main issues that should be addressed for identifying research and development (R&D) opportunities for further development of UAV for CBRN operations.

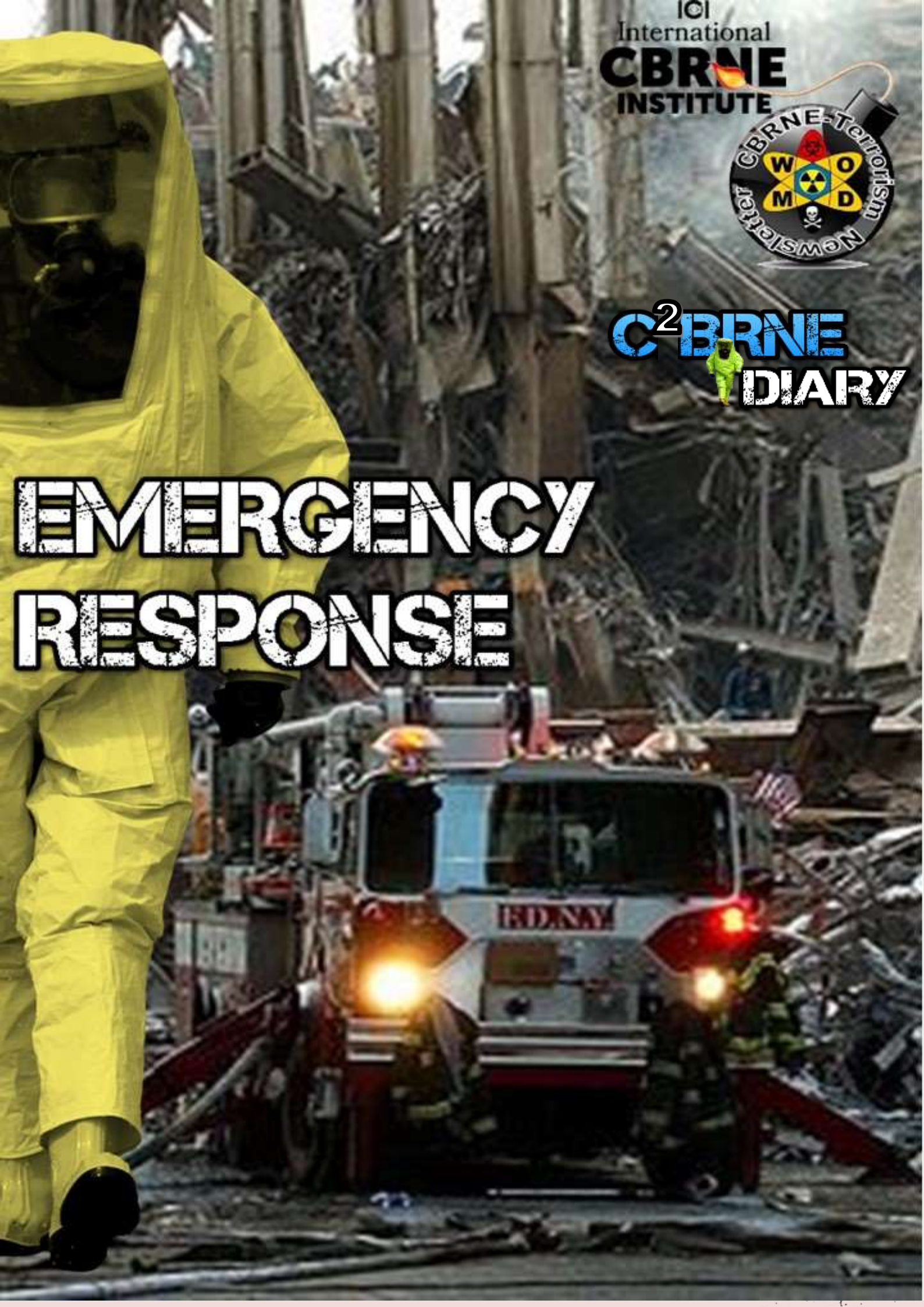
Autonomous Gyrocopter to Deliver Heavy Cargo

Source (+video): https://i-hls.com/archives/93576

Aug 07 – The German Aerospace Center (DLR) has been at work developing an autonomous gyrocopter that is intended to ship cargo. The Automated Low Altitude Air Delivery (ALAADy) system is designed to deliver heavy payloads autonomously at lower altitudes.
With online shopping gaining more and more momentum, transporting goods to the customer has become a massive operation and industry in its own right. In an effort to make delivery services more efficient, many companies have been showing interest in the use of UAVs.
However, many small quadcopters are simply too small to carry heavier cargo and using conventional aircraft can be very expensive. It's this problem that the ALAADy system is addressing.
A gyrocopter is an aircraft that seems similar to a helicopter, however, in most scenarios, isn't capable of vertical flight. The ALAADy gyrocopter last tested has two rotors, one above the aircraft creating lift and the other behind the aircraft creating forward propulsion.

Gyrocopters are convenient for this application due to their short takeoff and landing ability, cheapness to operate, and capability of flying low and slow. If the engine were to fail, then the top rotor will slow down the gyrocopter's fall, bringing it to the ground in a safer manner.
The ALAADy system has been in development since 2016, and has recently flew a test flight. **The target**

is to be able to carry cargo weighing up to 200 kilograms for distances up to 500 kilometers.
The latest gyrocopter used to test the system is a 450 kilogram modified commercial gyrocopter. Newatlas.com reports that test flight have been completed at an altitude of up to 150 meters and speeds up to 100 kilometers per hour. Researchers are now looking to increase its autonomous capabilities.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
EMERGENCY
RESPONSE
FDNY

American Nurses Not Prepared for a Catastrophe: Study

Source: http://www.homelandsecuritynewswire.com/dr20190724-american-nurses-not-prepared-for-a-catastrophe-study

July 24 – **On average, American colleges and universities with nursing programs offer about one hour of instruction in handling catastrophic situations such as nuclear events, pandemics, or water contamination crises**, according to two recent studies coauthored by a nursing professor at the University of Tennessee, Knoxville.

"Events that can cause greater impact but are less likely to occur, usually receive less training hours," said Roberta Lavin, executive associate dean and professor in UT's College of Nursing. Lavin is coauthor of the studies published in the *Journal of Perinatal and Neonatal Nursing and Nursing Outlook*.

UT says that the studies' results come from two surveys that were sent to all colleges and universities that offer nursing programs in the United States.

The surveys revealed that most students said they were not getting enough instruction in emergency response, while professors and lecturers said they were not prepared to teach how to offer care during and after catastrophic situations.

"Emergencies are not just the exact moment a disaster hits; it is also the aftermath. How do we evacuate a town? How do we carry out care for other chronic, sometimes life-lasting consequences that derive from these situations? That is the big challenge," said Lavin.

One study examined the management of Zika fever and water contamination crises and was focused on nurses' preparedness to attend pregnant women and children, two populations that are often overlooked in emergency plans.

In addition to nursing schools, that same study also assessed the preparedness of Master of Public Health programs, medical schools, and Doctor of Osteopathy programs in America.

"Even though all accreditation standards require this type of preparation, we are not putting enough emphasis on it," said Lavin.

Lavin and her coauthors now are working to offer resources to help close that knowledge gap. One of the actions they are taking is to design educational modules for instructors to use in their classes. The units are licensed under Creative Commons and can be downloaded free of charge; users can adjust the courses to meet the needs of their communities.

"We are putting people out there to attend these emergencies, and we owe it to them to prepare them right," Lavin said.

Paramedics Add Another Set of Hands with New CPR Technology

Source: https://www.govtech.com/em/safety/Paramedics-Add-Another-Set-of-Hands-with-New-CPR-Technology.html

Aug 14 — A new piece of equipment has been introduced to Hall Ambulance paramedics that serves as essentially another person on scene — and provides continuous compressions while implementing improved blood flow at the same time.

AutoPulse, a ZOLL Medical Corp. invention, provides high-quality CPR to victims of sudden cardiac arrest. The "unique device" will allow Hall Ambulance paramedics to give treatment quickly while also continuing compressions consistently — which increases one's likelihood of surviving, said Bryan Pank, senior EMS account executive for ZOLL.

The new piece of equipment was introduced at a press conference Monday afternoon.

Here's how it works: The machine itself consists of a board and a "lifeband," which actually gives compressions. First responders will put a person experiencing sudden cardiac arrest on the board and place the lifeband around their chest, which will then tighten based on the circumference of the person's chest. From there, "the magic of the bloodflow really occurs," Pank said — the lifeband begins to give compressions.

This can be especially useful when paramedics are called to a scene with unfavorable conditions such as a stairwell, a hallway with sharp corners, or a cramped elevator. Paramedics can utilize AutoPulse to continue compressions as they are moving the person into a more stable area, said Chris Leone, manager for Hall Critical Care Transport.

With the AutoPulse, paramedics are able to administer compressions much more efficiently as compared to using just their hands — AutoPulse allows fewer pauses between compressions.

More than 600 paramedics and EMTs from Hall Ambulance and firefighters from the Kern County Fire Department and the Bakersfield Fire Department have been trained on how to use the device over the past two weeks, Leone said.

Eighty of the AutoPulse devices will be placed in each Hall Advanced Life Support and Basic Life Support ambulance within the next few days, Leone said. Hall Critical Care Transport will also be using the device on its ground unit.

Governments Failing to Understand Global Catastrophic Risks: Report

Source: http://www.homelandsecuritynewswire.com/dr20190816-governments-failing-to-understand-global-catastrophic-risks-report

Aug 16 – The plausible global catastrophic risks include: tipping points in environmental systems due to climate change or mass biodiversity loss; malicious or accidentally harmful use of artificial intelligence; malicious use of, or unintended consequences, from advanced biotechnologies; a natural or engineered global pandemic; and intentional, miscalculated, accidental, or terrorist-related use of nuclear weapons.

Researchers from Cambridge's Center for the Study of Existential Risk (CSER) the other day released a new report on what governments can do to understand and inform policy around these risks, which could threaten the global population.

The likelihood that a global catastrophe will occur in the next 20 years is uncertain, say the researchers, but the potential severity means that national governments have a responsibility to their citizens to manage these types of risks.

Des Browne, former U.K. Secretary of State for Defense, said: "National governments struggle with understanding and developing policy for the elimination or mitigation of extreme risks, including global catastrophic risks. Effective policies may compel fundamental structural reform of political systems, but we do not need, nor do we have the time, to wait for such change.

"Our leaders can, and must, act now to better understand the global catastrophic risks that are present and developing. This report offers a practical framework for the necessary action."

Governments must sufficiently understand the risks to design mitigation, preparation and response measures. But political systems often do not provide sufficient incentives for policymakers to think about emerging or long-term issues, especially where vested interests and tough trade-offs are at play.

Additionally, the bureaucracies that support government can be ill-equipped to understand these risks. Depending on the issue or the country, public administrations tend to suffer from one or more of the following problems: poor agility to new or emerging issues, poor risk management culture and practice, lack of technical expertise and failure of imagination.

Cambridge notes that the report provides 59 practical options for how governments can better understand the risks. Ranging from improving risk management practices to developing better futures analysis, to increasing science and research capability, most national governments must take major policy efforts to match the scale and complexity of the problem, say the researchers.

Catherine Rhodes, CSER's Executive Director, said: "This report gives policy-makers a set of clear, achievable and effective options. Few countries are making efforts to understand these risks, so most governments will be able to draw policy ideas from the report.

"In the U.K., the government is ahead of its peers when it comes to conducting national risk assessments, delivering foresight and horizon-scanning and engaging with the academic community. But even it needs new approaches to understand and deal with global catastrophic risks."

Professor Lord Martin Rees, Astronomer Royal and co-founder of CSER, said: "Global problems require global solutions. But countries must also act individually. Without action, these catastrophic risks will only grow over time, whether it be on climate change, ecothreats, synthetic biology or cyber.

"Governments have a responsibility to act, both to minimize the risk of such events, and to make plans to cope with a catastrophe if it occurred. And those that take the initiative will set a positive example for the rest of the world. Protect your citizens and be a world leader – that decision is available to every country."

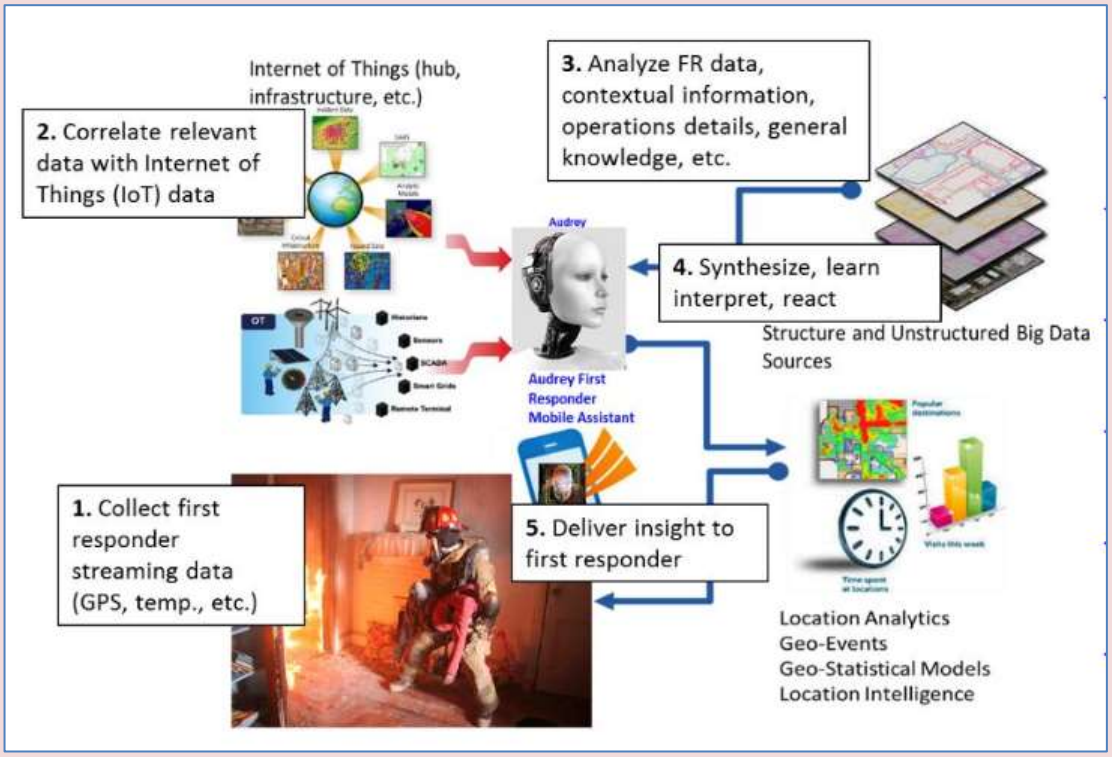
Evaluate AI capabilities in Helping Paramedics

Source: http://www.homelandsecuritynewswire.com/dr20190816-evaluate-ai-capabilities-in-helping-paramedics

Aug 16 – Paramedics must make numerous life-saving decisions, often in the back of an ambulance with limited time. While they at times call doctors for additional medical directives, precious seconds tick away for the patient during these back-and-forth conversations. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) recently partnered with Canada's Department of National Defense Science and Technology Organization, Defense Research and Development Canada Centre for Security Science (DRDC CSS) to examine whether artificial intelligence could be used to improve that information overload.

Together with the NASA Jet Propulsion Laboratory and the Hastings-Quinte Paramedic Services in Ontario, Canada, S&T and DRDC CSS conducted an experiment with S&T's **Assistant for Understanding Data Reasoning Extraction and Synthesis (AUDREY),** a human-like reasoning system, to determine if AUDREY can perform data fusion, and provide tailored situational awareness information to the paramedic. AUDREY assists the paramedic by augmenting the human decision-making process, helping sort and prioritize through the vast

amounts of data being reported to a paramedic through the introduction of new technologies and their already complex operational tempo.



"Responders are inundated with information; why shouldn't they use available technology to help them weed out information that isn't needed or provide verification of information – all to aid patient care," said DHS S&T Program Manager Denis Gusty. "This exercise used S&T-developed technology to aid paramedics and help them provide more efficient care. AUDREY successfully demonstrated how AI can support responders."

Cross-border Collaborations

S&T says that S&T's relationship with its Canadian counterparts goes back to 2010 with the start of the Canadian-U.S. Resiliency Experiment Series (CAUSE), in which communication technology was tested on both sides of the border. The AUDREY-Hastings experiment continued this cross-border initiative and focused on the unique challenges paramedics face, from patient assessment to ambulance transport to hospital transfer.

"This experiment was to improve the patient care point of view," explained Doug Socha, Chief of the Hastings-Quinte Paramedic service. "When paramedics are consulting on patient treatment plans with physicians, this takes the paramedic and the physician away from their patients. This experiment was to make improvements on that side to save time and also to increase the patient safety aspect."

One of the potential enhancements AUDREY can offer the paramedic community is in the area of medication safety. With just a photo, the paramedic can confirm a drug and dosage is correct before administering it to the patient.

"We took a picture of the medication the paramedic was about to administer and sent that to AUDREY, which confirmed it was the right drug," Socha shared. "Paramedics are in the back of the ambulance by themselves making critical decisions, and they don't have the luxury of the emergency room with other professionals who can be the second set of eyes to ensure the right medication is about to be administered."

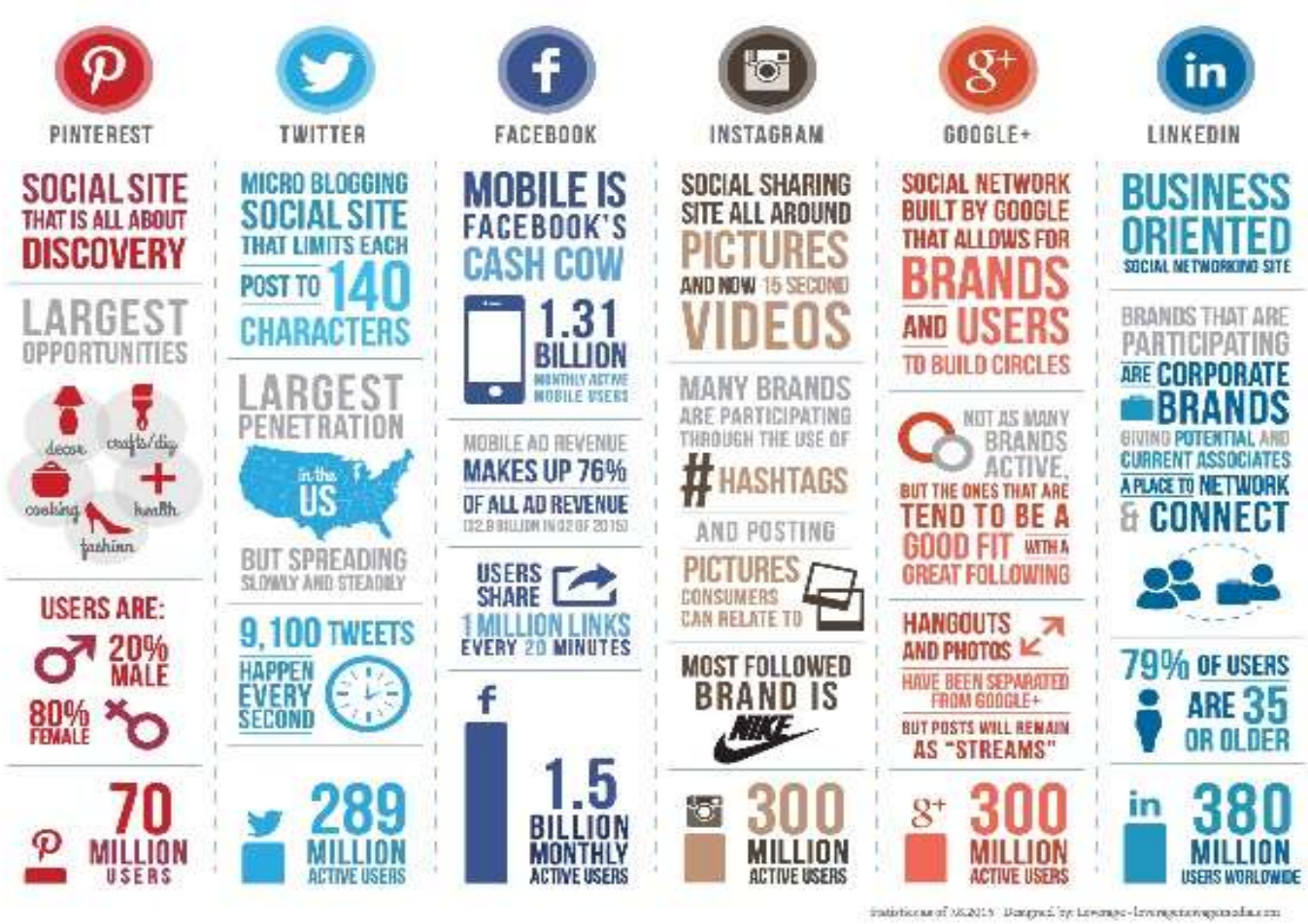
Socha pointed out another improvement: the ability to do visual recognition of the Electronic Patient Care Report. "A lot of the time we do chart audits and quality assurance processes after the fact. By using AUDREY, we are moving that safety aspect immediately to the time of patient care. Right to the back of the ambulance."

Next Steps

Local Hastings-Quinte paramedics participated in the experiment, and their feedback on AUDREY's performance will ensure the technology is developed into something truly useful for frontline paramedics. An After-Action Report is being prepared on the experiment results and is expected to be made public in the fall of 2019.

The U.S. and Canada have a shared interest in improving the experience of paramedics to make their jobs easier and to fulfill the need to save lives, Gusty explained.

"While I know that the paramedics will always have the final decision when it comes to patient care, the support of AUDREY will result in more efficient transfer to the hospital and support from the paramedic in the field," said Rick Phillips, Hastings County Warden.



The Role of Social Media and Artificial Intelligence for Disaster Response

Source: https://www.slideshare.net/mimran15/the-role-of-social-media-and-artificial-intelligence-for-disaster-response


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
ASYMMETRIC
THREATS

The Sea Is Rising. Can You Save Your Town?

Source: http://www.homelandsecuritynewswire.com/dr20190724-the-sea-is-rising-can-you-save-your-town

July 24 – That headline is also your mission in The Ocean Game, the *LA Times*' deceptively simple online simulation of city governance in the face of climate change. The game accompanies an in-depth look at how various California coastal communities are responding to the effects of rising seas caused by global warming.

Thomas Gaulkin writes in the *Bulletin of the Atomic Scientists* that California may not be the most vulnerable part of the world that will experience the effects of sea-level rise in the coming decades, but the problems it faces are not at all trivial. According to the *Times*, more than $150 billion in private and public property may be underwater by the end of the century, including two-thirds of Southern California's beaches. Critical habitats for birds and endangered species could disappear forever.

Rosanna Xia's full report is well worth reading. She focuses on the challenges facing individual cities like San Francisco—where "the cost of building levees, seawalls and other measures to withstand six and a half feet of sea-level rise and a 100-year storm could cost as much as $450 billion"—and Imperial Beach, which added 300,000 cubic yards of sand to replenish its beaches, but will eventually have to retreat inland.

What Will Communities Do When the Water Runs Dry?

Source: http://www.homelandsecuritynewswire.com/dr20190731-what-will-communities-do-when-the-water-runs-dry

July 31 – Earlier this summer, the sixth-largest city in India, Chennai, ran out of water. The cause wasn't just a weak monsoon. Over-extraction of groundwater, unmaintained reservoirs, runaway urban growth and leaking pipelines all played a role.

Chennai's four reservoirs are puddles of cracked mud. Some parts of the city have not had piped water for five months. An Indian government think tank predicts Day Zero for 21 Indian cities next year.

Water crises are now global. Cape Town, South Africa, narrowly escaped Day Zero last year, but it's still at risk, as are Sao Paulo and Mexico City. Iraq, Morocco and Spain also face water shortages.
Two years ago, eight Arizona State University students spent a month living in a Mojave Desert ghost town in the dead of summer, living on 4 gallons of water per person per day and no air conditioning. A hybrid art-science experiment, it started off as a water exercise and turned into a lesson on collaboration no one expected.
The idea was co-directed by two ASU faculty members: Marco Janssen, director of the Center for Behavior, Institutions and the Environment and a professor in the School of Sustainability, and Adriene Jenik, a professor of intermedia in the Herberger Institute for Design and the Arts. They created a near-future fictional scenario and dubbed the experiment Drylab2023.
Recent news has transformed Drylab2023 into more of a training scenario than an experiment. *ASU Now*'s Scott Seckel talked to Jenik about the crises, the eerily prescient experiment and the nexus

between the two. Seckel has edited the answers for length and clarity.

Scott Seckel: The sixth-largest city in India is out of water, and 21 other Indian cities are facing Day Zeros next year. What are your predictions on the outcomes: mass migration on a scale that makes the Syrian diaspora look like a casual commute? Life with a daily water supply similar to Drylab2023? Any predictions about impacts to industry and urban life?

Adriene Jenik: What we are seeing in Chennai right now is a devastating illustration of human-driven climate disruption. A short and sparse monsoon season has not replenished water storage, reservoirs and aquifers that people depend on for water consumption and agriculture; the large and developing population has been drilling wells deeper and deeper, rapidly draining groundwater reserves. Their freshwater ecosystem of marshes, streams and estuaries has been covered with landfill and built upon, further impacting weather systems and the resilience of the natural systems. The more well-to-do (and their neighbors and friends) are able to continue on, for the moment, without many disruptions due to private wells, but the poor and aspirational find their lives organized around the sound of the water truck and reconfigured economically, socially and aesthetically in relation to the scarcity of this precious resource.
Sadly, these disruptions are not hard to predict. They are a regular part of the forecasting and planning of large businesses and national, regional and local governments, including our own country's military forecasting. But the effects are not in a distant imagined future. Many don't realize that the current humanitarian crisis on our southern national border is caused in part by climate migration, revealing the complex impacts of our historic overconsumption of natural resources.
It is hard for me to picture a near future where access to clean, fresh water continues in as plentiful a way as it is in most of our country at this moment. Between aging city water

infrastructure threatening water quality, increased privatization of water sources, groundwater contamination as a result of fracking and other extractive technologies and the increase in climate extremes including drought and desertification of land that affects agriculture, the current thoughtless use of water in our culture will not be sustained for long.

One vision does turn in the direction of an apocalyptic scenario where water scarcity produces increased conflict and increases the desperation caused by the gap between the rich and poor — with the rich retaining access to this precious resource and the poor dying of thirst and disease. Pretty grim.

Another vision, which Drylab2023 shows is just as plausible, is that people will join together as a community to honor and steward this precious resource. Dr. Elinor Ostrom, ASU faculty and Nobel Prize winner, through her observations of cultures around the world, showed that the management of a commons is doable and not at all unusual. She and her research partners even outlined some design principles that made it more likely to occur and be sustained successfully over time. We can learn from our indigenous colleagues and their communities, who treat water as medicine and understand it as the sacred life force that it is, that there are other ways to live in relation to our water. We can be proactive in overhauling our building and industrial codes so that they incorporate greywater and composting systems, and we can rethink our diets by moving away from animal protein.

As you can see, the rethinking of water necessitates a rethinking of all of our living systems, so this will take immense political and social will. I am hopeful that these initial Day Zero events — like the one last year that forged significant changes in water use and management in Cape Town, South Africa — are not just seen as far-off problems befalling impoverished nations, but are understood as warning signs for us to not continue in a "business as usual" fashion.

Seckel: At the end of Drylab2023, participants hoarded sizeable amounts of "personal" water they'd saved up. No one squandered it on things like showers, but there wasn't a lot of sharing either. Do you think this is predictive of how a similar situation will shake out socially in reality?

Jenik: I was personally shocked and surprised at what ended up happening in Drylab in relation to this "hoarding" issue. When we first designed the project, each person was to be granted 2 gallons of water for personal use (so as to not dehydrate) and 2 gallons for the common pool to be negotiated with others. Upon arriving on site, with the co-directors no longer involved in decision-making but solely serving as chaperones and observers of the process, a subset of the group started to lobby for a 3:1 distribution — 3 gallons personal, 1-gallon common pool. The rest of the group went along, even as they recognized and commented upon the degree of distrust they had taken on from growing up in such an individualistic culture. This decision was especially poignant, as several of the students from nonwhite backgrounds understood that they had a different experience of community — that their needs had been met within community settings and as a result, they had a greater sense of trust.

Most disappointing was that even though the data showed that they had plenty of water to share after week three and they could easily change to a 2:2 distribution, many participants still argued against changing. I believe that if the experiment had gone on longer than 30 days that the data would have won the day, but what happened certainly underlined the critical importance of trust and community-building for the success of these changes long term. Trust takes time and is more difficult as we scale to a larger population, and so we can see that if we are in a crisis and rushing changes through, and if they are enacted across a large scale of population, they are less likely to be embraced.

Seckel: According to research, nearly half of the human population is living with water scarcity, inhabiting places unable to fully meet their drinking, cooking and sanitation needs. What are your thoughts on that?

Jenik: As informed as we believe we are, many of us live in an illusory bubble of constant access — and growing in amount and speed — to natural resources and consumer goods. Even if we are aware of the impacts of water scarcity throughout the world, we don't understand ourselves and our overconsumption as the cause or connected. One of the more profound lessons of Drylab2023 was a deeper understanding for each participant and the directors of the ways in which we are implicated personally and culturally in what is happening. Few cultures waste as much water as we doThe average daily water usage in Tempe is 80-100 gallons per day.. It is this waste and overconsumptive lifestyle that is now glorified and "the dream" of many other peoples and cultures — no wonder people continue to put themselves in danger to migrate! It is our responsibility to join with other privileged cultures around the world to address the possibility of another way of living — to honor and value and

support, rather than degrade and deign to "improve," the water conservation and land stewardship that indigenous and poor cultures have developed over millennia. Can we be humble and learn these lessons even as we develop technological innovations?

Another lesson learned was that fostering community while bringing beauty and mindfulness to the process of daily living can actually elevate what at first seems like a life of hardship and depravation. Again, ancient cultures already know this!

Seckel: Do you plan to resurrect Drylab2023?

Jenik: I would very much like to continue offering this as an immersive/experiential learning module and am putting effort in the next few years into developing an ongoing offering, either within ASU or with another external partner. On-campus ASU presentations have shown a significant interest among students for participating in future offerings. Ideally, our ASU community could face the existential challenge presented us, and take on further responsibility as a "sustainable campus" to encourage the radical rethinking of our use patterns. In some cases, as with Drylab2023, it could forge a new lifelong relationship to water; for all it would increase empathy and understanding of the real hardships and obstacles of people living without clean fresh water.

Jakarta's Giant Sea Wall Is Useless If the City Keeps Sinking

Source: http://www.homelandsecuritynewswire.com/dr20190731-jakarta-s-giant-sea-wall-is-useless-if-the-city-keeps-sinking

July 31 – Late last week, president Joko Widodo of Indonesia told the AP that he's fast-tracking a decade-in-the-making plan for a giant sea wall around Jakarta, a city that's sinking as much as 8 inches a year in

places—and as seas rise, no less. Models predict that by 2050, a third of the city could be submerged. It's an urban existential crisis the likes of which the modern world has never seen.

Matt Simon writes in *Wired* that deploying a sea wall, however, is a massive political and engineering problem in any country, to say nothing of Indonesia's struggles with a literal underlying crisis: Jakarta's people are pumping too much groundwater, and consequently the land is collapsing underneath them. If Jakarta can't find a way to hydrate its people some other way, it'll keep sinking, pulling that new sea wall down with it. It's a glimpse of a dark future for much of human civilization, which stubbornly clings to coasts around the world.

Think of Jakarta as sitting on top of giant water bottles, aka aquifers. Forty percent of its 10 million residents get their water from pumping, so they've been draining those bottles, which consequently collapse, leading to land subsidence. This, by the way, is not unique to Jakarta: California's Central Valley has sunk by as much as 30 feet for the same reason. But because other nations have dealt with the problem, Jakarta knows how to fix it.

The Soviets planned to wipe out the U.S. with a huge tsunami. How?

Source: https://www.rbth.com/history/330748-soviets-planned-huge-tsunami

July 31 – The project to annihilate the U.S. with a wave of biblical proportions was the brainchild of a future Nobel Peace Prize laureate.

In September 1961, *The New York Times* reported that the Soviet Union was preparing to test a powerful explosion. The plan was to detonate 100 million tons of strategically placed TNT, causing waves that would devastate the U.S. Pacific and Atlantic coasts.

The project, codenamed ***Lavina* (Avalanche)**, envisaged the creation of an artificial tsunami as a cleaner alternative to nuclear weapons, yet still ferocious enough to cause massive casualties among the civilian population. It gets even more disturbing when the project leader's name is mentioned, for it was none other than Andrei Sakharov, the renowned physicist and Nobel Peace Prize winner, widely considered one of the greatest humanists of the 20th century. How can that be?

How to create a catastrophe

The deadly project, which bore more than a passing resemblance to the movie *The Day After Tomorrow*, was not actually a Russian idea. The first attempts to cause a tsunami were carried out by the Americans themselves. Their top-secret operation Project Seal was essentially identical in purpose: to wipe the enemy off the face of the earth with a superpowerful wave.

It was conceived by naval officer E.A. Gibson, when he noticed how blasting operations to clear the coral reef around the Pacific Islands led to huge waves. Assuming the size of the wave to be directly dependent on the force of the explosion, the military decided to investigate this theory. Tests began in 1944 off the coast of New Caledonia, where 3,700 bombs were detonated, and later near Auckland, New Zealand.

"It was absolutely astonishing. First that anyone would come up with the idea of developing a weapon of mass destruction based on a tsunami ... and also that New Zealand seems to have successfully developed it to the degree that it might have worked," said New Zealand film-maker Ray Waru, who examined the military files buried in the national archives.

It wasn't long before the Soviet Union received intelligence reports on the US testing and thought it a great idea – far more effective than aircraft carrying nuclear warheads, which were trackable by air defenses. Then General Secretary Nikita Khrushchev ordered feasibility studies to be carried out.

"I was ashamed"

By that time, the USSR had already developed its own hydrogen bomb, one of the creators of which was physicist Andrei Sakharov. A team of scientists, him included, faced the task of testing the bomb in new conditions – water. The problem was how to deliver it.

In his memoirs, Sakharov later wrote: "After testing [the Tsar Bomb], I was concerned about the lack of means for carrying it (bombers were no good, they could be easily shot down). It meant that in a military sense, our work was futile. I decided that the carrier could be a large submarine-launched torpedo." A US naval base was earmarked as the strike target. "Sure, the destruction of ports – caused by the above- and underwater explosions as the 100-megaton torpedo 'jumped' out of the water – would have resulted in mass casualties," wrote Sakharov with brutal impassivity.

He goes on to tell how he shared his idea with Rear Admiral Petr Fomin, who headed the Soviet fleet's nuclear weapons and nuclear tests. Fomin was shocked by the project, calling it a "cannibalistic" massacre of the civilian population. "I was ashamed and never talked about my project with anyone again," Sakharov recalled.

But other methods were actively discussed. It was hypothesized that a torpedo armed with a superpowerful charge could be fired at a safe distance by fitting it with a timing mechanism. That way, it would explode at the right time, causing a tsunami. Another option was to turn the torpedo into a time bomb, and leave it off the US coast, able to be detonated at any time.

Could it really have worked?

Yes and no. A superpowerful bomb would indeed have produced a massive wave, but not, as the tests showed, on the scale imagined. This conclusion was reached independently by both the U.S. and the USSR.

Physicist Boris Altschuler says that in 2002 the Physics Institute of the Russian Academy of Sciences was paid a visit by several US nuclear physicists: "One of them told me in private that as a young man at the Los Alamos National Laboratory, he had been instructed to calculate the parameters of a hydrogen bomb capable of creating a wave with the power to destroy the USSR." He diligently did the sums as requested, and found that creating a 1 km-high tsunami in the Arctic Ocean would be feasible. Yet his report ended with a negative conclusion – the geographical size of the Soviet Union rendered the project impracticable. "The wave would not reach Moscow or the nuclear mines in Siberia. Not to mention the fact that the wave would move in concentric circles in all directions, including toward the US, Canada, and Europe," said the report.

Sakharov's colleague on the superbomb project, Yuri Smirnov, also poured cold water on the idea. The Atlantic is too shallow, while a giant tsunami in the Pacific would have destroyed only California. The Rockies would have stopped the wave going any further, which would have been pointless from a military point of view.

The US shelved the project, and Khrushchev, heeding the advice of the military and scientists, canceled the order to equip submarines with hydrogen bombs.

Will the real Sakharov please stand up

By the time Sakharov penned his memoirs, he had grown disillusioned with the Soviet government, admitting: "I tried to create an illusory world for myself as justification." But back in the 1950s, he had been a committed communist and believed that the country that had incinerated Hiroshima and Nagasaki could one day do the same to his native land.

Moreover, he considered it his moral duty to neutralize this threat, and thus never expressed remorse for suggesting "cannibalistic" projects (for which he was awarded the title of academician (of the Soviet Academy of Sciences) at the tender age of 32). Sakharov genuinely believed that his ideas would prevent, not provoke, WW3. "Thermonuclear weapons have yet to be used against people in war. My most cherished dream (more profound than anything else) is for this never to happen, for thermonuclear weapons to curb war, but never be applied."

"He lived too long in some extremely isolated world where little was known about events in the country, about the lives of people in other sectors of society, and about the history of the country in which and for which they worked," noted writer and historian Roy Medvedev, who was Sakharov's contemporary and later biographer.

By 1975, when Sakharov was awarded the Nobel Peace Prize, he was already the voice of the dissident and human rights movement in the Soviet Union, and one of the chief exposers of the Stalin-era crimes for Western audiences.