05\21

HZS C²BRNE DIARY

Dedicated to Global First Responders

May 2021

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DIRTY R-NEWS

The Speed of Ocean Currents Is Changing in a Major Way, Scientists Warn

By Navid Constantinou, et al.

Source [+video]: https://www.sciencealert.com/ocean-currents-are-getting-faster-and-we-don-t-know-how-this-impacts-climate-2

Apr 26 – Scientists already know the oceans are rapidly warming and sea levels are rising. But that's not all. Now, thanks to satellite observations, we have three decades' worth of data on how the speeds of ocean surface currents are also changing over time. In research published on 23 April in the journal *Nature Climate Change* we detail our findings on how ocean currents have become more energetic over large parts of the ocean.

EDITOR'S COMMENT: Perhaps this study can be used to calculate the movement of radio-contaminated water released into the ocean from the Fukushima nuclear power plant. The same might apply for nuclear power plant accidents in closed seas like that in the Arab Gulf that might pollute neighboring countries.

It's not radioactive Disneyland: Visit Chernobyl, but respect it.

By Margarita Kalinina-Pohl

Source: https://thebulletin.org/2021/04/its-not-radioactive-disneyland-visit-chernobyl-but-respect-it/

Apr 26 – This year is rich in commemorative anniversaries of natural and man-made disasters stemming from the use of nuclear energy for peaceful and military purposes. In March, we solemnly observed the 10th anniversary of the Fukushima nuclear disaster. On April 26, we marked 35 years since the largest nuclear accident at the Chernobyl Nuclear Power Plant. At end of August, the international nuclear nonproliferation and antinuclear movement will celebrate the 30th anniversary of the closure of the Semipalatinsk nuclear testing site. Besides catastrophic impacts on humans and environments, these grim places have something else in common; they have emerged as nuclear tourist destinations, with the Chernobyl (Chornobyl in Ukrainian) Exclusion Zone especially popular among aficionados of "dark" tourism.

Images of the desolate town of Pripyat with graffiti-laden buildings and its iconic, never-used Ferris wheel, adjacent villages with abandoned and overgrown houses, a kindergarten with mutilated dolls and teddy bears, and Duga—a gargantuan steel structure used as part of the Soviet missile defense early-warning radar network—flood social media. Selfies by ordinary tourists or professional photos featuring scantily clad models depict Chernobyl today as a nuclear theme park or an Armageddon landscape. Some pose with resettlers—villagers who returned to their homes following the disaster despite government warning and who continue to live in small dilapidated villages without running water. Others are pictured with Geiger counters wearing hazmat suits or plastic raincoats, depending on what a particular tour operator has in stock. There is an abundance of kitsch souvenirs at nearby kiosks at the Chernobyl Exclusion Zone entrance checkpoint where tourists are welcomed with blasting pop music. The zone's entrance does resemble a theme park entrance with buses and tourists smoking and casually chatting while waiting for their turn to enter. Permission is required, which can be acquired as part of an organized tour or through a professional visit arranged through the State Agency of Ukraine on the Exclusion Zone Management.

Simon the Fox waiting by a road to the Chernobyl Nuclear Power Plant. Credit: Margarita Kalinina-Pohl (2018).

What is lesser known to most visitors is that the state agency also manages the Chernobyl Exclusion Zone infrastructure, including eight state enterprises with over 6,000 personnel. The Territory of Special Industrial Use, encompassing a 6-mile (10-km) radius around the Chernobyl Nuclear Power Plant, houses radioactive waste and spent nuclear fuel storage facilities and will never be used or inhabited by people again. The Chernobyl Radiation and Ecological Biosphere Reserve, encompassing a 19-mile (30-km) radius of the plant, has become the largest environmental reserve in Ukraine, with more than 400 species of animals, birds, and fish. On the way to Reactor Unit 4, one can spot a fox named Simon (Semyon). Simon positions himself by a road leading to the reactor site and is rewarded with treats from employees and visitors.

Despite the presence of humans, animals, and lush vegetation, the Chernobyl Exclusion Zone remains one of the most contaminated places in the world with high levels of radioactive isotopes Cs-137 and Sr-90, especially in the zone's so-called Red Forest, named for the brown color of dead pines which absorbed high levels of radiation after the reactor meltdown. The exclusion zone is ravaged by occasional forest fires, with the most recent fires in April, 2020. These fires can potentially release radioactive substances into the atmosphere by burning contaminated vegetation. As that last fire took place during the COVID-19 pandemic, the human traffic in the region was minimal, which was a blessing to exclusion zone officials and firefighters.

Overgrown House of Culture (a community center) at one of the abandoned villages near the Chernobyl Nuclear Power Plant. Credit: Margarita Kalinina-Pohl (2018).

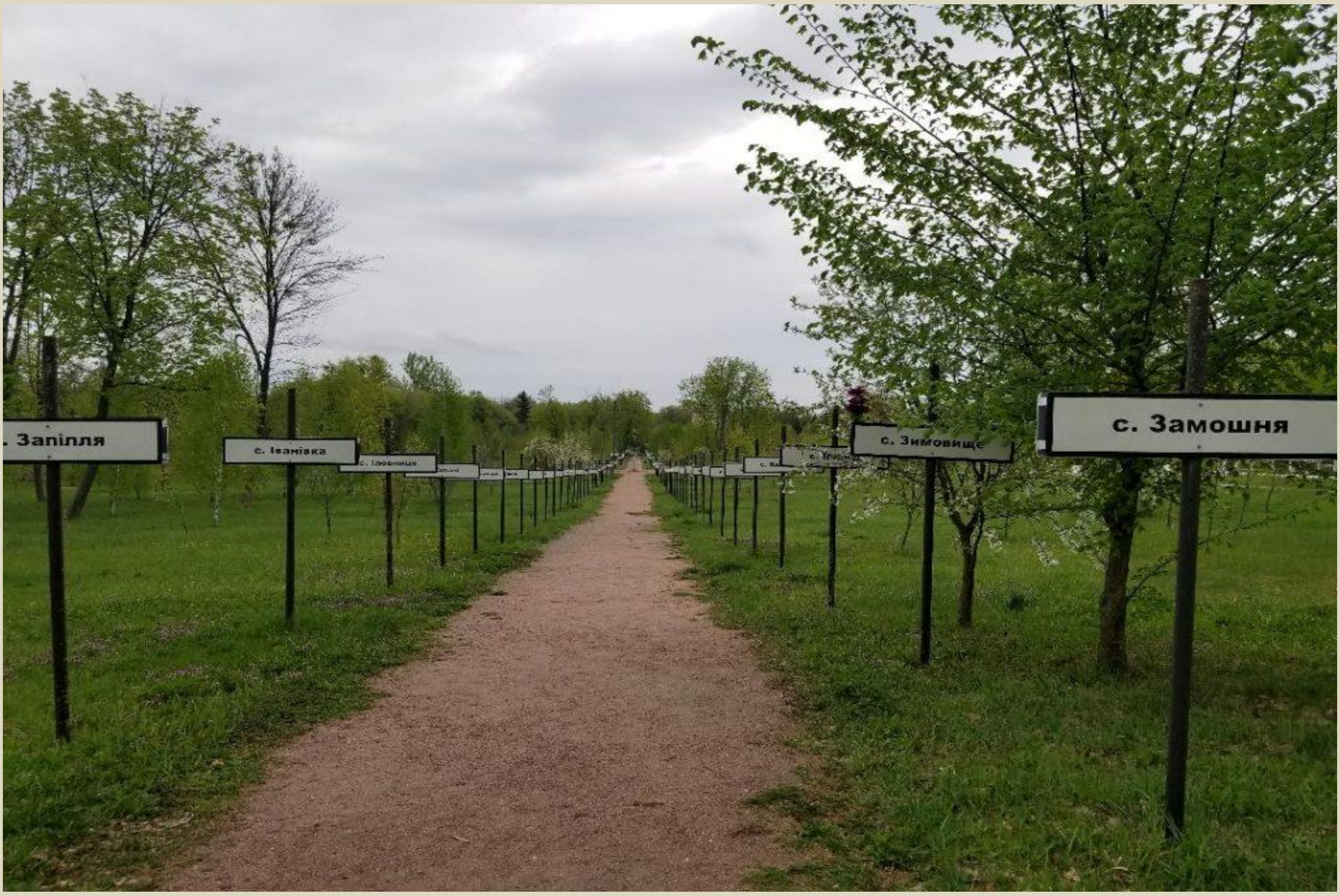
My two visits to the Chernobyl Exclusion Zone before the pandemic led me to reflect on how to enhance visitors' experiences there and at other nuclear disaster sites.

Most intrepid tourists I observed in Pripyat seemed to neglect that they were entering a territory of the largest anthropogenic disaster in the history of humankind. Due to the secrecy the Soviets employed in trying to cover up the Chernobyl accident, it is not feasible to provide exact estimates of how many people died and how many would die from radiation exposure. There is a widespread belief that millions of people were exposed to high levels of radiation. According to the 2005 UN report, fewer than 50 deaths had been directly attributed to radiation from the disaster, and the majority of these were first responders. The report's grim estimate was that about 4,000 people could eventually die of radiation exposure

Monument "To Those Who Saved the World." A monument to firefighters that died putting out the fire at Chernobyl Nuclear Power Plant. It is also dedicated to all Chernobyl liquidators (first responders) that cleaned up after the accident. Credit: Margarita Kalinina-Pohl (2018).

State Agency of Ukraine officials speak of "controlled access" and "visitors" instead of "tourism" and "tourists" to emphasize that all exclusion zone visitors and their actions are controlled and accounted for. Several authorized tour operators bring busloads of adventurers wishing to experience Chernobyl firsthand. There are plans to offer a tour to the Reactor 4 control room for those who dare to visit the ground zero.

A quick look at photos taken by exclusion zone visitors pouring onto social media makes one question their actions, which are often indicative of disrespectful and negligent behavior. This has caused HBO's *Chernobyl* producers to plead with tourists to be respectful of the tragedy behind the scene when taking pictures at the zone.



Alley of abandoned villages - 162 plaques with the names of permanently evacuated settlements during 1986-1991 after the Chernobyl accident. Credit: Margarita Kalinina-Pohl (2018).

Designating Chernobyl as an official tourist destination has been on Ukrainian President Zelensky's agenda, as well as fighting corruption at the exclusion zone, such as bribes that security officials collect from tourists, the illegal export of scrap, and the use of natural resources. What is lacking is a visitor center with a collection of declassified photos, documents, and oral histories of people who lived through the accident. This could be opened as a branch of the Ukrainian National Chernobyl Museum in Kyiv, which would offer a starting point for each tourist.

It is important to keep the memory of Chernobyl alive. Turning its exclusion zone into an open-air living museum will help preserve it for future generations, but only if we treat this place with respect and understanding that this is neither a theme park based on a popular post-apocalyptic video game nor an Instagram Hotspot. Chernobyl is not trendy and is not a popular culture phenomenon. Instead, it should be considered as a textbook example of grave consequences on people and the environment caused by a flawed reactor design combined with a human error. Most of all, this is a place of a large-scale humanitarian catastrophe that affected millions of lives and still presents environmental and health risks.

Street art at the dilapidated Prypyat's largest grocery store. Credit: Margarita Kalinina Pohl (2019).

“Dark” tourism, defined as traveling to sites associated with death and destruction, has been growing steadily since the 1990s. Nuclear tourism as a subset of this trend has become popular as many former nuclear sites become accessible. Fukushima Daiichi Nuclear Plant is one such destination where people can book a tour for an “unforgettable experience.” Some Kazakh travel agencies are attempting, with less success than their Ukrainian counterparts, to organize tours to the former Soviet nuclear testing site called Semipalatinsk Testing Site.

Most countries and companies put their tours on hold due to the COVID-19 pandemic. Once travel restrictions are lifted, people hungry for new experiences will venture out to places, including Chernobyl, Fukushima, and the former Semipalatinsk Testing Site. While waiting for the world to open, nuclear tourist wannabes can spend time reading about places they want to visit. If you or someone you know is considering the adventure of a lifetime to the aforementioned sites, here is a reading list to check out: *Chernobyl Prayer: Voices from Chernobyl* by Nobel Prize in Literature recipient Svetlana Alexievich, *On the Brink: The Inside Story of Fukushima Daiichi* by Ryuosha Kadota, et al., and *Atomic Steppe: How Kazakhstan Gave Up the Bomb* by Togzhan Kassenova (forthcoming). These and other books on similar topics will serve as guides to the history of nuclear disasters and nuclear tests which occurred at these places and will best prepare prospective visitors to experience these places in meaningful and respectful ways.

***Margarita Kalinina-Pohl** is a Senior Program Manager at the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey.*

UAE to test its ability to respond to a nuclear emergency

Source: https://www.thenationalnews.com/uae/government/uae-to-test-its-ability-to-respond-to-a-nuclear-emergency-1.1213257#3

Barakah Nuclear Power Plant in the Gharbiya region of Abu Dhabi. Courtesy Emirates Nuclear Energy Corporation

Apr 29 – The UAE will test its ability to respond to a nuclear emergency later this year.

More than 170 countries have been invited to participate in the large-scale simulation at Barakah Nuclear Power Plant on an unannounced date in the final three months of the year.

The exercise, called Barakah UAE, is one of the world’s most complex to conduct and is being held in conjunction with the International Atomic Energy Agency.

It is carried out every three to five years and aims to test the plant’s response capabilities and early notification system in the event of an emergency.

Scenarios will involve plans to protect the public and the environment.

The National Emergency Crisis and Disaster Management Authority will supervise the exercise, which will also involve the participation of Emirates Nuclear Energy Corporation, the Ministry of Foreign Affairs and International Co-operation, the Ministry of Interior, plus the Ministry of Health and Prevention, among other authorities.

Commercial power generation began at the plant in Abu Dhabi's Al Dhafra region in April, making the UAE the first Arab country to operate a nuclear energy plant.

When Barakah's four reactors are operational the plant will supply 25 percent of the UAE's electricity.

Why is Brazil not yet participating in the Nuclear Weapons Ban Treaty?

Source: https://ksusentinel.com/2021/05/03/why-is-brazil-not-yet-participating-in-the-nuclear-weapons-ban-treaty-03-05-2021-world/

May 03 – The world is appalled by the massacre caused by the pandemic, which in less than a year and a half has killed more than 3 million people worldwide and more than 400,000 in Brazil. In August 1945, a single atomic bomb instantly killed around 80,000 people in Hiroshima. Three days later, the only other in existence claimed 40,000 lives in Nagasaki. In a few days, more than 200,000 people died.

Today there are about 13,400 of these pumps, each about 3,000 times more powerful than the first. Their targets are densely populated cities.

However, strangely, we don't think about these things. In addition to the pandemic, the priority is climate change, which, without combined international efforts, could lead to immense disasters in the not too distant future.

The use of nuclear weapons, in turn, would cause immediate humanitarian and environmental slaughter and extinguish life as we know it. Since they haven't been used for the past 76 years, we don't care.

It is an unconscious attitude. It suffices to note that the nine countries which have these weapons do not exclude the possibility of using them, at least as a threat; but for it to be credible, the threat supposes a willingness to use it. Will the 185 countries which do not have one accept to live permanently under this risk?

Solving the climate problem is a task of enormous complexity. In the case of nuclear weapons, the solution is simpler. Climate change is due to economic causes, while possession of nuclear weapons is just a distorted assertion of power, with a capital P.

Russia and the United States have 95% of the total atomic weapons. If the two came to an agreement to eliminate them, China and the six other holder countries would accompany them. They all protest that they want to end nuclear weapons, but so far they don't seem willing to give up on this menacing club.

All other countries, including Brazil, have already pledged not to acquire nuclear weapons by accepting the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), in force since 1970. One hundred and thirteen countries have doubled this pledge by creating nuclear-weapon-free zones, as is the case in Latin America and the Caribbean.

Other weapons of mass destruction – biological and chemical – are already banned. In the absence of movement on the part of the nuclear states which, on the contrary, embarked on programs to modernize their arsenals, 122 United Nations member states proposed in 2015 a treaty banning nuclear weapons.

Brazil actively participated in the negotiation of the Nuclear Weapons Ban Treaty (NPT), concluded in 2017, and was the first country to sign it. Already signed by 86 countries and ratified by 54, it entered into force in January of this year.

Interestingly, Brazil has yet to ratify the TPAN, which is under consideration in the National Congress. The Treaty confirms and reinforces the obligation not to have atomic weapons, already assumed by Brazil in the NPT and in the free zone of Latin America and the Caribbean.

In addition, article 21 of the Federal Constitution provides that "any nuclear activity on the national territory will be admitted only for peaceful purposes and with the approval of the National Congress".

If the Brazilian State – National Congress and Government – does not ratify the Ban Treaty, this can only mean that there are doubts about the need for the elimination of nuclear weapons and about the commitments already made at the level. international, which would imply a violation of the above. clause of the Constitution.

Speak up, the National Congress.

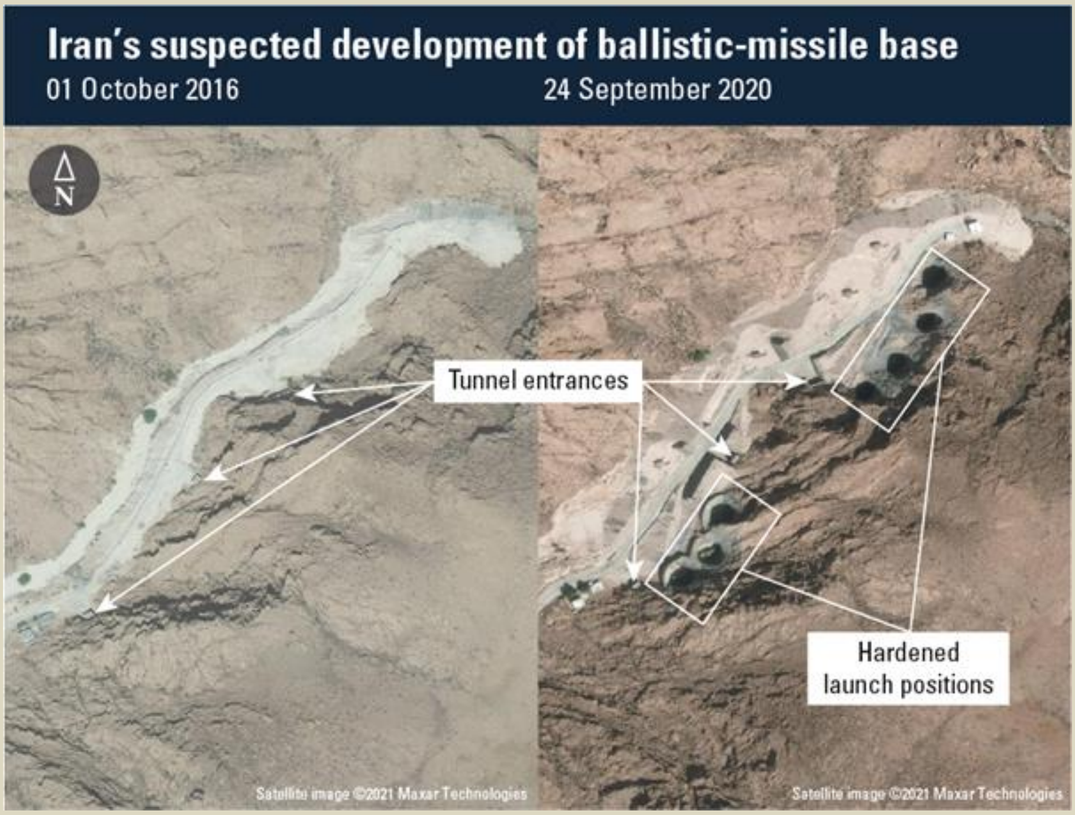
Silo mentality – Iran's Haji Abad missile base

By Joseph Dempsey

Source: https://www.iiss.org/blogs/military-balance/2021/04/iran-haji-abad-missile-base

May 04 – Open-source satellite imagery has revealed the suspected development of a new missile base near Haji Abad in Iran, possibly the first hardened launch site intended specifically for solid-fuel ballistic missiles. Given the regional significance of Iran's missile capability, these new structures will likely continue to attract attention from the intelligence community, explains Joseph Dempsey.

Iran may have developed a new design of hardened launch site, possibly the first intended specifically for solid-fuel ballistic missiles. Open-source satellite imagery of the suspected Islamic Revolutionary Guard Corps' missile base near Haji Abad reveals this development. Although Tehran has in recent years showcased several underground complexes (sometimes dubbed 'missile cities') – complete with cavernous launch silos – they have not included the Haji Abad structures. While Iran's ballistic-missile designs are road mobile, Tehran also deploys some in hardened static launch sites. Between 2017 and 2019, an underground facility near Haji Abad (28°19'44.02"N 55°56'34.20"E) was modified with the construction of large hollow circular structures, presumed to be accessible via underground tunnels. Comprising two groups – four structures below ground level and three semi-recessed into the landscape – each feature interior spaces some 20 metres in diameter, the latter group with outer walls at least 5 m thick.



Iran's suspected development of ballistic-missile base

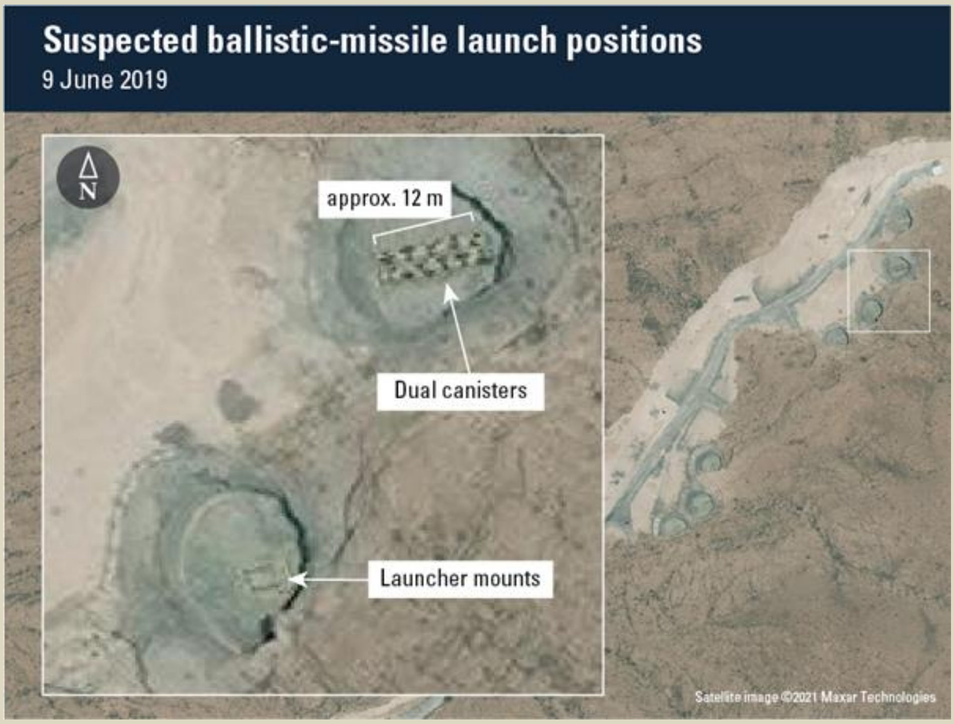
01 October 2016

24 September 2020

Satellite image ©2021 Maxar Technologies

Satellite image ©2021 Maxar Technologies

By December 2019, these seven structures each housed pairs of cylindrical objects measuring some 12 m in length with apparent – though somewhat limited – camouflage. Given their characteristics and protected placement, these may well be ballistic-missile launch canisters mounted horizontally.



Suspected ballistic-missile launch positions

9 June 2019

Satellite image ©2021 Maxar Technologies

Solid thinking

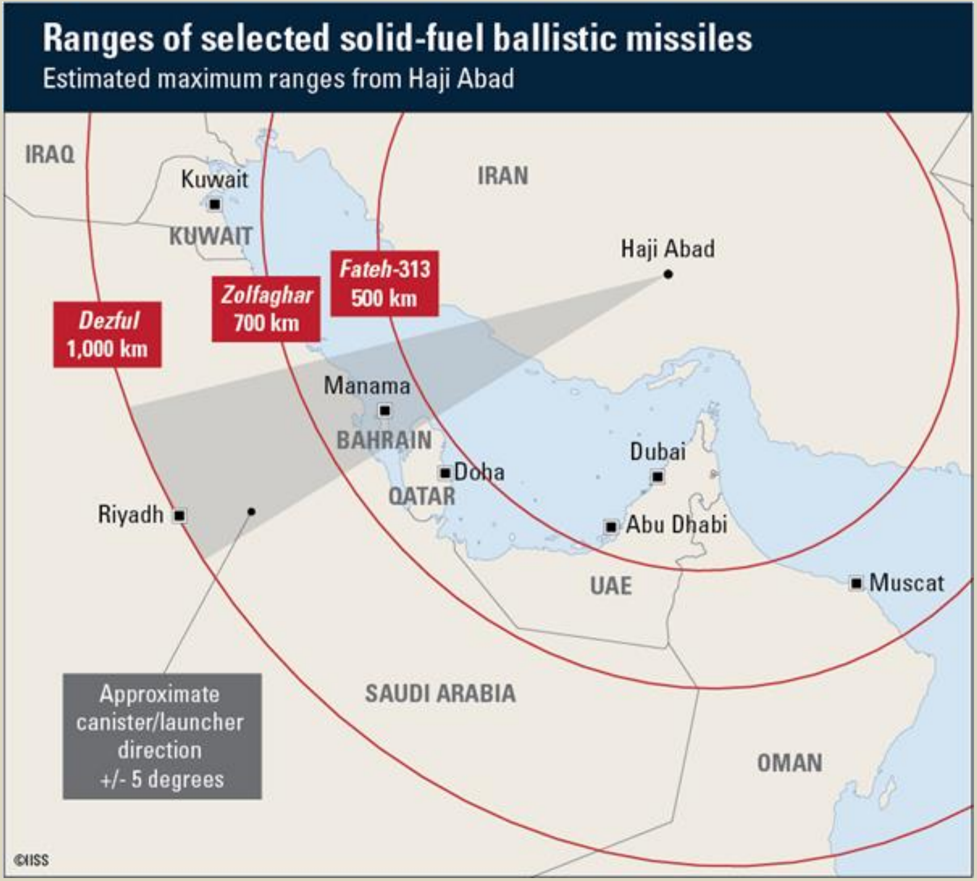
If indeed these are canisters housing ballistic missiles, then the missiles are probably solid-propellant-based. Liquid-fuelled missiles are fuelled prior to launch, and as such need to be readily accessible.

The corresponding reduction of launch-preparation time – from what can be hours for a liquid-fuelled missile to minutes for solid propellants – and other operational advantages are driving Iran's efforts to move away from a reliance on liquid-fuelled missiles.

The ongoing development of the *Fateh* family of short-range solid-propellant missiles continues to be central to these efforts. In the 20 years since the first flight test of the original *Fateh*-110, numerous variants have emerged with different guidance and range modifications. It is possible that the Haji Abad development may house a variant of the *Fateh* missile family.

A common characteristic of the *Fateh* series is that they are slant- rather than vertically launched. This offers one explanation for the large open-top design of the Haji Abad site. While predominantly rail-mounted and deployed from launch vehicles, the use of canisters provides better overall protection for the missile and could open up additional basing options. Indeed, a handful of examples of *Fateh*-series missiles being hot-launched (where solid motor ignition occurs within the canister) from canisters have recently emerged, showing the apparent practice of burying them in so-called 'missile farms'.

While Tehran has not made public the type of missiles that might be deployed from Haji Abad (there may be a degree of interchangeability between types), the location and specific characteristics of the site do offer some pointers.



Ranges of selected solid-fuel ballistic missiles

Estimated maximum ranges from Haji Abad

Most *Fateh* missiles – all those built around the original 610-millimetre-diameter body, at least – have ranges estimated at 250–300 kilometres. The *Raad*-500 and *Fateh*-313 variants use lighter composite casings, resulting in a 500-km range. These range limitations would mean that any of these missiles would only cover parts of the UAE and Oman from Haji Abad, assuming that it is not the *Hormuz* 1 or 2 anti-ship development of the *Fateh*. Deployments in this direction, if slant-launched, would also likely be impeded by the immediate topography. In available imagery, the suspected canisters and their launch mounts face southwest, estimated to be in the range of 238–243 degrees. It remains unclear if they can be rotated or if they are trained to a specific selection of targets, but this suggests extended-range members of the *Fateh* family would be candidate missiles if making landfall is required.

One candidate is the *Zolfaghar*, introduced in 2016, which has a larger-diameter 680-mm body with its length increased to 10.3 m. This gives the weapon a 700-km range with a 350-kg warhead. The missile is comparatively accurate, using inertial and satellite-based navigation. This was demonstrated in the January 2020 attack on the Ayn al Asad air base in Iraq, used by United States forces, as well as in strikes on Syria in 2017. The *Dezful* is a follow-on design introduced in 2019 that appears to be the same diameter and length but is claimed by Tehran to have a range of 1,000 km. In July 2020, Iran released footage showing missiles launched from a previously unseen large tube or canister design. Although the missile itself was unnamed, it appears consistent in both size and configuration with the *Zolfaghar* and *Dezful*. An example of this tube – with a crude missile mock-up – is also on display in Tehran.

A further, if perhaps less likely, candidate is the *Shahid Haj Qasem*, first shown in August 2020. The missile, named after the late Iranian Quds Force commander Qasem Soleimani, has a considerably increased diameter, in the region of 900 mm, and an estimated length of 11 m. A claimed range of 1,400 km would make this the first *Fateh* derivative to be classed as a medium-range ballistic missile. The service status of this missile, however, is unknown.

Iran continues to use more traditional silo-type missiles at other sites in addition to mobile basing, with the former in the past offering greater protection and concealment of launch preparations than more mobile options. This protection has been eroded considerably with the development of stand-off precision-guided weapons and penetrating warheads.

While the structures of the Haji Abad site provide additional side protection, complementing what is already challenging terrain for an attack, the launch positions remain vulnerable to top-down aerial strikes, and it is unclear why Tehran has not implemented any form of removable cover as a shield against intelligence-gathering satellites. Despite the apparent limitations, it may be a relatively inexpensive method of adding protection while preserving the quick reaction and increased accuracy offered by a fixed position.

In a sign that this idea may be gathering wider appeal, similar ongoing development of circular structures has been noted at a suspected missile base at Khorgu (27°31'39.22"N

56°26'59.39"E) – though some dissimilar interior elements may indicate a different purpose – and, possibly at an earlier stage, in excavations at Shiraz (29°27'28.37"N 52°29'18.53"E).

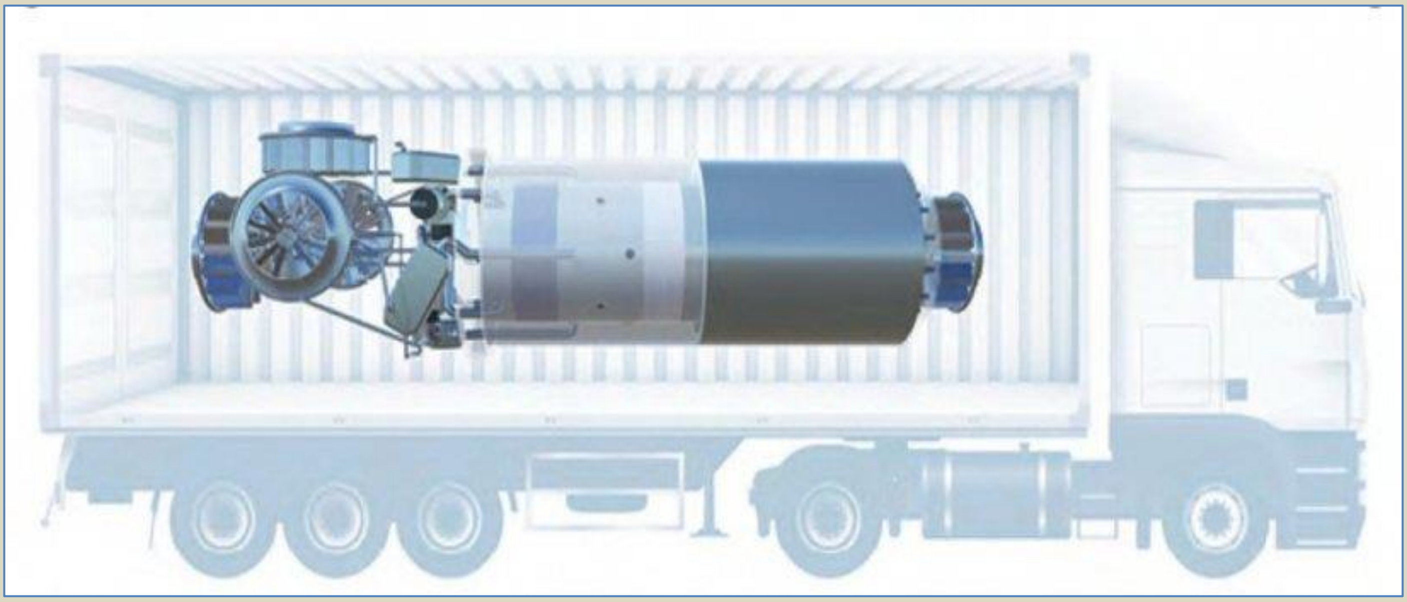
The regional significance of Iran's missile capability means these new structures will likely continue to attract attention from the intelligence community. Of particular interest will be any further developments and patterns of activity at these sites that might reveal the rationale behind the new structures.

Joseph Dempsey *is Research Associate for Defence and Military Analysis. Joseph is the development lead for the Military Balance+ online database, and contributes to* The Military Balance *and conducts other research.*

Nuclear Micro-Reactors

Source: http://www.homelandsecuritynewswire.com/dr20210504-nuclear-microreactors

May 04 – The idea of a nuclear power plant today evokes images of large cooling towers and expansive, warehouse-size buildings. Such facilities generate about a fifth of electricity in the United States without emitting greenhouse gases. A different picture of nuclear energy is emerging, however, in the form of micro-reactors that could fit on the back of a truck or inside a rocket to space. The promise of these micro-reactors is to provide the same reliable, zero-carbon power in remote settings or to support electrical power grid recovery.



Experts at the U.S. Department of Energy's (DOE) Argonne National Laboratory are developing strategies to bring micro-reactor concepts closer to commercial reality, working together with private industry and federal regulators. A micro-reactor might have a capacity of anywhere from a few kilowatts to 20 megawatts — far less than even the smallest operating U.S. nuclear power plant, which has a capacity of 581 megawatts. The low electricity output allows micro-reactors to have a smaller physical size and reduced costs, which would be enabled through factory manufacturing and design simplification.

Aside from being compact, micro-reactors must be designed to operate safely for many years — perhaps several decades. They can also be self-controllable, operating without the need for a constant human presence. While it's possible to build such a reactor with today's technology, it might not have the portability or the efficiency needed to operate on a military base, for example, or in an Arctic community where renewable alternatives such as wind or solar energy are not feasible.

"At Argonne, we've identified a few advanced technologies that could push micro-reactors much further," said Nicolas Stauff, principal nuclear engineer. Stauff is collaborating with companies such as HolosGen under DOE's Advanced Research Projects Agency-Energy's (ARPA-E) Modeling-Enhanced Innovations Trailblazing Nuclear Energy Reinvigoration (MEITNER) program for micro-reactor design and modeling efforts. He is also working with DOE's Nuclear Energy Advanced Modeling and Simulation (NEAMS) program, an effort spanning seven national labs, to develop new computer-based tools and capabilities for the design, analysis and potential licensing of nuclear reactors including micro-reactors.

As work proceeds on the design and deployment side, other experts at Argonne are lending technical assistance to regulators in determining the requirements for safety, safeguards and security for micro-reactors. "With new reactor designs coming online in the next decades, we are creating a framework to ensure confidence in how these reactors are being built, sited and constructed," said Andrew Breshears, principal nuclear chemist at Argonne.

Here are a few of the ways Stauff, Breshears and colleagues are moving micro-reactors forward.

Pumping the Breaks for Low-Enriched Fuel

Subatomic particles called neutrons enable the fission reaction that creates energy in a reactor. But in order for that to happen reliably, the neutrons need to be slowed down — a process called moderation. Typically, graphite is used for moderation, but graphite "adds a lot of weight and takes up a lot of room," Stauff said. To find an alternative to graphite, Stauff and Yinbin Miao, principal materials scientist, formed a team to develop an advanced moderation module with metal hydrides, compounds in which metal is bonded to hydrogen. Though metal hydrides alone would decompose at the high temperatures within a nuclear reactor, the module employs an innovative, multilayered enclosure that protects the moderator without compromising its performance. More moderation enables the use of low-enriched uranium fuel, which is desirable from a safeguards and security standpoint because it is difficult to weaponize.

Passive Cooling with Heat Pipes

Nuclear reactors require cooling, which is typically achieved by pumping a fluid that can transfer the reactor's heat to the power conversion cycle. A solution developed at Argonne, the Versatile Heat Transfer Module, removes heat from the reactor via a heat pipe — no pumping power needed. "It's just natural evaporation, circulation and recondensation of the fluid inside the heat pipe that cools down the reactor," Stauff said. "It's a fully passive heat transfer mechanism." Argonne's technology, developed by Stauff and Miao's team, is using a lined and coated envelope of silicon carbide — a crystalline compound of silicon and carbon — and a metal hydride wick filled with a small amount of liquid metal. The design enables exceptionally compact reactor designs while enhancing inherent safety and facilitating autonomous control.

Materials for Gas-Cooled Reactors

Argonne's work with HolosGen is focused on a high-temperature gas-cooled mini-reactor designed to fit into a standard 40-foot shipping container, funded in part by DOE's MEITNER and Gateway for Accelerated Innovation in Nuclear programs. The gas used for this concept, helium, does an excellent job of conveying heat away from the reactor, but it's notoriously prone to leaks. To address this problem, Argonne researchers have developed a silicon carbide-based coolant sleeve using advanced coating to allow the helium to circulate at a high velocity while remaining fully sealed inside.

Computer Code Analysis

The nuclear industry relies on a suite of computer codes to evaluate and model various aspects of a reactor: how the fuel behaves, how high the temperature gets, and a host of other variables that determine safety and efficiency. However, these traditional tools are usually not directly compatible with the unconventional technologies being developed for micro-reactors. As part of the NEAMS program, which is developing modern codes for advanced nuclear energy technologies, Argonne has assembled a team of reactor physics experts to gain experience with micro-reactor modeling problems, identify modeling gaps and demonstrate capabilities to support industry users. Using the Bebop high-performance computing cluster at Argonne's Laboratory Computing Resource Center, researchers are working to solve complex multi-physics modeling problems that are unique to micro-reactor designs. Stauff and colleagues are also training users in the private sector at companies such as Oklo and Westinghouse to use the codes to accelerate development of their advanced reactor concepts.

Safety-Informed Safeguards and Security Framework

Whether a micro-reactor is deployed for charging electric trucks on the highway or in a remote community, the Nuclear Regulatory Commission (NRC) needs to make sure it will operate safely and remain secure. Breshears is leading a multidisciplinary study on a safety-informed domestic safeguards framework for the agency that will be completed this year. The framework will address the many considerations involved when assessing the construction and operation of a mini-reactor. These include questions about how the reactor needs to be managed, what kind of physical protection it might need and how sensitive nuclear materials are handled and accounted for. As with any energy facility, mini-reactors must be hardened to face risks that range from weather events to intruders. "Inherently safe from an earthquake doesn't necessarily mean inherently safe from a disgruntled actor," Breshears said. "We're accounting for a variety of scenarios in this framework, both for the NRC and for vendors to understand what they're expected to bring to the table when it comes to domestic safeguards."

Western India
PUNJAB
UTTARANCHAL
HARYANA
Delhi
Pakistan
Jaipur
RAJASTHAN
Udaipur
GUJARAT
MADHYA PRADESH
Ellora and Ajanta
MAHARASHTRA
Mumbai
Arabian Sea
ANDRA PRADESH
N
GOA
0.5 Kilometers
0.5 Miles

2 men arrested, over 7kg of uranium seized in India

Source: https://www.dawn.com/news/1622541

May 07 – The case was registered on Wednesday after a report from the Bhabha Atomic Research Centre in Mumbai confirmed the seized material is highly radioactive. — Photo courtesy Hindustan Times

Indian police seized over seven kilogrammes (15.4 pounds) of **natural uranium** and arrested two men in the western Maharashtra state for "illegally possessing" the highly radioactive substance, an authority said on Thursday.

According to the anti-terrorism squad in Maharashtra, the confiscated material is **worth around $2.9 million** and an investigation into the case is under way.

"We had received information that one person identified as Jigar Pandya was going to illegally sell pieces of uranium substance, a trap was laid and he was arrested," the Maharashtra police said.

"Investigation into the case revealed that another person identified as Abu Tahir gave him these pieces of uranium."

The police said a huge quantity of substance was recovered when Tahir was apprehended.

The case was registered on Wednesday after a report from the Bhabha Atomic Research Centre in Mumbai confirmed the seized material is highly radioactive.

"A report was received that the substance is natural uranium. It's highly radioactive and dangerous to human life," the police said.

A police official told *Anadolu Agency* on the condition of anonymity that the accused are being questioned to know the source of the seized material and where it would be sent.

According to local news agency *Press Trust of India*, the two accused appeared before a local court on Wednesday which remanded them in the custody of the anti-terrorism squad till May 12.

It is the second time in India that such a highly radioactive substance has been seized by police in recent years. In 2016, police seized almost 9kg (19.8 pounds) of depleted uranium in the Thane area of Maharashtra.

Uranium is used in several areas, including nuclear explosives and medical techniques.

Emerging Nuclear Energy Countries

(Updated March 2021)

Source: https://www.world-nuclear.org/information-library/country-profiles/others/emerging-nuclear-energy-countries.aspx

About 30 countries are considering, planning or starting nuclear power programmes, and a further 20 or so countries have at some point expressed an interest. In the following list, links are provided for those countries that are covered by specific country pages:

- In Europe: Albania, Serbia, Croatia, Portugal, Norway, Poland, Estonia, Latvia, Lithuania, Ireland, Turkey.
- In the Middle East and North Africa: Gulf states including Saudi Arabia, Qatar and Kuwait; Yemen, Israel, Syria, Jordan, Egypt, Tunisia, Libya, Algeria, Morocco, Sudan.
- In west, central and southern Africa: Nigeria, Ghana, Senegal, Kenya, Uganda, Tanzania, Zambia, Namibia, Rwanda, Ethiopia.
- In Central and South America: Cuba, Chile, Ecuador, Venezuela, Bolivia, Peru, Paraguay.
- In central and southern Asia: Azerbaijan, Georgia, Kazakhstan, Mongolia, Bangladesh, Sri Lanka, Uzbekistan.
- In SE Asia and Oceania: Indonesia, Philippines, Vietnam, Thailand, Laos, Cambodia, Malaysia, Singapore, Myanmar, Australia.
- In east Asia: North Korea.

Despite the large number of these emerging countries, they are not expected to contribute very much to the expansion of nuclear capacity in the foreseeable future – the main growth will come in countries where the technology is already well established. However, in the longer term, the trend to urbanisation in less-developed countries will greatly increase the demand for electricity, and especially that supplied by base-load plants such as nuclear. The pattern of energy demand in these countries will become more like that of Europe, North America and Japan.

Some of the above countries can be classified according to how far their nuclear power programmes or plans have progressed:

- Power reactors under construction: Bangladesh, Turkey.

- Contracts signed, legal and regulatory infrastructure well-developed or developing: Egypt, Poland.
- Committed plans, legal and regulatory infrastructure developing: Jordan, Uzbekistan.
- Well-developed plans but commitment pending/deferred: Thailand, Indonesia, Kazakhstan, Saudi Arabia; Vietnam (deferred), Lithuania (deferred).
- Developing plans: Nigeria, Kenya, Laos, Morocco, Algeria, Philippines, Ghana, Rwanda, Ethiopia.
- Discussion as policy option: Israel, Namibia, Mongolia, Singapore, Albania, Serbia, Croatia, Estonia & Latvia, Libya, Azerbaijan, Sri Lanka, Tunisia, Syria, Qatar, Sudan, Cuba, Venezuela, Bolivia, Paraguay, Peru, Chile.
- Officially not a policy option at present: Albania, Australia, New Zealand, Portugal, Norway, Ireland, Kuwait, Myanmar, Malaysia, Cambodia, Rwanda, Tanzania, Zambia, Syria, Qatar.

A July 2017 report by the International Atomic Energy Agency (IAEA) on *International Status and Prospects of Nuclear Power*[1] said that some 28 member states without nuclear power plants “are considering, planning or starting” nuclear power programmes at present. Of these 28 un-named countries, it said that two have started construction of their first nuclear power plant, two have ordered their first nuclear power plant, five have made the decision to invest and are preparing infrastructure, seven are actively preparing prior to final decision, and 12 are considering a nuclear power programme. The IAEA said that a further 20 countries have expressed an interest in nuclear power.

One major issue for many countries is the size of their grid system. Many nuclear power plants are larger than the fossil fuel plants they supplement or replace, and it does not make sense to have any generating unit more than about one-tenth of the capacity of the grid (maybe 15% if there is high reserve capacity). This is so that the plant can be taken offline for refuelling or maintenance, or due to unforeseen events. The grid capacity and quality may also be considered regionally, as with Jordan for instance. In many situations, as much investment in the grid may be needed as in the power plant(s). Kenya sought to evaluate its grid system before considering the generation options.

Another issue is that of licensing reactor designs. Emerging countries generally do not have the expertise for this, and must initially rely on design licensing by countries such as the UK, USA, France, Russia and China while they focus on building competence to license the actual operation of plants.

State-owned nuclear companies in Russia and China have taken the lead in offering nuclear power plants to emerging countries, usually with finance and fuel services. The following table charts the main influence in countries with various agreements but not yet any plants under construction (see also the relevant tables in the information papers on China and Russia):

RUSSIA			CHINA	OTHER
Jordan	Nigeria	Venezuela	Sudan	Poland
Egypt	Ghana	Bolivia	Kenya	Lithuania
Tunisia	Ethiopia	Paraguay	Thailand	Philippines
Algeria	Sudan	Myanmar	Uganda	Kenya
Morocco	Zambia	Indonesia	Cambodia	
	Kazakhstan			

IAEA support for new nuclear programmes

In all countries governments need to create the environment for investment in nuclear power, including professional and independent regulatory regime, policies on nuclear waste management and decommissioning, and involvement with international non-proliferation measures and insurance arrangements for third-party damage.*

* See Safeguards to Prevent Nuclear Weapons Proliferation, and Liability for Nuclear Damage respectively.

In different countries, institutional arrangements vary. Usually governments are heavily involved in planning, and in developing countries also financing and operation. As emerging nuclear nations lack a strong cadre of nuclear engineers and scientists, construction is often on a turnkey basis, with the reactor vendor assuming all technical and commercial risks in delivering a functioning plant on time and at a particular price. Alternatively the vendor may be set up a consortium to build, own and operate the plant. As the industry becomes more international, new arrangements are likely, including public-private partnerships.

The IAEA sets out a phased 'milestone' approach to establishing nuclear power capacity in new countries, applying it to 19 issues. In broad outline the three phase approach is (milestones underlined):

- **Pre-project phase 1** (1-3 years) leading to knowledgeable commitment to a nuclear power programme, resulting in set up of a nuclear energy programme implementing organization (NEPIO). This deals with the programme, not the particular projects after phase 2.

- **Project decision-making phase 2** (3-7 years) involving preparatory work after the decision is made and up to inviting bids, with the regulatory body being established. In phase 2 the government role progressively gives way to that of the regulatory body and the owner-operator.
- **Construction phase 3** (7-10 years) with regulatory body operational, up to commissioning and operation.

In 2009 the IAEA began offering **Integrated Nuclear Infrastructure Review (INIR)** missions to evaluate the status of countries' nuclear infrastructure development, building on member states' self-evaluation. The first three were to Jordan, Indonesia and Vietnam. Since then, INIR reviews have been conducted in Bangladesh, Belarus, Egypt, Ghana, Kazakhstan, Malaysia, Morocco, Niger, Nigeria, Philippines, Poland, Saudi Arabia, Thailand, Turkey and United Arab Emirates. In 2013 an INIR mission was to South Africa – the first country with an operating nuclear power programme that has requested this service.

More broadly than these INIR missions are **Nuclear Energy System Assessments (NESA)**, using the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) methodology to help countries develop long-term national nuclear energy strategies. The INPRO methodology identifies a set of Basic Principles, User Requirements, and Criteria in a hierarchical manner as the basis for the assessment of an innovative and sustainable nuclear system. The NESA programme helps members "in gaining public acceptance, getting assistance in nuclear energy planning in their country, and increasing awareness of innovations in nuclear technologies". NESAs have been carried out in Belarus, Kazakhstan, Ukraine and Indonesia.

IAEA **Site and External Events Design (SEED)** missions review the design and siting of nuclear plants against external hazards specific to the site. The programme arose from the Fukushima accident and involves the IAEA's International Seismic Safety Centre (ISSC), which has conducted over 430 site external hazard evaluations since 1980.

The IAEA also has an **Integrated Regulatory Review Service (IRRS)** to scrutinise the regulatory structures in particular countries, upon invitation from the government. Though mostly used for countries with established nuclear power, it is also used for countries embarking upon nuclear power programmes, as in Iran in 2010, Poland early in 2013, Jordan and Vietnam in 2014, UAE and Indonesia in 2015, Bangladesh and Belarus in 2016.

In March 2020 the IAEA published new guidance to countries planning to adopt nuclear power in a document titled Initiating Nuclear Power Programmes: Responsibilities and Capabilities of Owners and Operators. It takes into account more than ten years of experience and good practices in countries that are introducing nuclear power, as well as lessons learned during INIR missions, and IAEA technical assistance activities to newcomer countries. Together with the nuclear energy programme implementing organization (NEPIO) and the nuclear regulatory body, the nuclear plant owner-operator is one of the three key organizations identified in the 'milestone' approach. The publication is a significant revision of a document first issued in 2009.

WANO and ASN support for new nuclear programmes

For new entrants to the nuclear industry which are moving towards fuel loading in their first reactor, the World Association of Nuclear Operators (WANO) offers pre-startup peer reviews as part of its peer review programme, particularly to address the situation of new plants in countries and organisations without previous nuclear power experience. WANO's goal is to do a pre-startup review on every new nuclear power plant worldwide. The reviews seek to evaluate how each operating organization is prepared for startup and make recommendations for improvements based on the collective experience of the world industry.

In January 2008, the French Nuclear Safety Authority (ASN) indicated that it would pay attention to new nuclear power projects in countries with no experience in this area. ASN said it takes at least five years to set up the legal and regulatory infrastructure for a nuclear power programme, two to ten years to license a new plant, and about five years to build a power plant. That means a "minimum lead time of 15 years" before a new nuclear power plant can be started up in a country that does not already have the required infrastructure.

These comments relate to France's creation of Agency France Nuclear International (AFNI) under its Atomic Energy Commission (CEA) to provide a vehicle for international assistance. AFNI is focused on helping to set up structures and systems to enable the establishment of civil nuclear programmes in countries wanting to develop them.

DNA resistance to radiation field: forensic genotyping in a radiological incident scenario

By Javier Quinones Diez, Marta Fernández, Emiliano Mingorance, et al

The European Physical Journal Plus **volume 136**, Article number: 413 (2021)
Source: https://link.springer.com/article/10.1140/epjp/s13360-021-01407-x

Abstract

The objective of nuclear forensic science is to link an event that involves a radioactive or nuclear material with the personal and material means that have facilitated it. This implies

the collection and analysis of any physical evidence of the scene, both radioactive and nuclear material for its characterization as well as classical evidence like DNA, hair, fingerprints or blood. Collecting evidence in these circumstances can be potentially dangerous for the respondent due to the risk of radiation or radioactive contamination, so studying the stability of forensic evidence in the presence of radiation will allow taking a reasonable decision whether the probative utility that the evidence may have exceeds the dangers involved in its collection. In this context, this work addresses the resistance of classical forensic evidences to radiation. Thus, gamma post-irradiation results of DNA profiling from relevant biological samples are presented and discussed providing threshold values of radiation that, depending on the matrix, degrade DNA evidence.

Chernobyl's Molten Guts Are Warming Up, And Scientists Don't Know Why

Source: https://www.sciencealert.com/chernobyl-s-molten-guts-are-warming-and-it-could-go-critical-all-over-again

May 12 – Over the past five years, a sensor keeping count of neutron emissions deep within the rubble of the Chernobyl nuclear power plant has kept track of a gradual spike in activity.

The rising count might be nothing. It might even drop back down again, given time. Scientists aren't exactly keen on taking any chances, as the potential for a runaway nuclear fission reaction in the future can't be ruled out until we know what's going on.

Unfortunately, the precise location of the decaying material beneath debris and heavy slabs of concrete makes detailed investigations and potential fixes all that more challenging.

As reported by *Science Magazine's* Richard Stone, researchers at the Institute for Safety Problems of Nuclear Power Plants (ISPNPP) in Kyiv, Ukraine, are yet to determine whether the noted rise in neutrons heralds pending disaster, or is more of a storm in a nuclear tea-cup.

"There are many uncertainties," ISPNPP's Maxim Saveliev told Stone. "But we can't rule out the possibility of [an] accident."

In what ranks as perhaps history's most notorious nuclear accident, the Unit Four reactor at the Chernobyl complex underwent a devastating meltdown in late April, 1986, following an unexpected drop in power during a key safety test.

The resulting explosions of compressed steam cast a pall of radioactive material far across Europe, contributing to the premature deaths of what could amount to tens of thousands of people.

Within the rooms and corridors of the demolished facility itself, super-heated uranium fuel collected in pools mixed with molten zirconium cladding, graphite control rods, and liquefied sand to produce a hellish lava that eventually solidified into monoliths of fuel-containing materials, or FCMs.

Over the decades, uranium isotopes have continued to shoot off the occasional neutron from their nuclei. Those that happen to get close enough to another isotope's nucleus risk upsetting their own delicate balance, driving free more neutrons.

Given a high enough concentration of atoms, the chain reaction of lost neutrons can generate enormous amounts of energy in a short amount of time, with potentially explosive consequences.

Neutrons ejected from the decaying heat of a uranium atom typically move a little too fast to be easily captured. This all changes when neutrons are forced to pass through certain media, such as water. Slowed down, they have a much higher chance of sticking to a nucleus and triggering its own decay.

With this in mind, it comes as little surprise that fission rates spike inside FCMs whenever they get wet.

For years, huddled beneath a hastily erected sarcophagus referred to as the Shelter, Unit Four's ruins sat semi-exposed to the elements, allowing heavy downpours to seep inside the tangled mess of collapsed concrete and old machinery.

Amid fears that rainwater could send fission inside the FCMs into overdrive, engineers have managed to coat most of them in a neutron-absorbing solution of gadolinium nitrate.

A more robust covering was completed over the site in November 2016. The vast structure, called the New Safe Confinement (NSC), does a vastly better job of keeping everything dry.

Yet the space beneath the old Unit Four reactor – what was once room 305/2 – is still buzzing, with neutron emissions rising slowly but significantly since the NSC was erected.

Assuming it isn't wet, it isn't clear what's behind the slow rise in neutron numbers. By the reckoning of ISPNPP, it's possible this particular mix of materials has had an even easier time generating chain reactions of neutrons as it dehydrates.

Exactly why, and what to do about it, remain pressing questions, especially as the area continues to slowly dry out over time. Given where it sits, soaking it in gadolinium nitrate could be tricky. As is getting a dedicated sensor up closer to the source of the neutrons, beyond obstacles that might be interfering with measurements.

With emissions rising so slowly, risk of threats in the near future seem low. Worst-case scenarios would also fall far short of the 1986 catastrophe.

Still, given the delicate, crumbling state of the FCMs – and that room 305/2 is thought to contain around half of the reactor's original fuel – even a small explosion could blast radioactive debris far enough to make its containment a concern.

There are plans for a clean-up of the fuel underway, with an interim storage facility currently awaiting a license from the Ukrainian regulator.

For now, little can be done but watch and keep on counting, hoping that in time, Chernobyl's ticking will fall quiet once again.

The Nuclear Threat in the New Information Age

By Daryl G. Kimball

Source: https://www.indepthnews.net/index.php/opinion/4441-the-nuclear-threat-in-the-new-information-age

May 12 — An informed and mobilized public is essential to human survival in the nuclear age—and effective and independent journalism is essential to revealing the hard truths, the consequences, and the choices that nuclear weapons pose for all of us.

Since the first U.S. atomic bombings of the cities of Hiroshima and Nagasaki, journalists have played an essential role in delivering facts—and dismantling the fictions—about the world's most dangerous weapons.

As the late physicist, U.S. government nuclear weapons advisor, and nuclear disarmament advocate Dr. Sidney Drell wrote in 1983, matters of nuclear weapons and nuclear policy are "too important to be left to the experts .... All of us are the targets of these undiscriminating weapons of mass destruction. There is, therefore, no excuse for us not to constitute an informed and an effective public constituency insisting on the imperative of arms control".

Equipped with information about the catastrophic risks of nuclear weapons and common-sense strategies to reduce and eliminate them, ordinary people, along with concerned scientists, physicians, and diplomats have organized and successfully pressed their political leaders to slow and reverse the nuclear arms race.

The result of public mobilization against the Bomb has been a vast body of bilateral and multilateral agreements to end nuclear testing, curb the spread of nuclear weapons and nuclear know-how, and to cap and verifiably eliminate nuclear arsenals. And, beginning this year, the new Treaty on the Prohibition of Nuclear Weapons entered into force, establishing yet another tool in the legal framework for disarmament that further reinforces the taboo against nuclear weapons.

None of this might have been possible without the work of journalists and editors who have, over many decades, brought to light the dangers of the bomb, who have documented the intense public debate surrounding nuclear weapons and how and whether to eliminate them.

For example, it took the pioneering, on-the-ground reporting by John Hersey published in *The New Yorker* in August 1946 to finally reveal the horrific consequences of nuclear weapons—the blast, heat, radiation effects—that the U.S. occupation authorities tried to hide from the world.

Unfortunately, during the early Cold War years, many mainstream news outlets in the United States and Europe downplayed the risks, many could not breakthrough the veil of secrecy that surrounded nuclear matters, and many simply failed to question the official government line.

In the Soviet Union, of course, where the news media was essentially another arm of the government, it was even more difficult for ordinary citizens to learn about the devastating human and environmental effects of nuclear weapons production and testing, and to challenge dangerous nuclear policies.

With the help of concerned nuclear scientists and public health experts, however, some specialty journals and newspapers helped fill the gaps in the public record. In 1962 for example, The *New England Journal of Medicine* published a groundbreaking series of articles by a group of physicians documenting the effects of a Soviet nuclear attack on an American city and the devastation of the medical and emergency response infrastructure. Appearing just months ahead of the Cuban Missile Crisis, the articles exploded the myth that one or another side could "prevail" in a nuclear war.

In other cases, modest but important newspaper reporting helped catalyze events that inspired action in support of disarmament on a massive scale. In February 1979, *The St. Petersburg [Fla.] Times* newspaper enlisted the help of Arms Control Association Executive Director William Kincade and freelance journalist Nan Randall to help write a four-day series of articles describing the effects of a Soviet nuclear warhead exploding over the city.

Randall's account drew the attention of the Office of Technology Assessment (OTA), a federal scientific advisory agency, which enlisted her to write a similar account for the 1979 OTA report on "The Effects of Nuclear Weapons." That report would, in turn, become an inspiration for the director and writer who was tapped to create an ABC-TV docudrama on the human consequences of nuclear conflict titled *The Day After.*

When it was broadcast the evening of November 20, 1983, *The Day After* drew some 100 million viewers, then a record audience for a made-for-television movie. The movie boosted public U.S. support for the nuclear freeze movement, demanded the attention of government policy makers, (including President Ronald Reagan), and prompted action to reduce the danger.

Then as now, the mass media is still the main source of public information about the dangers of the Bomb and efforts to eliminate the nuclear threat. In today's hyper-information age in which the fact is hard to discern from fiction, government disinformation is taking on new forms, independent news networks with a special focus on covering developments and ideas related to the world's most dangerous weapons are more vital than ever.

Since 1983, *IDN-InDepthNews* and its network of contributors and correspondents has provided invaluable coverage for people worldwide who are concerned about the nuclear weapons threat. Today, the long-running struggle to eliminate the nuclear weapons threat has taken on a new urgency as global nuclear competition and the risk of nuclear war is growing.

In this dangerous new phase of the nuclear age, the focused coverage that *IDN-InDepthNews* provides on effective solutions and ideas and actions to strengthen the guardrails against nuclear catastrophe and advance progress toward a world free of nuclear weapons is more vital than ever.

***Daryl G. Kimball** is the executive director of Arms Control Association and publisher of Arms Control Today since 2001*.

Palomares, a Spanish Chernobyl

Source: https://thesaxon.org/palomares-a-spanish-chernobyl/42240/

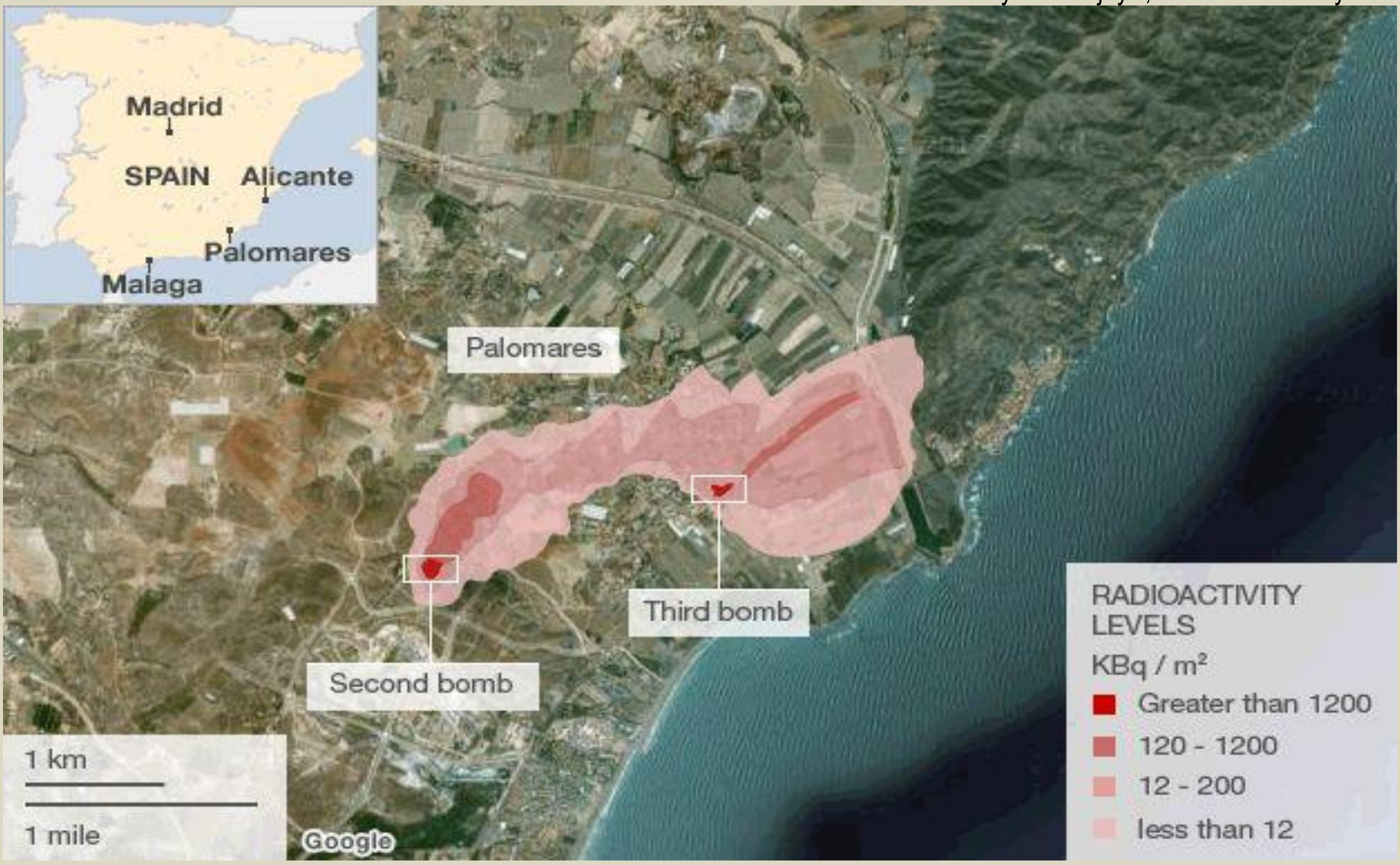
May 15 – 35 years after the Chernobyl nuclear accident, the documentary series **Palomares: Beach and Plutonium Day** plunges us into the history of what could have been the worst radioactive catastrophe in Europe. Something that happened much closer than anyone might think, on Spanish soil. Faced with the rise of true crime reports, the platforms have launched into investigative reports that serve to reconstruct and shed new light with the perspective of the years on some of the events that have had the greatest impact on Spanish society. The Palomares accident was one of those episodes that needed a review, especially considering that the censorship of the time caused highly biased information to reach the population about what was happening. In addition to interviews with some of the direct protagonists, this four-episode miniseries features material that was considered secret and recreations of the events.

If not for the serious environmental consequences and the risk to human health, the Palomares incident kept all the elements to become a comedy of **Luis Garcia Berlanga**. If in the movie **Calabuch** (1956) by the Valencian filmmaker was an atomic scientist who was hiding in an idyllic town on the Mediterranean coast of the world and from the destruction that he had created, in Palomares it was the weapons of mass destruction themselves that were lost in the small population of **Almeria**. Up to four nuclear missiles were lost after the tragic accident between two US military aircraft on **January 17, 1966** while carrying out refueling maneuvers mid-flight. Three could be located in the first days, but it took almost three months until they were able to find the fourth.

The phrase: "My commander has missed a bomb" can give rise to an intense fictional political thriller of **Michael Bay** or a very Spanish comedy, one of those in which we show our ability to laugh at those botched things that are so much ours. US military and Spanish civil guards working together to locate the bombs, while the rulers on duty try to hide the seriousness of the situation from the world. Not long ago psychosis had set in in the United States and fear of a nuclear missile attack from the USSR was the order of the day. Four years had passed since the Cuban missile crisis and there were citizens who had built nuclear shelters on their farms prepared for the worst. The series explains that there were planes permanently in the air to respond to the USSR in the event of a nuclear attack, a scenario in which Spain was a strategic location. It was the time when North America signed up for Made in Spain. The country was not only the setting for filming great film productions, but also the ground on which to set up their bases. Military who arrive in that Spain in which **Ava Gardner** he ran the spree that **Paco Leon** he told us in Arde Madrid. The Franco dictatorship had managed to end the international isolation that Spain had after the end of the Second World War and did and let the North American Army do as it pleased to keep a powerful ally happy.

Manuel Fraga's iconic bath with the American ambassador on the beaches of Almería.

The citizens of that small town on the coast of Almería knew little about the risks of radioactivity and saw the coming and going of the military more as an event, in which they could perfectly have taken to the streets with little flags while they sang that of "Americanos We welcome you with joy ", which we already saw in another Berlaguiano classic, **Welcome Mr Marshall**. The Americans might well see us as those gentlemen who smell like garlic, but there it was **Paco the Bomb**, who from the first day pointed with his finger where the lost bomb was, which they did not want to pay attention to. After all, they had the most advanced instruments that told them that the projectile was somewhere else. You don't have to explain where the bomb was at the end, right?

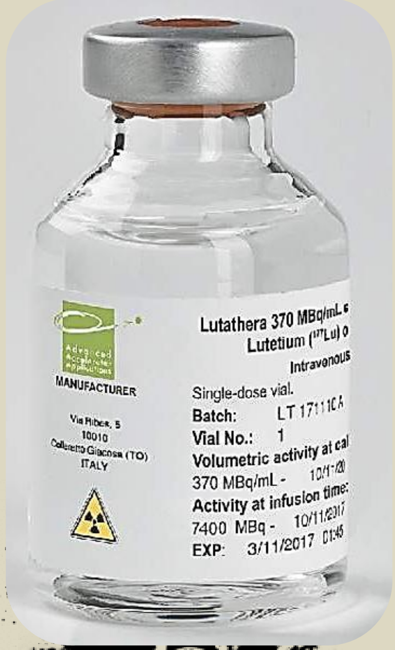


Another of the key moments in the documentary is the story of the bathroom of then **Minister of Information and Tourism, Manuel Fraga**, together with the US ambassador to the coast of Almería to try to stop the effect of panic and that the fatal accident did not scare potential customers from the then emerging Spanish tourist industry. There was a black legend that even questioned that this iconic scene had been filmed in the area affected by the nuclear alert, an extreme that ditch this documentary. It should not be forgotten that the event occurred before the international press that did not have the limitations of censorship to tell what was happening in Spain in their countries. The series underlines the propaganda success that the scene had, since Fraga's dip in black and white and a swimsuit is the first that comes to mind the most common of mortals every time someone tells us about the Palomares accident. Not the bombs in the middle of the field or at the bottom of the sea, nor the equipment that was day and night measuring radioactivity in the area. Although, how many times have we not realized the seriousness of a situation until the politician on duty has come out saying that everything was under control and was safe?

Those responsible for this documentary already delighted us more than a year ago with a review of the delirious history of El Palmar de Troya, a series that aspired to become the Wild, Wild Country a la española with a sect born during the last years of the Francoism in a Spain that was beginning to open its eyes to the world. As in the previous report, they had to go to **fictional scenes** for the reconstruction of some of the key moments of the plot. Many years have passed for sufficient graphic material to be available, while some of the protagonists of these events are already deceased. The problem with these fictional scenes is that they take away a bit of credibility from the plot, since sometimes it is not well distinguished when we are facing real images or recreations. Moments that do not stop reminding us of the great fiction series that could have been.

A Dead Man Was Cremated in Arizona Without Anyone Knowing He Was Radioactive

Source: https://www.sciencealert.com/a-dead-man-was-cremated-in-arizona-without-anyone-knowing-he-was-radioactive



May 17 – In 2017, a 69-year-old man with pancreatic cancer went to hospital with abnormally low blood pressure. Sadly, he died only two days later, and his remains were cremated.

What nobody at the hospital or the crematorium knew, was that this hadn't been the man's only recent trip to hospital.

Just one day earlier, in fact, he had been injected with a radioactive compound at another hospital to treat his tumor – and when his mortal remains were incinerated, this radioactive and potentially dangerous dose of lutetium Lu 177 dotatate was still inside his body.

This case, reported in a research letter published in 2019, illustrates the collateral risks potentially posed by on average 18.6 million nuclear medicine procedures involving radiopharmaceuticals performed in the US every year.

While rules regulate how these drugs are administered to living patients, the picture can become less clear when those patients die, thanks to a patchwork of different laws and standards in each state – not to mention situations like the 69-year-old man, whose radioactive status simply slipped through the cracks.

"Radiopharmaceuticals present a unique and often overlooked postmortem safety challenge," researchers from the Mayo Clinic explained in a case note.

"Cremating an exposed patient volatilizes the radiopharmaceutical, which can then be inhaled by workers (or released into the adjacent community) and result in greater exposure than from a living patient."

In this patient's case, once the treating physicians and the radiation safety department at the initial hospital became aware of the man's death, they got in touch with the crematorium.

Almost a month after the cremation took place, they used a Geiger counter to detect radiation levels inside the cremation chamber and on equipment, including the oven, vacuum filter, and bone crusher.

What they found were low but nonetheless elevated levels of radiation, while a spectroscopic personal radiation detector identified the primary radionuclide culprit – lutetium Lu 177, the same radioactive compound used to treat the man.

"This wasn't like the second-coming of Chernobyl or Fukushima, but it was higher than you would anticipate," case co-author and radiation safety officer Kevin Nelson told The Verge in 2019.

While there's no definitive proof specifically linking the patient's radiopharmaceutical dosage to the radiation levels detected in the crematorium, it's certainly the most likely explanation for how those trace levels of lutetium Lu 177 could be there.

It's also the first time radioactive contamination of crematory facilities has been documented like this.

But that's not the most concerning part of the story.

When the researchers analysed the crematorium operator's urine to see if the employee had also been contaminated by radiation exposure, they couldn't find any traces of lutetium Lu 177.

They did find something, though: a different radioactive isotope, called technetium Tc 99m. The worker said they had never been exposed to the compound as part of a nuclear medicine procedure.

Because of this, the researchers say it's plausible the operator could have been exposed to volatilized technetium Tc 99m while cremating *other* human remains – and if they're right, we could be looking at a broader issue here, as opposed to an isolated, unfortunate one-off.

Still, the amount of radiation we're talking about is very low, so even while the problem of accidental volatilization could be widespread in the cremation industry, it may not actually be as dangerous as it sounds.

"I don't think this is an issue that may entail any risk of cancer or other radiation-induced illnesses," cancer researcher Paolo Boffetta from the Icahn School of Medicine at Mount Sinai told UPI at the time.

"Having said that, it's clear it's a possible source of exposure, and if someone is exposed regularly, every week or every few days, then it may become a source of concern."

Given more than half of all Americans eventually get cremated, postmortem management of individuals who receive radioactive drugs is an area the US health system needs to work on, the researchers say.

This includes better ways of evaluating radioactivity in deceased patients (prior to them being cremated), and also standardizing ways of notifying crematoriums about their clients.

After all, nobody really has any idea how often this is happening.

As nuclear scientist Marco Kaltofen from the Worcester Polytechnic Institute in Massachusetts, who wasn't involved with the research, told BuzzFeed News: "They only happened to catch this one case because normally they don't look."

▶▶ **The findings were reported in *JAMA*.**

Nuclear Terrorism Could Be Intercepted by Neutron-Gamma Detector

Source: http://www.homelandsecuritynewswire.com/nuclear-terrorism-could-be-intercepted-neutron-gamma-detector

May 20 – Scanning technology aimed at detecting small amounts of nuclear materials was unveiled by scientists in Sweden, with the hope of preventing acts of nuclear terrorism.

Bo Cederwall, a professor of physics at KTH Royal Institute of Technology, says the technology can be used in airports and seaports for routine inspection of passengers and goods. The research is published and featured in the journals *Science Advances*.

A form of tomography, the system enables quick 3D imaging of the source of neutron and gamma ray emissions from weapons-grade plutonium and other special nuclear materials, Cederwall says.

The so-called Neutron-Gamma Emission Tomography (NGET) system goes beyond the capabilities of existing radiation portal monitors, by measuring the time and energy correlations between particles emitted in nuclear fission, and using machine learning algorithms to visualize where they're coming from. The system looks for coincidences of neutron and gamma ray emissions—which when mapped together in real-time allow pinpointing their origin.

"The technology has a very high sensitivity and can within a few seconds detect gram-amounts of plutonium depending on the application and the plutonium isotope composition," Cederwall says. "It takes a little longer to get a really good picture so you can see exactly where the plutonium is. However, this can be done completely automatically."

But NGET isn't only for nuclear weapons and radiation-dispersing "dirty bombs"—it can be used to detect environmental radiation too, such as leaks from nuclear facilities or even natural sources. Cederwall says the research group is looking into equipping drones with the NGET system for this purpose.

"In case of a radiological emergency, It is extremely important to be able to quickly map the radioactive contamination in the environment in order to protect the population in the best possible way," he says.

More nukes and a regional pivot: Britain unveils its long-awaited defense review

Source: https://www.defensenews.com/global/europe/2021/03/16/more-nukes-and-a-regional-pivot-britain-unveils-its-long-awaited-defense-review/

Mar 16 — Britain is to substantially increase its stockpile of nuclear warheads in response to a deteriorating security environment, the government said in a long-awaited review of defense, security and foreign policy released March 16.

The move would see Britain increase the inventory to no more than 260 warheads, reversing a decision made a decade ago to cut the maximum from 225 to 180 by the mid-2020s.

Depending on exactly how many warheads the country intends to acquire, it could see the strategic weapons count increase by more than 40 percent.

Britain is deliberately ambiguous about how many nuclear warheads it possesses, but that hasn't always been the case. In 2015, then-Defence Secretary Michael Fallon announced that the reduction would see Vanguard-class submarines carry 40 warheads and no more than eight Trident missiles. One of the Royal Navy's fleet of four Vanguard subs is always at sea and armed.

The government said its decision in the Integrated Review to raise warhead numbers is justified by developing technological and doctrinal threats.

"Some states are now significantly increasing and diversifying their nuclear arsenals. They are investing in novel nuclear technologies and developing new 'warfighting' nuclear systems which they are integrating into their military strategies and doctrines and into their political rhetoric to seek to coerce others," the review read. "The increase in global competition, challenges to the international order, and proliferation of potentially disruptive technologies all pose a threat to strategic stability."

Britain is in the early stages of designing a new warhead to eventually arm the four Dreadnought-class submarines destined to replace the Vanguard boats starting early in the next decade. The review said construction of the first Dreadnought-class sub is going according to budget and schedule.

What else did the review say?

Announcing the new warhead numbers was one of several major initiatives emerging from what Prime Minister Boris Johnson previously labeled Britain's biggest foreign policy and defense shakeup since the end of the Cold War.

The review confirmed the government's previously cited intention to pivot foreign and defense policy toward the Asia-Pacific region. The "tilt" toward the region, as the review put it, is Britain's response to the growing economic power of regional countries and China's increasing influence on its neighbors and beyond. It's no coincidence the first deployment of the Royal Navy's new aircraft carrier, the HMS Queen Elizabeth, is to take place in the region later this year.

The review warned that while "China presents the biggest state-based threat to the UK's economic security," London will have to continue to deal with Beijing on trade and international issues like climate change, even while verbally scraping over problems like Hong Kong's autonomy and human rights violations in Xinjiang.

"We will continue to pursue a positive economic relationship, including deeper trade links and more Chinese investment in the UK. At the same time, we will increase protection of our critical national infrastructure, institutions and sensitive technology, and strengthen the resilience of our critical supply chains," said the review

Howard Wheeldon, of Wheeldon Strategic Advisory, sees Britain's revived interest in the Asia-Pacific region as trade-focused.

"This would appear on the surface to be more about securing a place at the future international table and, of course the most important element for government, protecting and enhancing our international trade. Equally true is that this is also about securing lost trust with our allies," he told Defense News

What's next for Britain's military?

A second part of the review and a new defense-industrial base strategy are scheduled to be published next week, when the Ministry of Defence reveals the winners and losers in a big shakeup of the military.

The first part of the Integrated Review signaled some potential changes are on the way. Ships, armored vehicles, combat aircraft and Army personnel numbers are all in the firing line as Britain cut capabilities, in part to create financial headroom for new investments in the areas of space, cyber and artificial intelligence, among other new technologies.

It's unclear whether the government can deliver on the optimistic tone struck by the review, Wheeldon said.

"Actions always speak louder than words, but that takes nothing away from what is contained in today's section of the Integrated Review process: increasing the U.K.'s stockpile of nuclear missiles; full commitment to Dreadnought; investment in AI; Space Command; cyber; growing U.K. science and technology power; building U.K. national resilience; protecting national interests on a global scale; reaching out in respect [to] conflict and stability; homeland security' U.K. national resilience and countering state threats; defense; disruption and deterrence," he said.

"This is a big document full of intentions and hope."

Next up, according to the review, is the implementation of "a new defense and security industrial strategy aligned with the Government's plan for growth. It will constitute a more strategic approach to our core industrial base."

"The Government will move away from the 2012 policy of 'competition by default' and prioritize UK industrial capability where required for national security and operational reasons. We will also reform and revitalize our approach to acquisition, exports and international collaboration, including greater use of government-to-government arrangements," the review explained.

A Trident II D5 missile breaks the surface of the water having been fired from HMS Vanguard, a British strategic missile submarine. (British Defence Ministry)

Paul Everitt, the chief executive of the lobbying group ADS, said the shift away from the competition by default is the right way to go to support local industry.

"The government's intention to move away from 'competition by default' as the primary route to achieving value for money in defense procurement is welcomed by industry," Everitt told

Defense News. “Under this approach, the U.K.’s defense and security sectors can deepen their partnership with government to better support our national ambitions and secure the U.K.’s national security objectives.”

Meanwhile, in Parliament ...

The unveiling of the Integrated Review coincided with the publication of the parliamentary Public Account Committee’s annual look at the state of the MoD’s procurement plans. The committee’s figures suggest that while the ministry may have big ambitions, it also has big financial problems, despite the government making available a large amount of cash to help balance the books and fund modernization.

As has become customary, the report on the ministry’s equipment plans and finances made for grim reading. For the fourth year running, the committee labelled the equipment plan “unaffordable.”

The worst-case scenario is a “potential £17.4 billion black hole” (U.S. $24.2 billion) in the equipment program between 2020 and 2029, the committee said. That’s substantially more than last year, when the committee estimated that potential “black hole” for 2019-2029 at £13 billion.

The MoD, on the other hand, found the expected funding shortfall for the current 10-year period is £7.3 billion.

Johnson’s government last November pledged an additional £16.5 billion for the next four financial years to help fund military modernization. Together, with an annual 0.5 percent real-term increase for the subsequent six years after 2024, the defense budget is expected to receive a boost of £30 billion over 10 years.

None of the figures in the committee’s report count the cost of military modernization as part of the Integrated Review. Whatever the modernization costs turn out to be, some of the additional money appropriated for defense will go toward plugging that financial “black hole.” Ministry officials have already indicated that not all of the money would go toward acquiring new and revolutionary kit.

The committee warned the MoD to get its modernization effort under control as well as find savings and make cuts before any new strategy is delivered.

Meg Hillier, the committee chair, put it this way: ”What is crucial is that this new money is not just eaten up, once again, by the constant, debilitating time and budget overruns that have been eroding our national defense and security for years.”

Biden Must Be Clear About What Nuclear Weapons Are For

By Adam Mount

Source: https://foreignpolicy.com/2021/05/12/biden-nuclear-weapons-review-sole-purpose/

May 12 – President Joe Biden has assumed command of the U.S. nuclear arsenal at a particularly turbulent time. The Trump administration, consistent with former President Donald Trump’s own fixation on the destructiveness of nuclear weapons, accelerated programs to develop a new generation of warheads and delivery vehicles, sought a new low-yield warhead and a new sea-launched cruise missile, and added vague new language to U.S. declaratory policy that expanded the role of nuclear weapons in deterring non-nuclear attacks. As the Department of Defense is struggling with an enormous “bow wave” of modernization costs across the force, these efforts sometimes diverted funds away from critical conventional priorities. The overall effect was to increase the nation’s reliance on its nuclear forces at the expense of more credible conventional deterrence options.

During the campaign, Biden pledged to reduce, rather than increase, reliance on nuclear weapons. He stated, “the sole purpose of the U.S. nuclear arsenal should be deterring—and if necessary, retaliating against—a nuclear attack,” and he promised to review the U.S. policy that reserves the right to use nuclear weapons first in a conflict. His initial national security guidance and his secretary of state have reiterated the goal of reducing reliance on nuclear weapons

But what does “sole purpose” mean in practice? The term originated in the 1960s, and the idea even earlier, but it is not clear how the concept would apply to today’s world. It could be a transformative change that has sweeping consequences for U.S. nuclear force structure and deterrence strategy, or it could be just rhetoric. The answer will depend on how the president defines sole purpose—and whether he replaces the antiquated Nuclear Posture Review with a process that can determine how conventional and other tools can safely reduce reliance on nuclear weapons.

In its 2010 Nuclear Posture Review, the Obama-Biden administration explicitly considered a move to sole purpose, which it regarded as a statement about the types of attacks that nuclear weapons would deter. That document stated that the United States was “not prepared at the present time to adopt a universal policy that deterring nuclear attack is the sole purpose of nuclear weapons,” because they still play a role in deterring a nuclear, chemical, or biological attack in a “narrow range of contingencies.” Sole purpose in this sense is a statement that nuclear weapons pertain to a sole type of attack: Nuclear weapons would deter *nuclear* attacks—not conventional, chemical, and biological attacks.

Seven years later, in his last days in office, then-Vice President Biden reported that “the president and I strongly believe we have made enough progress that deterring—and if necessary, retaliating against—a nuclear attack should be the sole purpose of the U.S. nuclear arsenal” and that they were “confident we can deter … nonnuclear threats through other means.” But they did not make the change; they left it for a Hillary Clinton administration that never came.

Since the 2010 Nuclear Posture Review, Biden’s definition of sole purpose has evolved. His phrasing in the 2017 speech and in subsequent campaign statements pertains not only to the type of attack but the function of nuclear weapons—which is deterrence and, if necessary, retaliation for nuclear attacks. This definition seems to say that nuclear weapons don’t just pertain to a sole type of attack—they have a “sole function” in responding to nuclear attacks.

As he and his National Security Council draft guidance for the next defense policy reviews in the next months, they should give a clear and explicit definition of sole purpose. What is the opposite of a sole purpose policy? Is it a policy that nuclear weapons also deter nonnuclear attacks, or is it a policy in which nuclear weapons also perform functions other than deterrence?

Deterrence is the obvious use of nuclear weapons, but there are other potential functions. One option is that nuclear weapons are useful for tactical warfighting—for striking battlefield targets for military advantage in a limited conflict. Another is that weapons are useful for strategic warfighting—for limiting damage to the United States or an ally by conducting large-scale strikes against an enemy’s nuclear forces before they can be launched. Another is that nuclear weapons are uniquely valuable for signaling U.S. resolve in response to a nuclear attack. Another is that they might prevent a nuclear-armed adversary from developing new strategic capabilities, or hedge against that risk. Another is that nuclear weapons might be uniquely capable in assuring allies of U.S. intentions to defend them from nuclear or nonnuclear attacks. All these and more were mentioned in the 2018 Nuclear Posture Review as critical roles of U.S. nuclear weapons.

It might indeed be the case that deterrence depends on having a warfighting arms capability, a damage limitation capability, a nuclear option for signaling resolve, a hedge against racing, and a strong nuclear assurance. But it also might not. In defining sole purpose, the president will be defining the requirements of deterrence.

When the president and National Security Council issue guidance to the Pentagon for the next defense reviews, they could define the sole purpose of nuclear weapons as a sole function, as appropriate to a sole type of attacks, or they could decline to provide a specific definition. If the president does not provide a clear definition of sole purpose, a Pentagon review would likely water down the doctrine until it represents only a modest shift that pertains to a handful of chemical and biological weapons targets.

In either of the latter two cases, force structure and planning are likely to remain largely unaffected. Though the president could choose to cut or delay an acquisition program or two, the arsenal would likely remain large, diverse, postured for a range of functions, prepared for use at a moment’s notice, and central for plans to control escalation of a limited conflict. If it was not accompanied by visible changes to force structure or plans, adversaries would doubt that U.S. policy had changed, limiting its benefits for strategic stability. Lastly, a sole purpose declaration of this type could be easily rescinded by a future president. Its primary consequences would be political: acclaim from disarmament groups, disapproval from Republicans, and some tension with allies. Sole category, or an undefined sole purpose, would likely not reduce reliance on nuclear weapons.

A “sole function” statement, in contrast, could have transformative effects on both force structure and operational planning. A nuclear arsenal that is not postured for warfighting might be significantly smaller, less diverse, and less expensive. Eliminating of certain functions would effectively increase reliance on advanced conventional forces. While conventional options are already available for most targets relevant to a limited conflict, confining nuclear weapons to a sole function could force planners to prioritize the development of conventional responses to an adversary’s aggression or coercive first use of a nuclear weapon, helping to avoid a situation where a president feels constrained by America’s reliance on nuclear weapons. It would fit well with a commonsense statement that a U.S. president would not use nuclear weapons if they had viable conventional options available.

Like other declaratory policy, sole purpose is consequential to the extent that it affects force structure and operational planning. For a sole purpose statement to achieve Biden’s objectives—strengthening strategic stability and reducing U.S. reliance on nuclear weapons—it will have to be clearly defined in terms of the functions of nuclear weapons, accompanied by clear guidance for how the Pentagon should implement the shift, and receive sustained investment of time from senior political appointees to review acquisitions plans and operational concepts to ensure they comport with the president’s preferences.

As the president provides clear guidance about the purpose of nuclear forces, he should also direct changes to how the Pentagon structures its policy review to ensure the changes are implemented safely and effectively. Since the end of the Cold War, each new administration has conducted both a Nuclear Posture Review and a broader defense review. In the most recent cycle, the 2018 review argued that new nuclear options were critical for deterrence in a limited conflict with a nuclear-armed adversary, while the concurrent National Defense Strategy described a strategy predicated on multiple layers of conventional forces. But there was little or no sense of how the two strategies would relate to each other. This partitioned process cannot provide clear guidance to planners developing operational concepts for managing escalation or to services trying to rationally appropriate finite funding between nuclear and conventional capabilities.

The purpose of the Nuclear Posture Review is not to find the best way to deter the threats the United States faces but to explain what nuclear weapons might deter. A separate nuclear review doesn't help the U.S. government find the right tools for the job; it helps it find a job for this particular tool. It encourages excessive reliance on nuclear weapons by setting nuclear requirements in isolation from a broader strategy.

The United States needs a single integrated review that develops a common strategy for deterring limited conflict with nuclear-armed adversaries with nuclear, conventional, cybersecurity, and space capabilities.

Part of an integrated strategy review would be examining conventional-nuclear integration, which was a leading priority for the Trump administration but remained only a slogan that was attached to efforts to integrate nuclear and conventional forces to reflect integrated adversary strategies, ensure that nuclear forces could carry out signaling and employment missions during a limited conflict, and procure dual-capable strike and command-and-control systems. None of these is a good reason to integrate nuclear and conventional forces. The Biden administration should review these efforts, and the operational plans that follow from them, to ensure integration of conventional and nuclear forces strengthens strategic stability and reduces, rather than increases, reliance on nuclear weapons.

In practice, an integrated review is the only way to safely reduce reliance on nuclear weapons, because it provides a format to develop a strategy that determines the roles and capabilities of both nuclear and conventional forces. As reliance on nuclear forces declines, a corresponding increase in reliance on conventional forces may require complementary or compensatory changes to conventional posture. Importantly, it would allow the United States to discuss these measures with allies and impress upon them an important fact: Because nuclear weapons cannot defend them, they must cooperate with the United States on combined strategy to manage escalation in a limited conflict with nuclear-armed adversaries. Ultimately, this will be more reassuring than reliance on tenuous signals of nuclear assurance.

Biden comes into office with strong preferences on nuclear weapons. But it will not be enough to issue a statement and let the chips fall where they may. Sole purpose can strengthen U.S. deterrence posture—but only if senior officials are willing to devote the time and attention required to achieve its transformative potential.

***Adam Mount** is a senior fellow and the director of the Defense Posture Project at the Federation of American Scientists.*

EDITOR'S COMMENT: In contrast, as you have already read in the Editorial of this issue of *C²BRNE Diary*, the Pakistanis have a concrete, clear view of what nuclear weapons are for.

Schneider Electric to help develop the United Arab Emirates first waste-toenergy plant.

Source: https://www.thenationalnews.com/business/energy/schneider-electric-tohelp-develop-the-uae-s-first-waste-to-energy-plant-1.1203801

Apr 14 – The Sharjah waste-to-energy facility will have the capacity to process 37.5 tonnes of non-recyclable solid municipal waste per hour, and will help divert more than 300,000 tonnes from landfill on an annual basis.

It's first time I'm crying while watching TV. Such a loss...
Over 300 kg nuclear weapon will be destroyed ....
Sanders

International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

EXPLOSIVE NEWS

Researchers at IIT Bombay design hand-held device that can detect explosives

Source: https://www.hindustantimes.com/cities/others/iitb-researchers-design-hand-held-explosive-detection-device-101619157174737.html

Apr 23 – Researchers at the National Center of Excellence in Technology for Internal Security (NCETIS) of the Indian Institute of Technology (IIT), Bombay, have designed a hand-held explosive detection device that can detect explosives.
Director, Subhasis Chaudhuri, on Tuesday, announced that some units of the device were now being used by the Travancore Devaswom Trust in Sabarimala, Kerala.
"We have been asked by the Trivandrum Police to give a live demonstration for the department procurement," said Seema Periwal, a senior programme manager for NCETIS. Six units of BEAGLEZ are also in use by three departments of the Indian Army.
BEAGLEZ is a light-weight hand-held device that can detect Trinitrotoluene (TNT), hexahydro-1,3,5-trinitro-1,3,5-triazine (RDX), Pentaerythritol tetranitrate (PETN), Semtex and other plastic explosives used in home-made, military explosives and improvised explosive device (IED).
The device can find application in screening people, checkpoints, post-blast search, vehicles, buildings, terrorist hotspots, places of importance, crowded establishments and environment.
BEAGLEZ was designed and commercialised by a team of researchers led by Anil Kumar, professor in the department of chemistry at IIT Bombay, in collaboration with Bigtec Labs, a Bengaluru-based science and technology company. The device has sensitivities that can be at par with canines.

Syrian landmines wash into Lebanon due to floods

Source: https://www.arabnews.com/node/1857786/middle-east

Syrian refugee tents in Bar Elias town are inundated with floodwaters, Bekaa valley, Lebanon, January 7, 2019. (Reuters)

May 12 – As authorities continue to find and extract landmines left behind from the Lebanese Civil War, a new wave of explosives has entered the country's border due to a natural disaster.

The Lebanese Armed Forces on Wednesday said landmines planted along the Lebanese-Syrian border have washed into Lebanese territories due to winter flooding.

“Landmines planted on the Lebanese-Syrian borders are a result of the Syrian conflict,” a Lebanese military source told Arab News. “As these mines drifted into Lebanese territories, it has become harder for the Lebanese army to clear them. Multiple accidents have been recorded this year, which has injured many who were not familiar with the nature of the foreign objects they found.”

The source said a majority of accidents occurred in the northern border region due to the flooding and soil erosion caused by the winter floods. All injuries were on Lebanese soil.

The army command issued a statement, which warned “ammunition comes in different shapes and sizes and may be camouflaged in different ways and dispersed randomly.”

Areas that are potentially contaminated with landmines are not marked with signs or barbed wire to warn people yet. The army command has urged citizens to avoid suspicious areas, stay on paved roads, and not to approach or tamper with any object or unexploded ordnance.

The Lebanese Mine Action Center (LMAC), which is part of the Lebanese Armed Forces, has been carrying out the Lebanese National Mine Action Program with support from the UN Development Program to cover shortfalls.

The LMAC aims to secure a safe country where civilians can walk and move freely without the threat of landmines by the year 2025.

The center’s mission focuses on areas in south Lebanon, which is the most contaminated area with landmines and suspicious objects.

“The closer we get to a minefield in the remote areas of south Lebanon, the more red-painted stones we see,” United Nations Interim Force in Lebanon (UNIFIL) Officer Captain Yang Dong from China said.

“The red stones remind us of safe and unsafe areas. They remind us not to step around. If there are red stones nearby, it is dangerous and there could be some mines there.”

In January 2020, the UNIFIL’s scope of work increased with the signing of a new agreement with the LMAC while the country marked International Day for Mine Awareness and Assistance in Mine Action on April 4.

Over the past five years, the UNIFIL’s demining efforts have cleared nearly 5 million square meters of mine-infested land in south Lebanon. It has also destroyed more than 43,500 landmines, bombs, and unexploded ordnances.

The threat of landmines is real and spreading awareness is vital for the Lebanese people.

Since 1975, landmines and unexploded materials left behind from the Lebanese Civil War have led to 3,847 deaths and injuries. The most casualties were recorded in 2006 when 209 people were killed or injured, including 40 children under the age of 12.

Gaza's enhanced rocket technology challenges Israel's defenses

By Michael J. Armstrong

Source: https://www.upi.com/Top_News/Voices/2021/05/18/israel-Gaza-Israel-rocket-technology/5671621338293/

May 18 – Gaza militants have launched their "Sword of Jerusalem" rocket war with Israel by firing a symbolic salvo at Jerusalem and bigger ones elsewhere. Israel's "Guardian of the Walls" operation responded with Iron Dome interceptors at home and airstrikes in Gaza.

As someone who's researched Israeli missile defense systems for several years, the situation initially seemed to me like a repeat of their 2014 conflict, which showcased Israel's advanced defenses. But militants in Gaza have enhanced their rocket technology and tactics. That's reminiscent of 2008, when Israel was more vulnerable to rockets and waged a three-week military offensive against Gaza.

According to the Israel Defense Forces, roughly 3,100 rockets have been fired from Gaza. That's about as many as during the seven-week battle in 2014. (All rocket numbers in this article were reported by the Israel Defense Forces or Israel Security Agency. There is no way to independently verify most of them.)

Israeli news reports say they've caused 10 civilian deaths and more than 564 injuries, while Israeli countermeasures have killed almost 200 Palestinians and resulted in scenes of carnage and devastation.

The counts have risen so quickly because Gaza militants have improved their rockets and their usage of them.

Improved rocketry

The most noticeable change this year is larger quantities. Gaza militants fired 470 rockets during the first 24 hours and have averaged 408 per day. Those numbers easily beat the one-day maximums of 316 in 2012 and 192 in 2014.

The firing is also better coordinated. Rather than launching many small attacks spread across the day, they've unleashed larger salvos of up to 137 rockets within five minutes. That's much improved, though still far slower than regular army artillery units.

Accuracy has improved, too. About 50 percent of the rockets arriving over Israel have threatened populated areas. That's up from 22 percent in 2012 and 18 percent in 2014. Fewer rockets land in empty fields after missing their targets.

Larger, longer-range rockets are also more common now. During previous conflicts, Israel's southern cities endured most of the fire. This time, Tel Aviv, in central Israel more than 34 miles from Gaza's border, is routinely targeted.

Rocket reliability, however, has dropped. About 15 percent have failed at launch, versus under 10 percent during previous conflicts.

Destructive impact

The improved technology and tactics make barrages more destructive. My calculations suggest at least 134 rockets have hit populated areas.

During the first four days of this conflict, one Israeli died for every 206 rockets reaching the country. That approaches the one-per-204 rate of 2008, when Israel's defenses were weaker. By comparison, it took 270 rockets to kill a civilian in 2012 and 1,429 in 2014.

The injury rate, about one for every three rockets arriving overhead, also resembles 2008. And many buildings have been damaged.

These results imply that shock-and-awe destruction is the 2021 strategy of Gaza militants. By comparison, the 2014 operation mostly featured economic attrition. Israel suffered relatively few civilian casualties but heavy financial costs from the prolonged disruption.

Both then and now, Israel has responded with several countermeasures.

Blocking (many) rockets

Iron Dome interceptors provide the best-known defense. Israel claims the systems intercepted 1,210 rockets last week, or 90 percent of the rockets they engaged. That's about the percentage they achieved in 2014, too, though perhaps not in 2012.

Are they always achieving it now?

With bigger barrages and greater accuracy, more rockets are arriving together above each target. That means there's more risk the interceptors will become overloaded and let some rockets through.

Suppose the systems sometimes block "only" 80 percent of rockets. That's still impressive. But it means the portion penetrating then doubles from 10 to 20 percent, causing twice the destruction.

My research seven years ago analyzed this tactic. It showed that high-performing interceptors can seem "fragile" -- once their capacity is exceeded, damage on the ground soars.

That research also studied the idea of firing directly at interceptor systems to disable them. Sure enough, one barrage recently made such an attempt. That was likely a waste of ammo, as their rockets aren't accurate enough yet for such small targets.

Ironically, one Iron Dome system was briefly disabled two days earlier by an equipment malfunction. That let some extra rockets through.

Israel also has extensive warning systems and bomb shelters. Those prevent as many casualties as interceptors do, but don't stop property damage.

Airstrikes are another Israeli countermeasure. Its aircraft began bombing rocket stockpiles and launchers last week, followed by production sites and other targets.

But while its bombers can destroy rocket stockpiles and workshops, they don't have much immediate effect on firing rates. My analysis of previous operations found that airstrikes didn't decrease daily fire rates; only ground assaults did that.

Collateral damage is another problem. Bombs have damaged or completely destroyed many buildings. And almost 200 Palestinian militants and civilians have died so far.

What next?

Gaza's 14,000-rocket arsenal could support short-range barrages for months.

But it will likely run out of long-range rockets sooner, making a truce look more attractive. Israel might favor a truce soon, too, as it runs out of meaningful airstrike targets.

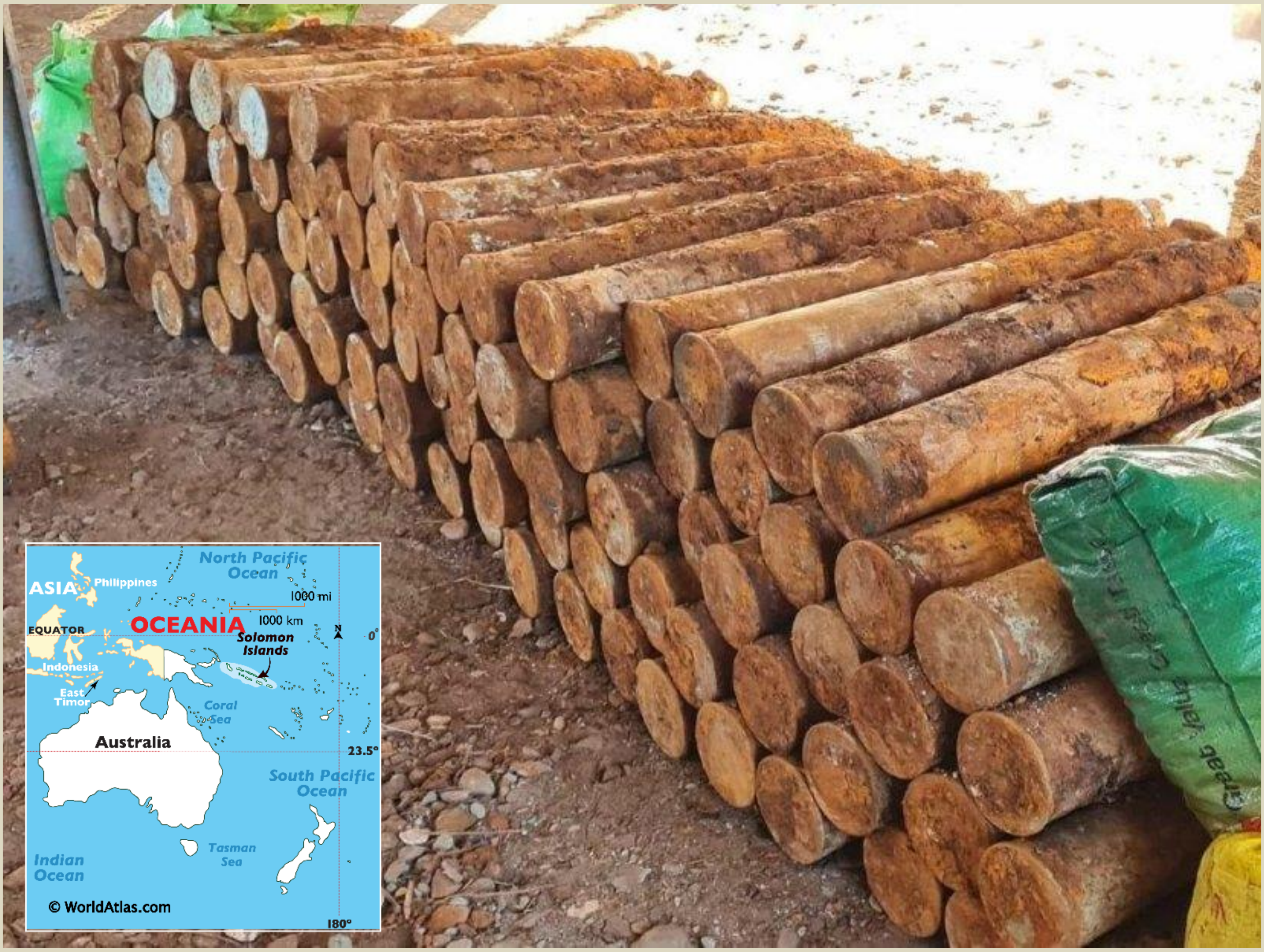
Let's hope that truce happens soon. The alternatives are a prolonged war of aerial attrition, or a costly ground battle in Gaza.

***Michael J. Armstrong** is an associate professor of operations research at the Goodman School of Business at Brock University.*

▶▶ **Read also:** https://www.al-monitor.com/originals/2021/05/hamas-uses-large-rocket-arsenal-latest-escalation-round-israel

Be careful when you dig in your garden!

It happened in the Solomon Islands: 100 unexploded WWII US 105mm artillery munition!



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

CYBER NEWS

C2BRNE DIARY

New Vulnerability Affecting Computers Globally

Source: http://www.homelandsecuritynewswire.com/new-vulnerability-affecting-computers-globally

May 03 – In 2018, industry and academic researchers revealed a potentially devastating hardware flaw that made computers and other devices worldwide vulnerable to attack.

Researchers named the vulnerability Spectre because the flaw was built into modern computer processors that get their speed from a technique called "speculative execution," in which the processor predicts instructions it might end up executing and preps by following the predicted path to pull the instructions from memory. A **Spectre attack** tricks the processor into executing instructions along the wrong path. Even though the processor recovers and correctly completes its task, hackers can access confidential data while the processor is heading the wrong way.

Since Spectre was discovered, the world's most talented computer scientists from industry and academia have worked on software patches and hardware defenses, confident they've been able to protect the most vulnerable points in the speculative execution process without slowing down computing speeds too much.

They will have to go back to the drawing board.

A team of University of Virginia School of Engineering computer science researchers has uncovered a line of attack that breaks all Spectre defenses, meaning that billions of computers and other devices across the globe are just as vulnerable today as they were when Spectre was first announced. The team reported its discovery to international chip makers in April and will present the new challenge at a worldwide computing architecture conference in June.

The researchers, led by Ashish Venkat, William Wulf Career Enhancement Assistant Professor of Computer Science at UVA Engineering, found a whole new way for hackers to exploit something called a "micro-op cache," which speeds up computing by storing simple commands and allowing the processor to fetch them quickly and early in the speculative execution process. Micro-op caches have been built into Intel computers manufactured since 2011.

Venkat's team discovered that hackers can steal data when a processor fetches commands from the micro-op cache.

"Think about a hypothetical airport security scenario where TSA lets you in without checking your boarding pass because (1) it is fast and efficient, and (2) you will be checked for your boarding pass at the gate anyway," Venkat said. "A computer processor does something similar. It predicts that the check will pass and could let instructions into the pipeline. Ultimately, if the prediction is incorrect, it will throw those instructions out of the pipeline, but this might be too late because those instructions could leave side-effects while waiting in the pipeline that an attacker could later exploit to infer secrets such as a password."

Because all current Spectre defenses protect the processor in a later stage of speculative execution, they are useless in the face of Venkat's team's new attacks. Two variants of the attacks the team discovered can steal speculatively accessed information from Intel and AMD processors.

"Intel's suggested defense against Spectre, which is called LFENCE, places sensitive code in a waiting area until the security checks are executed, and only then is the sensitive code allowed to execute," Venkat said. "But it turns out the walls of this waiting area have ears, which our attack exploits. We show how an attacker can smuggle secrets through the micro-op cache by using it as a covert channel."

Venkat's team includes three of his computer science graduate students, Ph.D. student Xida Ren, Ph.D. student Logan Moody and master's degree recipient Matthew Jordan. The UVA team collaborated with Dean Tullsen, professor of the Department of Computer Science and Engineering at the University of California, San Diego, and his Ph.D. student Mohammadkazem Taram to reverse-engineer certain undocumented features in Intel and AMD processors.

They have detailed the findings in their paper: "I See Dead µops: Leaking Secrets via Intel/AMD Micro-Op Caches"

This newly discovered vulnerability will be much harder to fix.

"In the case of the previous Spectre attacks, developers have come up with a relatively easy way to prevent any sort of attack without a major performance penalty" for computing, Moody said. "The difference with this attack is you take a much greater performance penalty than those previous attacks."

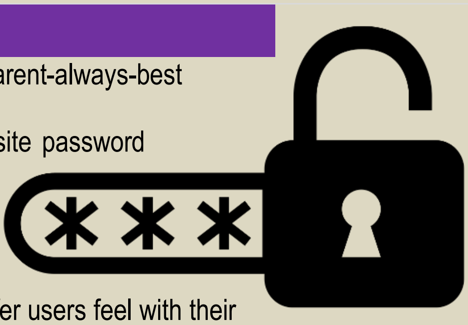
"Patches that disable the micro-op cache or halt speculative execution on legacy hardware would effectively roll back critical performance innovations in most modern Intel and AMD processors, and this just isn't feasible," Ren, the lead student author, said.

"It is really unclear how to solve this problem in a way that offers high performance to legacy hardware, but we have to make it work," Venkat said. "Securing the micro-op cache is an interesting line of research and one that we are considering."

Venkat's team has disclosed the vulnerability to the product security teams at Intel and AMD.

Ren and Moody gave a tech talk at Intel Labs worldwide April 27 to discuss the impact and potential fixes. Venkat expects computer scientists in academia and industry to work quickly together, as they did with Spectre, to find solutions.

Complex Passwords Aren't Always Best



Source: http://www.homelandsecuritynewswire.com/dr20210507-complex-passwords-arent-always-best

May 07 – Research from James Cook University shows increasingly complex website password restrictions often leave users frustrated and lead to poor password security.

Associate Professor Roberto Dillon investigated how users react to increasingly complex password requirements and whether those rules compromise password security.

"Our results confirm that the tougher the constraints of creating the passwords the safer users feel with their information," he said. "However, the results show that a large number of restrictions can frustrate users."

Dr. Dillon said this frustration led to 75% of participants using strategies to remember their passwords, including strategies that compromise their security.

"The most popular strategy was using the same password for multiple sites," he said.

Dr. Dillon and his team conducted a survey where users were asked to create a password following an increasing number of restrictions, ranging from "passwords must contain at least eight characters" to "passwords must be different from the latest five passwords."

Participants were also asked if they used any strategies to remember their passwords, as well as the situations where they would be tempted to use those strategies.

"Websites often require passwords that include a combination of special characters, numbers, upper- and lower-case letters, and more," he said. "This makes passwords less likely to be compromised by hackers, but harder for users to invent a password and to remember it."

While measures such as password managers and two-factor authentication protocols offer solutions to password management and securing privacy, Dr. Dillon said they still suffer from usability issues and demonstrate inconvenience to users.

He suggests a better approach was to ask users to create a long but meaningful password phrase.

"This is easy to remember but long enough to hinder brute-force hacking attacks," he said. "At the same time, providers should avoid adding several restrictions as it makes it more likely for users to resort to workarounds that compromise security."

Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed

Source: https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/

May 09 – Top U.S. fuel pipeline operator Colonial Pipeline shut its entire network, the source of nearly half of the U.S. East Coast's fuel supply, after a cyber attack on Friday that involved ransomware.

The incident is one of the most disruptive digital ransom operations ever reported and has drawn attention to how vulnerable U.S. energy infrastructure is to hackers. A prolonged shutdown of the line would cause prices to spike at gasoline pumps ahead of peak summer driving season, a potential blow to U.S. consumers and the economy.

"This is as close as you can get to the jugular of infrastructure in the United States," said Amy Myers Jaffe, research professor and managing director of the Climate Policy Lab. "It's not a major pipeline. It's the pipeline."

Colonial transports 2.5 million barrels per day of gasoline, and other fuels through 5,500 miles (8,850 km) of pipelines linking refiners on the Gulf Coast to the eastern and southern United States. It also serves some of the country's largest airports, including Atlanta's Hartsfield Jackson Airport, the world's busiest by passenger traffic.

The company said it shut down its operations after learning of a cyberattack on Friday using ransomware.

"Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation," it said.

While the U.S. government investigation is in early stages, one former official and two industry sources said the hackers are likely a professional cybercriminal group.

The former official said investigators are looking at a group dubbed "DarkSide," known for deploying ransomware and extorting victims while avoiding targets in post-Soviet states. Ransomware is a type of malware designed to lock down systems by encrypting data and demanding payment to regain access.

Colonial said it had engaged a cybersecurity firm to help the investigation and contacted law enforcement and federal agencies.

The cybersecurity industry sources said cybersecurity firm FireEye (FEYE.O) was brought in to respond to the attack. FireEye declined to comment.

U.S. government bodies, including the FBI, said they were aware of the situation but did not yet have details of who was behind the attack.

President Joe Biden was briefed on the incident on Saturday morning, a White House spokesperson said, adding that the government is working to try to help the company restore operations and prevent supply disruptions.

The Department of Energy said it was monitoring potential impacts to the nation's energy supply, while both the U.S. Cybersecurity and Infrastructure Security Agency and the Transportation Security Administration told Reuters they were working on the situation.

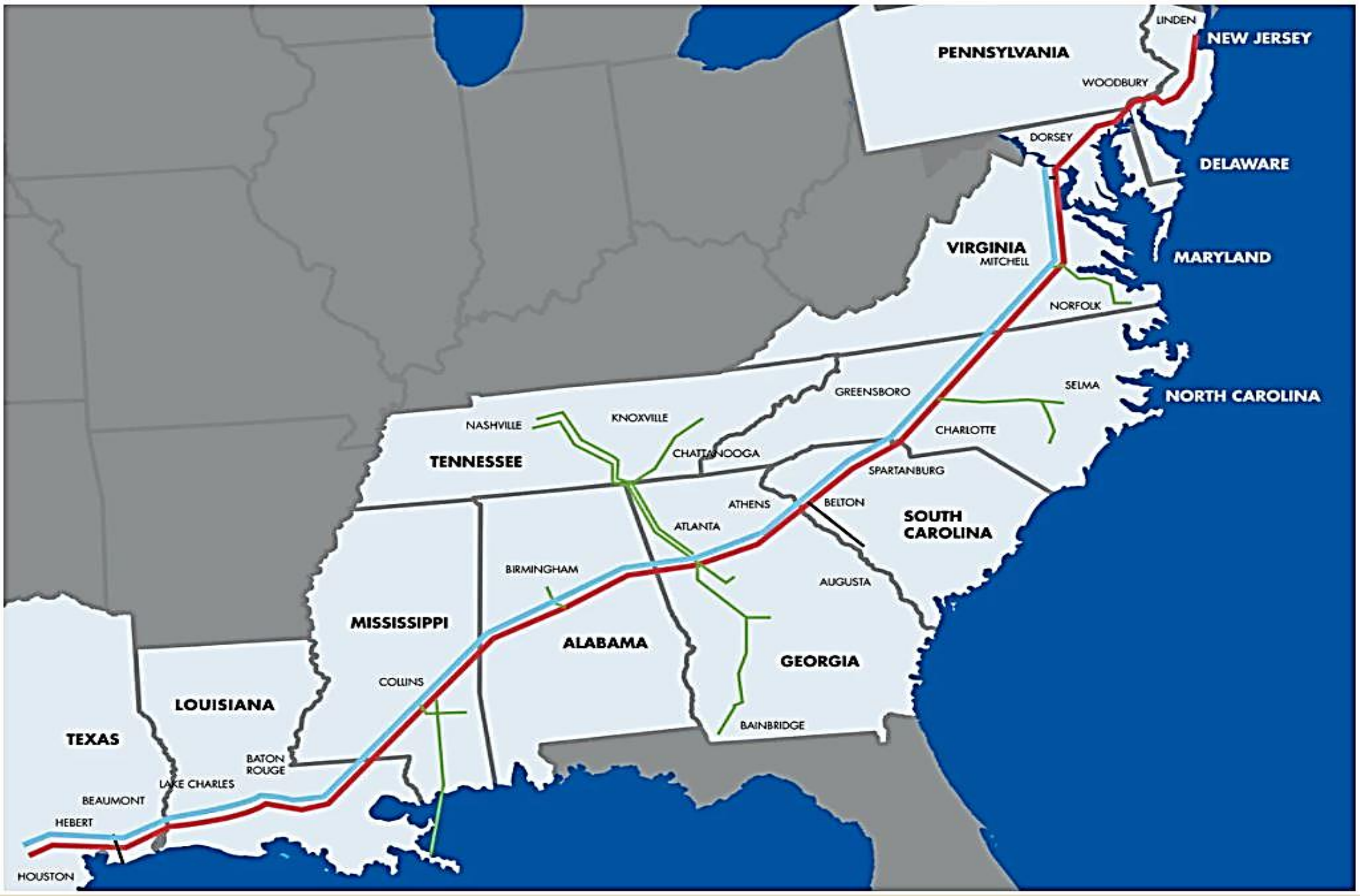
"We are engaged with the company and our interagency partners regarding the situation. This underscores the threat that ransomware poses to organizations regardless of size or sector," said Eric Goldstein, executive assistant director of the cybersecurity division at CISA.

Colonial did not give further details or say how long its pipelines would be shut.

The privately held, Georgia-based company is owned by CDPQ Colonial Partners L.P., IFM (US) Colonial Pipeline 2 LLC, KKR-Keats Pipeline Investors L.P., Koch Capital Investments Company LLC and Shell Midstream Operating LLC.

"Cybersecurity vulnerabilities have become a systemic issue," said Algirde Pipikaite, cyber strategy lead at the World Economic Forum's Centre for Cybersecurity.

"Unless cybersecurity measures are embedded in a technology's development phase, we are likely to see more frequent attacks on industrial systems like oil and gas pipelines or water treatment plants," Pipikaite added.



Pump price worries

The American Automobile Association said a prolonged outage of the line could trigger increases in gas prices at the pumps, a worry for consumers ahead of summer driving season.

A shutdown lasting four or five days, for example, could lead to sporadic outages at fuel terminals along the U.S. East Coast that depend on the pipeline for deliveries, said Andrew Lipow, president of consultancy Lipow Oil Associates.

After the shutdown was first reported on Friday, gasoline futures on the New York Mercantile Exchange gained 0.6% while diesel futures rose 1.1%, both outpacing gains in crude oil.

Gulf Coast cash prices for gasoline and diesel edged lower on prospects that supplies could accumulate in the region.

"As every day goes by, it becomes a greater and greater impact on Gulf Coast oil refining," said Lipow. "Refiners would have to react by reducing crude processing because they've lost part of the distribution system."

Oil refining companies contacted by Reuters on Saturday said their operations had not yet been impacted.

Kinder Morgan Inc (KMI.N), meanwhile, said its Products (SE) Pipe Line Corporation (PPL) serving many of the same regions remains in full service.

PPL is currently working with customers to accommodate additional barrels during Colonial's downtime, it said. PPL can deliver about 720,000 bpd of fuel through its pipeline network from Louisiana to the Washington, D.C., area.

The American Petroleum Institute, a top oil industry trade group, said it was monitoring the situation.

Ben Sasse, a Republican senator from Nebraska and a member of the Senate Select Committee on Intelligence, said the cyberattack was a wakeup call for U.S. lawmakers.

"This is a play that will be run again, and we're not adequately prepared," he said, adding Congress should pass an infrastructure plan that hardens sectors against these attacks.

Colonial previously shut down its gasoline and distillate lines during Hurricane Harvey, which hit the Gulf Coast in 2017. That contributed to tight supplies and gasoline price rises in the United States after the hurricane forced many Gulf refineries to shut down.

Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom

Source: https://finance.yahoo.com/news/colonial-pipeline-paid-hackers-nearly-141548661.html

May 14 – Colonial Pipeline Co. paid nearly $5 million to Eastern European hackers on Friday, contradicting reports earlier this week that the company had no intention of paying an extortion fee to help restore the country's largest fuel pipeline, according to two people familiar with the transaction.The company paid the hefty ransom in difficult-to-trace cryptocurrency within hours after the attack, underscoring the immense pressure faced by the Georgia-based operator to get gasoline and jet fuel flowing again to major cities along the Eastern Seaboard, those people said. A third person familiar with the situation said U.S. government officials are aware that Colonial made the payment.

Once they received the payment, the hackers provided the operator with a decrypting tool to restore its disabled computer network. The tool was so slow that the company continued using its own backups to help restore the system, one of the people familiar with the company's efforts said.

A representative from Colonial declined to comment. Colonial said it began to resume fuel shipments around 5 p.m. Eastern time Wednesday.

When Bloomberg News asked President Joe Biden if he was briefed on the company's ransom payment, the president paused, then said: "I have no comment on that."

The hackers, which the FBI said are linked to a group called DarkSide, specialize in digital extortion and are believed to be located in Russia or Eastern Europe.

On Wednesday, media outlets including the Washington Post and Reuters, also based on anonymous sources, reported that the company had no immediate intention of paying the ransom.

Ransomware is a type of malware that locks up a victim's files, which the attackers promise to unlock for a payment. More recently, some ransomware groups have also stolen victims' data and threatened to release it unless paid -- a kind of double extortion.

The FBI discourages organizations from paying ransom to hackers, saying there is no guarantee they will follow through on promises to unlock files. It also provides incentive to other would-be hackers, the agency says.

However, Anne Neuberger, the White House's top cybersecurity official, pointedly declined to say whether companies should pay cyber ransoms at a briefing earlier this week. "We recognize, though, that companies are often in a difficult position if their data is encrypted and they do not have backups and cannot recover the data," she told reporters Monday.

Such guidance provides a quandary for victims who have to weigh the risks of not paying with the costs of lost or exposed records. The reality is that many choose to pay, in part because the costs may be covered if they have cyber-insurance policies.

"They had to pay," said Ondrej Krehel, chief executive officer and founder of digital forensics firm LIFARS and a former cyber expert at Loews Corp., which owns Boardwalk Pipeline. "This is a cyber cancer. You want to die or you want to live? It's not a situation where you can wait."

Krehel said a $5 million ransom for a pipeline was "very low." "Ransom is usually around $25 million to $35 million for such a company. I think the threat actor realized they stepped on the wrong company and triggered a massive government response," he said.

A report released last month by a ransomware task force said the amount paid by victims increased by 311% in 2020, reaching about $350 million in cryptocurrency. The average ransom paid by organizations in 2020 was $312,493, according to report.

Colonial, which operates the largest fuel pipeline in the U.S., became aware of the hack around May 7 and shut down its operations, which led to fuel shortages and lines at gas stations along the East Coast.

Cybersecurity Executive Order Includes New Contractor Requirements, FedRAMP Overhaul

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/cybersecurity-executive-order-includes-new-contractor-requirements-fedramp-overhaul/

May 13 – President Biden signed an executive order Wednesday outlining actions to strengthen cybersecurity including requiring baseline security standards in software purchased by the government and requiring compromised companies that contract with the federal government to report breaches for the benefit of others potentially vulnerable in government or industry.

A senior administration official told reporters on a call shortly before the White House announced the order that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency would be leading the effort to define the details of reporting requirements, which would be on a sliding time scale based on the severity of the incident with the most severe cyber incidents needing to be reported within three days. Within 60 days, the Office of Management and Budget, Defense Department, Justice Department, Office of the Director of National Intelligence, and DHS will review and recommend updates to IT and OT contract requirements.

"Companies need to share information about the incident: the vulnerability, what occurred," the official said. "We're really focused on information that's important to be used to get out information to better help other entities defend themselves."

The order, which has been in the works since the second week of the Biden administration, says the contract update recommendations would ensure "service providers collect and preserve data, information, and reporting relevant to cybersecurity event prevention, detection, response, and investigation on all information systems over which they have control, including systems operated on behalf of agencies, consistent with agencies' requirements," share incident data "relevant to any agency with which they have contracted" with that agency, work with federal investigators, and "share cyber threat and incident information with agencies, doing so, where possible, in industry-recognized formats for incident response and remediation."

Within 120 days, DHS and OMB should "take appropriate steps to ensure to the greatest extent possible that service providers share data with agencies, CISA, and the FBI as may be necessary for the Federal Government to respond to cyber threats, incidents, and risks."

"It's hard to learn from each incident and ensure that, broadly, government and companies have information to protect themselves," the official said. "So we've pushed the authority as far as we could and said, 'Anybody doing business with the U.S. government will have to share incidents so that we can use that information to protect Americans more broadly.'"

As far as improving its own security posture, the executive order says the federal government "must adopt security best practices; advance toward Zero Trust Architecture; accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS); centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks; and invest in both technology and personnel to match these modernization goals." The head of each agency has 60 days to submit its plan to move toward these goals, and agencies are required to progress in cloud technology "in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents."

DHS and GSA, through FedRAMP, will "develop security principles governing Cloud Service Providers (CSPs) for incorporation into agency modernization efforts." Within 90 days, a federal cloud security strategy will be developed and guidance delivered to agencies. Within

60 days, DHS is expected to deliver a cloud-service governance framework that "shall identify a range of services and protections available to agencies based on incident severity." Agencies have six months to "adopt multi-factor authentication and encryption for data at rest and in transit," or provide "written rationale" why they can't.

GSA will also have to "begin modernizing FedRAMP" with a new training program for agencies, improving standardized communication, incorporating automation throughout the lifecycle, digitizing and streamlining vendor documentation, and instituting relevant compliance frameworks.

To improve software supply chain security, the order directs the National Institute of Standards and Technology to develop guidelines including "criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves, and identify innovative tools or methods to demonstrate conformance with secure practices." The preliminary guidelines are due in six months. A definition of the term "critical software" will be agreed upon by NIST, NSA, DHS, OMB, and ODNI within 45 days, and within the month after that DHS "shall identify and make available to agencies a list of categories of software and software products in use or in the acquisition process meeting the definition of critical software" with security guidelines coming within 60 days after that.

Guidelines will also be issued by NIST within 60 days for recommended "minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing)." NIST will also spearhead initiatives to educate the public on the security capabilities of Internet-of-Things (IoT) devices.

"We're working to bring visibility to the security of software, akin to the way New York brought visibility to cleanliness in New York City restaurants by requiring restaurants to post simple ratings like A, B, C, or D regarding the cleanliness in their windows," the senior administration official said. "Visibility matters."

Homeland Security Secretary Alejandro Mayorkas will be responsible for establishing a new Cyber Safety Review Board — with members from the Defense Department, Justice Department, CISA, NSA, FBI, and the private sector (and depending on the incident, OMB) — to review and assess incidents affecting government systems and the private sector, analyzing threat activity, vulnerabilities, mitigation activities, and agency responses. At a minimum, the board would be convened after a cyber incident serious enough to trigger the establishment of a Cyber Unified Coordination Group.

"Recent cybersecurity incidents impacting SolarWinds, Microsoft, and Colonial Pipeline are a stark reminder that malicious cyber activity can significantly disrupt Americans' daily lives and threaten our national security," Mayorkas said in a statement late Wednesday on the executive order. "Addressing these risks to our way of life is a shared responsibility that depends upon close collaboration between the public and private sectors."

In addition to establishment of the cyber review board, he said, the executive order "will empower DHS and our interagency partners to modernize federal cybersecurity, expand information-sharing, and dramatically improve our ability to prevent, detect, assess, and remediate cyber incidents. We look forward to taking immediate steps to implement this Executive Order to help federal government agencies improve their security posture by modernizing programs and systems, developing a standard playbook for incident response."

The order states that DHS "shall develop a standard set of operational procedures (playbook) to be used in planning and conducting a cybersecurity vulnerability and incident response activity respecting FCEB Information Systems," with guidance to agencies distributed later by OMB. The playbook will include "a requirement that the Director of CISA review and validate FCEB Agencies' incident response and remediation results upon an agency's completion of its incident response."

To increase "visibility into and detection of cybersecurity vulnerabilities and threats to agency networks," the executive order calls for an Endpoint Detection and Response (EDR) initiative "to support proactive detection of cybersecurity incidents within Federal Government infrastructure, active cyber hunting, containment and remediation, and incident response." The order also includes provisions to improve agency collection and maintenance of data on cyber incidents "for both investigation and remediation purposes."

CISA Acting Director Brandon Wales called the order "an important step forward in bolstering our nation's cybersecurity" and stressed that his agency "serves a central role in implementing this executive order."

"This executive order will bolster our efforts to secure the federal government's networks, including by enabling greater visibility into cybersecurity threats, advancing incident response capabilities, and driving improvements in security practices for key information technology used by federal agencies. And because the federal government must lead by example, the executive order will catalyze progress in adopting leading security practices like zero-trust architectures and secure cloud environments," Wales said.

"The cybersecurity landscape is constantly changing, and this executive order reflects the need for a sustained commitment and urgent progress," he added. "We are now moving forward with this same commitment and urgency to implement the president's executive order to defend against the threats of today and secure against the risks of tomorrow."

The senior administration official told reporters that those drafting the order looked at recent cyber incidents but asked more broadly, "What are the foundational reasons why incidents occur?"

"So, as we looked, for example, at SolarWinds, you know, we saw the way the SVR compromised SolarWinds in the way they built software. And we said, fundamentally, building software, like building a building, must be done with standards on networks that are segregated, where users have to use multi-factor authentication to log in," the official said.

Rolling out agency standards in a tight timeframe is critical as "the federal government needs to be a leader in this space," the official said.

"We worked hard to find the best way to set aggressive and achievable efforts within what could be achieved in an executive order, and really to pilot all of these different efforts that have been discussed for a while, and to use the power of federal procurement to say, 'If you're doing business with us, we need you to practice really good — really good — cybersecurity. And, most importantly, we really need you to focus on secure software development.' Right?"

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill.*

Gaming – Now as Terrorism Threat

Source: https://i-hls.com/archives/108623

May 20 – A new domestic terrorism threat has been evident in the US, a report warns. Gamification, in which violent extremists liken attacks to video games and try to achieve a high score or kill count, will likely "continue to inspire future plots" along with the societal-collapse ideology of accelerationism, said a joint domestic terrorism report to Congress from the FBI and Department of Homeland Security.

The threat posed by international and domestic threat actors has evolved significantly since 9/11. "The greatest terrorism threat to the Homeland we face today is posed by lone offenders, often radicalized online, who look to attack soft targets with easily accessible weapons," the report said. "Many of these violent extremists are motivated and inspired by a mix of socio-political goals and personal grievances against their targets."

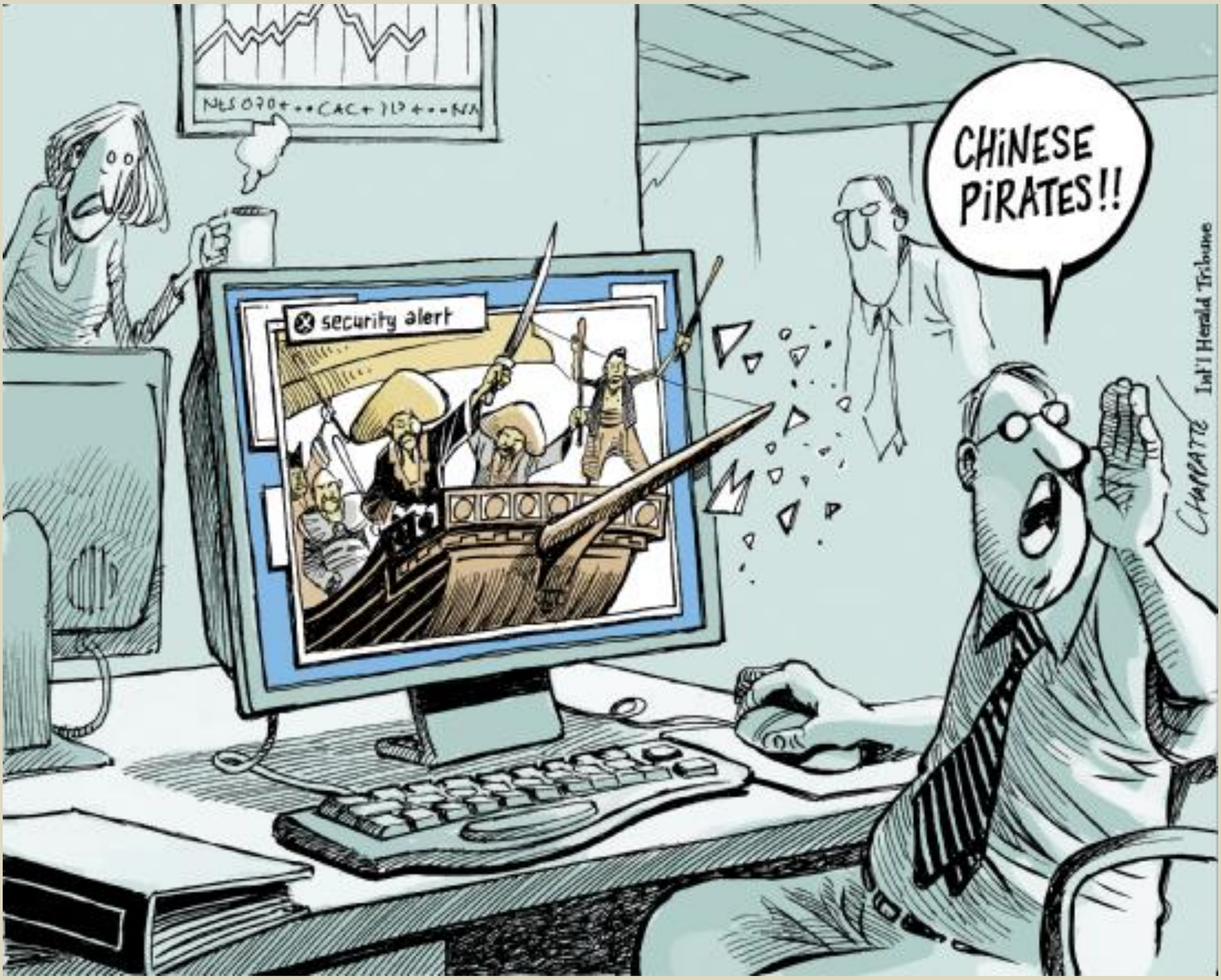
"Our agencies had high confidence in this assessment based on the demonstrated capability of radically/ethnically motivated violent extremists (RMVEs) in 2019 to select weapons and targets to conduct attacks, and the effectiveness of online RMVE messaging calling for increased violence," the report stated.

"Additionally, other domestic violent extremists (DVEs) likely would continue to engage in non-lethal violence and other criminal activity, and DVE reactions to socio-political events and conditions could increase attacks.

”Five domestic violent extremist attacks in 2019 resulted in 32 deaths. White supremacists inflicted the attacks that caused 24 of those deaths.“Themes like ‘gamification’ and ‘accelerationism’ partly inspired some of the attacks in 2019 and likely will continue to inspire future plots,” the report said.

Messaging from RMVEs espousing the superiority of the white race has furthered this narrative by framing previous attacks as resulting in a ‘score.’ Additionally, widely disseminated propaganda on online forums and encrypted chat applications that espouse similar themes regarding kill counts could inspire future attackers to mobilize faster or attempt increasingly lethal and more sophisticated attacks.

”Both the FBI and DHS assessed DVEs “likely would continue to focus on attacking soft targets and use gamification to encourage higher fatality attacks,” as hstoday.us reports.



ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

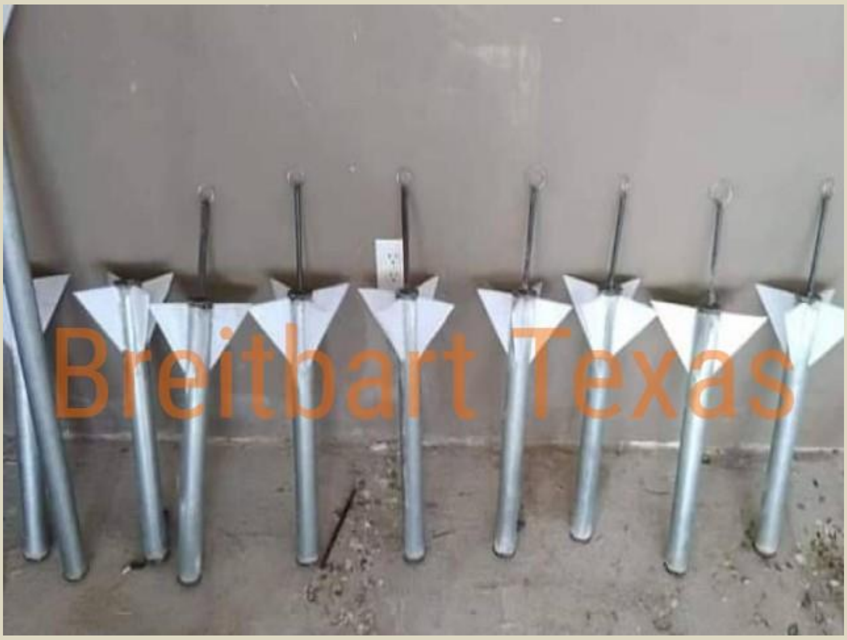
Mexican Cartels Weaponize Drones to Drop IEDs

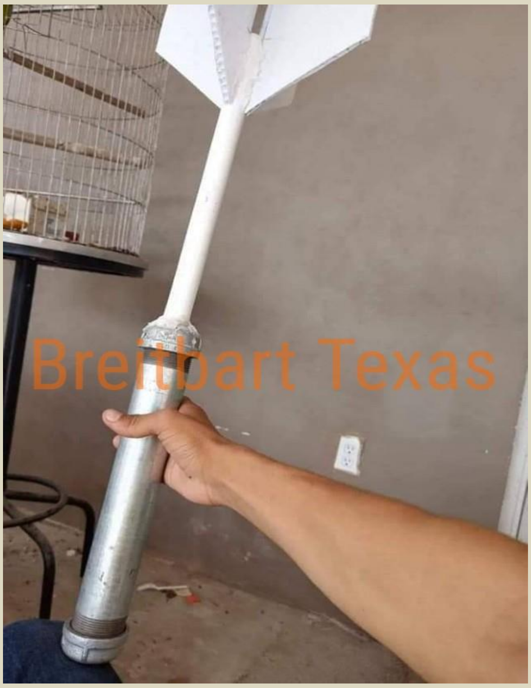
Source: https://www.breitbart.com/border/2021/04/25/exclusive-photos-cartels-in-mexico-weaponized-drones-to-drop-ieds/

Apr 25 – Drug cartels fighting a fierce turf war in western Mexico began weaponizing commercial drones by turning them into delivery systems for improvised explosive devices (IEDs). Breitbart Texas obtained exclusive photographs of the explosives devices and the methods used by cartel operators.

This week, Mexican authorities confirmed that two police officers in Michoacán were injured by an attack from cartel gunmen who used commercial drones to drop IEDs, Breitbart Texas reported. The attack came after state police officers removed a series of roadblocks aimed at keeping rival cartels from using armored SUVs to carry out attacks in their attempts to take control.

While various news outlets in Mexico claimed that Cartel Jalisco Nueva Generacion (CJNG) instigated the attack, law enforcement sources in Michoacán revealed to Breitbart Texas that authorities believe an alliance known as Carteles Unidos were actually the ones behind the drone attacks. That criminal organization is made up of smaller regional cartels including Los Viagras, various self-defense groups, and remnants of La Familia Michoacana who are openly fighting off an invasion from CJNG. Carteles Unidos claims to have financial and manpower support from CJNG's archrival — the Sinaloa Cartel. For several weeks, rival cartels carried out a series of fierce clashes where they used makeshift armored vehicles, explosives, and high-powered weapons. Mexico's government is largely unable to do anything to address the raging violence that has been ongoing for weeks.





Breitbart Texas obtained a series of photographs showing members of Carteles Unidos making and testing a series of IEDs. The devices appear to be made out of pipes shaped like a mortar round. Those IEDs are then attached to commercial drones and then dropped from the air.

Information obtained exclusively by Breitbart Texas revealed that the operator behind the development of the weaponized drones claims to have had U.S. military training. However, Breitbart Texas was not able to confirm the claim.

Countering Iran's Growing Drone Threat

By Seth J. Frantzman

Source: https://www.meforum.org/62252/iran-growing-drone-threat

Apr 27 – Earlier this month, pro-Iranian groups used a drone to strike against U.S. forces in Iraq for the first time. It was just the latest in a series of attacks carried out against American troops in the country, many of which have involved volleys of small rockets. And it highlighted the growing threat of Iranian drone attacks in the Middle East.

The drone threat is setting off alarms at the Pentagon. General Kenneth McKenzie, who leads the U.S. Central Command, told the House Armed Services Committee on April 20 that "for the first time since the Korean War, we are operating without complete air superiority." Central Command, which deals with the increasing threat of drone attacks from countries such as Iran and terrorist groups such as ISIS, argues that better air defense is needed to track and thwart such attacks.

An Iranian drone launches during a large-scale combat exercise in Semnan, Iran, on January 6, 2021. (WANA/Reuters)

Iran is rapidly becoming a drone power in the Middle East. Tehran has transferred drones to Yemen for many years, increasing their range and effectiveness in the war that Iranian-backed Houthi rebels are waging against Saudi Arabia. Iran also used a drone against Israel in 2018 and has used them to harass U.S. ships in the Persian Gulf and even photograph an American aircraft carrier. The bad news is that Iran's drones are getting more deadly, and their range is increasing: Some of them carry warheads, and Iran says they can travel up to 2,000 kilometers. The good news is that people are waking up to the threat, and U.S. allies such Israel are developing new air-defense systems, including lasers, to combat it.

How did we get to the point where adversaries of the U.S. are fielding unmanned aircraft that can threaten the wealthiest, most powerful military in the world? In the 1990s and early 2000s, sophisticated drones were a closely guarded secret of U.S. spy agencies and the Air Force. But in recent years, America's adversaries — including China, Iran, Russia, and others — have developed large military drones. Some of these are called "kamikaze drones," because they are designed with a warhead built into them and they fly into their targets. Iran used such drones against Saudi Arabia in 2019, targeting the world's largest facility for crude-oil production and stabilization. They are pre-programmed and fly to a target. They can evade radar and air defenses if their programmers can get them to fly low enough or find a way to hide them.

The U.S. military knows that it needs to develop an "integrated system" to defend against drones. America's government and its defense industry already work closely with Israel on air-defense systems such as Israel's Iron Dome. The U.S. Army has acquired two batteries of the Israeli system over the past year. But the challenge is deploying systems at U.S. bases and facilities and preparing for future threats.

The U.S. needs to be more agile in adopting new technologies and working with allies such as Israel on new defenses to counter-drone attacks. Military procurement moves slowly, but the threat posed by Iran's drones is growing rapidly. Iran invests in drones, cruise missiles, precision-guided munitions, and ballistic missiles because it can easily traffic these systems to terror groups such as Hezbollah while avoiding blame for the mayhem they cause. And that, in turn, means investment in defenses is only part of the puzzle; intercepting Iranian intelligence is also important, so we can ascertain its smuggling routes.

In the larger picture, this isn't just about the threat posed by Iran's drones in the Middle East. Our other adversaries aren't blind. They can see the pressure Iran has been able to put on us and our allies by investing in drones, and they're already following suit. China, for instance, is rapidly building a drone army and has exported its drones to U.S. partners such as Saudi Arabia. If we are to maintain our edge in the geopolitical conflicts to come, we must make a concerted effort to invest in drone-defense systems that can counter the threat.

***Seth J. Frantzman** is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at The Jerusalem Post.*

Tracking Drones in Urban Settings

Source: http://www.homelandsecuritynewswire.com/dr20210513-tracking-drones-in-urban-settings

May 13 – Look, up in the sky! It's a bird! It's a plane! It's…actually pretty easy for radar to tell the difference. Flying aliens from Krypton notwithstanding, there are simply not many things moving through the mostly empty, wide-open skies that are as big and fast as an airplane.

But if radar signals move down from the clouds and into a city's streets, there are suddenly many objects that can be mistaken for one another. With only distance, speed and direction to go on, drones can easily be "hidden in plain sight" on radar displays among slowly moving cars, bicyclists, a person jogging or even the spinning blades of an air conditioning unit.

As drones become more popular and more worrisome from a security standpoint, many projects have sought to engineer systems to spot them. During his time as a Defense Advanced Research Projects Agency (DARPA) program manager, Jeffrey Krolik, professor of electrical and computer engineering at Duke University, launched one such project called "Aerial Dragnet." Using a network of drones hovering above a cityscape or other large, developed area in need of defense, multiple types of sensors would peer down into the city's canyons and pick out any drones. The project has recently successfully concluded with an urban test in Rossyln, Virginia, but challenges remain in discriminating drones from urban "clutter."

Using a fleet of friendly drones to find enemy drones makes sense in a setting for a military unit that is trying to secure a wide urban area. However, in settings where protection of a fixed asset such as an embassy, hospital or encampment is the goal, a system that can maintain a perimeter from a safe stand-off distance is required. Once again funded by DARPA, Krolik is turning to radar, machine learning and specialized hardware to make a drone surveillance system with sufficient range to allow drones to be detected and stopped before they reach a protected area in a city.

"Systems exist that can detect the signals used to control off-the-shelf drones, but they tend to be pretty expensive and there are already commercial drones that can be flown autonomously without any radio control at all," said Krolik. "We need detection systems that can spot these things wherever and whenever they're airborne, regardless of how they're being controlled."

While a computer can be trained to visually spot a drone, an optical system would have a very limited range. A telescopic lens could be used, but then its field of view would be greatly constrained. Instead, Krolik is turning to the same technology that turned the tide against aerial enemies in World War II—radar. But the 1940s technology is getting a 2020s upgrade with the help of a type of machine learning called Deep Neural Networks (DNN).

Teaching Radar Street Smarts

Krolik's idea is to set up a radar antenna to scan the area of urban landscape under surveillance. Over the course of a few days or weeks, in the absence of drones, the DNN trains itself to differentiate between cars, bicycles, people and other objects by learning their kinematics, seen as "micro-Doppler" in the radar returns, as well as the paths they take moving through the space.

"Most systems are designed in a laboratory to be taken out into the field," said Krolik. "This one learns from its environment, because most of the time a drone isn't there."

For example, cars generally follow paths defined by roadways. And while bicycles and pedestrians have more variable dynamics, their micro-Doppler signatures are very distinctive. Over time, the algorithm learns what radar signals are normal for a given space so that when a drone flies by, with propeller motion and trajectory that is very different to what is normally found in the area, it will trip an alarm.

So far, it's working. On Duke's campus, the system has been able to successfully classify drones versus cyclists, pedestrians, cars and other objects 98 percent of the time.

To be clear, Krolik and his team aren't flying drones across campus at all hours of the day and night. Instead, they train the algorithm to learn the normal traffic around the Science Drive parking garage and separately collect data from a drone flying in Duke Forrest. They then put the data together computationally and let the DNN go to work on the resulting mashup.

Hardwiring a Neural Network

For help with the drone-spotting DNN algorithm, Krolik turned to Helen Li, the Clare Boothe Luce Professor of Electrical and Computer Engineering at Duke. DNNs essentially work by sliding a window over an image in a grid-like fashion, determining which feature is present in each window, and passing that information on to a new layer of data. The process repeats itself until the image is distilled into its most basic features that allow the program to categorize it.

DNNs are inevitably computationally dense programs that can tie up a traditional CPU for far longer than a drone surveillance system would require. The algorithm, however, can be sped up by breaking the tasks into pieces that can be processed simultaneously. A common choice for hardware to tackle this challenge are Graphics Processing Units (GPUs), which are specialized processors originally designed to accelerate graphics rendering that is also useful for machine learning, video editing and gaming applications.

But anyone who has ever compiled an hour-long video or lost track of time gaming knows that GPUs produce a lot of heat by consuming a lot of power. To make their drone detection system more efficient, Li instead turned to Field Programmable Gate Arrays (FPGAs).

"While a GPU is super powerful, it's also wasteful," said Li. "We can instead make an application-specific design that is just right for radar signal processing."

As the name implies, FPGAs can be designed and redesigned to process certain tasks more efficiently by hardwiring some of the computation into the device itself. This allows computer scientists to be surgical with how much computational power to provide each aspect of the algorithm.

“An FPGA can be optimized for a specific neural network model without having to support any other models in different configurations and sizes,” continues Li, who helped start the trend of using FPGAs for machine learning applications. “And where typical codes first have to go through an operating system and compilers before reaching the hardware, our approach essentially implements the DNN algorithm directly on the FPGA boards.”

Setting the Bar High

The result is a system that not only spots drones with 98 percent accuracy, but a system that also consumes 100 times less energy than a similar GPU-based system would, all while maintaining the performance and speed required to work in real-time.

Krolik and Li think the results so far are promising, and DARPA thinks so too. After completing the first half-million-dollar phase of the project and presenting their results, the project was funded for a second half-million-dollar grant over nine months. Their challenge over that extended period of time?

Birds.

“As it turns out, when you’re only looking at the speed and bearing of a flying object, a bird can look a lot like a drone,” said Krolik. “With the help of staff at the Duke Gardens, we’ve been collecting radar data on a wide variety of birds around the garden’s duck pond. So far, our DNN algorithm has been able to differentiate birds from drones with over 97 percent accuracy. Now we have to put it all together to detect drones versus birds, cars and pedestrians in a truly urban setting. It’s been a lot of fun working with Helen and the rest of the team, and we have the rest of the summer to figure it out.”

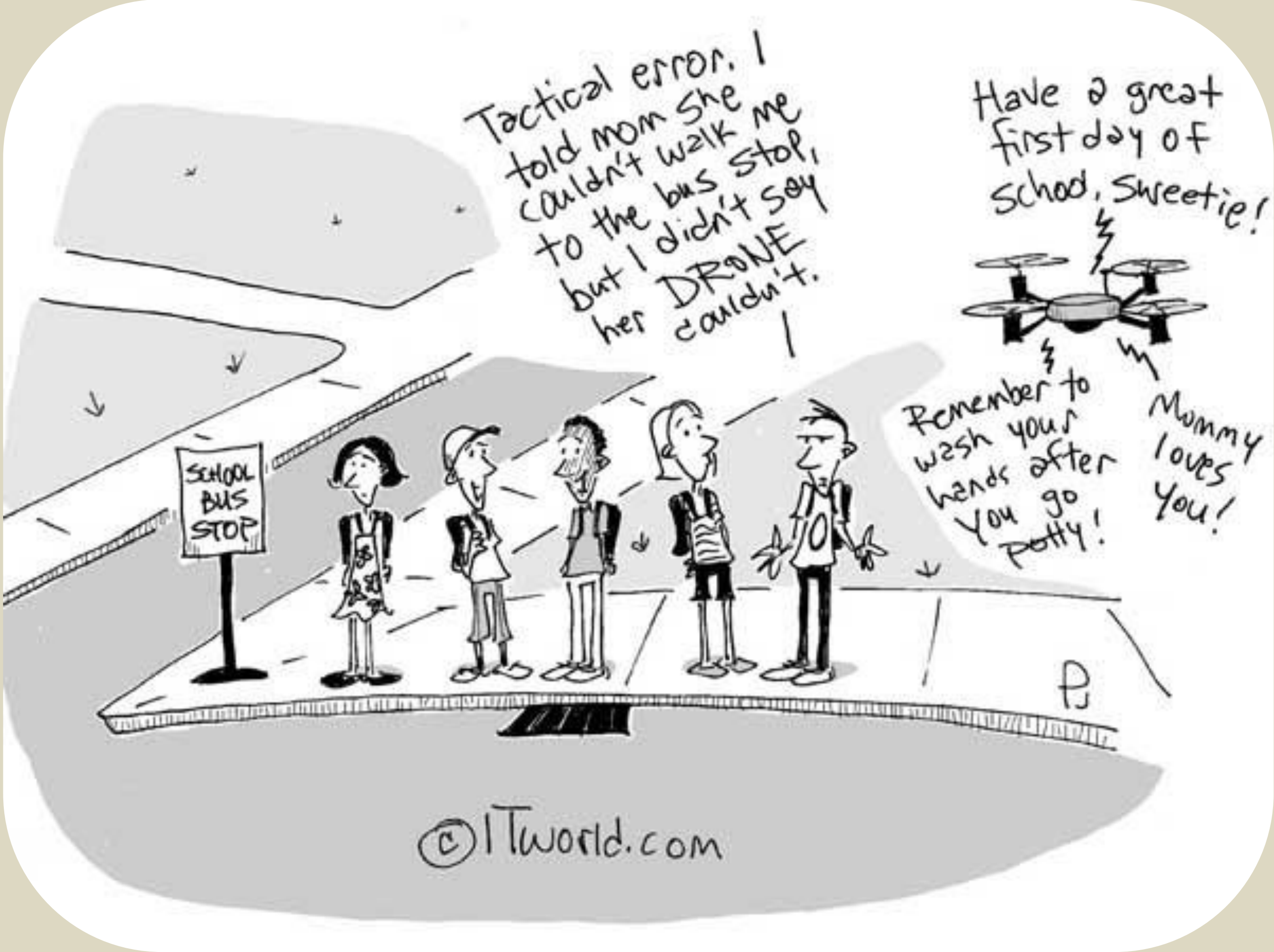
Drones used to inspect Tokyo’s subway tunnels

Source: https://dronedj.com/2020/02/27/drones-inspect-tokyo-subway-tunnels/

Drones demonstrated their usefulness during a recent Tokyo Metro Co. demonstration, showing reporters how it’s utilizing drones to improve tunnel safety. The inspection drones were flown at the Koto Ward facility in Tokyo and have been using drones since the 6th of February to inspect tunnels.

The drone takes on a similar appearance to Flyability’s Elios 2 inspection drone with a cage surrounding it along with a camera, and a bright LED light attached to it. The drone has a diameter of 22 cm, weighs 1.15 kg and can fly for up to five minutes at up to a height of 50 meters.

Tokyo Metro Co. has implemented drones to complete inspections in an effort to improve tunnel safety and to reduce the need for scaffolding and heavy equipment. Both are currently used when inspecting the almost 200 km of tunnels that run under Tokyo.
During the demonstration, an employee flew the drone in a 5.5-meter high training tunnel with a video feed being sent to a monitor where other workers are inspecting the footage for any defects in the tunnel. The drone also takes photos for later inspection and if anything of concern was found by the drone.
The company plans to roll out drone inspections throughout the whole tunnel network in the next few years, with the Marunouchi line being added to the list before the end of the year. Tokyo Metro Co. told The Japanese News, “We want to use drones to do more for safety.”


Tactical error. I told mom she couldn't walk me to the bus stop, but I didn't say her DRONE couldn't.
Have a great first day of school, sweetie!
Remember to wash your hands after you go potty!
Mommy loves you!
SCHOOL BUS STOP
PJ
©ITworld.com

EMERGENCY RESPONSE

ASPR CBRNE Science

Source: https://www.phe.gov/about/aspr/Pages/CBRNE-Science.aspx

The use of chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) devices has the potential to cause mass casualties and high levels of destruction. When preparing for or responding to emergencies involving CBRNE agents, it is critical for medical personnel and other responders to have immediate access to the best available information and resources.

ASPR[1] CBRNE Science is an innovative means to bringing experiential, evidence-basis, and science and medicine to preparedness and response to CBRNE incidents. CBRNE Science brings together experts that understand both the science and operations to provide leadership decision support, operational guidance, and emergency management support. CBRNE Science employs an incubator approach that utilizes small teams, working groups, and task groups on a day-to-day basis to collaboratively inform CBRNE response solutions and, as needed, actual response activities and leadership decisions.

This approach has led to the development of guidance and resources; better understanding of response capabilities; and enhanced domestic and global preparedness through education, information, and expert support. In response to an accidental or intentional CBRNE incident domestically or internationally, CBRNE Science provides coordinated strategic, technical, and operational leadership, advice, and guidance for all levels of the medical response regarding medical and public health impacts and interventions.

Mission

Improve overall of public health emergency preparedness by:

- Providing medical and health-related CBRNE subject matter and operational expertise across the spectrum of ASPR preparedness and response;
- Recognizing, anticipating and evaluating gaps in the Nation’s medical and public health response systems; and
- Working through cooperative professional interactions to develop innovative, evidence-based interventions that strengthen the Nation’s medical and public health emergency response.

Vision

The nation’s health and response systems and communities will be prepared, responsive and resilient to limit the adverse health impacts of CBRNE emergencies.

What We Do

- **Expertise and Collaboration** – CBRNE Science coordinates SMEs and provides a unique linkage and node for technical and operational expertise to inform the activities of ASPR and other partner efforts. Experts also participate in exercises, deployments, and other response activities.
- **Resources and Guidance** – By applying evidence-based decision making to preparedness planning, the CBRNE Science develops innovative, novel approaches and guidance to improve understanding of the best ways to prepare for, respond to and recover from a CBRNE incident. The goal is to ensure that the best science is incorporated to develop feasible, multi-use, collaborative resources and guidance.
- **Implementation and Outreach** – To enhance national preparedness, CBRNE Science utilizes a strategic approach and tools for outreach, integration, and implementation of the plans, concepts, guidance, and resources. This approach is integrated with the ASPR Regional Emergency Coordinator (REC) program and the requirements of partners, and stakeholders. CBRNE Science is also the ASPR focal point for such operational capabilities as the Radiation Injury Treatment Network (RITN).

Select Initiatives

- Developed web-based tools and guidelines to enhance national preparedness and just-in-time response
  - Radiation Emergency Medical Management (REMM)
  - Chemical Emergency Medical Management (CHEMM)
  - State and Local Planners Playbook for Medical Response to a Nuclear Detonation

[1] Assistant Secretary for Preparedness and Response

FEMA Announces Operational Guidance for Disaster Response and Recovery in Pandemic Environment

Source: https://www.hstoday.us/subject-matter-areas/emergency-preparedness/fema-announces-operational-guidance-for-disaster-response-and-recovery-in-pandemic-environment/

May 19 – For the second year in a row, FEMA is prepared to respond to disasters as the nation continues to recover from the COVID-19 pandemic.

FEMA released the "COVID-19 Pandemic Operational Guidance: All-Hazards Incident Response and Recovery," a document aimed at helping emergency managers plan for disaster response and recovery, while adhering to public health guidelines to prevent the spread of COVID-19.

For more than a year, the emergency management community has been operating in a pandemic environment, and FEMA has emphasized the importance of all state, local, tribal and territorial (SLTT) governments applying lessons learned from 2020, as they prepare for operations in 2021. To aid in that effort, this document serves as a tool for governments, outlining not only guidance based on lessons learned and best practices, but also guidance related to new priorities that have arisen in recent months. This document builds upon the guidance released last year and:

- Describes continued challenges to disaster operations posed by COVID-19 and planning considerations, based on science and the best available data, for emergency managers in addressing those challenges.
- Outlines considerations for SLTT governments related to planning COVID-19 testing and vaccination operations. This includes an overview of how FEMA supports SLTTs to establish and operate testing facilities and vaccination sites that ensure fair and equitable distribution of vaccines to all individuals who want one.
- Provides updated resources (e.g., checklists, reports, and other guidance) reflecting current lessons learned and best practices for operating in a pandemic environment to enable emergency managers to best adapt response and recovery plans.
- Outlines how FEMA plans to continue adapting response and recovery operations to the evolving COVID-19 risks to ensure prioritization for life safety, life sustainment, workforce protection and to maintain the delivery of FEMA's programs.

FEMA is offering a series of webinars throughout the month of June to further educate people on the pandemic operational guidance:

- Webinar 1 – 10 a.m. ET, Thursday, June 3.
- Webinar 2 – 3 p.m. ET, Tuesday, June 8.
- Webinar 3 – 11 a.m. ET, Thursday, June 10.
- Webinar 4 – 7 p.m. ET, Wednesday, June 16.
- Webinar 5 – 1 p.m. ET, Thursday, June 17.

FEMA will continue operating under the framework of locally executed, state/tribal managed and federal supported incident response. By creating a shared understanding of expectations among FEMA and state, local, tribal and territorial partners, the nation will be better positioned to achieve operational outcomes in disaster response and recovery efforts.

▶▶ Read more at FEMA