C²BRNE DIARY

Dedicated to Global First Responders

January 2022

01\22

PART B

Hope

is the only thing stronger than fear

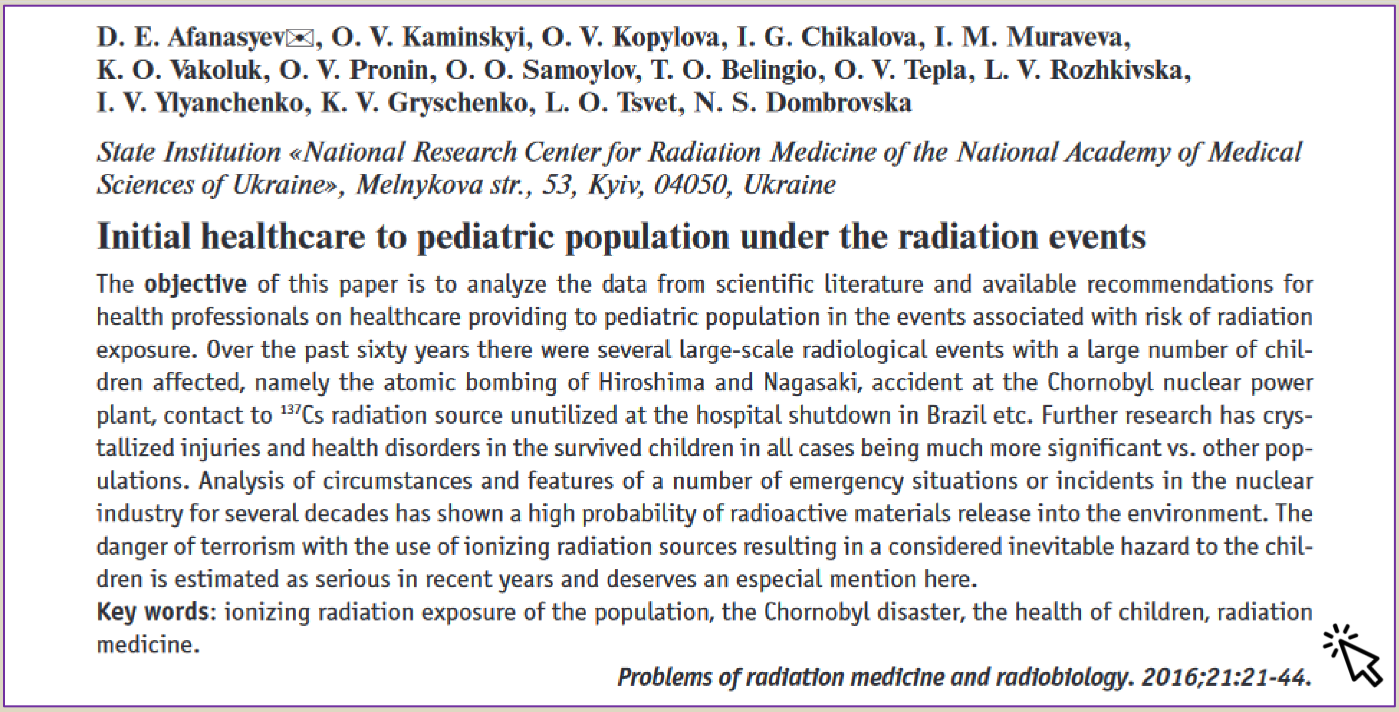
www.cbrne-terrorism-newsletter.com

International CBRNE Institute

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DIRTY R-NEWS



D. E. Afanasyev✉, O. V. Kaminskyi, O. V. Kopylova, I. G. Chikalova, I. M. Muraveva, K. O. Vakoluk, O. V. Pronin, O. O. Samoylov, T. O. Belingio, O. V. Tepla, L. V. Rozhkivska, I. V. Ylyanchenko, K. V. Gryschenko, L. O. Tsvet, N. S. Dombrovska

State Institution «National Research Center for Radiation Medicine of the National Academy of Medical Sciences of Ukraine», Melnykova str., 53, Kyiv, 04050, Ukraine

Initial healthcare to pediatric population under the radiation events

The **objective** of this paper is to analyze the data from scientific literature and available recommendations for health professionals on healthcare providing to pediatric population in the events associated with risk of radiation exposure. Over the past sixty years there were several large-scale radiological events with a large number of children affected, namely the atomic bombing of Hiroshima and Nagasaki, accident at the Chornobyl nuclear power plant, contact to ^{137}Cs radiation source unutilized at the hospital shutdown in Brazil etc. Further research has crystallized injuries and health disorders in the survived children in all cases being much more significant vs. other populations. Analysis of circumstances and features of a number of emergency situations or incidents in the nuclear industry for several decades has shown a high probability of radioactive materials release into the environment. The danger of terrorism with the use of ionizing radiation sources resulting in a considered inevitable hazard to the children is estimated as serious in recent years and deserves an especial mention here.

Key words: ionizing radiation exposure of the population, the Chornobyl disaster, the health of children, radiation medicine.

Problems of radiation medicine and radiobiology. 2016;21:21-44.

Iran holds air defense drill near Bushehr nuclear plant

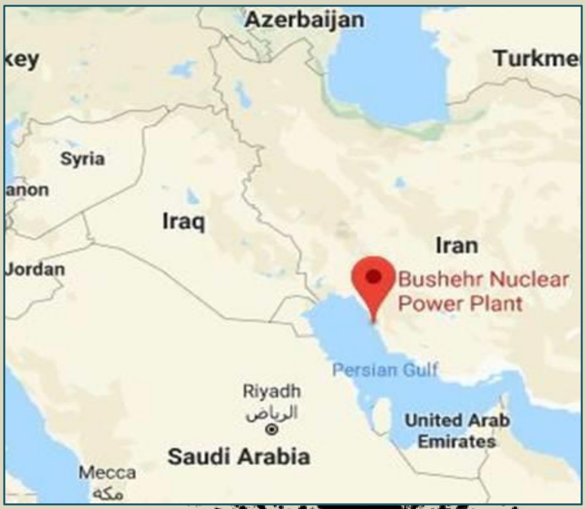
Source: https://www.aljazeera.com/news/2021/12/20/iran-holds-air-defence-drill-over-bushehr-nuclear-plant

Dec 20 – Iran has held an air defence drill in the vicinity of its southwestern Bushehr nuclear power plant amid ongoing tensions over the country's nuclear programme.

State media reported that the drill was conducted in the early hours of Monday to the south of the Bushehr province and also over parts of the Persian Gulf.

The drill comes days after the latest round of talks in Vienna to restore Iran's nuclear deal with world powers which ended with some modest gains but no agreement.

Israel has opposed efforts to revive the 2015 deal, which lifted sanctions on Tehran in exchange for curbs on its nuclear programme and has continued to threaten direct military action against Iranian nuclear facilities.



Nournews, a media outlet close to Iran's security forces, reported last week that security forces assess there may be a credible possibility Israel would launch an attack in an effort to thwart the talks in Vienna.

On Monday, it quoted Gholamali Rashid, the commander of the Islamic Revolutionary Guard Corps' (IRGC) Khatam al-Anbiya military base, as also mentioning the Vienna talks, and adding that any potential Israeli attack would not be possible without the US giving its approval.

"If such threats are implemented, the Islamic Republic's armed forces will mount thrashing attacks against all centres, bases, paths, and spaces used to enable the violation, and against the origins of the violation, based on its trained operational plans," the commander was quoted as saying.

Earlier this month, a loud explosion was heard and the air defence system near Iran's main nuclear facilities in Natanz was activated. State media said at the time the explosion was caused by a missile fired as part of an air defence drill and there was no hostile object.

The Natanz facilities were the target of two main sabotage attacks, which Iran blamed on Israel, in 2020 and 2021. There was also another sabotage attack in June, also blamed on Israel, on a centrifuge parts assembly workshop in Karaj near capital Tehran.

The seventh round of nuclear talks in Vienna between Iran and the world powers party to the accord the US abandoned in 2018 closed with modest progress on Friday. Talks are expected to resume in the coming days before the end of the current year.

Iran and Western powers have so far been at odds in the talks over which sanctions need to be lifted, and what measures Iran needs to take to scale back down its advancing nuclear programme.

Israel's Dimona nuclear reactor isn't Chernobyl, but does have vulnerabilities

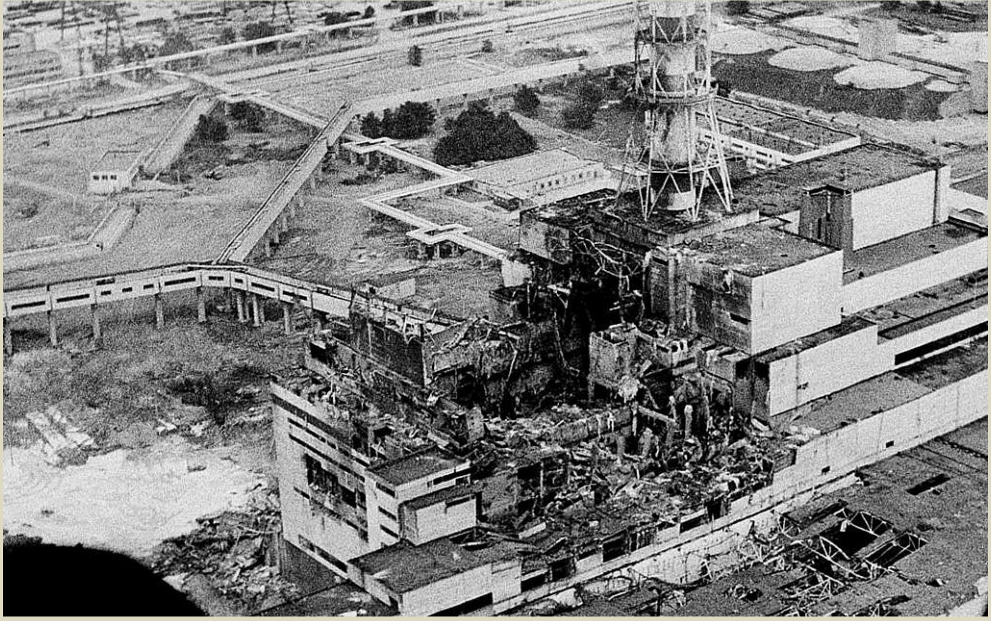
Source: https://www.timesofisrael.com/israels-dimona-nuclear-reactor-isnt-chernobyl-but-does-have-vulnerabilities/

2019 – The hit television miniseries "Chernobyl" has reminded the world of the ever-present specter of a nuclear catastrophe made possible by the deadly combination of negligence, ignorance and incompetence.

On April 26, 1986, one of the four nuclear reactors at Chernobyl suffered a catastrophic power surge during a spectacularly mismanaged safety test. The resulting explosion and fire sent plumes of radioactive isotopes throughout the area, since the power plant lacked a containment structure. Contamination spread through large parts of the Soviet Union and Europe. Estimates put the long-term death toll at anywhere from 4,000 to over 93,000; the 1,000 sq. mile exclusion zone around the reactor remains one of the world's most radioactively contaminated areas.

The Chernobyl disaster is one of two nuclear incidents to receive a level 7 designation on the International Nuclear Event Scale, indicating a major accident with widespread ramifications. The second was the earthquake-sparked 2011 Fukushima nuclear reactor disaster in Japan.

The effects of the reactor explosion are still seen and felt today, inside the exclusion zone and far beyond, with a still unfolding impact on people, wildlife and plants. Notably, hundreds of thousands of so-called liquidators risked their lives and long-term health to contain the radiation after the explosion, including some 1,500 who live in Israel and are woefully neglected by the government.



An aerial view of the Chernobyl nuclear power plant, the site of the world's worst nuclear accident, is seen in April 1986, made two to three days after the explosion in Chernobyl, Ukraine. In front of the chimney is the destroyed 4th reactor. (AP Photo)

Could such a catastrophe occur in Israel's own nuclear reactor, the Shimon Peres Negev Nuclear Research Center outside Dimona, in the south of the country? In a rocket strike on the facility — which Iran, Hezbollah, Palestinian Islamic Jihad, Hamas and Syria have each threatened or attempted to carry out — would large swaths of the Jewish state become contaminated with radioactive material? Or what about in a large earthquake along the Syrian-African rift, which is expected at some point in the coming years?

Fortunately, experts say, the simple answer is no.

Dimona and Chernobyl are of vastly different scales and models, and they serve vastly different functions. As a result, the potential for damage in southern Israel is orders of magnitude smaller even in a worst-case scenario, the experts say.

The same is true of the Soreq Nuclear Research Center outside the central town of Yavne, the core of which is even smaller than Dimona's.

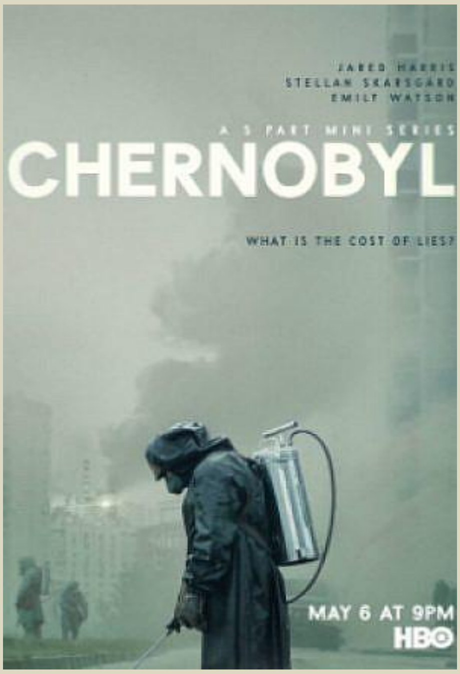
However, there are safety concerns connected to Dimona — namely that its core is aging, and will nevertheless continue to be used as Israel is unlikely to get a new one — and these often go undiscussed in public due to the largely classified nature of the facility, which produces fissile material for nuclear weapons, according to foreign media reports.

Israel is believed by foreign governments and media to be the Middle East's sole nuclear power, but has long refused to confirm or deny that it has nuclear weapons, and officially maintains that the Dimona plant focuses on research and energy provision.

Dimona isn't Chernobyl

The Vladimir Ilyich Lenin Nuclear Power Plant outside Chernobyl supplied 10 percent of the electricity requirements for Ukraine. Its four reactors produced 12,800 megawatts of thermal output and 4,000 megawatts of electricity.

As a result of this high level of energy output, the secondary explosion of its reactor in 1986 was estimated to be similar to that of 10 tons of TNT.



Poster for 'Chernobyl,' the 2019 HBO miniseries. (HBO)

The Shimon Peres Negev Nuclear Research Center, named for the former president who worked for its creation in the 1950s as director-general of the Defense Ministry, comes nowhere close to that level of energy production. The precise thermal output of its far, far smaller nuclear reactor is not known, but has been estimated at between 26 and 150 megawatts — or between 492 and 86 times less than Chernobyl's — according to the Arms Control Association, a US-based nonproliferation group.

(The Soreq facility's core, which was given to Israel by the United States, produces just five megawatts of thermal output.)

This massive difference in size results in a massive difference in the potential for damage.

During the 1967 Six Day War, Israel's air defense batteries shot down an Israeli fighter jet that accidentally strayed too close to Dimona after it was damaged when flying over Jordan

Dimona, unlike Chernobyl, was built with a containment structure meant to prevent radioactive material from escaping in the case of a meltdown or other disaster. A metal-and-concrete structure known as a sarcophagus was constructed around Chernobyl after the fact.

In addition, the Shimon Peres Negev Nuclear Research Center has been under threat almost since its construction, which has necessitated the Israeli government to put its safety (and thus the safety of those living nearby) at a premium.

During the 1967 Six Day War, these air defense batteries shot down an Israeli fighter jet that accidentally strayed too close to the sensitive site after it was damaged when flying over Jordan.

A memorial sign to builders who made the first hastily constructed sarcophagus over the 4th reactor destroyed in the 1986 fatal explosion stands at the Chernobyl nuclear plant, in Chernobyl, Ukraine, Friday, April 20, 2018. A reactor at the Chernobyl nuclear power plant exploded on April 26, 1986, leading to an explosion and the subsequent fire spewed a radioactive plume over much of northern Europe. (AP Photo/Efrem Lukatsky)

The reactor, which was constructed below ground for added protection, is still guarded by a myriad of air defense units, which remain at the highest alert during periods of heightened tensions.

In 2007, amid peak fears of Syrian retaliation after Israel destroyed the country's nuclear reactor, a commander of a Patriot missile defense battery guarding the site told Israeli television that any aircraft that "deviates even slightly from its route, sets off an alarm and risks [an interceptor] missile being fired."

The Dimona core also has in place a series of earthquake protection measures, Eli Abramov, then-deputy director general of the reactor, told US officials in 2007, according to a WikiLeaks document.

In 2018, in rare public remarks, the head of the Israeli Atomic Energy Commission, Ze'ev Snir, said the country had been reinforcing the Dimona nuclear reactor in light of threats made by Iran and Hezbollah.

"We cannot ignore the repeated and explicit threats made by Iran and its proxies to attack Israel's nuclear sites," he said.

"These outrageous threats require Israel to take action and continue to protect and defend its nuclear facilities. These facilities are constantly upgraded and reinforced, in line with IAEA safety guidelines, in order to withstand any attack," Snir said.

The military wing of the Gaza-based Islamic Jihad terror group releases a video threatening rocket attacks on the nuclear reactor in Dimona and other sensitive sites in Israel, May 4, 2019. (Screen grab)

But almost as important as the vastly smaller size of Dimona, and the active and passive defense measures in place around it, is the fact that it is a research reactor, not a power plant.

Electricity-producing nuclear reactors, by their nature, are meant to be cost-effective. Any interruption of their output comes with a tremendous price, both in money lost and in the effect on the surrounding populations that rely on its power, which becomes a factor in deciding whether or not to shut down the reactor.

Not so in Dimona, where all operations can be halted immediately at any sign of trouble, without fear that such a move will cause large portions of Israel to go dark, according to an expert who asked not to be identified.

Modern reactors can also be taken offline rapidly by flooding the reactor with boron, an element that is able to absorb the neutrons released by nuclear fission.

This does not immediately remove all danger, but within minutes it can stop the reactions inside the core and allow the reactor to begin to cool down. The expert compared this to removing a boiling kettle from the stove: The water inside might still be hot, but it is no longer boiling and can start returning to room temperature.

In this Feb. 10, 2016 file photo, a member of the media tour group wearing a protective suit and a mask looks at the No. 3 reactor building at Tokyo Electric Power Co's (TEPCO) tsunami-crippled Fukushima Dai-ichi nuclear power plant in Okuma, Fukushima Prefecture, northeastern Japan. (Toru Hanai/Pool Photo via AP, File)

"A competent operator will, at the first sign of trouble, shut down the reactor," he said.

This could be at the first alert of an incoming rocket or missile from Syria, Iran or Lebanon, an initial indication of seismic activity ahead of an earthquake, or a case of a malfunction in the reactor.

A competent operator will, at the first sign of trouble, shut down the reactor

An emergency shutdown was not immediately performed in Chernobyl, and when it was belatedly executed, the shutdown process proved catastrophically flawed, which was central to the disaster. The reactor — a Soviet RBMK model, which is seen as an inherently dangerous variety — entered a positive feedback loop, generating more power instead of less before it blew.

One of the other main issues following a nuclear accident or an attack is a loss of power to the reactor itself, which prevents operators from controlling the reactions inside.

This caused the 2011 Fukushima disaster in Japan when a tsunami knocked out the generators that fed power to the pumps that moved coolant through the reactor. This led to meltdowns and explosions. Two people were killed in the initial disaster, and six others were exposed to high amounts of radiation. The cleanup is expected to take 30 to 40 years.

Following Fukushima, nuclear reactors began employing backups to their backups — large batteries in addition to fuel-powered generators — in order to ensure that they would always have a supply of electricity in the case of an accident.

The expert said he would not and could not say definitively what methods would be used to shut down Dimona or what backups are in place to provide it with power, but indicated that the above are reasonable assumptions.

What does an attack on Dimona look like?

In 2008, the non-proliferation Arms Control Association simulated a rocket strike on the Dimona nuclear reactor under the guidelines of the US Department of Defense's Hazard Prediction and Assessment Capability (HPAC), a method of estimating the effects of a nuclear disaster.

As many specific details about the Shimon Peres Negev Nuclear Research Center are kept classified and subject to the military censor, this study acknowledges that it is only a rough approximation of the potential damage caused by a rocket attack on the facility.

Soldiers in the IDF Home Front Command perform an exercise simulating an atomic, biological and chemical attack in 2011. (Yuval Haker/Israel Defense Forces)

In addition to the aforementioned unknown thermal output, the ACA's Bennett Ramberg was unable to factor in the "potentially significant contributions that could come from on-site spent fuel and high-level waste from reprocessing or separated plutonium." (In addition to a reactor, the Dimona facility also acts as a storage center for the entire country's nuclear waste.)

According to Ramberg, a successful rocket attack on the reactor — one that manages to get past the site's air defenses and breaches the site's containment dome — would "disperse the heavy water surrounding the reactor core; and create explosions and fire involving the nuclear fuel elements, ejecting radioactive material into a puff carried away from Dimona by prevailing winds."

Counterintuitively, the ACA study found that a more powerful strike on the Dimona nuclear reactor could be a safer one. Such an attack could "so fracture and scatter the reactor core that the absence of concentrated fires would diminish the release" of radioactive material, Ramberg wrote.

The HPAC calculations determined that the deadliest time of year for an attack on the core would be during the month of February, when the seasonal winds would push the radioactive molecules released in an explosion toward the relatively high-population West Bank. There it could cause hundreds to over a thousand cases of cancer among residents of the area, depending upon the reactor's level of thermal output.

According to Ramberg's study, an attack in the summer would send these radioactive clouds away from Israel and toward Jordan's "thinly populated south."

However, as the countries and groups most expected to carry out such an attack would likely not be seeking to harm Jordanians or the mostly Palestinian residents of the West Bank, the ACA article sees late fall as the most likely time for an attack, not the winter or summer.

An attack in November would mean the fall winds would carry the "radioactive plume in a northwesterly direction over the city of Dimona (a community of 30,000 inhabitants) and then toward Beersheba before scattering toward Israel's heavily populated coastal plain housing approximately four million inhabitants," Ramberg wrote in 2008. The population sizes have not dramatically changed in the interim 11 years.

The ACA study found that the largest immediate problems following a successful strike on the Shimon Peres Negev Nuclear Research Center would come in the form of two main radioactive molecules: iodine-131 and cesium-137.

Iodine-131 is a relatively short-lived but highly dangerous radioactive isotope that is produced in nuclear fission by plutonium and uranium. The molecule can collect inside people's thyroid glands, causing cancer as it degrades over the years, making it deadlier for children than for adults, studies have found.

The molecule decays rapidly, making it a serious immediate problem but not a long-lasting one, and its effects can be significantly mitigated by giving those who come in contact with it large doses of a non-radioactive iodine compound, which dilutes the contents of the thyroid and thus minimizes the number of ionizing molecules.

Tablets containing such compounds — known as Lugol's iodine — have already been distributed to residents of Dimona and the towns in the immediate vicinity of the Soreq reactor.

A woman mourns at the Chernobyl victims' memorial in the Ukrainian capital of Kiev on April 26, 2016. (AFP PHOTO / Anatolii Stepanov)

Cesium-137 presents a significantly different challenge. This molecule remains in the environment for a far longer amount of time before it eventually breaks down. It is one of the main radioactive molecules that keeps the so-called "exclusion zone" of Chernobyl contaminated more than 30 years after the disaster.

In a nuclear catastrophe in Dimona, cleaning up this molecule — which can easily mix with groundwater and is readily absorbed by people, animals and plants — would present a significant challenge, requiring large amounts of resources. This radioactive molecule is still being found in marine life around Japan, some eight years after the meltdown at the Fukushima nuclear reactor.

The threat to humans is reduced by the reactor's distance from populated areas. Due to the Dimona core's relatively small size, the contamination would also likely be limited to the area immediately surrounding the reactor.

The Israeli military's Home Front Command also maintains a unit specifically trained in rapidly responding to atomic, biological and chemical disasters.

Rocket attacks aren't the only threat

In addition to the overt threats posed to the Dimona nuclear reactor by terror groups and enemy nations, as well as by earthquakes and other natural disasters, one of the less-discussed concerns surrounding the core is its advancing age and Israel's apparent resolve to keep it running regardless, the expert said.

The Dimona nuclear core, which was given to Israel by France and went active in the early 1960s, is one of the oldest still operating in the world.

Originally designed to operate for 40 years, the core is now being pushed to remain in service for twice that, according to the expert. This is not from frugality or unwillingness on Israel's part to purchase a new core, but a legal inability or disinclination by the countries that produce these cores to sell one to the Jewish state, as Jerusalem refuses to sign the Treaty on the Non-Proliferation of Nuclear Weapons, which is meant to prevent the spread of nuclear weapons.

As a result of Israel's inability to replace the nuclear core, it is motivated to keep it in service for as long as possible, the atomic expert said, replacing and upgrading whatever parts it can and carefully monitoring the components it can't for any possible "show-stopping" signs of trouble, notably in its aluminum reactor tank.

He compared Israel's situation with the Dimona core to someone with a car they feel they need and can't afford to replace.

"You would spare no effort in keeping it functional," he said.

View of the Israeli nuclear reactor located in the Sorek valley in the Judean hills, December 15, 2011. (Yaakov Naumi/Flash90)

The initial four-decade expiration date for the Dimona core was based on the limits of the technology of the time. In the interim half-century, additional methods of monitoring the health of the nuclear core that have come into existence are being used to ensure that it can be safely operated for longer.

In April 2016, scientists at Tel Aviv University revealed 1,527 defects and flaws to the concrete-coated aluminum core using an innovative ultrasound technique that was performed first in 2007 and again in 2015. The scientists noted that none of these flaws had grown during that 8-year span. These defects were labeled and continue to be monitored to check if they get larger.

"There is no maximum time for the reactor's work. The continued operation of the facility is subject to compliance with clear and stringent occupational safety criteria," Tourism Minister Yariv Levin said, speaking on behalf of the government in 2016, following the report.

"The ultrasound test performed at the reactor… was part of the strict maintenance procedures. This test did not indicate any problem in the reactor that would require it to cease operations," he said.

Despite the government's assurances, several Israeli nuclear experts — including some of the scientists who founded the Dimona reactor — as well as politicians have for years been calling for the aging core to be shut down over the risks it posed.

Uzi Even, a chemistry professor at Tel Aviv University who was involved in the creation of the reactor, has been at the forefront of this charge, arguing that the core has outlived its usefulness.

"If you're asking me if there is a point in continuing operating a 53-year-old reactor, the answer is certainly not," he said in a 2016 radio interview, following the reports of the Dimona core's 1,527 flaws.

The atomic expert did not call for the reactor's immediate closure, but said it must be shuttered at the slightest problem with its irreplaceable parts.

"The things that you have to actively monitor — if there's a problem, you have to shut it down. If irreplaceable parts are damaged, you must close the core," he said.

One of the central issues regarding Dimona's safety is that it has no independent oversight. Since Israel is a non-signatory of the nuclear non-proliferation treaty, the International Atomic Energy Agency do not inspect the site, nor do American inspectors, who did monitor the reactor in its early days until they determined that their checks were effectively worthless as many aspects of the site were being kept hidden from them. Instead, the reactor is monitored by Israel's Atomic Energy Commission — the same body that is responsible for running it.

The highly classified nature of the work there also limits the amount of public debate about the nuclear research center.

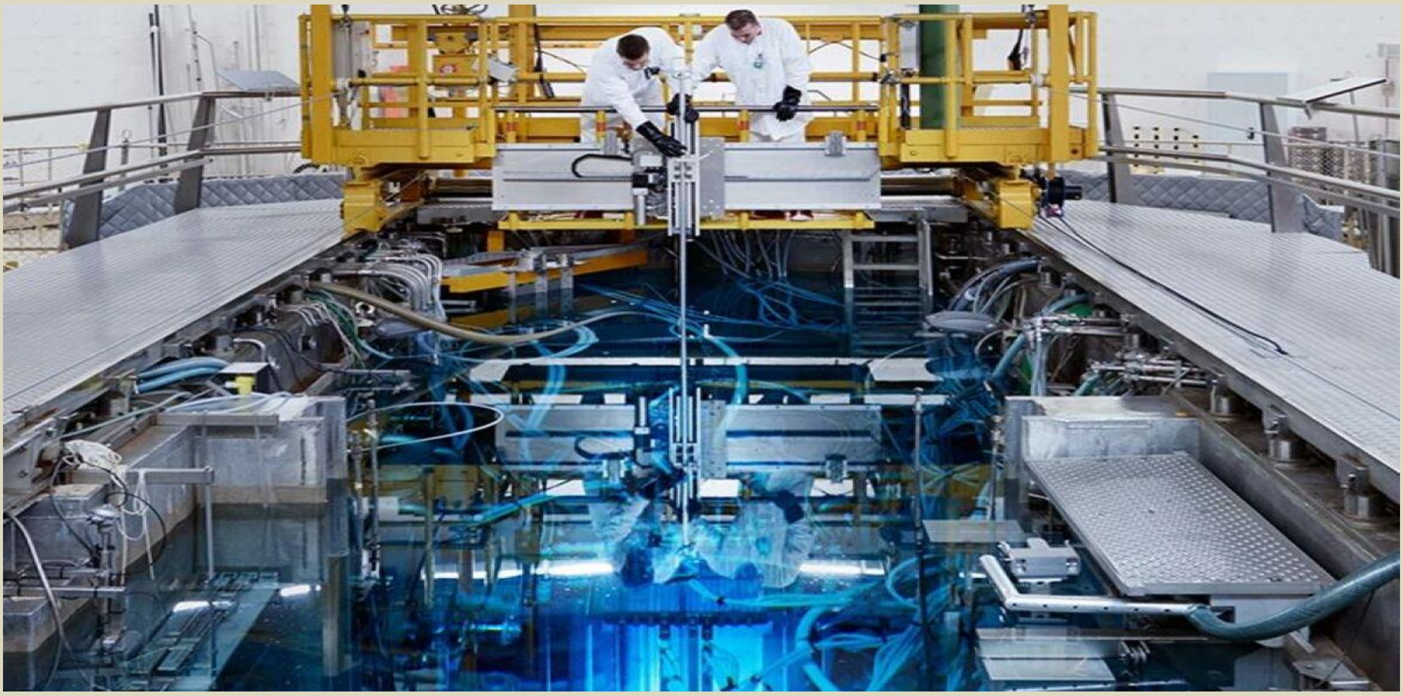
Efforts to allow the State Comptroller's Office, which performs independent investigations of various aspects of the government and military, to release its findings about the Dimona core have been blocked over the years by the Prime Minister's Office on grounds that their publication threatened national security.

Indeed, a court order was required to allow the printing of a 2016 comptroller report, which dealt solely with the actions of the civilian company, Rotem Industries Ltd., that markets the commercial findings of the Dimona reactor — not with the functioning and safety of the nuclear core.

This secrecy and lack of independent oversight means Israelis (and to a lesser extent Jordanians) can only hope that the government is doing its all to prevent a nuclear catastrophe — albeit one that would be far smaller than Chernobyl.

Is thorium the future of nuclear power?

Source: https://newatlas.com/science/thorium-nuclear-power-future-reactors/



The Netherland's Petten nuclear facility is studtying thorium reactor technology (NRG)

Dec 28 – Unless you're really into trivia about gas lanterns and the mantles that make their light so bright, you've probably never heard of thorium, but you may hear a lot more about it in the future. This unassuming metal could one day rival uranium as the nuclear fuel of choice.

What is thorium?

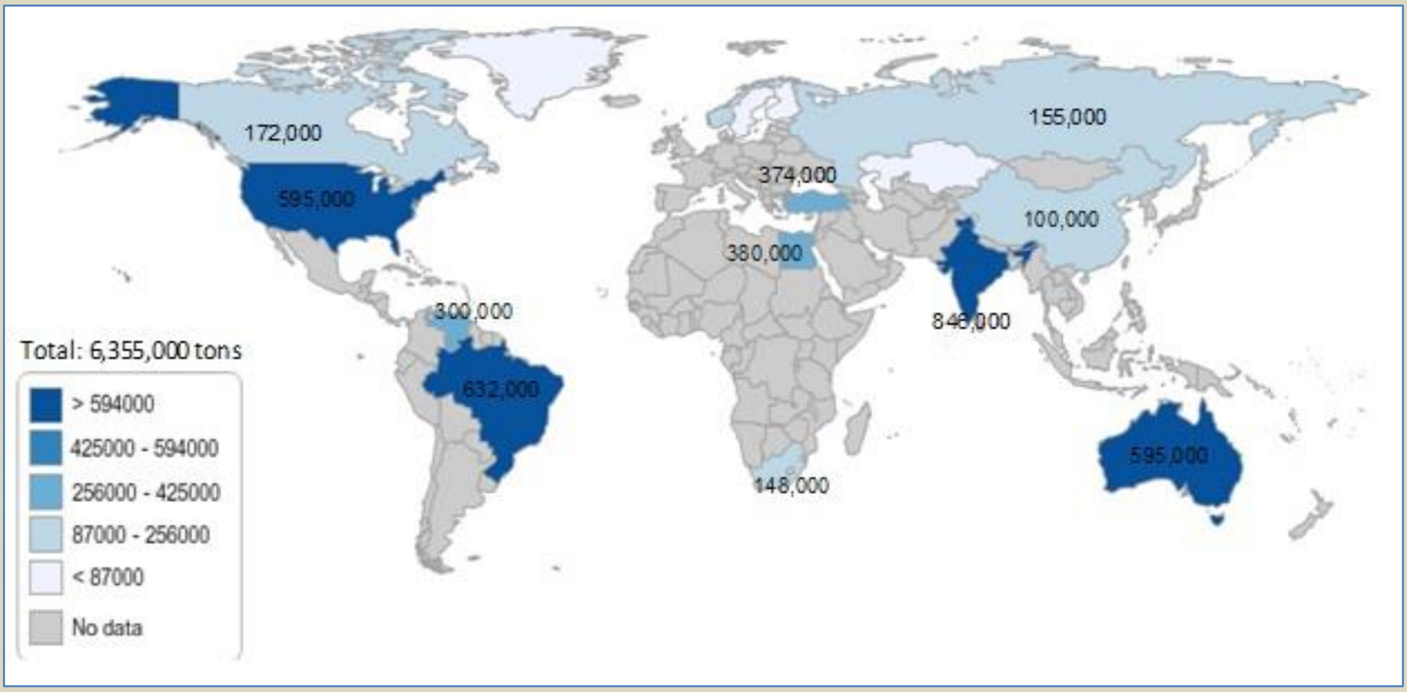
Discovered in 1828 by the Swedish chemist Jons Jakob Berzelius, thorium is named after Thor, the Norse god of thunder. It is a slightly radioactive metal found in trace in rocks and soils all over the world and is particularly abundant in India and the state of Idaho.

Thorium has only one major isotope – ^{232}Th – and its others only exist in minute traces. This isotope eventually decays into the lead isotope ^{208}Pb. But what makes thorium interesting is that ^{232}Th can easily absorb passing neutrons, turning it into ^{233}Th. This new isotope, in a matter of minutes, emits an electron and an antineutrino to become ^{233}Pa, an isotope of palladium. With a half-life of 27 days, this then converts into a uranium isotope called ^{233}U.

In other words, nuclear fuel.

The challenge is to design fuels and reactors that can produce more ^{233}U than the reactor consumes. If this can be achieved, then thorium has an advantage over uranium, which cannot produce more fuel or "breed" in a conventional reactor. It's also possible to mix thorium and plutonium into a hybrid fuel, where uranium is produced as the plutonium is consumed.

The trick is to find the optimum mix and arrangement of the fuel to handle the neutrons and their absorption. Thorium also absorbs fast neutrons, so they can be used in fast molten salt and other Generation IV reactors that are now emerging, with uranium or plutonium fuel to initiate fission – though it doesn't work as well as ^{238}U.



Estimated thorium resources in 2014 (tons)

Thorium reactors

A number of thorium reactors have been built since 1960, starting with the thorium-based nuclear reactor at Oak Ridge National Laboratory and a few research reactors are in operation today. Today, thorium is seen by some as a thousand year solution to energy and environmental problems, but one that is offset by high start-up costs and a number of technical hurdles.

Part of the reason why development has been so slow is that uranium-based reactors and the infrastructure to support them had a long head start after the Second World War. The development of liquid-metal fast-breeder reactor (LMFBR) in the 1970s seemed much more promising than thorium for commercial applications and the US government largely abandoned thorium research after 1973.

By the early 21st century, many engineers in the field weren't even aware of thorium reactors. Today, there are a number of different thorium reactor designs under development, especially in India and China. Here's a look at some of the thorium reactors that are operating, being built, or are still on the drawing board.

Advanced Heavy Water Reactor (AHWR)

These are reactors where the neutrons are slowed down or moderated by heavy water, which is chemically identical to ordinary light water, but the hydrogen atoms are replaced by deuterium, which is hydrogen with an extra neutron (^{2}H). Cooling is by light water naturally circulating in a pool driven by gravity. Because thorium absorbs neutrons, it makes a very good fuel for AHWRs. In addition, the technology has already been used for decades in heavy water reactors like CANDU. Once the driver fuel has been replaced with recycled ^{233}U, 80 percent of the energy produced is from the thorium cycle.

The latest Indian design, the AHWR-300 reactor, will use a thorium core when it comes on line at the Bhabha Atomic Research Centre (BARC), in Mumbai.

Aqueous Homogeneous Reactor (AHR)

Aqueous homogeneous reactors (AHR) differ from other reactors in that they have nuclear salts like uranium sulfate or uranium nitrate dissolved in either light or heavy water, which acts as fuel source, coolant, and moderator. By using heavy water, it's possible to introduce a soluble thorium salt into the mix.

Boiling Water Reactor (BWR)

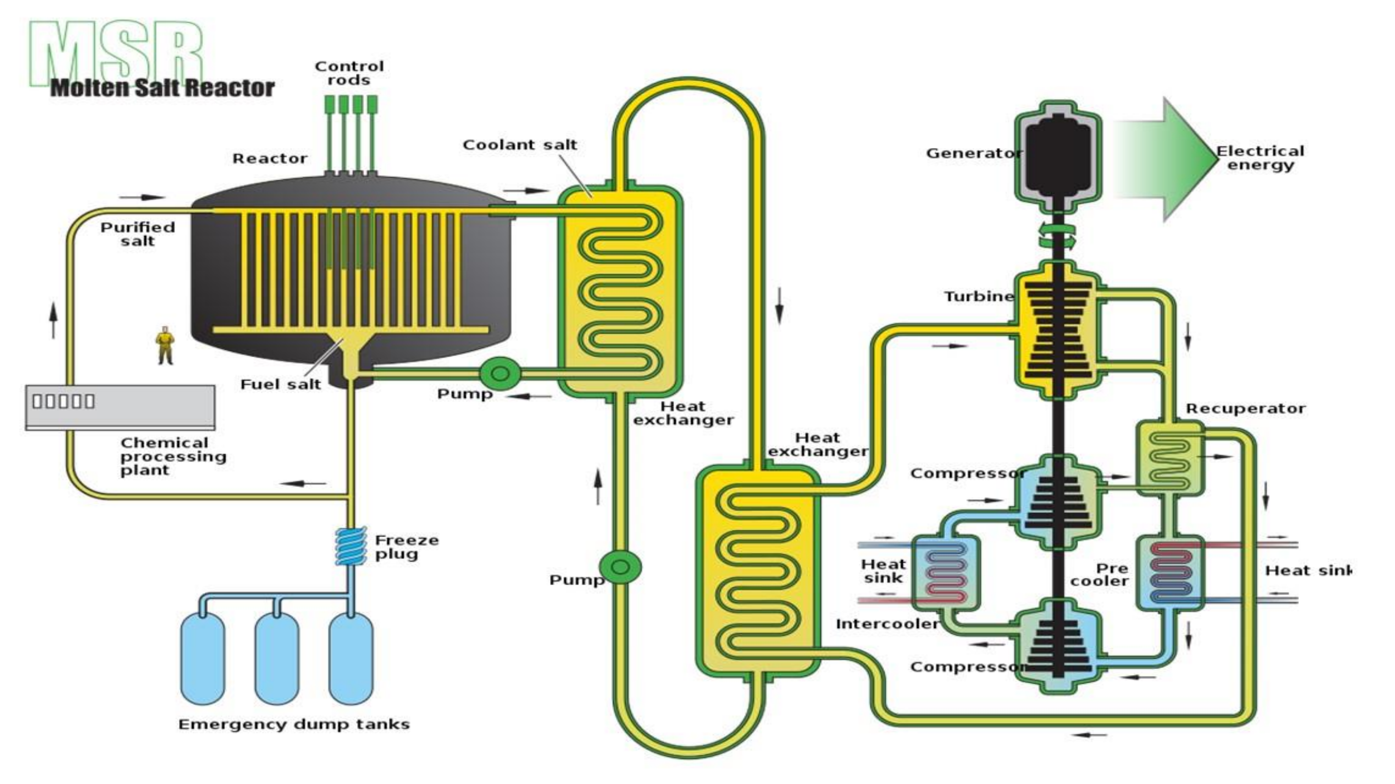
As the name implies, boiling water reactors work by boiling the coolant water to produce steam to spin turbines. They have the advantage of having a flexible design with fuel rods of different lengths and compositions that can be arranged in the core to suit thorium-plutonium fuels. In these reactors, it's possible to configure the thorium elements to turn the BWR into a breeder reactor that produces more fuel than it consumes, which isn't normally possible with thermal neutron cores.

Pressurized Water Reactor (PWR)

Pressurized Water Reactors (PWR) are one of the most common nuclear reactors and use a core set in a pressure vessel to raise the water temperature. While it's possible to produce thorium fuel elements for these reactors, their design isn't very flexible and can't produce significant amounts of ^{233}U.

Molten Salt Reactor (MSR)

Molten Salt Reactors (MSR) use a mixture of salts heated to up to 700 °C (1,292 °F) as both a coolant and a container for the nuclear fuel. In this case, a mixture of thorium fluoride and uranium fluoride mixed into the salts instead of contained in fuel rods. This not only makes the reactor more efficient, but removes the need for heavy structures to contain the reactor because it operates at atmospheric pressure and allows for passive safety systems in the event of a shutdown. In addition, the reactor can be regularly refueled and cleansed of byproducts through a chemical loop, and it has the potential to be a breeder reactor.



High-Temperature Gas-Cooled Reactor (HTR)

High-Temperature Gas-Cooled Reactors (HTR) are Generation IV reactors that use thorium-based fuels in the form of pebbles coated with pyrolytic carbon and silicon carbide layers, which retain fission gases, and then coated with graphite that acts as a moderator and protects the fuel from high temperatures. These pebble bed reactors are fed with fuel at the top and the spent pebbles are removed from the bottom. Cooling is through the circulation of inert helium gas.

Fast Neutron Reactor (FNR)

Fast Neutron Reactors (FNR) use fast neutrons instead of slow or thermal neutrons used in reactors of the conventional variety. This type of reactor doesn't need a moderator to function and it can burn thorium, but it can also use depleted uranium, which is in large supply and relatively cheap.

Accelerator Driven Reactor (ADS)

The Accelerator Driven Reactor (ADS) is a concept reactor that could use thorium mixed with plutonium. In this design, the fuel is kept at a lower density than would be needed to sustain a nuclear reaction. Instead, the fuel is bombarded with neutrons generated by a particle accelerator. This makes it very safe and produces very short-lived nuclear waste, but building an accelerator that's reliable enough for such a reactor remains a major obstacle.

Advantages & Disadvantages

Thorium as a future nuclear fuel offers a number of advantages and disadvantages compared to uranium. Not the least of these is that another fuel source would vastly increase available energy resources. Thorium is as abundant as lead in the Earth's crust and the supply in the United States could meet the country's energy needs for a thousand years, without the extensive enrichment needed for uranium fuels. In addition, some thorium reactor designs could produce less nuclear waste than current pressurized reactors, and the waste produced decays much faster than the isotopes from conventional fuels. On the other side of the coin, developing a thorium nuclear power system would require expensive development and testing, which is difficult to justify, since uranium is relatively cheap and very little of the cost of building a reactor is in the fuel. In addition, uranium-based fuels would still be needed as a driver to start the nuclear reaction, which means that both the thorium and uranium infrastructures need to be preserved. Then there is the matter of ^{233}U, which is difficult to handle because of radiation issues because it contains traces of ^{232}U, which is a very active gamma ray emitter.

Misconceptions

The idea of using thorium to produce energy is has attracted a number of misconceptions and even outright conspiracy theories. Part of this is because many designs for thorium reactors are advanced Generation IV and breeder reactors. This seems to have confused people into thinking all thorium reactors are something more advanced than uranium reactors, and that thorium and breeder reactors are synonymous. In some circles, this has elevated thorium into a wonder technology that's supposedly being suppressed by dark forces up to no good.

One persistent misconception is that thorium can't be used to make nuclear weapons and this is why the technology was abandoned. This is true if one is talking about thorium itself, but the ^{233}U it produces can and has been used in a bomb, though it's too radioactive to be handled by anyone but experts and if the design isn't just right, the ^{233}U will pre-detonate and the weapon won't function correctly.

Some have argued that thorium was suppressed by the Nixon administration because it couldn't be used to produce plutonium, which is used in nuclear weapons. This doesn't hold up, because the US has always kept its civilian and military nuclear programs strictly separate. Also, civilian reactors aren't suited to producing weapon-grade plutonium anyway.

In fact, thorium was largely given up on for economic reasons – the fuel was expensive to fabricate and uranium was still needed in the mix.

Another misconception is that there is more thorium than uranium. While it is true that there is three times as much thorium in the Earth's crust compared to uranium, thorium isn't soluble in water, while uranium is. This means that the oceans hold roughly five billion tonnes of uranium, as opposed to 6.4 million tons of thorium in the Earth's crust, and more will leach out of the crust into the sea as it is extracted.

Long story short, while thorium could power our civilization for thousands of years, if sea extraction becomes practical, uranium could power humanity until we have to move to another star because the Sun has grown too old.

However, thorium is abundant and readily accessible in places like India, which is taking advantage of its native supplies to build thorium reactors. At any rate, since most advanced nuclear reactors are breeders, the fuel question could quickly become moot.

This last bit is particularly important because, while thorium reactors produce much less long-term transuranic nuclear wastes than uranium reactors, fast neutron breeder reactors combined with reprocessing hold the same promise.

The future

Currently, thorium is enjoying a revival, with experiments on molten salt thorium technology in the Netherlands and reactors being built not only in India, but also in China and elsewhere. In a world becoming increasingly concerned about carbon emissions, calls to expand carbon-zero nuclear power's share of the world market are becoming stronger. It may well be that as Generation IV reactor technology comes on line, our energy will come from a grid with both uranium and thorium in the mix.

That is, if fusion power isn't made practical by then. If it is, all bets are off.

US affirms new interpretation for high-level nuclear waste

Source: https://statesville.com/news/science/us-affirms-new-interpretation-for-high-level-nuclear-waste/article_0d7c99f7-56df-55c8-9cc6-150bdecc655a.html

In this May 11, 2015, file photo, nuclear waste is stored in underground containers at the Idaho National Laboratory near Idaho Falls, Idaho. The Biden administration has affirmed a Trump administration interpretation of high-level radioactive waste that is based on the waste's radioactivity rather than how it was produced. The U.S. Department of Energy announcement last week means some radioactive waste from nuclear weapons production stored for decades in Idaho, Washington and South Carolina could be reclassified and moved for permanent storage elsewhere.

Dec 30 — The Biden administration has affirmed a Trump administration interpretation of high-level radioactive waste that is based on the waste’s radioactivity rather than how it was produced.

The U.S. Department of Energy announcement last week means some radioactive waste from nuclear weapons production stored in Idaho, Washington and South Carolina could be reclassified and moved for permanent storage elsewhere.

“After extensive policy and legal assessment, DOE affirmed that the interpretation is consistent with the law, guided by the best available science and data, and that the views of members of the public and the scientific community were considered in its adoption,” the agency said in a statement to The Associated Press on Wednesday.

The Biden administration's affirmation of the new interpretation came after various groups offered letters of support and opposition to the agency after Biden became president, leading to the notice in the Federal Register making clear where the administration stood. Biden has reversed Trump policy in other areas.

The policy has to do with nuclear waste generated from the reprocessing of spent nuclear fuel to build nuclear bombs. Such waste previously has been characterized as high level. The new interpretation applies to waste that includes such things as sludge, slurry, liquid, debris and contaminated equipment.

The agency said making disposal decisions based on radioactivity characteristics rather than how it became radioactive could allow the Energy Department to focus on other high-priority cleanup projects, reduce how long radioactive waste is stored at Energy Department facilities, and increase safety for workers, communities and the environment.

The department noted that the approach is supported by the Blue Ribbon Commission on America's Nuclear Future, formed during the Obama administration.

The department identified three sites where waste is being stored that will be affected by the new interpretation.

In Idaho, it's stored at an 890-square-mile (2,300-square-kilometer) Energy Department site in the southeastern part of the state that includes the Idaho National Laboratory. In Washington, the waste is stored at the Hanford Nuclear Reservation, a decommissioned nuclear site in the south-central part of the state that produced plutonium for nuclear bombs. In South Carolina, it's stored at the 310-square-mile (800-square-kilometer) Savannah River Site, home of the Savannah River National Laboratory.

The department, in the statement to the AP, said it "is committed to utilizing science-driven solutions to continue to achieve success in tackling the environmental legacy of decades of nuclear weapons production and government-sponsored nuclear energy research."

The agency also last week made public a draft environmental assessment based on the new interpretation to move some contaminated equipment from the Savannah River Site to a commercial low-level radioactive waste disposal facility located outside South Carolina. Potential storage sites are located in Andrews County, Texas, and in Clive, Utah.

Previously, the agency through a public process and using the new interpretation, approved moving up to 10000 gallons (37,854 liters) of wastewater from the Savannah River Site, with some going to Texas.

A similar public process would be used concerning additional waste at the Savannah River Site or in the other two states.

The nation has no permanent storage for high-level radioactive waste. Reclassifying some of the high-level waste under the new interpretation means it can legally be sent to commercial facilities for storing waste deemed less radioactive.

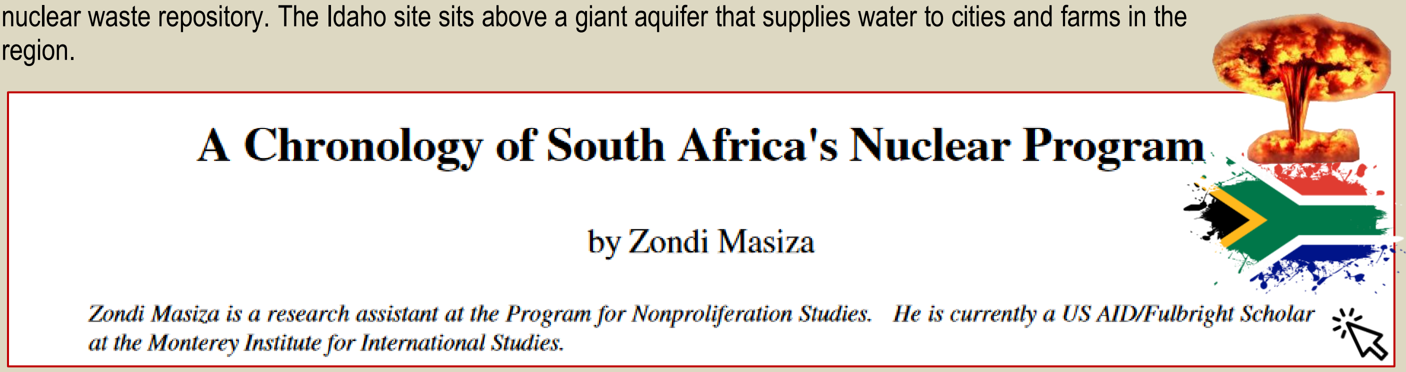
Edwin Lyman, director of Nuclear Power Safety at the Union of Concerned Scientists, a nonprofit, said his group agreed that radioactive waste should be classified using technical analysis rather than a legal definition.

But he also said "any decision made under this new interpretation has to be backed up by solid analysis and a strong commitment to public health and safety and environmental protection."

He also said he was concerned that the new interpretation could hinder development of permanent storage for high-level radioactive waste, which mostly sits above ground at sites where it was produced.

"It shouldn't be used as an excuse not to move forward with a repository," Lyman said. "That's the danger."

The Energy Department was shipping high-level waste to Idaho until a series of lawsuits between the state and the federal government in the 1990s led to a settlement agreement. The agreement is seen as preventing the state from becoming a high-level nuclear waste repository. The Idaho site sits above a giant aquifer that supplies water to cities and farms in the region.



A Chronology of South Africa's Nuclear Program

by Zondi Masiza

Zondi Masiza is a research assistant at the Program for Nonproliferation Studies. He is currently a US AID/Fulbright Scholar at the Monterey Institute for International Studies.

Israel's Mossad bombed German, Swiss firms to stop Pakistani nukes - report

By Benjamin Weinthal

Source: https://www.jpost.com/international/article-691435

The Mossad is suspected of detonating bombs and issuing threats to German and Swiss companies in the 1980s that energetically worked to aid the Islamic Republic of Pakistan in its nascent nuclear weapons program.

The prominent Swiss daily Neue Zürcher Zeitung (NZZ) first reported on the findings on Saturday. According to the paper, "The suspicion that the Mossad might be behind the attacks and threats soon arose. For Israel, the prospect that Pakistan, for the first time, could become an Islamic state with an atomic bomb posed an existential threat."

The paper reported that Pakistan and the Islamic Republic of Iran worked closely together in the 1980s on the construction of nuclear weapons devices. According to the NZZ, the intensive work of companies from Germany and Switzerland in aiding Iran's nuclear program "has been relatively well researched."

However, "New, previously unknown documents from archives in Bern and Washington sharpen this picture."

The paper quoted the Swiss historian Adrian Hänni who said the Mossad was likely involved in the bomb attacks of Swiss and German companies, adding, however, there was no "smoking gun" to prove the Mossad carried out the attacks.

The Organization for the Non-Proliferation of Nuclear Weapons in South Asia, a previously unknown entity, claimed credit for the explosions in Switzerland and Germany.

The NZZ reports on the role of the late Pakistani nuclear scientist, Abdul Qadeer Khan, the father of Pakistan's atomic weapons program, who crisscrossed Europe during the 1980s to secure technology and blueprints from Western institutions and companies for a nuclear weapons device. The paper wrote that Khan met in a Zurich hotel with a delegation of Iran's Organization for Atomic Energy in 1987. The Iranian delegation was led by the engineer Masud Naraghi, the chief of Iran's nuclear energy commission.

Two German engineers, Gotthard Lerch and Heinz Mebus, along with Naraghi, who earned his PhD in the USA, met with Khan's group in Switzerland. Additional meetings took place in Dubai in the UAE.

With the fast-moving efforts by Pakistan to jumpstart its nuclear weapons program, the US government sought, without success, to get the German and Swiss governments to crack down on companies in their countries that were aiding Pakistan. Suspected Mossad agents allegedly took action in Switzerland and Germany against the companies and engineers involved in aiding Pakistan.

According to the NZZ, "A few months after the unsuccessful intervention of the American state department in Bonn [then-capital of West Germany] and Bern, unknown perpetrators carried out explosive attacks on three of these companies: on February 20, 1981 on the house of a leading employee of Cora Engineering Chur; on May 18, 1981 on the factory building of the Wälischmiller company in Markdorf; and finally, on November 6th, 1981, on the engineering office of Heinz Mebus in Erlangen. All three attacks resulted in only property damage, only Mebus's dog was killed."

The paper noted that " The explosives attacks were accompanied by several phone calls in which strangers threatened other delivery companies in English or broken German. Sometimes the caller would order the threats to be taped. 'The attack that we carried out against the Wälischmiller company could happen to you too' - this is how the Leybold-Heraeus administration office was intimidated. Siegfried Schertler, the owner of VAT at the time, and his head salesman Tinner were called several times on their private lines. Schertler also reported to the Swiss Federal Police that the Israeli secret service had contacted him. This emerges from the investigation files, which the NZZ was able to see for the first time."

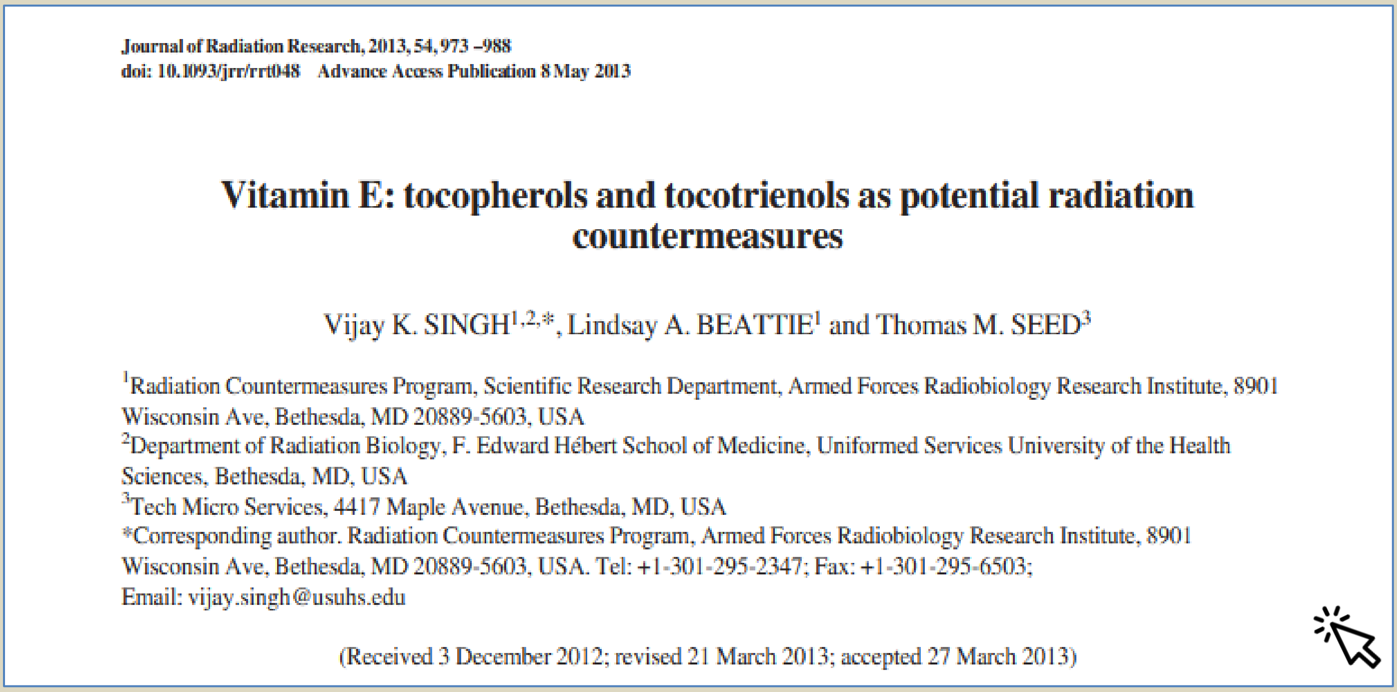
Schertler said an employee of the Israeli embassy in Germany, who was named David, contacted the VAT executive. The company head said that David urged him to stop "these businesses" regarding nuclear weapons and switch to the textile business.

Swiss and German companies derived significant profits from their business with the Khan nuclear weapons network. The NZZ reported "Many of these suppliers, mainly from Germany and Switzerland, soon entered into business worth millions with Pakistan: Leybold-Heraeus, Wälischmiller, Cora Engineering Chur, Vakuum-Apparate-Technik (VAT, with the chief buyer Friedrich Tinner) or the Buchs metal works, to name but a few to name a few. They benefited from an important circumstance: the German and Swiss authorities interpreted their dual-use provisions very generously: Most of the components that are required for uranium enrichment, for example, high-precision vacuum valves, are primarily used for civil purposes."

The NZZ reported that recently the National Security Archive in Washington published diplomatic correspondence from the US State Department from Bonn and Bern in 1980.

"This shows how the US resented the two countries' casual handling of the delicate deliveries to Pakistan. In a note from an employee, Bern's behavior was described as a 'hands-off approach' - the local authorities were accordingly accused of turning a blind eye. In the now released dispatches, which were previously classified as secret, those companies are listed for the first time that the US has accused of supporting the Pakistani nuclear weapons program with their deliveries. The list included around half a dozen companies each from Germany and Switzerland."

Benjamin Weinthal covers Middle East affairs for The Jerusalem Post and is a fellow at the Foundation for Defense of Democracies.



Journal of Radiation Research, 2013, 54, 973 –988
doi: 10.1093/jrr/rrt048 Advance Access Publication 8 May 2013

Vitamin E: tocopherols and tocotrienols as potential radiation countermeasures

Vijay K. SINGH[1,2,*], Lindsay A. BEATTIE[1] and Thomas M. SEED[3]

[1]Radiation Countermeasures Program, Scientific Research Department, Armed Forces Radiobiology Research Institute, 8901 Wisconsin Ave, Bethesda, MD 20889-5603, USA
[2]Department of Radiation Biology, F. Edward Hébert School of Medicine, Uniformed Services University of the Health Sciences, Bethesda, MD, USA
[3]Tech Micro Services, 4417 Maple Avenue, Bethesda, MD, USA
*Corresponding author. Radiation Countermeasures Program, Armed Forces Radiobiology Research Institute, 8901 Wisconsin Ave, Bethesda, MD 20889-5603, USA. Tel: +1-301-295-2347; Fax: +1-301-295-6503;
Email: vijay.singh@usuhs.edu

(Received 3 December 2012; revised 21 March 2013; accepted 27 March 2013)

China's Nuclear Buildup is About More Than Nukes

Source: https://www.homelandsecuritynewswire.com/dr20220104-china-s-nuclear-buildup-is-about-more-than-nukes

Jan 04 – U.S.-China nuclear and strategic stability will be tested in the coming year after a series of revelations in 2021 about Beijing's nuclear program. It is expanding the size and sophistication of its arsenal, potentially growing its total stockpile to 1,000 warheads by 2030, or just over a quarter of America's 3,800 warheads. Jacob Stokes writes in *Just Security* that China also has tested a weapon system that flies into orbit carrying a hypersonic weapon — missile systems that fly five times the speed of sound and can maneuver to avoid defenses — and dug hundreds of new silos for intercontinental ballistic missiles (ICBMs). In addition, Beijing is reportedly consolidating its nuclear triad of bombers, submarines, and ICBMs; moving to a launch-on-warning posture; and exploring new "exotic" nuclear systems.

He adds:

> These developments raise questions about what is motivating China to pursue such capabilities, how nuclear modernization connects to the larger regional security dynamic, and how Washington should respond. The multitude of technical intricacies in this area — from the features of particular weapons systems to nuclear deterrence logic — are (understandably) often difficult for non-specialists to get their arms around. It is possible to understand the overall picture, though, by examining the issues as four concentric circles that show how nuclear-specific issues intertwine with broader concerns in both Beijing and Washington about advanced conventional capabilities and U.S.-China competition overall.

Stokes explains the four concentric circles:

- The first and innermost circle contains the nuclear weapons themselves, along with missile defenses, including the advancements mentioned earlier.
- Another more speculative ambition, but one voiced by the head of U.S. Strategic Command, among others, is that China is trying to "break out" of being a second-tier nuclear power and sprint to parity with the United States and Russia.
- The second circle that illustrates how nuclear-weapons issues intersect with broader concerns includes non-nuclear systems that are capable of strategic effects, a nebulous term that generally means massive destruction that shapes the character of a conflict.
- Among these are conventionally armed ballistic, cruise, and hypersonic missiles of various ranges. China has the world's largest arsenal of such missiles that can be fired from land, a fact that played a big role in the U.S. decision to withdraw from the Intermediate-Range Nuclear Forces (INF) Treaty in 2019.
- The third circle shows that the aforementioned military capabilities are arrayed in an East Asian region featuring several major flashpoints.
- The fourth and outermost circle showing the overlap between nuclear concerns and broader issues contains the overall U.S.-China relationship. Washington

> and Beijing are feuding across nearly every dimension of bilateral relations — not just the military sphere but also in economics, diplomacy, technology, and governance.

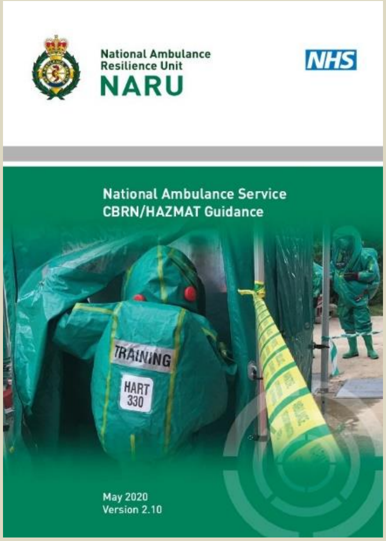
Stokes concludes:

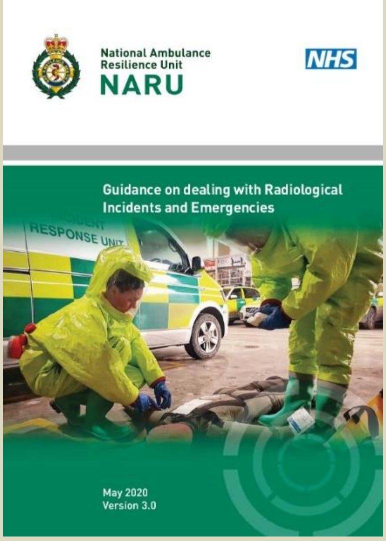
> The U.S.-China nuclear and strategic relationship has entered a new stage. Navigating it successfully to uphold deterrence and sustain regional peace and security will require a comprehensive approach that takes into account all four concentric circles and formulates sober, purposeful responses. Pursuing nuclear and strategic stability between the United States and China will likely prove harder than ever — but it is perhaps more important than ever, too.

New NARU Radiation Guidance and CBRN Guidance publications

Source: https://naru.org.uk/new-naru-radiation-guidance-and-cbrn-guidance-publications-imminent/

The 2020 *NARU National Ambulance Service CBRN/HAZMAT Guidance* significantly updates the original 2014 version and aims to support a consistent and structured approach by NHS ambulance resources as part of a multi-agency response to CBRN incidents, such as the poisoning of Alexander Litvinenko in 2006 or the Salisbury Novichok poisoning in 2018.





The *NARU Guidance on Dealing with Radiological Incidents and Emergencies* is a revision of the original National Health Service (NHS) guidance issued in March 2010 and takes into account operational feedback from Ambulance Trusts and consultation with Partner Agencies. It is also aligned to the Joint Emergency Services Interoperable Programme (JESIP) where applicable.

The guidance set out in this document aims to meet the requirements of the Health and Safety at Work (HaSaW) Act 1974, Ionising Radiations Regulation 2017 and accompanying Approved Code of Practice (IRR17) and the Radiation (Emergency Preparedness and Public information) Regulations 2019 (REPPIR).

It is applicable to the planning, preparation and response to operations and incidents where radiation may be encountered, giving rise to the potential for exposure to ambulance personnel and/or contaminated patients.

This includes deliberate acts that may cause infrastructure failure and/or mass patients, as well as incidents at nuclear and non-nuclear premises and during the transportation of radioactive materials. It will assist in ensuring a safe and coordinated emergency service response to such incidents.

The two documents will be published onto the central PROCLUS reference library which is only accessible to serving NHS ambulance HART team members and ambulance service EPRR staff here: https://ambulance.pro-clus.co.uk.

●▶ For more information contact Christian Cooper.

Why joint US-South Korean research on plutonium separation raises nuclear proliferation danger

By Frank N. von Hippel and Jungmin Kang

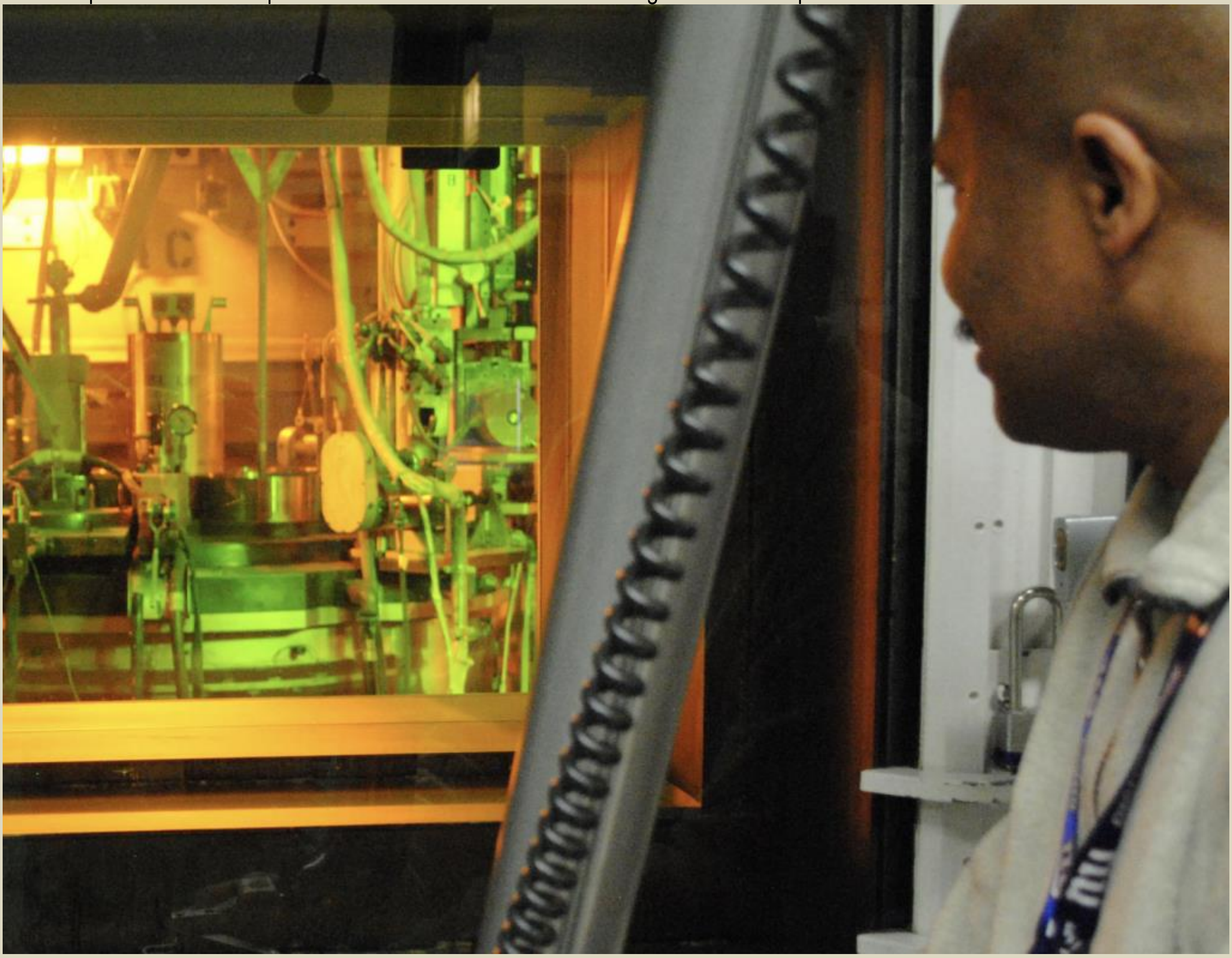
Source: https://thebulletin.org/2022/01/why-joint-us-south-korean-research-on-plutonium-separation-raises-nuclear-proliferation-danger/

Jan 13 – South Korea, like the United States, has long relied on nuclear power as a major source of electric power. As a result, it has amassed large stores of spent nuclear fuel and, as in the United States, has experienced political pushback from populations around proposed central sites for the spent fuel.

South Korea also has a history of interest in nuclear weapons to deter North Korean attack. The United States stationed nuclear weapons in South Korea during the Cold War but withdrew them in 1991. North Korea conducted its first nuclear test in 2006. US and South Korean policy is to seek the elimination of North Korea's nuclear weapons and achieve a

nuclear-weapon-free Korean peninsula. That goal currently appears distant, but South Korea acquiring nuclear weapons could make it even more distant.

South Korea's interest in spent fuel disposal and in a nuclear-weapon option account for the Korea Atomic Energy Research Institute's dogged interest in the separation of plutonium from its spent fuel. Two US Energy Department nuclear laboratories, Argonne National Laboratory (outside of Chicago) and the Idaho National Laboratory (which originated as Argonne's reactor test site), have encouraged that interest because of their own interests in plutonium separation. Now, a secret, leaked, joint South Korean-US report shows deliberate blindness to the economic and proliferation concerns associated with plutonium separation and lays the basis for policies that would put South Korea on the threshold of being a nuclear-weapon state.



Idaho National Laboratory's Fuel Conditioning Facility supports work to demonstrate the technical feasibility of a nuclear recycling technique called pyroprocessing. Photo Credit: Fuel Conditioning Fact Sheet, Idaho National Laboratory.

The report was produced by the Argonne and Idaho National Laboratories and the Korea Atomic Energy Research Institute at the end of 2021. It addresses their 10 years of collaborative research and development (R&D) on plutonium separation, using a "pyroprocessing" technology developed by Argonne.

South Korea's government has accepted the report as a justification for continued joint R&D on pyroprocessing and sodium-cooled reactors, and the Biden administration is not seeking an independent review. The leaked pages raise serious concerns, however, about the completeness and quality of the analysis. With regard to costs, the enthusiasts who authored the report ignored the lessons of decades of failed efforts to commercialize these dangerous technologies. Their strategy appears to keep their collaboration alive until new administrations come into power in South Korea and the United States, which they hope will allow the Korea Atomic Energy Resrach Institute to actually build a prototype pyroprocessing plant and a plutonium-fueled reactor.

Plutonium's nuclear-weapon background

Plutonium was originally separated during World War II to make nuclear weapons. The chain-reacting material in the Nagasaki bomb was plutonium and virtually all the world's 10,000 nuclear weapons today contain miniaturized versions of the Nagasaki bomb.

After World War II, plutonium also was promoted as a nuclear fuel. Argonne National Lab was originally established to develop what were expected to be the reactors of the future—liquid-sodium-cooled plutonium "breeder" reactors that would be fueled by plutonium while transmuting uranium into more plutonium than they consumed.

The dream of a world fueled by plutonium became a nightmare in 1974, however, when India used some of the plutonium the US Atoms for Peace program had helped India separate to test its first nuclear-weapon design and the US discovered that four other countries, including South Korea, were going down the same track.[1]

Since 1974, the United States has mostly opposed the civilian separation of plutonium—especially in states that do not have nuclear weapons. Today, Japan is the only non-nuclear-armed state that separates plutonium. The Korea Atomic Energy Research Institute has domestic political support, however, for its demand that South Korea have the same right to separate plutonium as Japan. This due largely to Japan's persistence in separating plutonium and memories of Japan's exploitive and sometimes brutal occupation of the Korean peninsula from 1910 to 1945.

Civilian plutonium separation and proliferation

US reprocessing policy dates back to the 1960s and early 1970s, when the United States Atomic Energy Commission (AEC) promoted worldwide the importance of reprocessing power reactor spent fuel to recover the plutonium it contains. The AEC projected that uranium-efficient liquid-sodium-cooled, plutonium-fueled "breeder" reactors would soon take over from conventional water-cooled reactors. It worried that insufficient separated plutonium would be available to provide startup fuel for the breeders.

In 1974, however, India reminded the world that plutonium is a dual-use material. (See above.) In reaction to India's nuclear test, US policy flipped under the Ford and Carter administrations to opposing plutonium separation for civilian purposes. In parallel, Congress, concerned that the Atomic Energy Commission was skewing national energy policy toward nuclear power and not taking nuclear power plant safety seriously enough, broke up the AEC into the Nuclear Regulatory Commission and what became the Energy Department.

Then, in 1977, the new Carter administration decided that the US domestic plutonium program was neither necessary nor economic. Breeder advocates fought back. In 1983, however, after the estimated cost of the Energy Department's demonstration breeder reactor had increased fivefold, Congress ended the program. US nuclear utilities agreed—on the condition that the Energy Department would build a deep repository for their spent fuel.

The Energy Department nevertheless allowed the nuclear power divisions of Argonne and the Idaho National Laboratory (INL) to continue their research and development work in Idaho, using the Experimental Breeder Reactor II and an adjoining compact spent fuel "pyroprocessing" plant built to recycle its fuel.

Instead of dissolving the spent fuel in nitric acid as the nuclear weapon states have done to recover plutonium for their nuclear weapons programs, "pyroprocessing" dissolves spent fuel in molten salt and then a current is run through the salt to deposit the dissolved uranium and plutonium on electrodes.

In 1994, the Clinton administration finally shut down research and development on breeder reactors. It agreed, however, that the Idaho National Laboratory could use its pyroprocessing facility to process the accumulated Experimental Breeder II spent fuel into stable waste forms for disposal. (One of the authors—von Hippel—was the responsible official in the White House when these decisions where taken.)

When the Clinton administration was succeeded by the George W. Bush administration, however, Argonne resumed lobbying for pyroprocessing and, in 2001, persuaded an energy-policy task force led by then-Vice President Dick Cheney that pyroprocessing is "proliferation resistant" because the extracted plutonium is impure and unsuitable for nuclear weapons. On that basis, Argonne and INL were allowed to launch a collaboration on pyroprocessing research and development with Korea.

The Korea Atomic Energy Research Institute was enthusiastic. It had been blocked from pursuing reprocessing R&D since it had been discovered in 1974 that the institute was part of a nuclear-weapon program launched by South Korea's then dictator, General Park Chung-hee.

At the end of the Bush administration, however, nonproliferation experts from six US national laboratories, including Argonne and INL, concluded that pyroprocessing is *not* significantly more proliferation resistant than conventional reprocessing because it would be relatively easy to remove the weakly radioactive impurities from the plutonium separated by pyroprocessing.

Tense US-South Korea negotiations over peaceful nuclear cooperation

The finding that pyroprocessing is not proliferation resistant precipitated a struggle between the Obama administration and South Korea's government during their negotiations for a new US-Republic of Korea Agreement of Cooperation on the Peaceful Uses of Nuclear Energy.

The new agreement was required to replace the existing agreement, which was due to expire in 2014. But the negotiations stalemated when South Korea, under President Park Guen-hye (General Park's daughter!), demanded the same right to reprocess the Reagan administration had granted Japan in 1987.

Ultimately, the two countries agreed to kick the issue down the road to 2021 when a joint 10-year INL-Argonne-Korean Atomic Energy Research Institute study on the technical and economic "feasibility" and the nonproliferation "acceptability" of pyroprocessing was due to be completed.

On this basis, South Korea's Atomic Energy Research Institute, Argonne, and INL were allowed to continue their joint pyroprocessing research and development.

President Park Guen-hye was impeached for corruption in 2017 and was succeeded by President Moon Jae-in, whose policy has been to phase out nuclear power in South Korea. The Korea Atomic Energy Research Institute argues, however, that, independent of the future of nuclear power in South Korea, pyroprocessing of the spent fuel from South Korea's pressurized water reactors and the fissioning of the recovered plutonium in sodium-cooled reactors will be essential to spent fuel management in South Korea.

South Korean presidents are limited to a single five-year term and the next presidential election will occur in March 2022, leaving the future of South Korea's nuclear-energy policy uncertain.

At the beginning of September 2021, INL and the Korea Atomic Energy Research Institute submitted a 10-year report on their joint fuel cycle study. Instead of making a policy recommendation on the future of pyroprocessing, however, the Korea-US Joint Nuclear Fuel Cycle Research Steering Committee decided to continue the joint research. A senior US official with knowledge of the situation, told us that "at least three or four more years will be necessary for the two governments to be in a position to draw any actual conclusions related to the technical and economic feasibility and nonproliferation acceptability of pyroprocessing on the Korean Peninsula."

Considering South Korea's imminent presidential election and the overburdened policy agenda in Washington, this is understandable. But there is no justification for keeping secret the joint report on the findings of the 10-year joint "feasibility" study.

Leaks from the secret "feasibility" report

On September 1, South Korea's Yonhap news agency reported that the Korea-US Joint Nuclear Fuel Cycle Research Steering Committee had "officially approved" a joint report from the US and South Korean nuclear laboratories. This report contained the results of their assessment of tradeoffs involved in pyroprocessing the spent fuel of South Korea's pressurized water reactors and the fissioning of the recovered plutonium and other transuranic (heavier than uranium) elements in sodium-cooled reactors. The news agency wrote:

"This report analyses the technical and economic feasibility of pyroprocessing and [sodium-cooled fast-neutron reactors], which have been studied for the past 10 years by the Idaho Research Center, Argonne Research Institute, and Korea Atomic Energy Research Institute.

"The US Department of State, Department of Energy, and the Nuclear Security Administration participated in the [Fuel Cycle Study] Steering Committee [translated from Korean]."

According to the *Korea Economic Daily*, "the two countries agreed not to reveal details of the report." And, indeed, both the South Korean and US governments have refused to release the report for independent peer review.

Excerpts from the feasibility study have been leaked, however. They reveal that INL and the Korea Atomic Energy Research Institute have learned nothing from 50 years of failed efforts in the United States, Russia, France, the United Kingdom, Japan, and India to commercialize sodium-cooled reactors. They also have learned nothing from INL's own 20 years of failure to complete the pyroprocessing of the irradiated fuel produced by its Experimental Breeder Reactor II.

With regard to the economics, the feasibility study concluded that pyroprocessing pressurized-water-reactor spent fuel to recover its contained plutonium and building enough sodium-cooled reactors to fission the plutonium would add only 6 percent to the cost of a nuclear kilowatt hour. The estimate of this relatively small cost increase was based, however, on a misuse of INL's own *Advanced Fuel Cycle Cost Basis* report. When one looks at the huge quoted uncertainties of numbers given in that report, it becomes clear that the 6 percent number quoted in the feasibility study is meaningless.

It appears also that the nuclear laboratory analysts assumed that pressurized water reactors and sodium-cooled fast-neutron reactors would operate with the same "load factors"—the ratio of the annual electric power output to the output if the reactor had operated at full capacity all year. Globally, the load factors of pressurized water reactors have mostly been between 70 and 90 percent. But, of the nine sodium-cooled experimental and prototype reactors that have been connected to the grid, four have had load factors of three percent or less and the median reactor had a load factor of 18 percent. This poor reliability is largely due to sodium leaks, which are much more serious than water leaks since sodium burns on contact with air and generates explosive hydrogen gas on contact with water (see this video).

Load factors matter. If, for example, the sodium-cooled reactors proposed for fissioning the plutonium produced by South Korea's water-cooled reactors operated at one quarter the average load factor of the water-cooled reactors, four times as many would be required as assumed in the joint-lab report.

Similarly, the cost of pyroprocessing is given in the joint report as between $1,050 and $1,471 per kilogram of spent fuel. This is tiny fraction of the cost of INL's own pyroprocessing venture, however. During the most recent five years of its 20-year effort, INL has achieved a pyroprocessing rate of only about 0.1 ton of Experimental Breeder Reactor II fuel per year at a cost of over $80,000 per kilogram.

In 2000, INL contracted with the Energy Department to pyroprocess about 25 tons of used fuel from the Experimental Breeder Reactor II within 10 years. Of that fuel, about three tons were from the reactor core and 22 tons were from a uranium "blanket" surrounding the reactor. During that 10-year period, only 13 percent of the material was treated. As of the end of September 2021, after 20 years, INL's pyroprocessing program manager reported that cumulatively only about one ton of the core fuel had been pyroprocessed, and INL was looking into alternative, simpler technologies for treating the blanket material.

With regard to nonproliferation, the joint study apparently focused exclusively on the ability of the International Atomic Energy Agency (IAEA) to safeguard the pyroprocessing process. Its report concluded, "Based on US and ROK safeguards performance models, and the performance of [destructive assay] measurements in the study, a 30 MT/yr [metric ton per year] facility *may* be able to meet IAEA detection goals for *abrupt* material loss of a significant quantity (emphasis added)."

A "significant quantity" is the IAEA's term for the 8 kilograms of plutonium it assumes would be sufficient to build a Nagasaki-type bomb. It would take 14 plants with a 30 metric ton per year throughput to keep up with the spent fuel discharged by South Korea's 21 operating pressurized water power reactors. By the IAEA's metric, each of those plants would separate enough plutonium for 30 to 40 nuclear bombs.

The report was silent on the more difficult challenge of detecting the gradual withdrawal of a significant quantity of plutonium over perhaps a year.

The central proliferation issue remains, however: The large flow of separated plutonium produced by pyroprocessing would make South Korea a latent nuclear-weapon state—like Japan. That is a very relevant concern since, according to a recent poll, 71.3 percent of South Korea's public thinks the country should have nuclear weapons.

Based on the excerpts, if the feasibility study were released, it would not survive peer review. It is therefore most unfortunate that South Korea's government has accepted the report uncritically as an endorsement of pyroprocessing, and the Biden administration has not released it for independent peer review.

Exaggerated claims of spent-fuel-management benefits

Immediately after it received the INL-Argonne-Korea Atomic Energy Research Institute "feasibility" study, South Korea's Science Ministry, which funds the institute, established a Feasibility Review Committee to consider the laboratories' report. At the end of December 2021, that committee reportedly concluded

"the pyroprocessing and [sodium-cooled fast-neutron reactor] system has potential as a spent fuel management technology with…safety, and nuclear non-proliferation, and [the Feasiblity Review Committee] submitted a review report containing recommendations [for the Korea Atomic Energy Research Institute] to continue R&D."

As this conclusion suggests, the rationale for South Korea's interest in pyroprocessing and sodium-cooled fast reactors is the claim that pyroprocessing can facilitate spent fuel management. The Korea Atomic Energy Research Institute's argument for this claim is summarized in one of the articles reporting the Feasibility Review Committee's recommendation:

"[A sodium-cooled fast reactor] is a technology that reduces the volume and toxicity of spent nuclear fuel by separating transuranium elements from spent fuel and incinerating them. Through [pyroprocessing], the volume of spent nuclear fuel can theoretically be reduced to 1/20 and [the recovered plutonium can be] recycled as [sodium-cooled-fast-reactor fuel]."

Any type of reprocessing separates the residual uranium in the fuel that has not fissioned or been converted to plutonium. This would, as claimed, reduce the mass of the radioactive waste by about 95 percent. But that reduction would be approximately offset by the mass of glass that would be added to the fission products to immobilize them and by the creation of other radioactively contaminated waste streams by reprocessing and the fabrication of fuel containing plutonium.

The main argument made today by advocates of spent fuel reprocessing and of recovering and fissioning the long-lived "transuranic" (heavier than uranium) elements produced in the fuel is that doing so would dramatically shorten from millions to hundreds of years the hazard from deeply buried spent fuel. The claim is that plutonium and the other transuranics dominate the long-term radioactive toxicity from spent fuel.

It has been known for a quarter of century, however, that separating out and fissioning the transuranic elements would *not* result in a significant reduction of the hazard from deeply buried spent fuel.

Three decades ago, the US Energy Department asked the US National Academies to study exactly this question. The resulting massive report, *Nuclear Wastes: Technologies for Separations and Transmutation*, found that, because of their low solubility in deep oxygen-free ground water, plutonium, and other transuranic isotopes would *not* dominate the dose at the surface from a deep spent fuel repository. Instead, the dose would be dominated by soluble long-lived fission products: iodine 131 (16-million-year half-life), technicium 99 (200,000 years), and cesium 135 (2 million years) and by the activation product, carbon 14 (5,700 years). The committee therefore concluded, "Taken alone, none of these dose reductions [from the separation and fissioning of transuranic elements] seem large enough to warrant the expense and additional operational risk of transmutation." The "operational risk" would include nuclear-weapon proliferation and the serious accident risks associated with reprocessing.

In 2011, SKB, the company responsible for disposing of Sweden's spent fuel, published an analysis of the doses from a beyond-worst-case scenario in a spent-fuel repository in which the spent fuel casks and the layers of relatively impermiable bentonite clay around them fail immediately. SKB calculated the contributions by different radioisotopes in the fuel to the doses received by a subsistence farmer on the surface as shown in Figure 1.

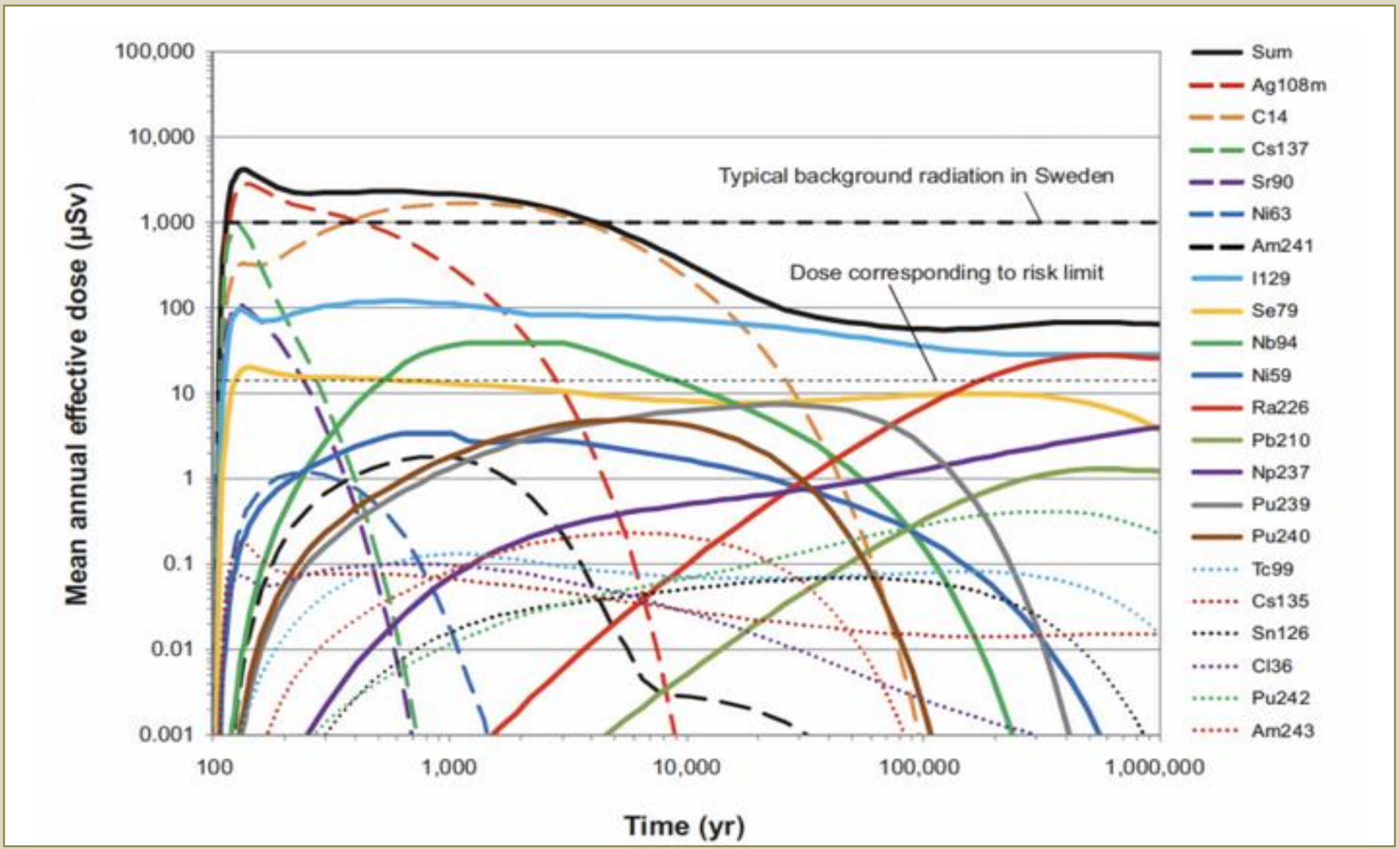


Figure 1. SKB found that, after a few hundred years, carbon 14, and then, after about 20,000 years, iodine 129 would dominate the radiation doses to a subsistence farmer on the surface above a failed spent-fuel repository. After about 200,000 years, the dose from radium 226 from the decay of uranium 238 in the fuel that had originated in a uranium mine would be comparable to that from iodine 129. (Source: SKB. Used with permission.)

A similar result was obtained by a senior researcher at the Korea Atomic Energy Research Institute in 2009[2] but has been ignored by that organization.

The final argument that has been made by Argonne and the Korea Atomic Energy Research Institute for reprocessing and transmutation of plutonium and the other transuranic elements is that the reduced long-term heat output from the radioactive waste would make possible a more compact repository because the temperature of the clay and rock must be kept below damage thresholds. The benefit of a smaller repository would be bought, however, at the cost of sodium-cooled reactors and reprocessing facilities that would costs tens of billions.

In fact, the area of a South Korean future underground repository might not be that large. Currently, there is a moratorium on launching construction on new nuclear power plants in South Korea and the policy is not to extend the licenses of heavy-water-reactor power plants beyond 30 years and pressurized reactors beyond 40 years (60 years for the most recent design). On that basis, South Korea's four heavy-water reactors will generate about 12,000 tons of spent fuel and its 26 pressurized water reactors (including four under construction) will generate about 26,000 tons.[3] These numbers are comparable to the 16,000 and 20,000 tons of spent fuel from heavy-water and pressurized water reactors respectively assumed in the Korea Atomic Energy Research Institute's Korean Reference Spent Fuel Disposal System, whose tunnels would cover an underground area of about 5 square kilometers. This is smaller than the areas associated with some of South Korea's nuclear power plants. Furthermore, the surface manifestations of underground repositories are small and tunnels at a depth of 500 meters do not compete for space with infrastructure on the surface (Figure 2).

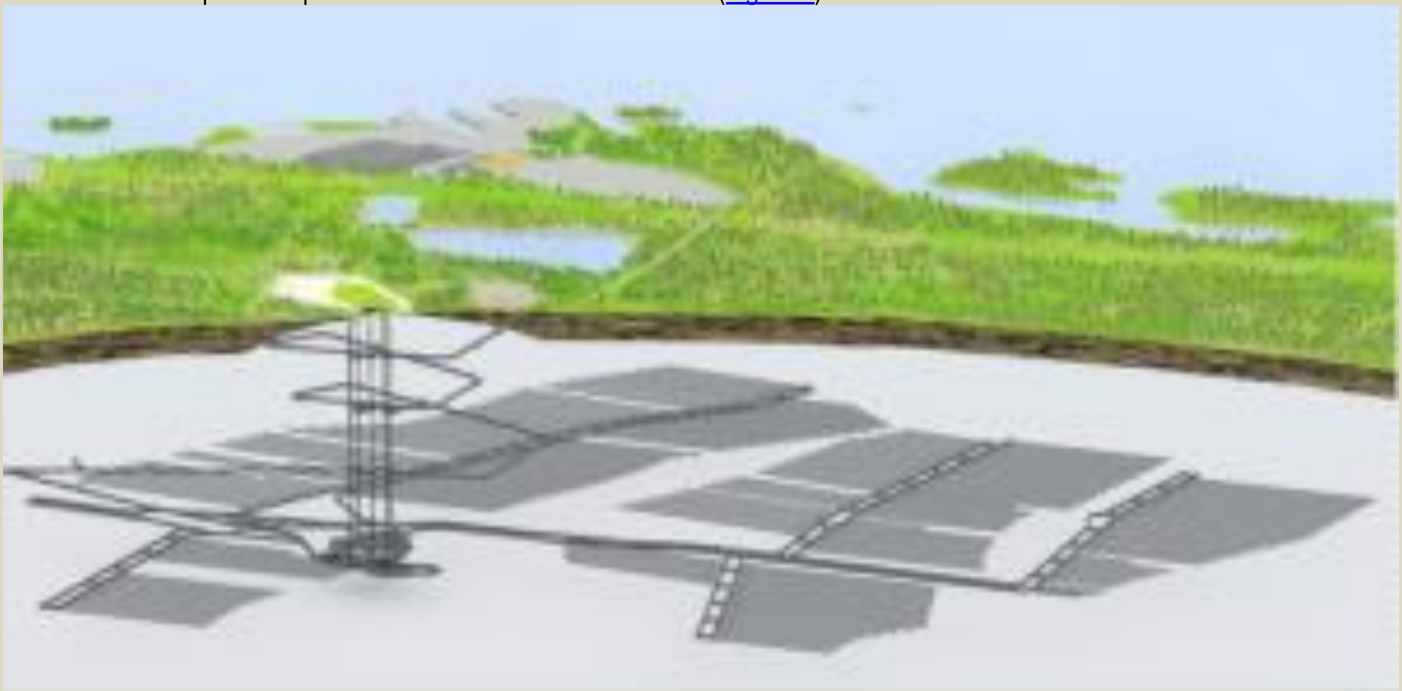


Figure 2. Layout of Finland's under-construction Onkalo repository for a design capacity of 9,000 tons of spent fuel. The only associated surface structures are those at the top of the lifts and ventilation shafts, and the construction tunnel that winds down around them. (Source: Posiva).

In any case, the problems with locating spent fuel repositories are not physical. They are political. Citizens may fear spent-fuel repositories, but they should fear more those who peddle the much more dangerous technologies of pyroprocessing and sodium-cooled reactors.

ENDNOTES:

[1] Frank von Hippel, Masafumi Takubo and Jungmin Kang, *Plutonium: How Nuclear Power's Dream Fuel Became a Nightmare* (Springer, 2019) https://link.springer.com/book/10.1007/978-981-13-9901-5.

[2] Yongsoo Hwang and Ian Miller, "Integrated model of Korean spent fuel and high level waste disposal options," in *Proceedings of the 12th International Conference on Environmental Remediation and Radioactive Waste Management,* Liverpool, UK, Oct. 11-15, 2009, paper no. ICEM2009-16091, 733-740.

[3] Other assumptions made were 90 percent capacity factors for the reactors and "burnups" of 7 and 50 Megawatt-days per kilogram of spent fuel for the heavy-water and pressurized-water reactors respectively.

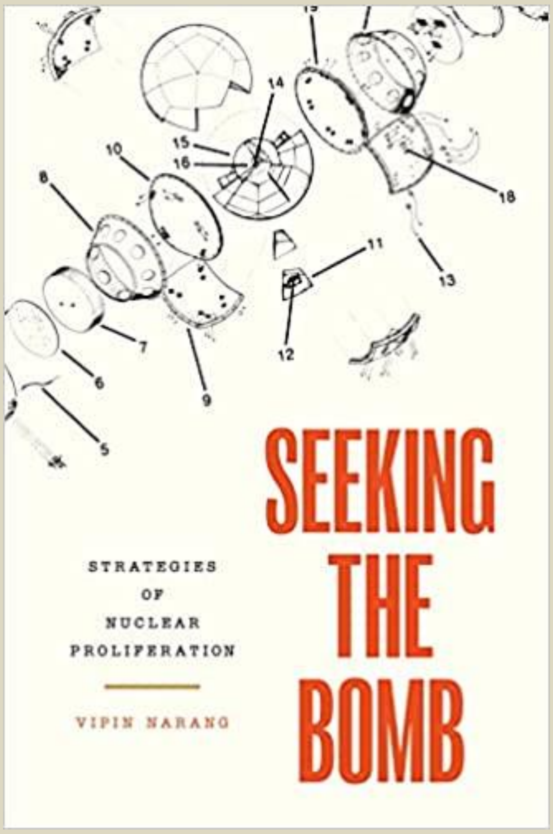
Frank N. von Hippel is a co-founder of the Program on Science and Global Security at Princeton University's School of Public and International Affairs, a founding co-chair of the International Panel on Fissile Materials, and a member of the *Bulletin*'s Board of Sponsors. A former assistant director for national security in the White House Office of Science and Technology, von Hippel's areas of policy research include nuclear arms control and nonproliferation, energy, and checks and balances in policy making for technology.

Jungmin Kang, an independent consultant and South Korea's member of the International Panel on Fissile Materials, chaired South Korea's Nuclear Safety and Security Commission in 2018.

Examining How Countries Go Nuclear — and Why Some Do Not

By Peter Dizikes

Source: https://www.homelandsecuritynewswire.com/dr20220114-examining-how-countries-go-nuclear-and-why-some-do-not



Jan 14 – Political scientist Vipin Narang's new book, *Seeking the Bomb: Strategies of Nuclear Proliferation*, makes sense of the complex history of nuclear weapons programs.

In 1993, South Africa announced to a largely surprised world that it had built nuclear weapons in the 1980s, before dismantling its arsenal. For the first time, a country outside of the elite world powers had obtained nuclear capabilities while keeping matters a secret from almost everyone else.

To this day, South Africa remains the only country to have pulled off that exact trick. Other countries have gone nuclear in other ways. A half-dozen countries with more economic and political clout than South Africa have built weapons on their own timetables. Three other countries — Israel, Pakistan, and North Korea — have developed nuclear weapons while being supported by larger allies. And many wealthy countries, including Australia, Brazil, Germany, Japan, and South Korea, have chosen not to pursue weapons programs.

Recognizing these different paths to proliferation is an essential part of arms control: Grasping how one country is pursuing nuclear weapons can help other countries constrain that pursuit.

"There's meaningful variation in how states have thought about pursuing nuclear weapons," says says Vipin Narang, an MIT political scientist and expert on nuclear strategy. "It changes how we think about stopping them. It changes how we think about managing them. It's an important question."

Narang believes that too often, we imagine that all countries pursue nuclear weapons the way the U.S. and Soviet Union did during and after World War II — a swift race culminating in the rapid buildup of arsenals, leaving little room for intervention. But that paradigm applies to almost no other country.

"We think of proliferators as a stylized Manhattan Project," says Narang, the Frank Stanton professor of Nucear Security and Political Science at MIT. "But the U.S. and the Soviet Union are really the only ones who had Manhattan projects, and the rest of the nuclear weapons powers look different."

Narang has detailed these differences in a new book, "Seeking the Bomb," published today by Princeton University Press. In it, he develops a comprehensive typology of nuclear programs around the world; examines why countries take different routes to nuclear development; and outlines the policy implications.

"There is a growing likelihood that the United States will have to confront proliferation attempts from not just foes but friends and frenemies as well," Narang writes in the book.

Sprinters and Hedgers

In recent decades, scholarship has usually focused on why countries acquire nuclear weapons — with the leading answers being security, prestige, and domestic political dynamics. But Narang's book centers the question of how, not why, countries seek to become nuclear-equipped.

"No one had asked how states pursue nuclear weapons, and examined the different ways they have to deal with nonproliferation [agreements], their own resource constraints, domestic politics, and states trying to stop them," Narang says.

At least 29 countries have made efforts to become nuclear; 19 have specifically tried to develop nuclear bombs, and 10 have succeeded. Narang's book puts all of them into four categories: countries he labels "sprinters," "hedgers," those benefitting from "sheltered pursuit," and "hiders."

The "sprinters," the simplest category to understand, consist of the U.S., Soviet Union, Great Britain, France, China, and India — big countries that could develop nuclear weapons independently, and did.

Then there are "hedgers," the countries that have potential to develop nuclear weapons but hold off doing so, because of geopolitical considerations or a lack of domestic political support. Germany, Japan, and South Korea are U.S. allies who are not eager to make themselves targets for nuclear-armed states, and instead work with the U.S. on defense matters. Should U.S. support waver, those countries might be more likely to pursue their own programs.

“Seeking the Bomb” actually details three subcategories of hedging. Japan and Germany are “insurance hedgers,” wary of American abandonment. “Hard hedgers,” such as Sweden or Switzerland, are not as close to the U.S. but still decided not to pursue weapons acquisition. And “technical hedgers,” including Argentina and Brazil, have technological pieces in place for nuclear program but have not weaponized those capabilities.

“Hedging is very prominent across countries, including Japan, South Korea, Turkey, Saudi Arabia, and Iran,” Narang says. “It’s a really meaningful category that is written out of the proliferation literature because we all focus on states that get the bomb, and not the ones that don’t know if they want it yet. They put the pieces in place to exercise the option quickly if they decide to.”

By contrast, countries undertaking “sheltered pursuit” use their alliances with superpowers to develop nuclear weapons. Israel, for one, could finish building nuclear weapons in the 1960s partly because of tacit support from the U.S. By 2006, North Korea had built its own weapons with the partial support of China.

“North Korea wouldn’t have been able to get nuclear weapons without China giving it shelter,” Narang observes.

Hide and Seek

Very few countries find themselves in the situation where a powerful ally will tacitly endorse their nuclear program, however. And if a country wants nuclear weapons but cannot get help from a superpower, it is most likely to work in secret. These are the “hiders,” in Narang’s typology.

“If you don’t have shelter, then your only option is to hide,” Narang says. “And hiding is a very risky strategy, as most get caught along the way — Libya, Iraq, Syria.”

In 2007, for instance, Israeli jets bombed a North Korea-designed nuclear reactor built in Syria, where President Bashar al-Assad had been pushing a nuclear program forward.

“No one thought Assad would try to hide a North Korean nuclear reactor above ground,” Narang says. “He came within weeks of the finish line.” Moreover, Narang adds of such leaders, “Often times the calculation is they’ll lose the program but not the regime,” Narang says. “Assad lost the reactor, but he’s still in power.” In other cases, such as Iraq and Libya, U.S. military action drove nuclear-minded leaders from power.

And yet, the case of South Africa indicates it is at least possible to push a covert nuclear program all the way through.

“South Africa is every hider’s inspiration,” Narang says.

At the time, the U.S. had suspected South Africa was engaged in a nuclear program, and then-South Africa President Pik Botha had told U.S. leaders in 1981 that the country had expanding nuclear “capacities.” But the U.S. had little concrete information about what was really happening.

“South Africa’s really the only hider that got out of the barn,” Narang says. “Neither the U.S. nor the Soviet Union wanted South Africa to get nuclear weapons, but because it was in the Southern Hemisphere, we didn’t have good eyes on the program, and [the country] was very good at hiding and obfuscating what its enrichment and plant capabilities were.”

So on the one hand, the South African case remains an anomaly. Still, “hiders” can be very dangerous to global stability.

“It’s most likely they create the risk of a crisis when they’re discovered and the great powers seek to end the program,” Narang says. “And if they succeed, precisely the states you least want to have nuclear weapons, have nuclear weapons. Either way a hider is disruptive. … It either ends poorly for them, or it ends poorly for us.”

The Future: Nuclear Arms Management

“Seeking the Bomb” includes a model Narang built incorporating certain factors — technical capabilities, domestic politics, strategic considerations — that should lead countries into one category of weapons development or another. Narang found the model correctly predicts over 85 percent of the historical cases correctly. That could help policy experts and other analysts assess future nuclear threats.

“I think there are two categories that are going to be particularly prominent in coming decades,” Narang says. “In the Middle East, you’re going to have a contagion of hedgers.” At the same time, he says, “Hiders are getting smarter. … I don’t take it for granted that we’ll be able to stop all hiders indefinitely. These hedgers and hiders are going to be the most prominent categories in the future.”

Both “hedgers” and some “hiders” can be dealt with diplomatically, Narang observes, through means such as the 2015 Joint Comprehensive Plan of Action [JCPOA] that limited Iran’s nuclear program but has now been dropped by the U.S.

“The JCPOA is rare because there are very few instruments and vehicles that have pushed states back from hiding to hard hedging,” Narang says. “For it to be torpedoed over domestic politics is just a tragedy. There’s no guarantee we’re going to get back to it.”

“Seeking the Bomb” has been praised by other political scientists. Caitlin Talmadge, an associate professor of security studies at Georgetown University, called it “an exceptional book, one of the most important to come out in the field in decades," adding: "It will become the definitive work on its subject matter and be widely read by academic, policy, and general audiences."

For his part, Narang emphasizes the fraught nature of today's nuclear landscape. After a few decades trending toward disarmament, nuclear stockpiles are growing, and nuclear proliferation is less a problem that can be ended than an issue that needs astute management.

"Everybody wants a solution to the nuclear problem," Narang says. "I think my conclusion, while pessimistic, is realistic. While nuclear technology exists, nuclear weapons are unlikely to go away. It's not a problem to be solved, it's a problem to be managed. I think for the next several decades we'll be dealing with these problems."

Peter Dizikes is the social sciences, business, and humanities writer at the MIT News Office.

The Progress of Iran's Nuclear Weapons Program

Source: https://www.homelandsecuritynewswire.com/seworld20220114-the-progress-of-iran-s-nuclear-weapons-program

Jan 14 – The Institute for Science and International Security has issued the third edition of its authoritative *Peddling in Peril* (PPI 2021-2022), a comprehensive ranking of the effectiveness of national strategic trade controls. PPI 2021-2022 ranks 200 countries, territories, and entities according to their capabilities and demonstrated success in implementing export, import, transit, and transshipment controls of strategic goods and technologies. These controls are key to thwarting the spread of nuclear weapons, other destructive weapons, and the means to make them.

Here are the Institute's five of the important findings about Iran's pursuit of nuclear weapons.

1) Iran can have enough weapon-grade uranium for a nuclear weapon in as little as three weeks.

As of November 2021, Iran had enough enriched uranium hexafluoride (UF6) in the form of near 20 and 60 percent enriched uranium to produce enough weapon-grade uranium (WGU), taken here as 25 kilograms, for a single nuclear weapon in as little as three weeks. It could do so without using any of its stock of uranium enriched up to 5 percent as feedstock. The growth of Iran's stocks of near 20 and 60 percent enriched uranium has dangerously reduced breakout timelines.

●▶ **See the Institute's Analysis of *IAEA* Iran Verification and Monitoring Report - November 2021 — click *here.***

2) Iran could detonate a nuclear explosive underground in as little as six months, rattling the Middle East profoundly, destabilizing the region perhaps irretrievably.

Although Iran would need longer to field a credible, reliable nuclear-tipped ballistic missile, it knows enough to build a nuclear explosive and build an underground nuclear test site. While most of the public focuses on deliverable nuclear weapons, many lose sight of Iran's extensive knowledge and experience in building nuclear weapons and the immense damage resulting from a nuclear explosion.

●▶ **To learn more about Iran's nuclear weapons expertise, read the Institute's 19-page Highlights of Iran's Perilous Pursuit of Nuclear Weapons, click *here.* To obtain Iran's Perilous Pursuit of Nuclear Weapons as an e-book or a paperback, click *here.***

3) Iran has made key irreversible nuclear advances, perforating the Joint Comprehensive Plan of Action, perhaps irretrievably.

With its multiple violations of the Joint Comprehensive Plan of Action (JCPOA), Iran has reached previously uncharted territory, accumulating important new knowledge, experience, and practice, representing a significant degree of nuclear capability banned to Iran by this point in time under the JCPOA. Its progress has collapsed the JCPOA's overall purpose of keeping Iran twelve months from being able to produce enough weapon grade uranium for a nuclear weapon. If the JCPOA is simply revised rather than strengthened, as promised by the Biden Administration, it will be far weaker than before and a flimsy deterrent against Iran building nuclear weapons in the next decade.

●▶ **See Iran's Recent, Irreversible Nuclear Advances — click *here.***

4) Iran is mastering the construction and operation of advanced centrifuges far faster than anticipated.

Iran has rapidly increased its number of advanced centrifuges, so far doubling the number from before the JCPOA and planning to triple the pre-JCPOA quantity over the next several months. The most important advanced centrifuges today are the IR-2m, IR-4, and IR-6 centrifuges. Because of their far greater enrichment outputs, they are more useful in a speedier breakout to weapon-grade uranium or a more difficult to detect sneak out in a clandestine enrichment plant

●▶ See A Comprehensive Survey of Iran's Advanced Centrifuges — click *here.*

5) Iran remains one of the most egregious violators of strategic trade controls and sanctions.

The Institute's 2021/2022 *Peddling Peril Index* (PPI), the only public effort to comprehensively rank national strategic trade control systems ranks Iran as 196 out of 200, clustered with the likes of North Korea, South Sudan, and Yemen.

Overall, the *Peddling Peril Index* continues to present a troubling picture of the state of worldwide efforts to stop the illicit trade in goods critical to nuclear weapons, other WMD, and conventional arms.

●▶ See the Peddling Peril Index for 2021/2022 — click *here*

Enec to produce 85% of Abu Dhabi's clean electricity by 2025

Source: https://www.thenationalnews.com/business/2022/01/12/enec-to-produce-85-of-abu-dhabis-clean-electricity-by-2025/

Jan 12 – The Emirates Nuclear Energy Corporation is set to produce 85 per cent of Abu Dhabi's clean electricity by 2025 in line with the UAE's pivot towards green energy projects, its chief executive has said.

The Barakah nuclear power plant also has the potential to generate one million tonnes of hydrogen per year, Mohamed Al Hammadi told the Gulf Intelligence UAE energy forum on Wednesday.

"In the UAE we have a proactive and science-based approach to energy policy that has enabled the country to lead the way and towards a sustainable energy future," Mr Al Hammadi said.

"We were the first in the region to sign the Paris Agreement in 2016 and recently became the first Opec nation to commit to achieving net-zero by 2050."

The UAE plans to invest $160 billion over the next three decades to accelerate clean energy development. The country is building world's largest solar plant in Al Dhafra region of Abu Dhabi as well as other projects in Dubai.

The Emirates also recently completed the construction of Unit 3 of the Barakah Nuclear Energy Plant, the Arab world's first multi-unit operating nuclear energy plant.

Unit 1 of the plant is already fully operational and Unit 2 was recently connected to the main grid and continues to undergo testing.

"This is only the beginning. The potential for clean energy moving forward is wide reaching and the role of nuclear and renewable is instrumental in this, with the UAE showing the way towards the cleaner future," Mr Al Hammadi said.

Four units of the nuclear plant have the potential to generate about one million tonnes of hydrogen per year, he said.

"At the same time, the oil and gas industry is also playing an important and crucial role in the generation of hydrogen, with plans of expansions to generate hydrogen through the carbon capture, usage and storage are already under way," Mr Al Hammadi said.

The new developments "illustrate how both the nuclear and the oil and gas sector are working together to put the UAE on the path to becoming a key player in green hydrogen generation".

The UAE, the Arab world's second largest economy, is bullish on hydrogen and has been drawing up a comprehensive road map to position itself as an exporter of clean fuel and tap into its future potential.

In January, Adnoc, Mubadala and ADQ formed an alliance to develop a hydrogen economy in the country, focusing on low-carbon green and blue hydrogen as part of the Emirates' continued energy diversification efforts.

Last December, Adnoc and Taqa said they would join Mubadala Investment Company to become shareholders in Masdar, which will help boost the clean energy company's renewable power capacity to more than 50 gigawatts by 2030.

Hydrogen comes in various forms including blue, green and grey. Blue and grey hydrogen are produced from natural gas, while green hydrogen is derived from renewable sources.

Globally, the hydrogen project pipeline has grown seven-fold since December 2020 as the world focuses on energy transition, a recent study by Wood Mackenzie found.

Nuclear Notebook: Israeli nuclear weapons, 2022

By Hans M. Kristensen and Matt Korda

Source: https://thebulletin.org/premium/2022-01/nuclear-notebook-israeli-nuclear-weapons-2022/

Jan 17 – Conducting research on Israeli nuclear weapons has historically been very challenging, not least because Israel purposely does not acknowledge its own possession of nuclear weapons. Moreover, Western governments normally do not include Israel in their descriptions of nuclear-armed states. Additionally, Israeli nuclear whistleblowers have faced significant penalties; in 1986, former nuclear technician Mordechai Vanunu was kidnapped by Israeli intelligence services and spent 18 years in prison after giving a detailed interview about Israel's nuclear program to the *Sunday Times* (Myre 2004). This chilling effect means that individuals with knowledge of Israel's nuclear program have been understandably reluctant to provide on-the-record information, which dilutes the ability of open-source researchers to analyze Israel's nuclear forces. Thankfully, over the past two decades, historians like Avner Cohen and William Burr have contributed invaluable research that has made previously unknown nuances of Israel's opaque nuclear policy available to the public.[1]

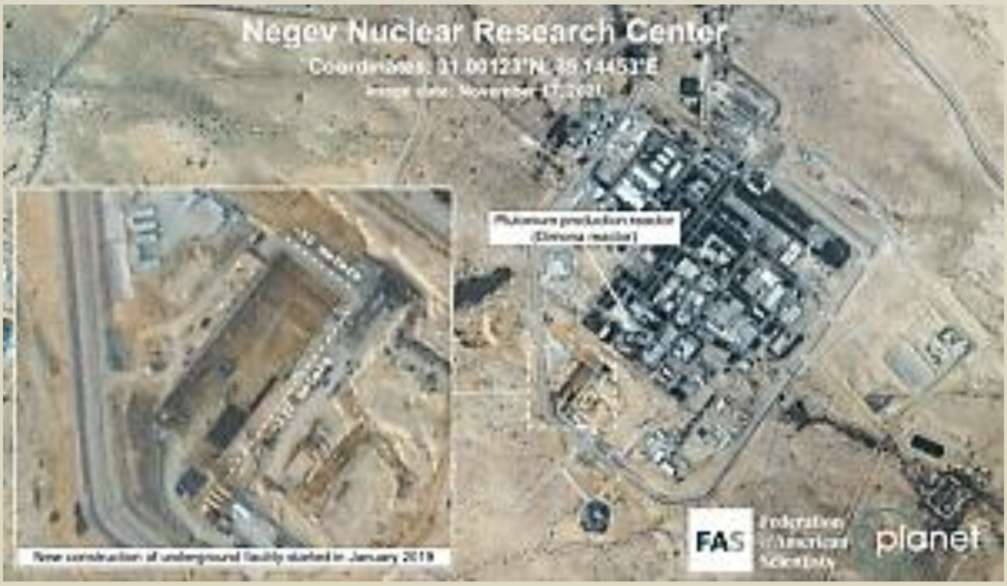
Additionally, since 1997 a US law known as the Kyl-Bingaman Amendment has prohibited US companies from publishing satellite imagery at a resolution that is "no more detailed or precise than satellite imagery of Israel that is available from commercial sources." For decades, this has meant that the majority of commercially available satellite imagery of Israel has been limited to a resolution of approximately two meters, making it very difficult to analyze in detail. However, in June 2020, the US Commercial Remote Sensing Regulatory Affairs Office announced that it would now allow commercial imagery providers to offer enhanced imagery of Israel at a resolution of 0.4 meters (National Oceanic and Atmospheric Administration 2020). The move was made in order to bring American imagery providers in line with their foreign counterparts, which had already been producing imagery at that level for several years. As a result, we have incorporated higher-resolution imagery into this article.

The history of Israel's nuclear program

The Israeli nuclear weapons program dates back to the mid-1950s, when the country's first prime minister, David Ben Gurion, began to explore a nuclear insurance plan in order to offset the combined conventional superiority of Israel's neighboring Arab states. As historian Avner Cohen writes, "Ben Gurion's determination to launch the nuclear project was the result of strategic intuition and obsessive fears, not of a well-thought-out plan. He believed Israel needed nuclear weapons as insurance if it could no longer compete with the Arabs in an arms race and as a weapon of last resort in case of an extreme military emergency" (Cohen 1998). Ben Gurion tapped Shimon Peres—who would later become Israel's prime minister—to lead Israel's nuclear program. Under Peres' stewardship, Israel purchased a substantial package, including a research reactor and plutonium separation technology, from France in 1957, as well as 20 tons of heavy water from Norway in 1959 (Cohen and Burr 2015). The ground for the Negev Nuclear Research Center was broken near Dimona in early 1958.

Although the Negev center was always intended for the development of nuclear weapons, the United States did not become aware of its true purpose for another decade, even after US intelligence became aware of its construction in 1958 (Cohen and Burr 2021). This was largely due to a highly successful Israeli deception and disinformation campaign aimed at convincing US inspectors that the complex was for civilian use. The deception campaign included lying to US officials by first telling them that the Negev center was the site of a textile factory. Next, they said that the Negev center was instead a purely civilian research center that did not contain the chemical reprocessing plant it would need to produce nuclear weapons (Cohen and Burr 2015). Investigative journalist Seymour Hersh's book, *The Samson Option*, includes a short description of the Israeli deception scheme:

"A false control room was constructed at Dimona, complete with false control panels and computer-driven measuring devices that seemed to be gauging the thermal output of a twenty-four-megawatt reactor (as Israel claimed Dimona to be) in full operation. There were extensive practice sessions in the fake control room, as Israeli technicians sought to avoid any slips when the Americans arrived. The goal was to convince the inspectors that no chemical reprocessing plant existed or was possible" (Hersh 1991).


Negev Nuclear Research Center
Coordinates: 31.00123°N, 35.14451°E
Image date: November 17, 2021
Plutonium production reactor (Dimona reactor)
New construction of underground facility started in January 2019
FAS Federation of American Scientists
planet

New construction near the plutonium production reactor at the Negev Nuclear Research Center near Dimona. Image @ 2021 Planet Labs.

Several factors appear to have contributed to the United States' susceptibility to the Israeli deception campaign. Given Israel's strong resistance to a formalized inspection protocol, the United States declined to pressure Israel to commit to one, instead acquiescing to Israel's preference to consider the arrangement as "scientific visits" instead of "inspections."

Additionally, declassified documents suggest that the United States was unaware of the degree of Franco-Israeli cooperation, and particularly the Negev center package's inclusion of a large underground chemical reprocessing plant for extracting weapons-grade plutonium. At the time, American intelligence incorrectly believed that it would be able to detect this critical facility's construction through on-site visits; however, without an agreed framework for comprehensive inspections, US visiting scientists were ill-equipped to assess the complete scope of the construction efforts at Negev. Additionally, as Avner Cohen suggests, the visiting scientists' mission "was not to challenge what they were told, but to verify it" (Cohen 1998, 107). As a result, they were unaware—and perhaps unwilling to consider the possibility—that a six-story underground reprocessing facility was being built right under their noses (Cohen and Burr 2021).

The construction of the chemical reprocessing plant was reportedly completed in 1965, and Israel began plutonium production in 1966 (Cohen and Burr 2020). It remains unclear exactly when Israel's first operational nuclear weapons were completed, although it is believed that Israel may have assembled—or attempted to assemble—its first crude nuclear devices during the May 1967 crisis immediately preceding the Six-Day War.

Nuclear ambiguity

Since the late 1960s, every Israeli government has practiced a policy of nuclear ambiguity. "Amimut," as it is known, deliberately obscures whether Israel actually possesses nuclear weapons, and if so, how its arsenal is operationalized. Since the mid-1960s, this policy has been publicly expressed—and recently reaffirmed by former prime minister Benjamin Netanyahu—as the phrase "We won't be the first to introduce nuclear weapons into the Middle East" (Netanyahu 2011).

The Israeli government's interpretation of "introducing" nuclear weapons, however, appears to have so many caveats that the statement itself is rendered essentially meaningless. This is because Israeli policymakers have previously suggested that "introducing" nuclear weapons would necessarily require Israel to test, publicly declare, or actually use its nuclear capability. Given that Israel has not officially done any of those things, the Israeli government can declare that it has not "introduced" nuclear weapons into the region, despite the high likelihood that in reality the country possesses a sizable nuclear arsenal.

Israel's policy of deliberate ambiguity was enshrined during the country's negotiations with the United States over the purchase of 50 F-4 Phantom aircraft during the late 1960s. The United States' and Israel's competing interpretations over the term "introduce" threatened to derail the arms sale entirely. In a July 1969 memorandum addressed to President Nixon, Henry Kissinger noted that "We and Israel differ on what 'introducing' nuclear weapons means. Ambassador Rabin believes only testing and making public the fact of possession constitute 'introduction.' We stated in the exchange of letters confirming the Phantom sale that we consider 'physical possession and control of nuclear arms' to constitute 'introduction" (US State Department 1969a).

During a meeting at the Pentagon in November 1968, Israel's ambassador to the United States, Yitzhak Rabin—who later succeeded Prime Minister Golda Meir as Israeli prime minister—said that "he would not consider a weapon that had not been tested to be a weapon." Moreover, he said, "There must be a public acknowledgement. The fact that you have got it must be known." Seeking clarity, US Assistant Secretary of Defense Paul Warnke

asked: “Then in your view, an unadvertised, untested nuclear device is not a nuclear weapon?” Rabin responded: “Yes, that is correct.” So, Warnke continued, an advertised but untested device or weapon would constitute introduction? “Yes, that would be introduction,” Rabin confirmed (US Defense Department 1968, 2, 3, 4).

In a follow-up exchange in July 1969, the Nixon administration plainly summarized its own understanding of the term “introduction:” “When Israel says it will not introduce nuclear weapons it means it will not possess such weapons.” The Nixon administration wanted Israel to accept the US definition, but the Meir government didn’t take the bait and instead claimed: “Introduction means the transformation from a non-nuclear weapon country into a nuclear weapon country” (US State Department 1969a). In other words, Israel construed its pledge not to be the first to introduce nuclear weapons to mean that that introduction was not about physical possession but about public acknowledgement of that possession.

Kissinger saw a way out of the disagreement: He informed President Nixon that the Israelis had defined the word “introduction” by “relating it to the NPT [Nuclear Non-Proliferation Treaty].” Kissinger’s argument was that the “distinction between ‘nuclear-weapon’ and ‘non-nuclear-weapon’ states is the one which the NPT uses in defining the respective obligations of the signatories.” He argued that the NPT negotiations “implicitly left … it up to the conscience of the governments involved” by being “deliberately vague on what precise step would transform a state into a nuclear weapon state after the January 1, 1967 cut-off date used in the treaty to define the nuclear states” (White House 1969b, 1). Kissinger also argued that the NPT does not define what it means to “manufacture” or “acquire” nuclear weapons and concluded that the new Israeli formulation “should put us in a position for the record of being able to say we assume we have Israel’s assurance that it will remain a non-nuclear state as defined in the NPT” (White House 1969b, 1).

Kissinger’s circuitous interpretation provided the United States with a way out of a diplomatic dilemma via a tacit understanding between Nixon and Meir. That is, the United States would no longer pressure Israel to sign the Nuclear Non-Proliferation Treaty as long as the Israelis kept their program restrained and invisible—meaning that Israel would not test nuclear weapons and would not acknowledge in public its possession of such weapons.

The goal of this interpretation, stated a July 1969 memo, was to break the diplomatic deadlock while avoiding direct complicity in Israel’s nuclear program, which would have contradicted the United States’ own non-proliferation policies. Specifically, the memo noted that the United States “cannot enforce a precise understanding” of what “introduction” means. Instead, the policy should be to “mainly concern ourselves with building a record that will permit us to defend taking our distance from a nuclear Israel if ever Israel’s use of those weapons threatens to involve us in nuclear confrontation” (White House 1969d). Despite this attempt to distance itself from Israel’s nuclear program, the United States’ clear willingness to turn a blind eye to Israeli proliferation is a double standard that has largely undermined its own credibility when criticizing the nuclear pursuits of other Middle Eastern countries.

After the end of the Cold War, Israel began to fear that the United States’ tacit support for Israel’s undeclared nuclear arsenal would soon fade, given US engagement on a possible Middle East nuclear-weapon free zone. As a result, Israel has reportedly requested that each American president since Bill Clinton sign a letter indicating that any future US arms control efforts would not affect Israel’s nuclear arsenal (Entous 2018a; Entous 2018b).

On a few rare occasions, some Israeli officials have made statements implying that Israel already has nuclear weapons or could “introduce” them very quickly if necessary. The first came in 1974, when then-President Ephraim Katzir stated: “It has always been our intention to develop a nuclear potential … We now have that potential” (Weissman and Krosney 1981, 105). Long after his retirement, in a 1981 *New York Times* interview, former defense minister Moshe Dayan also came close to violating the nuclear ambiguity taboo when he declared for the record: “We don’t have any atomic bomb now, but we have the capacity, we can do that in a short time.” He reiterated the official policy mantra: “We are not going to be the first ones to introduce nuclear weapons into the Middle East” (*New York Times* 1981). But his acknowledgement that “we have the capacity” and would quickly produce atomic bombs if Israel’s adversaries acquired nuclear weapons was a hint that Israel had in fact produced all the necessary components to assemble nuclear weapons in a very short time (*New York Times* 1981).

During a press conference in Washington with US President Bill Clinton and Jordan’s President Hussein in 1994, Israeli Prime Minister Yitzhak Rabin made a similar statement, saying “Israel is not a nuclear country in terms of weapons” and has “committed to the United States for many years not to be the first to introduce nuclear weapons in the context of the Arab-Israeli conflict. But at the same time,” he added, “we cannot be blind to efforts that are made in certain Muslim and Arab countries in this direction. Therefore, I can sum up. We’ll keep our commitment not to be the first to introduce, but we still look ahead to the dangers that others will do it. *And we have to be prepared for it*” (Rabin 1994; emphasis added).

The ambiguity left by Israel’s refusal to confirm or deny the possession of nuclear weapons prompted the BBC in 2003 to bluntly ask former Prime Minister Shimon Peres: “The term nuclear ambiguity, in some ways it sounds very grand, but isn’t it just a euphemism for deception?” Peres did not answer the question but confirmed the need for deception: “If someone wants to kill you and you use deception to save your life, it’s not immoral. If we wouldn’t [sic] have enemies we wouldn’t need deceptions” (BBC 2003).

Three years later, in a December 2006 interview with German television, then-prime minister Ehud Olmert appeared to compromise the deception when he criticized Iran for aspiring “to have nuclear weapons, as America, France, Israel, Russia" (Williams 2006). The statement, which he made in English, attracted widespread attention because it was seen as an inadvertent admission that Israel possesses nuclear weapons (Williams 2006). A spokesperson for Olmert later said he had been listing not nuclear states but "responsible nations" (Friedman 2006).

Ambiguity is not just about refusing to *confirm* possession of nuclear weapons but also about refusing to *deny* it. When asked during a 2011 CNN interview if Israel *does not* have nuclear weapons, Netanyahu did not answer directly but repeated the policy not to be the first to "introduce" nuclear weapons into the Middle East. Undeterred, the journalist followed up: "But if you take an assumption that other countries have them then that may mean you have them?" Netanyahu didn't dispute that but implied that the difference is that Israel doesn't threaten anyone with its arsenal: "Well, it may mean that we don't pose a threat to anyone. We don't call for anyone's annihilation … We don't threaten to obliterate countries with nuclear weapons but we are threatened with all these threats" (Netanyahu 2011).

Three cases of near-introduction

There have been three distinct incidents during which Israel reportedly came close to "introducing" nuclear weapons to the region, under its own narrow definition. The first instance was during the Six-Day War in June 1967, when according to primary sources and testimonies from former Israeli officials, a small team of commandos was tasked with conducting Operation "Shimson" (Samson)—a planned nuclear detonation for demonstrative purposes—in order to change the Arab coalition's military calculus. Given Israel's eventual military success in the war, this plan was never put into action (Cohen 2017).

The second instance reportedly came during the October 1973 Yom Kippur War, when Israeli leaders feared that Syria was about to defeat the Israeli army in the Golan Heights. The rumor first appeared in *Time* magazine in 1976, was greatly expanded upon in Seymour Hersh's book *The Samson Option* in 1991, and several unidentified former US officials allegedly stated in 2002 that Israel put nuclear forces on alert in 1973 (see e.g., Sale 2002).

However, an interview conducted by Avner Cohen with the late Arnan (Sini) Azaryahu in January 2008 calls into question the validity of this rumor. Azaryahu was senior aide and confidant to Yisrael Galili, a minister without portfolio who was Golda Meir's closest political ally and privy to some of Israel's most closely held nuclear secrets. In the early afternoon of the second day of the war—October 7, 1973—the Israeli military appeared to be losing the battle against Syrian forces in the Golan Heights. Azaryahu said that the defense minister, Moshe Dayan, asked Meir to authorize initial technical preparations for a "demonstration option"—that is, to ready nuclear weapons for potential use. But Galili and Deputy Prime Minister Yigal Allon argued against the idea, saying Israel would prevail using conventional weapons. According to Azaryahu, Meir sided with her two senior ministers and told Dayan to "forget it" (Cohen 2013). (For analysis of the Azaryahu interview and its implications, see Cohen 2008.)

A study by the Strategic Studies division of the Center for Naval Analyses in April 2013 appeared to confirm Meir's rejection of Dayan's "demonstration option" and that Israel's nuclear forces were not readied. The report states that the authors "did exhaustively scrutinize" the document files of US agencies and archives and interviewed a significant number of officials with firsthand knowledge of the 1973 crisis. Still, it also notes that "(n)one of these searches revealed any documentation of an Israeli alert or clear manipulation of its forces," and "none of our interviewees, save one, recalled any Israeli nuclear alert or signaling effort" during the Yom Kippur War (Colby et al. 2013, 31–32).

Even so, a single former official recalled seeing an "electronic or signals intelligence report" at the time that "Israel had activated or increased the readiness of its Jericho missile batteries." That, together with the extreme government secrecy that surrounds Israeli nuclear weapons in general, led the authors of the Center for Naval Analyses study to conclude that "the United States did observe some kind of Israeli nuclear weapons-related activity in the very early days of the war, probably pertaining to Israel's Jericho ballistic missile force … ." (Colby et al. 2013, 34). The study's overall assessment was that "Israel appears to have taken preliminary precautionary steps to protect *or prepare* its nuclear weapons and/or related forces" (Colby et al. 2013, 2; emphasis added).

The conclusion that Israel did something with its nuclear forces in October 1973—although not necessarily place them on full operational alert or prepare for a "demonstration option"—seems similar to the assertion made by Peres in 1995. In an interview with the authors of *We All Lost the Cold War*, Peres "categorically denied that Jericho missiles were made ready, much less armed. At most, he insisted, there was an operational check. The cabinet never approved any alert of Jericho missiles" (Lebow and Stein 1995, 463, footnote 47).

Evidently, some uncertainty persists about the 1973 events. But then, presumably as well as now, the Israeli warheads were not fully assembled or deployed on delivery systems under normal circumstances but stored under civilian control. And since no official confirmation was made back then either via a test or an announcement, no formal "introduction" of nuclear weapons occurred—at least in the opinion of Israeli officials.

The third potential instance of near-introduction came six years later, on September 22, 1979, when a US surveillance satellite known as the Vela 6911 detected what appeared to be a double-flash from a nuclear test in the southern parts of the Indian Ocean. (For background on the 1979 Vela incident, see Richelson 2006; Cohen and Burr 2016.)

Declassified US intelligence documents indicate the prevailing US belief at the time that the flash was the result of an Israeli nuclear test, possibly with South African logistical support. A subsequent 1980 White House panel concluded that the the Vela signal "was probably not from a nuclear event." However, US scientists and intelligence analysts, who believed that the panel's conclusions had been heavily biased in order to avoid a political confrontation with Israel, widely rejected these conclusions, according to newly declassified documents. Additionally, the documents appear to suggest that Israeli sources leaked confirmations about the nuclear test to US officials and journalists, but that these claims were either censored or not taken seriously (Cohen and Burr 2016). If the Vela incident was indeed an Israeli nuclear test, it is unclear whether it would constitute the "introduction" of nuclear weapons under Israel's narrow definition. That is, according to Yitzhak Rabin at the time of the negotiations in the late 1960s, "There must be a public acknowledgement. The fact that you have got it must be known" (US Defense Department 1968). Successive Israeli governments have never publicly acknowledged Israel's involvement in the Vela incident.

Stockpile size and warhead composition

Absent official public information from the Israeli government or intelligence communities of other countries, speculations abound about Israel's nuclear arsenal. Over the past several decades, news media reports, think tanks, authors, and analysts have presented a wide range of possibilities for the size of the Israeli nuclear stockpile, from 75 warheads to more than 400 warheads. Delivery vehicles for the warheads have been listed as aircraft, ballistic missiles, artillery tactical or battlefield weapons such as artillery shells and landmines, and more recently sea-launched cruise missiles.[2] We believe that many of these rumors are inaccurate and that the most credible stockpile number is less than one hundred warheads, probably on the order of 90 warheads for delivery by aircraft, land-based ballistic missiles, and possibly sea-based cruise missiles (see Table 1).

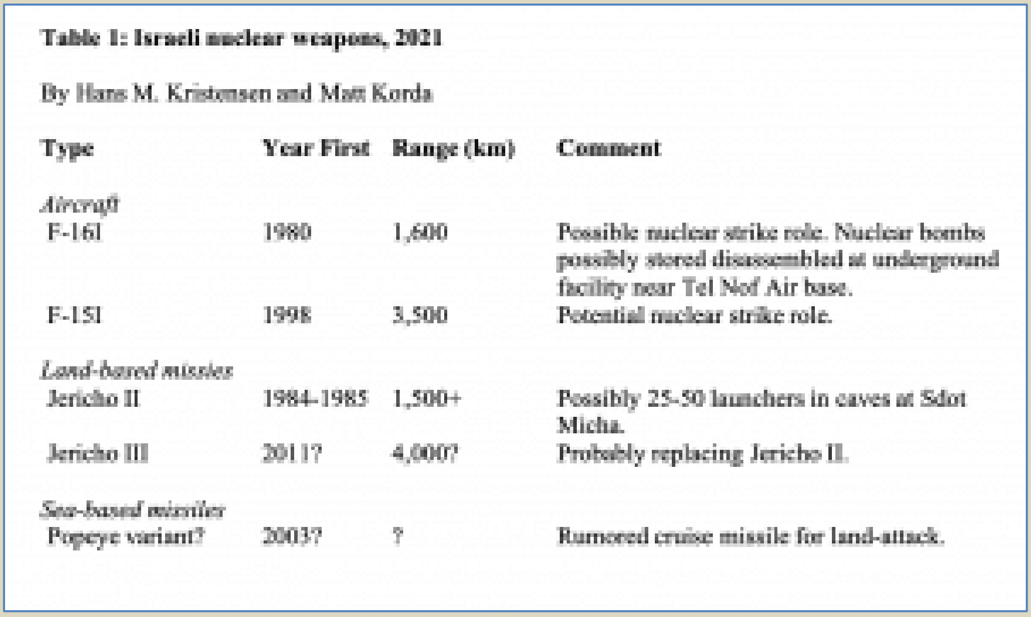


Table 1: Israeli nuclear weapons, 2021

By Hans M. Kristensen and Matt Korda

Type	Year First	Range (km)	Comment
Aircraft			
F-16I	1980	1,600	Possible nuclear strike role. Nuclear bombs possibly stored disassembled at underground facility near Tel Nof Air base.
F-15I	1998	3,500	Potential nuclear strike role.
Land-based missiles			
Jericho II	1984-1985	1,500+	Possibly 25-50 launchers in caves at Sdot Micha.
Jericho III	2011?	4,000?	Probably replacing Jericho II.
Sea-based missiles			
Popeye variant?	2003?	?	Rumored cruise missile for land-attack.

Table 1: Israeli nuclear weapons, 2021

The design and sophistication level of Israel's nuclear weapons is up for considerable debate. Frank Barnaby, a nuclear physicist who worked at the British Atomic Weapons Research Establishment, interviewed whistleblower and former nuclear technician Mordechai Vanunu in 1986. Barnaby later said that Vanunu's description of "production at Dimona of lithium-deuteride in the shape of hemispherical shells … raised the question of whether Israel had boosted nuclear weapons in its arsenal" (Barnaby 2004, 4). Although he didn't think Vanunu had much knowledge about such weapons, Barnaby concluded that "the information he gave suggested that Israel had more advanced nuclear weapons than Nagasaki-type weapons" (Barnaby 2004, 4).

Barnaby did not mention thermonuclear weapons in his 2004 statement, even though he concluded in his book *The Invisible Bomb* in 1989 that "Israel *may have* about 35 thermonuclear weapons" (Barnaby 1989, 25). At the time, the director of the CIA apparently did not agree but reportedly indicated that Israel *may be seeking* to construct a thermonuclear weapon (Cordesman 2005). Yet *The Samson Option* claims that US weapon designers concluded from Vanunu's information that "Israel was capable of manufacturing one of the most sophisticated weapons in the nuclear arsenal—a low-yield [two-stage] neutron bomb" (Hersh 1991, 199). The authors of *The Nuclear Express* in 2009 echoed that claim, stating that the product of Israel's partnership with South Africa would be "a family of boosted primaries, generic H-bombs, and a specific neutron bomb" (Reed and Stillman 2009, 174).

On the other hand, an April 1987 report by the Institute for Defense Analyses concluded—following a trip to Israel's Soreq Nuclear Research Center—that Israel lacked the computational sophistication to develop the "codes which detail fission and fusion processes on a microscopic and macroscopic level," which would be necessary for the development of thermonuclear weapons (Townsley and Robinson 1987).

If Israel was indeed behind the 1979 Vela incident, the country would have conducted only one known atmospheric nuclear test; this could indicate that Israel's nuclear weapons designs are not particularly sophisticated. It took other nuclear weapon states dozens of elaborate nuclear test explosion experiments to develop sophisticated weapon designs. According to some analysts, however, Israel had "unrestricted access to French nuclear test explosion data" in the 1960s (Cohen 1998, 82–83), so much so that "the French nuclear test in 1960 made two nuclear powers not one" (Weissman and Krosney 1981, 114–117). Until France broke off deep nuclear collaboration with Israel in 1967, France conducted 17 fission warhead tests in Algeria, ranging from a few kilotons to approximately 120 kilotons of explosive yield (CTBTO(n.d.); Nuclear Weapon Archive 2001). France did not conduct its first two-stage thermonuclear test until August 1968.

In sum, it remains highly challenging to assess Israel's design sophistication for its nuclear weapons. It is hypothetically possible that Israel developed two-stage thermonuclear weapons. Yet a more cautious analysis based upon Israel's plutonium production, testing history, design skills, force structure, and employment strategy suggests that its arsenal probably consists of single-stage, boosted fission warheads.

Most publicly available estimates of the number of Israeli warheads in its stockpile appear to be derived from a rough calculation of the number of warheads that could hypothetically be created from the amount of plutonium Israel is believed to have produced in its nuclear reactor at Dimona. The technical assessment that accompanied the 1986 *Sunday Times* article about former nuclear technician Mordechai Vanunu's disclosures, for example, estimated that Israel had produced enough plutonium for 100 to 200 nuclear warheads (*Sunday Times* 1986a, 1986b, 1986c).[3] In the public debate, this quickly became Israel *possessing* 100 to 200 nuclear warheads, the estimate that has been most commonly used ever since. Analysts are uncertain about the operational history or efficiency of the Dimona reactor's operation over the years, but plutonium production is thought to have continued after 1986. The International Panel on Fissile Materials estimates that as of the beginning of 2020, Israel may have a stockpile of about 980 ± 130 kilograms of plutonium (International Panel on Fissile Materials 2021). That amount could potentially be used to build anywhere between 170 and 278 nuclear weapons, assuming a second-generation, single-stage, fission-implosion warhead design with a boosted pit containing 4 to 5 kilograms of plutonium.[4]

Total plutonium production is a misleading indicator of the actual size of the Israeli nuclear arsenal, however, because Israel—like other nuclear-armed states—most likely would not have converted all of its plutonium into warheads; a portion is likely stored as a strategic reserve. Additionally, the total number of deliverable warheads would presumably be tied to Israel's limited number of aircraft and missiles that are equipped to deliver nuclear weapons, as well as to the limited number of targets that Israel would seek to strike in a conflict. As a result, estimates of the Israeli nuclear stockpile numbering in the hundreds of warheads may be exaggerated.

US government assessments offer more conservative estimates of Israel's nuclear arsenal. A classified 1999 Defense Intelligence Agency report leaked in 2004 described Israel's nuclear arsenal as numbering between 60 and 80 warheads in 1999, with the potential to grow to between 65 and 85 warheads by 2020 (Defense Intelligence Agency 1999).[5] In a similar vein, in 1998 a RAND Corporation study commissioned by the Pentagon concluded that Israel had enough plutonium to build 70 nuclear weapons (Schmemann 1998).

During the two decades that have passed since the DIA report, Israel presumably has continued the production of plutonium at Dimona for some of that time. Given Israel's presumed surplus of plutonium at this stage, the Dimona reactor's current primary role is likely producing tritium, in order to replenish the material as it decays. The Dimona complex has probably also continued producing nuclear warheads. Many of those warheads were probably replacements for warheads produced earlier for existing delivery systems, such as the Jericho II missiles and aircraft. Warheads for a rumored Jericho III ballistic missile would probably replace existing Jericho II warheads on a one-for-one basis. Warheads for the rumored submarine-based cruise missile, if true, would be in addition to the existing arsenal but probably only involve a relatively small number of warheads.

The reactor at Dimona is nearing the end of its useful design life, and the condition of the aluminum reactor pressure vessel—which cannot be replaced as part of a life-extension project—is believed to be deteriorating. Nevertheless, Israeli officials have indicated that they intend to keep the reactor operating until 2040 (Kelley and Dewey 2018). Satellite photos from February 2021 indicate that Dimona is currently undergoing its largest construction project in decades, with a large dig several stories deep located near the reactor (Gambrell 2021). It is unclear whether this new construction is related to Dimona's life-extension campaign. Eventually, the Dimona reactor will need to be replaced; however, Israel's non-party status to the Non-Proliferation Treaty means that it may face challenges purchasing a replacement reactor from another country. This is because it would theoretically be subject to strict export controls by the Nuclear Suppliers Group (Kelley and Dewey 2018).

Nuclear-capable aircraft

Since the 1980s, the F-16 has been the backbone of the Israeli Air Force. Over the years, Israel has purchased well over 200 F-16s of all types, as well as specially configured F-16Is. Various versions of the F-16 serve nuclear strike roles in the US Air Force and among NATO allies, and the F-16 is the most likely candidate for air delivery of Israeli nuclear weapons at the present time.

Since 1998, Israel has also used its 25 Boeing F-15E Strike Eagles for long-range strike and air-superiority roles. The Israeli version, known as the F-15I (or "Baz"), is characterized by greater takeoff weight—36,750 kilograms—and range—4,450 kilometers—than other F-15 models. Its maximum speed at high altitude is Mach 2.5. The plane has been further modified with specialized radar that has terrain-mapping capability and other navigation and guidance systems. In the US Air Force, the F-15E Strike Eagle has been given a nuclear role. It is not known if the Israeli Air Force has added nuclear capability to this highly versatile plane, but when Israel sent half a dozen F-15Is from Tel Nof air base to the United Kingdom in September 2019, a US official privately commented that Israel had sent its nuclear squadron (Kristensen 2019).

Israel has recently purchased 50 F-35s from the United States, becoming the first non-US country to operate the aircraft. The Israeli version of the aircraft—which will include indigenously designed electronic warfare suites, guided bombs, and air-to-air missiles—is known as the F-35I (named "Adir" for "awesome" or "mighty"). As of September 2021, Israel has received 30 F-35Is, operating them in three squadrons from Nevatim Air Base: the 140th ("Golden Eagle") squadron, the Israeli Air Force's first squadron of F-35s; the 116th ("Lions of the South") squadron; and the 117th ("First Jet") squadron, the latter of which is currently operating only as a training squadron. The remaining 20 F-25s are scheduled to be delivered by 2024 (Gross 2021; Pansky 2020). The F-35 squadrons are gradually replacing the aging F-16s; the 117th squadron was deactivated in October 2020 in order to swap out its F-16C/D aircraft with the requisite F-35 training systems (Gross 2020). The US Air Force is upgrading its F-35As to carry nuclear bombs, and Israel's Channel 2 reported that an unnamed "senior level US official" refused to say if Israel had requested such an upgrade for its F-35s (Channel 12 2014).

It is especially difficult to determine which Israeli wings and squadrons are assigned nuclear missions and which bases support them.

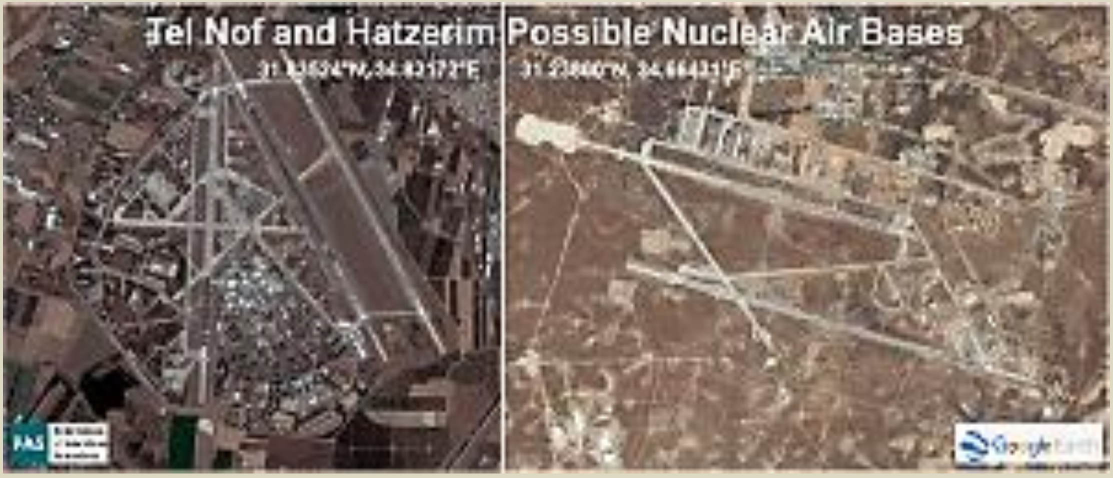


Figure 2: Tel Nof and possibly Hatzerim air bases might have nuclear weapons roles. Images © Maxar via Google Earth

The nuclear warheads themselves may be stored in underground facilities near one or two bases. Israeli F-16 squadrons are based at Ramat David Air Base in northern Israel; Tel Nof and Hatzor air bases in central Israel; and Hatzerim, Ramon, and Ovda air bases in southern Israel. Of the many F-16 squadrons, only a small fraction—perhaps one or two—would actually be nuclear-certified with specially trained crews, unique procedures, and modified aircraft. The F-15s are based at Tel Nof Air Base in central Israel, and Hatzerim Air Base in the Negev desert. We cautiously suggest that Tel Nof Air Base in central Israel and Hatzerim Air Base in the Negev desert might have nuclear missions.

Land-based ballistic missiles

Israel's nuclear missile program dates back to the early 1960s. In April 1963, several months before the Dimona reactor began producing plutonium, Israel signed an agreement with the French company Dassault to produce a short-range surface-to-surface ballistic missile. The missile system became known as the Jericho (or MD-620), and the program was completed around 1970 with 24 to 30 missiles.

Most sources assert that Jericho was a mobile missile, transported and fired from a transportable erector launcher (CIA 1974). But there have occasionally been references to possible silos for the weapon. A US State Department study produced in support of National Security Study Memorandum 40 in May 1969 concluded that Israel believed it needed a nearly invulnerable nuclear force to deter a nuclear first strike from its enemies, "i.e., having a second-strike capability." The study stated: "Israel is now building such a force—*the hardened silos of the Jericho missiles*" (US State Department 1969d, 7; emphasis added). It is not clear that the claim of "hardened silos" constituted the assessment of the US intelligence community or whether it referred to early construction of what is now thought to be mobile launcher bunkers at Sdot Micha, and only a few subsequent sources—

all non-governmental—have mentioned Israeli missile silos.[6] We have not found any public evidence of Jericho silos.

In collaboration with South Africa, in the late 1980s Israel developed the two-stage, solid-fuel, medium-range Jericho II that—for the first time—put the southern-most Soviet cities and the Black Sea Fleet within range. Jericho II, a modified version of the Shavit space launch rocket, was first deployed in the early-1990s, replacing the first Jericho. The Jericho was first flight-tested in May 1987 to approximately 850 kilometers (527 miles). The trajectory went far into the Mediterranean Sea. Another test in September 1989 reached 1,300 kilometers (806 miles). The US Air Force National Air Intelligence Center in 1996 reported the Jericho II range as 1,500 kilometers (930 miles) (NAIC 1996).

Given that approximately half of Iran (including Tehran) is beyond the range of Jericho II medium range ballistic missile, Israel is currently upgrading its arsenal with the newer and more capable three-stage Jericho III intermediate-range ballistic missile. The Jericho III reportedly has a range exceeding 4,000 kilometers, which would be able to target all of Iran, Pakistan, and all of Russia west of the Urals—including, for the first time, Moscow. Jericho III was first test-launched over the Mediterranean Sea in January 2008 and reportedly became operational in 2011. Unidentified defense sources told *Jane's Defence Weekly* that Jericho III constitutes "a dramatic leap in Israel's missile capabilities" (*Jane's Defence Weekly* 2008, 5), but many details and its current status are unknown. In July 2013, Israel tested an "improved" version of the Jericho III missile—possibly designated the Jericho IIIA—with a new motor that some sources believe may offer the missile an intercontinental range exceeding 5,500 kilometers (Ben David 2013a; Ben David 2013b). It is unclear whether Israel is replacing its Jericho II missiles with Jericho IIIs on a one-for-one basis, or if they are being deployed concurrently, although the former is more likely. Upgrades of suspected launcher bunkers at Sdot Micha began in 2014.

In recent years, Israel has conducted several test-launches of what it calls "rocket propulsion systems." These tests—which have been conducted in May 2015, May 2017, December 2019, and January 2020—are typically not accompanied by confirmation of an official test location (Agence France-Presse 2015; Ministry of Defense 2017; Kubovich 2019; Ministry of Defense 2020). However, local news sources and video footage indicate that the test site is likely to be Palmachim Air Base, Israel's Jericho missile and Shavit space launch vehicle test site located on the Mediterranean coast (Trevithick 2019). In April 2021, video footage captured a significant blast at Sdot Micha Air Base, which external analysts have suggested was likely to be another rocket engine test (Lewis 2021). Unlike the previous tests, however, the Defense Ministry did not provide a statement confirming it as such. The flurry of rocket propulsion test activity has stirred up speculation that Israel could be developing a newer version of its Jericho missile, possibly known as Jericho-IV.

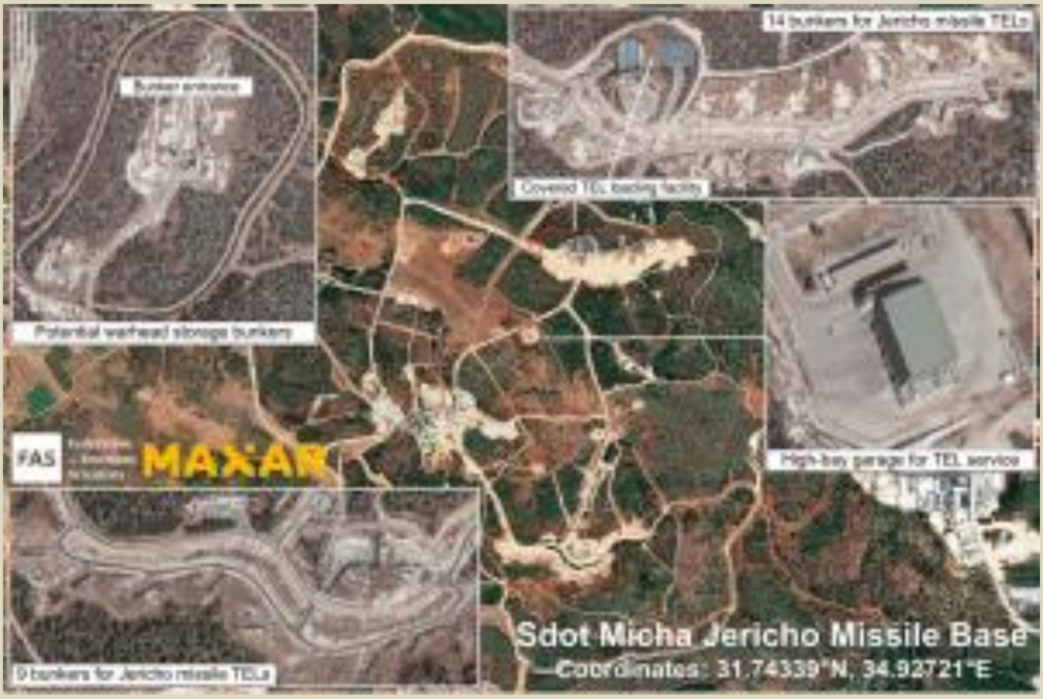

14 bunkers for Jericho missile TELs
Bunker entrance
Covered TEL loading facility
Potential warhead storage bunkers
High-bay garage for TEL service
FAS
MAXAR
9 bunkers for Jericho missile TELs
Sdot Micha Jericho Missile Base
Coordinates: 31.74339°N, 34.92721°E

Figure 3: The suspected Sdot Micha Jericho nuclear missile base includes two dozen bunkers for mobile launchers. Satellite imagery © 2022 Maxar Technologies (image date October 8, 2021).

How many Jericho missiles Israel has is another uncertainty. Estimates vary from 25 to 100. Most sources estimate that Israel has 50 of these missiles and place them at the Sdot Micha facility near the town of Zakharia in the Judean Hills, approximately 27 kilometers east of Jerusalem. (There are many alternative spellings and names for the base, including Zekharyeh, Zekharaia, Sdot Micha, and Sdot HaElla.)

Commercial satellite images show what appear to be two clusters of what might be caves or bunkers for mobile Jericho launchers at Sdot Micha. The northern cluster includes 14 caves and the southern cluster has nine caves, for a total of 23 caves. Newly available high-resolution imagery indicates that each cave appears to have two entrances, which suggests that each cave can hold up to two launchers. The satellite images show that caves' refurbishment began in 2014 and appeared complete in 2020. The upgrade also included upgrades to several tunnels to underground facilities. If all 23 caves are full, this would amount to 46 launchers. Each cluster also has what appears to be a covered high-bay drive-through facility, potentially for missile handling or warhead loading. A nearby complex with its own internal perimeter has four tunnels to underground facilities that could potentially be for warhead storage.

For the Jericho missiles to have military value, they would need to be able to disperse from their caves. The Sdot Micha base is relatively small at 16 square kilometers, and the suspected launcher caves are located along two roads, each of which is only about one kilometer long. This layout would provide protection against limited conventional attacks, but it would be vulnerable to a nuclear surprise attack. In a hypothetical crisis where the Israeli leadership decided to activate Israel's nuclear capability, the launchers presumably would leave Sdot Mischa and take up positions in remote launch areas. A US State Department background paper from 1969 stated that there was "evidence strongly indicating that several sites providing operational launch capabilities are virtually complete" (US State Department 1969c, 4; emphasis added).

Sea-based missiles and submarines

Israel currently operates three German-built Dolphin-class and two Dolphin II-class diesel-electric submarines. The Dolphin II-class submarines are functionally identical to the Dolphin-class submarines, but with the addition of an Air Independent Propulsion system, which alleviates the need for the submarine to raise a snorkel to the surface to supply air to the engines and recharge the batteries (Sutton 2017). This reportedly allows the Dolphin II-class submarines to remain underwater for at least 18 days at a time—more than four times longer than the Dolphin-class submarines (*Der Spiegel* 2012). A sixth submarine—the final submarine in the fleet of Dolphin subs—is currently being fitted out (Shoval 2019). In 2017, the Netanyahu government signed a memorandum of understanding with Germany to acquire three additional Dolphin II-class submarines to replace the three older Dolphin submarines; however, the procurement deal has been delayed due to an ongoing corruption scandal (Opall-Rome 2017). Although Israel's submarines are home-ported near Haifa on the Mediterranean coast, in recent years they have occasionally sailed through the Suez Canal, as a likely deterrence signal to Iran (*Times of Israel* 2020; *Times of Israel* 2021).

In addition to six standard 533 millimeter torpedo tubes, Israel's submarines are reportedly equipped with four additional specially-designed 650 millimeter tubes (Sutton 2017). Analysts speculate that the unusual diameter of these tubes means that they could be used to carry a sea-launched variant of the indigenously designed "Popeye Turbo" air-to-surface missile,[7] although rumors about a range over 1,000 kilometers were probably exaggerated. The German magazine *Der Spiegel* reported in 2012 that the German government had known for decades that Israel planned to equip the submarines with nuclear missiles. Former German officials said they always assumed Israel would use the submarines for nuclear weapons, although the officials appeared to repeat old rumors rather than provide new information. The article quoted another unnamed ministry official with knowledge of the matter: "From the beginning, the boats were primarily used for the purposes of nuclear capability" (*Der Spiegel* 2012).

Endnotes

1. For the National Security Archive's collections of declassified US government documents relating to Israel's nuclear weapons capability, see Cohen and Burr 2006; Cohen and Burr 2015; Cohen and Burr 2016; and Cohen and Burr 2020.
2. For examples of claims about tactical and advanced nuclear weapons, see Hersh 1991: 199–200, 216–217, 220, 268, 276 (note), 312, 319).
3. Frank Barnaby, who cross-examined Vanunu on behalf of the *Sunday Times*, stated in 2004 that the estimate for Israel's plutonium inventory—sufficient for "some 150 nuclear weapons"—was based on Vanunu's description of the reprocessing plant at Dimona (Barnaby, 2004: 3–4).
4. The four to five kilograms of plutonium per warhead assumes high-quality technical and engineering performance for production facilities and personnel. Lower performance would need a greater amount of plutonium per warhead and therefore reduce the total number of weapons that Israel could potentially have produced.
5. The secret document was leaked and reproduced in Scarborough (2004: 194–223). It is important to caution that as a Defense Intelligence Agency document, the report does not necessarily represent the coordinated assessment of the US intelligence community as a whole, only the view of one part of it. An excerpt from the Defense Intelligence Agency report is available at Kristensen and Aftergood (2007).
6. For an example of sources claiming Jericho missiles are deployed in silos, see Cordesman (2008). Cordesman references the Nuclear Threat Initiative country profile on Israeli missiles as the source for the silo claim. The NTI has since updated its page, which no longer mentions silos. See: https://www.nti.org/countries/israel/.
7. For a lengthier exploration of the history of Israel's sea-launched missile capability, see the *2014 Israel Nuclear Notebook*, available at: Kristensen and Norris 2014.

Hans Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press)

and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored Nuclear Notebook since 2001.

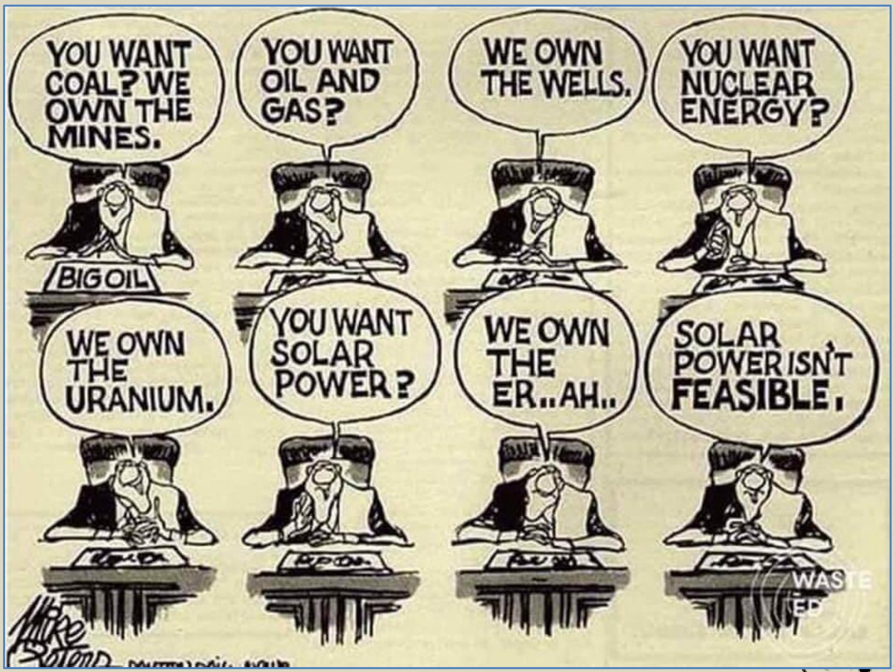
Matt Korda is a Senior Research Associate and Project Manager for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the Nuclear Notebook with Hans Kristensen. Matt is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Matt received his MA in International Peace & Security from the Department of War Studies at King's College London, and a BA in European Studies from the University of Toronto.

Military attacks against nuclear power plants

Source: https://en.wikipedia.org/wiki/Vulnerability_of_nuclear_plants_to_attack

Nuclear reactors become preferred targets during military conflict and, over the past three decades, have been repeatedly attacked during military air strikes, occupations, invasions and campaigns:

- On 25 March 1973, before its completion, the Atucha I Nuclear Power Plant in Argentina was temporarily taken over by the People's Revolutionary Army who seized a FMK-3 submachine gun and three .45 caliber handguns from the security detachment. When they retired they had a confrontation with the police, injuring two police officers.
- On 30 September 1980, during the Iran-Iraq War, the Islamic Republic of Iran Air Force carried out Operation Scorch Sword, a surprise airstrike on the Al Tuwaitha nuclear complex in Ba'athist Iraq, The raid, which occurred 17 kilometers southeast of Baghdad, damaged an almost complete nuclear reactor.
- In June 1981, Operation Opera was an Israeli Air Force air strike that completely destroyed Iraq's Osirak nuclear research facility.
- On 8 January 1982, the 70th anniversary of the formation of the African National Congress, Umkhonto we Sizwe, the armed wing of the ANC attacked Koeberg Nuclear Power Station while it was still under construction and planted four limpet mines inside the facilities. Damage from the explosions was estimated at R 500 million and the commissioning of the plant was put back by 18 months.
- Between 1984 and 1987, Iraq bombed Iran's Bushehr nuclear plant six times.
- In 1991, during the Persian Gulf War, the U.S. Air Force bombed three nuclear reactors and an enrichment pilot facility in Iraq.
- In 1991, during the Iraqi missile attacks on Israel and Saudi Arabia, Iraq launched Scud missiles at Israel's Dimona nuclear complex.
- In September 2007, Israel bombed a Syrian reactor under construction in Deir ez-Zor Governorate.



This 70s cartoon is still too accurate!

International CBRNE Institute

CBRNE-Terrorism Newsletter

C2BRNE Diary

EXPLOSIVE NEWS

Saudi Arabia appears to be building its own ballistic missiles with China's help

Source: https://www.cnbc.com/2021/12/26/saudi-arabia-appears-to-be-building-its-own-ballistic-missiles-with-chinas-help.html

Dec 25 – Saudi Arabia is building its own ballistic missiles with the help of China, according to United States intelligence assessments and satellite images.

The assessment of U.S. intelligence agencies is that **the kingdom, which is long thought to have acquired missiles from Beijing, is now manufacturing its own**, according to a source familiar with the matter and a U.S. official.

Satellite images obtained by NBC News also suggest that Saudi Arabia is producing ballistic missiles at a site west of the capital, Riyadh, according to researchers at the Middlebury Institute of International Studies at Monterey, in California.

"The key piece of evidence is that the facility is operating a 'burn pit' to dispose of solid-propellant leftover from the production of ballistic missiles," wrote Jeffrey Lewis and David Schmerler of the James Martin Center for Nonproliferation Studies at the Middlebury Institute.

They added that the site "appears to have been constructed with Chinese assistance."

The news was first reported by CNN on Thursday. The images were provided by commercial imaging company Planet Labs PBC.

The development could shift security calculations in the Middle East and further complicate the Biden administration's efforts to coax Iran back into its nuclear deal with world powers. It could also add another layer of complexity to Washington's relations with Beijing.

Iran and Saudi Arabia are regional foes and there will be concern that Riyadh's manufacturing of ballistic missiles could alter Tehran's calculations on its possible agreements in talks aimed at reviving the 2015 accord. The new development comes days before the talks, which have struggled to make any headway, are expected to resume in Vienna, and may make Iran even more unlikely to give up its own ballistic missiles.

"If Iran were to enter into negotiations over its missile programme, it would be unlikely to accept limits that did not also apply to other countries," wrote Mark Fitzpatrick, an associate fellow at the London-based International Institute for Strategic Studies, in an article about Saudi Arabia's ballistic missile program published by the institute in August.

Fitzpatrick, a former State Department official, said at the time that other than a general desire to keep pace with Iran, Riyadh's motivations for acquiring ballistic missiles were not entirely clear. Unlike Tehran, however, Saudi Arabia is not known to have initiated any work to develop a nuclear warhead for its missiles, he added.

Ballistic missiles are rocket-propelled weapons that can carry conventional explosives as well as nuclear warheads.

Nevertheless, the fact that Saudi Arabia is now known to be manufacturing its own ballistic missiles will spark concerns of a ramped-up arms race in a highly tense region that is already riven with conflict.

The Saudi Ministry of Media did not respond to requests for comment.

Britain on Friday condemned a launch of ballistic missiles by Iran in war games conducted this week.

"These actions are a threat to regional and international security and we call on Iran to immediately cease its activities," the Foreign Office said in a statement.

In 2018, former President Donald Trump withdrew the United States from the nuclear accord and re-imposed crippling sanctions on Iran. Tehran has since reduced its compliance with the deal, announcing that it would enrich uranium to up to 60 percent purity — significantly closer to the amount needed to make an atomic bomb.

In the past, Saudi Arabia's de facto leader, Crown Prince Mohammed bin Salman, has been clear that if Tehran develops a nuclear bomb, Riyadh will also do so.

"Saudi Arabia does not want to acquire any nuclear bomb, but without a doubt if Iran developed a nuclear bomb, we will follow suit as soon as possible," he told CBS in 2018.

The crown prince is attempting to transform Saudi Arabia from an oil-dependent nation into an economic powerhouse that is more accepted in the West.

The Saudis have long been U.S. allies and enjoyed a close relationship with the Trump administration, but those efforts to overhaul the country's image were tainted by the murder of journalist Jamal Khashoggi in the Saudi consulate in Istanbul in 2018.

Meanwhile, the **continued close military relationship between Saudi Arabia and China will also probably be of concern to the Biden** administration as it tries to manage a

complex and fraught relationship with Beijing, criticizing its human rights record while also cooperating with Chinese leaders on major global threats like climate change and the Covid-19 pandemic.

The White House did not immediately return a request for comment.

Asked to respond to these fresh indications it was aiding Saudi Arabia's push to produce ballistic missiles, China said it has always opposed the proliferation of weapons of mass destruction and their means of delivery, and implements strict export controls on missiles and related technologies, according to a statement from its Ministry of Foreign Affairs.

"China and Saudi Arabia are comprehensive strategic partners," the ministry said. "Such cooperation does not violate any international law and does not involve the proliferation of weapons of mass destruction."

It added that Beijing has always opposed unilateral sanctions and "will continue to take necessary measures to resolutely safeguard its rights and interests."

Saudi Arabia has been known to have purchased missiles from China in the past but has never built its own, the source familiar with the matter and the U.S. official confirmed.

EDITOR'S COMMENT: Each country has the right to do what is best for its protection. By now, we all are aware of the fact that there are no friends and allies just opportunistic partners with common goals.

Magawa, the landmine-sniffing hero rat, dies aged eight

Source: https://www.bbc.com/news/world-asia-59951255

Magawa was awarded the PDSA medal for gallantry – sometimes described as the George Cross for animals

Jan 11 – Magawa, the famous mine-clearing rat who was awarded a gold medal for his heroism, has died at the age of eight.

In a five-year career, the rodent sniffed out over 100 landmines and other explosives in Cambodia.

Magawa was the most successful rat trained by the Belgian charity Apopo to alert human handlers about the mines so they can be safely removed.

The charity said the African giant pouch rat "passed away peacefully" at the weekend.

It said Magawa was in good health and "spent most of last week playing with his usual enthusiasm". But by the weekend "he started to slow down, napping more and showing less interest in food in his last days".

Bred in Tanzania, Magawa underwent a year of training before moving to Cambodia to begin his bomb-sniffing career. There are thought to be up to six million landmines in the South East Asian country.

Trained to detect a chemical compound within the explosives, Magawa cleared more than 141,000 square meters (1,517,711 sq ft) of land - the equivalent of 20 football pitches.

He weighed 1.2kg (2.6lb) and was 70cm (28in) long. While that is far larger than many other rat species, Magawa was still small enough and light enough that he did not trigger mines if he walked over them.

Magawa was capable of searching a field the size of a tennis court in just 20 minutes - something Apopo says would take a person with a metal detector between one and four days.

In 2020, Magawa was awarded the PDSA Gold Medal - sometimes described as the George Cross for animals - for his "life-saving devotion to duty". He was the first rat to be given the medal in the charity's 77-year history.

The rat retired last June, after "slowing down" as he reached old age.

"All of us at Apopo are feeling the loss of Magawa and we are grateful for the incredible work he's done," the charity said in a statement.

His "amazing sense of smell" allowed "communities in Cambodia to live, work, and play; without fear of losing life or limb", it added.

Apopo has been raising its animals - known as HeroRATs - to detect landmines since the 1990s.

US Imposes Sanctions in Response to North Korean Missile Tests

Source: https://www.airforcemag.com/us-imposes-sanctions-north-korean-missile-tests/

Jan 12 – The Biden Administration has economically sanctioned five individual North Koreans, a Russian national, and a Russian company in response to six missile tests conducted by Pyongyang since September, which the Administration says violate U.N. Security Council resolutions. The sanctioned individuals are based in China and Russia.

The test of a hypersonic missile on Jan. 11 is "further evidence" that North Korea "continues to advance prohibited programs despite the international community's calls for diplomacy and denuclearization," said Brian Nelson, undersecretary of the treasury for terrorism and financial intelligence, in a statement for the press.

The sanctions target North Korea's "continued use of overseas representatives to illegally procure goods for weapons," and are aimed at countering Pyongyang's "weapons of mass destruction and ballistic missile programs," Nelson said.

The latest provocative launch occurred Jan. 10, when North Korea conducted a test of a hypersonic missile, which maneuvered before coming down in the Sea of Japan, some 435 miles from its launch point near the Chinese border. North Korea state media said it was the third test of a hypersonic missile, during which the vehicle made a "glide jump flight" followed by "corkscrew maneuvering." The missile was first tested last September, it said. It was the second test in a week—another was made Jan. 5. Pyongyang said both tests were successful, although some missile experts doubted the same missile was used in both instances.

North Korean dictator Kim Jong Un, who was present for the launch, said the hypersonic missile development is one element of the nation's "war deterrent."

North Korean leader Kim Jong Un, right, observed the hypersonic missile test launch held at the Academy of Defense Science on Jan. 11, 2022. Korean Central News Agency.

A More Advanced Missile

Photos released by Pyongyang showed a launching ballistic missile with a nosecone shaped like a hypersonic vehicle. South Korea's joint chiefs of staff issued a statement that the vehicle reached a speed of Mach 10 and an altitude of 37 miles; roughly half the distance to where space begins. The South Korean military leaders also assessed that the missile fired "is more advanced than the missile North Korea fired on Jan. 5," but said they are working with the U.S. to characterize and analyze the test.

The South Korean government said its military has the ability to "detect and intercept this projectile, and we are continuously strengthening our response system."

Nelson said the five sanctioned individuals provided goods, services, or cash to North Korea's Second Academy of Natural Sciences, believed to be the overseer of the missile program. Their "activities or transactions … have materially contributed to the proliferation of weapons of mass destruction or their means of delivery," he said. Any assets they have in the U.S. will be frozen and no American company can do business with them. Any U.S. or foreign company doing business with the sanctioned individuals or company will also be penalized.

The sanctioned persons were involved in obtaining metal alloys, software, and chemicals, as well as telecommunications equipment from Russia.

The Jan. 11 hypersonic test came just hours after five nations—Albania, France, Ireland, Japan, and the U.K., along with the U.S.—condemned the Jan. 5 test and called on U.N.

member states to enforce sanctions they agreed to impose on North Korea. The U.N. Security Council has banned Pyongyang from conducting any tests of ballistic missiles or weapons of mass destruction.

U.S. Indo-Pacific Command issued a statement Jan. 10 saying they were aware of the launch and are “consulting closely with our allies and partners.” The command said the launch “does not pose an immediate threat to U.S. personnel or territory, or to our allies,” but it “highlights the destabilizing impact” of North Korea’s “illicit weapons program.” It added that the U.S. commitment to the defense of Japan and South Korea “remains ironclad.” Indo-PACOM did not describe the missile as hypersonic, though, calling it “ballistic.” U.S. Forces Korea said that no U.S. or South Korean territory or personnel were at risk due to the launch.

A Pentagon spokesman added that the U.S. “takes any new capability seriously” and repeated the condemnation of Pyongyang’s testing of ballistic missiles, “which are destabilizing to the region and to the international community.”

Coincidentally, Derek M. Tournear, Space Development Agency director, said at an AFA Mitchell Institute for Aerospace Studies event Jan. 11 that satellites in low earth orbit will be deployed to detect hypersonic missiles by their heat signatures.

At about the same time as the North Korean missile launch, the Federal Aviation Administration issued a “ground stop” of air traffic in the West Coast region, saying it was a “matter of precaution,” but full operations were resumed within 15 minutes. However, air traffic controllers were confused by the alert and told some airborne aircraft that a “national” ground stop was in effect.

The North American Aerospace Defense Command and U.S. Northern Command said they did not issue any warning relative to the North Korean missile launch.

EDITOR’S COMMENT: What a supersonic reaction! Are the supersonic missiles gone now? Will Kim Jong Un lose more weight due to the stress caused by the sanctions? What??? A third missile in 9 days? Plus two SRBMs this time from a train! More sanctions please!

HOW WILL WE KNOW WHEN IT'S FINISHED?
YOU'LL HEAR THE SOUND OF ISRAELI JETS!
©2010 HARTFORD COURANT

ICI International CBRNE Institute

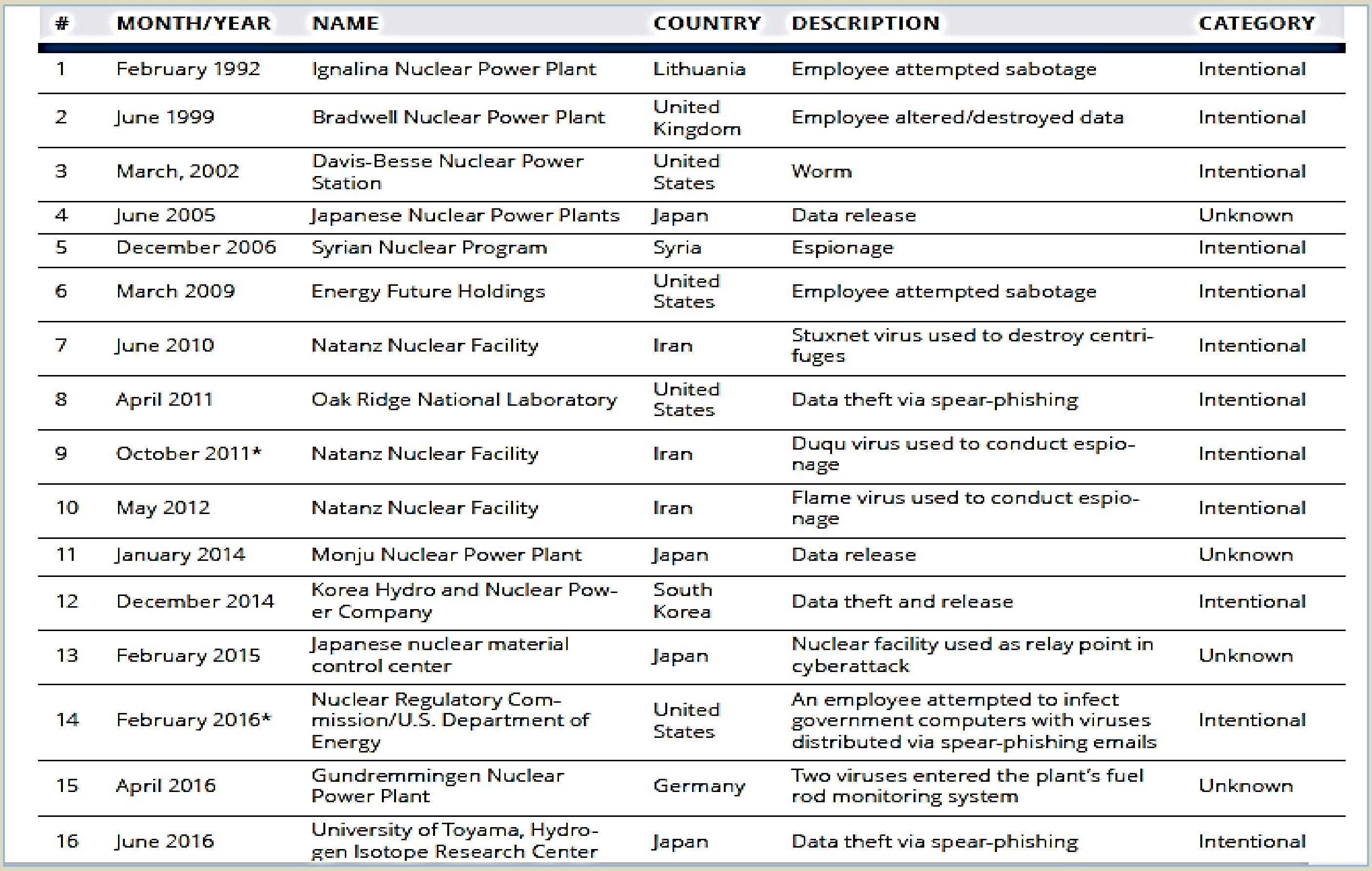
CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Chronology of cyber-attacks to nuclear facilities

Source: http://f3magazine.unicri.it/



#	MONTH/YEAR	NAME	COUNTRY	DESCRIPTION	CATEGORY
1	February 1992	Ignalina Nuclear Power Plant	Lithuania	Employee attempted sabotage	Intentional
2	June 1999	Bradwell Nuclear Power Plant	United Kingdom	Employee altered/destroyed data	Intentional
3	March, 2002	Davis-Besse Nuclear Power Station	United States	Worm	Intentional
4	June 2005	Japanese Nuclear Power Plants	Japan	Data release	Unknown
5	December 2006	Syrian Nuclear Program	Syria	Espionage	Intentional
6	March 2009	Energy Future Holdings	United States	Employee attempted sabotage	Intentional
7	June 2010	Natanz Nuclear Facility	Iran	Stuxnet virus used to destroy centrifuges	Intentional
8	April 2011	Oak Ridge National Laboratory	United States	Data theft via spear-phishing	Intentional
9	October 2011*	Natanz Nuclear Facility	Iran	Duqu virus used to conduct espionage	Intentional
10	May 2012	Natanz Nuclear Facility	Iran	Flame virus used to conduct espionage	Intentional
11	January 2014	Monju Nuclear Power Plant	Japan	Data release	Unknown
12	December 2014	Korea Hydro and Nuclear Power Company	South Korea	Data theft and release	Intentional
13	February 2015	Japanese nuclear material control center	Japan	Nuclear facility used as relay point in cyberattack	Unknown
14	February 2016*	Nuclear Regulatory Commission/U.S. Department of Energy	United States	An employee attempted to infect government computers with viruses distributed via spear-phishing emails	Intentional
15	April 2016	Gundremmingen Nuclear Power Plant	Germany	Two viruses entered the plant's fuel rod monitoring system	Unknown
16	June 2016	University of Toyama, Hydrogen Isotope Research Center	Japan	Data theft via spear-phishing	Intentional

Media Mis-Information and Dis-Information:Future Impact on Disaster Management

By Gilead Shenhar, Timothy Davis, Michael Hopmeier and Lori Settle*

J Homel Secur Emerg Mgmt 2021

Source: https://doi.org/10.1515/jhsem-2021-0017

> ***Seeing is not believing, it is only seeing.***
> –George MacDonald,The Princess and the Goblin

Are we prepared for the next communication revolution and the expectedimpacts on disaster management?Communications are simultaneously thebackbone and the Achilles heel of any disaster response, and they pervade everylevel of disaster crisis management, from ensuring that managers and leadersreceive timely information on status and relay that guidance to responders, toensuring that the public is informed, expectations are established, and actions arecoordinated (Meissner et al. 2002).In the past, connectivity and the ability to transmit a message were the foci ofcompromised communication; they included loss of cell phone towers, downedland lines disrupting internet access, and loss of electrical power. Compromisingthecontentof the message has rarely been a consideration. Until now...Does current disaster planning consider the consequences of syntheticmedia?Synthetic media can have positive uses: it can be created from stockimages and video and used to convey urgent crisis communications from a trustedspokesperson. However, existing video can also be altered by nefarious actors using off-the-shelf technology, artificial intelligence (AI; decision-making by a machine).

*Corresponding author: **Dr. Lori Settle, PhD,** Unconventional Concepts, Inc., Fort Walton Beach,FL, USA, E-mail: lsettle@unconventional-inc.com

Mr. Gilead Shenhar,MDM, Department of Emergency & Disaster Management, School of PublicHealth, Sackler Faculty of Medicine, Tel-Aviv University, Tel-Aviv-Yafo, Israel
Dr. Timothy Davis,MD, MPH, Adjunct Asst. Professor of Surgery (Primary) & Military EmergencyMedicine (Secondary); Guest Researcher, National Center for Disaster Medicine & Public Health(NCDMPH); Uniformed Services University of the Health Sciences (USUHS), Bethesda, Maryland,USA; and Asst. Professor Emeritus of Emergency Medicine, Emory University, Atlanta, Georgia, USA
Michael Hopmeier[1], MS, Unconventional Concepts, Inc., Fort Walton Beach, FL, USAJ Homel Secur Emerg Mgmt 2021; aop

References

Alexander, D. E. 2014. "Social Media in Disaster Risk Reduction and Crisis Management." *Science and Engineering Ethics* 20 (3): 717–33, https://doi.org/10.1007/s11948-013-9502-z.Search in Google Scholar

Ajaka, N., G. Kessler, and E. Samuels. 2019. *Seeing Isn't Believing: The Fact Checker's Guide to Manipulated Video*. Washington Post. Also available at .Search in Google Scholar

Brennen, J. S., F. Simon, P. N. Howard, and R. Kleis Nielsen. 2020. *Fact Sheet: Types, Sources, and Claims of COVID-19 Misinformation*. Reuters Institute for the Study of Journalism, University of Oxford, Oxford Internet Institute, and Oxford Martin School. (accessed April 7, 2020).Search in Google Scholar

BBC. n.d. "History – Edward Jenner." (accessed November 2, 2020).Search in Google Scholar

Covacio, S. 2003. "Misinformation: Understanding the Evolution of Deception." In 2003 Informing Science + IT Education Conference, January 2003.Search in Google Scholar

Freckelton, I. 2020. "COVID-19: Fear, Quackery, False Representations and the Law." *International Journal of Law and Psychiatry* 72: 101611, https://doi.org/10.1016/j.ijlp.2020.101611.Search in Google Scholar

Ignatidou, S. 2019. *AI-Driven Personalization in Digital Media: Political and Societal Implications*. London: Chatham House, The Royal Institute of International Affairs. Also available at .Search in Google Scholar

Jordan, M. I., and T. M. Mitchell. 2015. "Machine Learning: Trends, Perspectives, and Prospects." *Science* 349 (6245): 255–60, https://doi.org/10.1126/science.aaa8415.Search in Google Scholar

Liu, F., A. Burton-Jones, and D. Xu. 2014. "Rumors on Social Media in Disasters: Extending Transmission to Retransmission." In PACIS 2014 Proceedings 49. Also available at .Search in Google Scholar

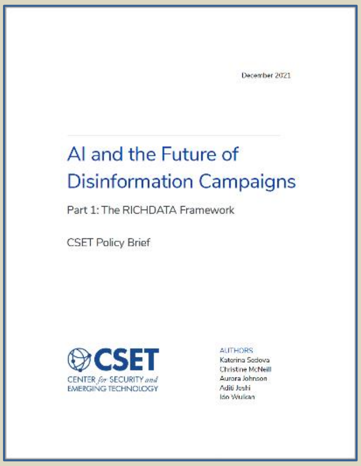
Meissner, A., T. Luckenbach, T. Risse, and T. Kirste. 2002. "Design Challenges for an Integrated Disaster Management Communication and Information System." In First IEEE Workshop on Disaster Recovery Networks (DIREN 2002), June 24, 2002, New York, NY.Search in Google Scholar

O'Conner, C., and M. Murphy. 2020. "Going Viral: Doctors Must Tackle Fake News in the Covid-19 Pandemic." *British Medical Journal* 369: m1587, https://doi.org/10.1136/bmj.m1587.Search in Google Scholar

Ovadya, A., and J. Whittlestone. 2019. *Reducing Malicious Use of Synthetic Media Research: Considerations and Potential Release Practices for Machine Learning*. arXiv Labs, Cornell University.Search in Google Scholar

Sellnow, T., M. Seeger, and R. Ulmer. 2011. "Chaos Theory, Informational Needs, and Natural Disasters." *Journal of Applied Communication Research* 30 (4): 269–92.Search in Google Scholar

Sherman, J. 2020. "Government Information Crackdowns in the Covid-19 Pandemic." Tech, Law, & Security Program, American University Washington College of Law. Joint PIJIP/TLS Research Paper Series, 57. Also available at .


December 2021

AI and the Future of Disinformation Campaigns

Part 1: The RICHDATA Framework

CSET Policy Brief

CSET CENTER *for* SECURITY *and* EMERGING TECHNOLOGY

AUTHORS
Katerina Sedova
Christine McNeill
Aurora Johnson
Aditi Joshi
Ido Wulkan

AI and the Future of Disinformation Campaigns Part 1: The RICHDATA Framework

By Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi and Ido Wulkan

Source: https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns/

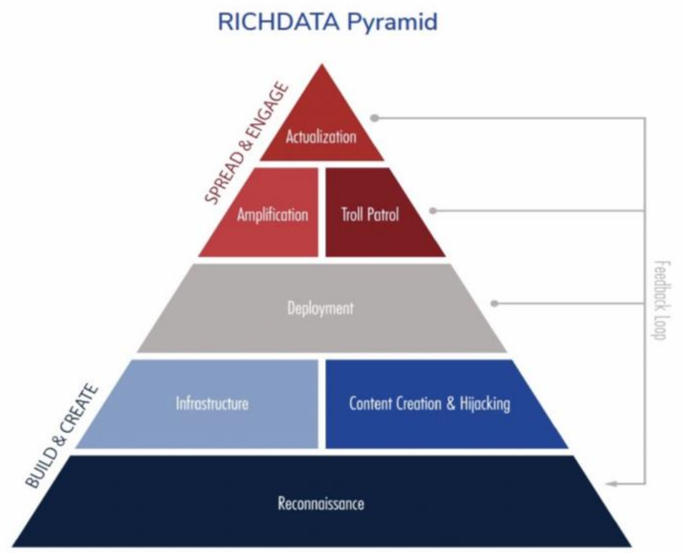
The age of information has brought with it the age of disinformation. Powered by the speed and data volume of the internet, disinformation has emerged as an insidious instrument of geopolitical power competition and domestic political warfare. It is used by both state and non-state actors to shape global public opinion, sow chaos, and chip away at trust. Artificial intelligence (AI),

[1] Michael Hopmeier is also a member of the Editorial Team of the *C^2BRNE Diary*.

specifically machine learning (ML), is poised to amplify disinformation campaigns—influence operations that involve covert efforts to intentionally spread false or misleading information.

In this series, we examine how these technologies could be used to spread disinformation. Part 1 considers disinformation campaigns and the set of stages or building blocks used by human operators. In many ways they resemble a digital marketing campaign, one with malicious intent to disrupt and deceive. We offer a framework, RICHDATA, to describe the stages of disinformation campaigns and commonly used techniques. Part 2 of the series examines how AI/ML technologies may shape future disinformation campaigns.

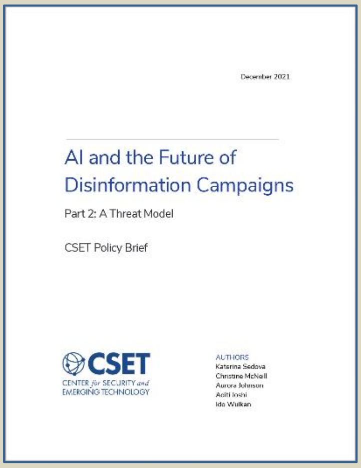
Figure 1. RICHDATA Pyramid



Source: CSET.

We break disinformation campaigns into multiple stages. Through reconnaissance, operators surveil the environment and understand the audience that they are trying to manipulate. They require infrastructure—messengers, believable personas, social media accounts, and groups—to carry their narratives. A ceaseless flow of content, from posts and long-reads to photos, memes, and videos, is a must to ensure their messages seed, root, and grow. Once deployed into the stream of the internet, these units of disinformation are amplified by bots, platform algorithms, and social-engineering techniques to spread the campaign's narratives. But blasting disinformation is not always enough: broad impact comes from sustained engagement with unwitting users through trolling—the disinformation equivalent of hand-to-hand combat. In its final stage, a disinformation operation is actualized by changing the minds of unwitting targets or even mobilizing them to action to sow chaos. Regardless of origin, disinformation campaigns that grow an organic following can become endemic to a society and indistinguishable from its authentic discourse. They can undermine a society's ability to discern fact from fiction creating a lasting trust deficit.

This report provides case studies that illustrate these techniques and touches upon the systemic challenges that exacerbate several trends: the blurring lines between foreign and domestic disinformation operations; the outsourcing of these operations to private companies that provide influence as a service; the dual-use nature of platform features and applications built on them; and conflict over where to draw the line between harmful disinformation and protected speech. In our second report in the series, we address these trends, discuss how AI/ML technologies may exacerbate them, and offer recommendations for how to mitigate them.


December 2021

AI and the Future of Disinformation Campaigns

Part 2: A Threat Model

CSET Policy Brief

CSET
CENTER for SECURITY and EMERGING TECHNOLOGY

AUTHORS
Katerina Sedova
Christine McNeill
Aurora Johnson
Aditi Joshi
Ido Wulkan

AI and the Future of Disinformation Campaigns Part 2: A Threat Model

By Katerina Sedova, Christine McNeill, Aurora Johnson, Aditi Joshi and Ido Wulkan

Source: https://cset.georgetown.edu/publication/ai-and-the-future-of-disinformation-campaigns-2/

The age of information enabled the age of disinformation. Powered by the speed and volume of the internet, disinformation has emerged as an instrument of strategic competition and domestic political warfare. It is used by both state and non-state actors to shape public opinion, sow chaos, and erode societal trust. Artificial intelligence (AI), specifically machine learning (ML), is poised to amplify disinformation campaigns—influence operations that involve covert efforts to intentionally spread false or misleading information.

In this series, we offer a systematic examination of how AI/ML technologies could enhance these operations. Part 1 of the series described the stages and common techniques of disinformation campaigns. In this paper, we examine how AI/ML technologies can enhance specific disinformation techniques and how these technologies may exacerbate current trends and shape future campaigns.

Our findings show that the use of AI in disinformation campaigns is not only plausible but already underway. Powered by computing, ML algorithms excel at harnessing data and finding patterns that are difficult for humans to observe. The data-rich environment of modern

online existence creates a terrain ideally suited for ML techniques to precisely target individuals. Language generation capabilities and the tools that enable deepfakes are already capable of manufacturing viral disinformation at scale and empowering digital impersonation. The same technologies, paired with human operators, may soon enable social bots to mimic human online behavior and to troll humans with precisely tailored messages. These risks may be exacerbated by several trends: the blurring lines between foreign and domestic influence operations, the outsourcing of these operations to private companies that provide influence as a service, and the conflict over distinguishing harmful disinformation and protected speech.

We conclude that a future of AI-powered campaigns is likely inevitable. However, this future might not be altogether disruptive if societies act now. Mitigating and countering disinformation is a whole-of-society effort, where governments, technology platforms, AI researchers, the media, and individual information consumers each bear responsibility.

Our key recommendations include:

- **Develop technical mitigations to inhibit and detect ML-powered disinformation campaigns.** Social media companies and Congress should inhibit access to user data by threat actors and their proxies. The U.S. government and the private sector should increase transparency through interoperable standards for detection, forensics, and digital provenance of synthetic media. Chatbots should be labeled so that humans know when they are engaging with an AI system.
- **Develop an early warning system for disinformation campaigns.** Expand cooperation and intelligence sharing between the federal government, industry partners, state and local governments, and likeminded democratic nations to develop a common operational picture and detect the use of novel ML-enabled techniques, enabling rapid response.
- **Build a networked collective defense across platforms.** Online platforms are in the best position to discover and report on known campaigns. Because these campaigns may occur across multiple platforms it's important to share information quickly to enable coordinated responses. All platforms, regardless of size, should increase transparency and accountability by establishing policies and processes to discover, disrupt, and report on disinformation campaigns. Congress should remove impediments to sharing threat information while enabling counter-disinformation research. Platforms and researchers should formalize mechanisms for cross-platform collaboration and sharing threat information.
- **Examine and deter the use of services that enable disinformation campaigns.** As ML-enabled content generation tools proliferate, they will be adopted by influence-as-a-service entities, further increasing the scale of AI-generated political discourse. Congress should examine the current use of these tools by firms providing influence for hire. It should build norms to discourage their use by candidates for public office.
- **Integrate threat modeling and red-teaming processes to guard against abuse.** Platforms and AI researchers should adapt cybersecurity best practices to disinformation operations, adopt them into the early stages of product design, and test potential mitigations prior to their release.
- **Build and apply ethical principles for the publication of AI research that can fuel disinformation campaigns.** The AI research community should assume that disinformation operators will misuse their openly released research. They should develop a publication risk framework to guard against the misuse of their research and recommend mitigations.
- **Establish a process for the media to report on disinformation without amplifying it.** Traditional media organizations should use threat modeling to examine how the flow of information to them can be exploited by disinformation actors and build processes to guard against unwittingly amplifying disinformation campaigns.
- **Reform recommender algorithms that have empowered current campaigns.** Platforms should increase transparency and access to vetted researchers to audit and help understand how recommendation algorithms make decisions and can be manipulated by threat actors. They should invest in solutions to counter the creation of an information bubble effect that contributes to polarization.
- **Raise awareness and build public resilience against ML-enabled disinformation.** The U.S. government, social media platforms, state and local governments, and civil society should develop school and adult education programs and arm frequently targeted communities with tools to discern ML-enabled disinformation techniques.
- AI-enabled disinformation campaigns present a growing threat to the epistemic security of democratic societies. Our report focuses on the social media and online information environment because they will be primarily impacted by AI-enabled disinformation operations. They are part of a larger challenge that has undermined societal trust in government and the information upon which democracies rely. While these recommendations may help stem the tide, the ultimate line of defense against automated disinformation is composed of discerning humans on the receiving end of the message. Efforts to help the public detect disinformation and the campaigns that spread it are critical to building resilience and undermining this threat.

Cybersecurity – What to Expect in 2022?

Source: https://i-hls.com/archives/112409

Jan 01 – Major cybersecurity trends expected in 2022 will be influenced to a large extent by digital shifts accelerated by COVID-19 events. These include working from home, increased reliance on e-commerce, mass mobile gaming, etc.

Some industries are more vulnerable to cyber-attacks than others. Companies that hold sensitive data or personally identifiable information are common targets for hackers. Businesses or organizations that are most vulnerable to cyber-attacks include banks and financial institutions, healthcare institutions, corporations with inclusive data such as product concepts, intellectual property, etc., and higher education institutes, which hold information on enrollment data, academic research, and more.

Cybercrime costs in 2025 are expected to reach $10.5 trillion in 2025, according to embroker.com.

According to digitalinformationworld.com, cybersecurity next year will be characterized by several major trends:

- A continuing incline in malware cybersecurity threats, with ransomware being a particularly expected form of them. The frequency of ransomware attacks has increased from one every 40 seconds in 2016 to one every 11 seconds in 2021.
- Increase in attacks via the Internet of Things (IoT) – connected electronic devices. While attacks via the IoT are already encountered, 2022 will most probably see a rise in not only individual threats but also the further sophistication of their delivery methods.
- Cybercriminals will move from identity theft to identity fraud, predicts the Identity Theft Resource Center in San Diego. Bad actors are accumulating personal identifying information, but they're not using it to target consumers as much as they used to do. Rather, they're using it in credential attacks on businesses. The increase in fraud will lead to another development in 2022 – a behavior change – consumers withdrawing from certain kinds of online activity.
- Increases in supply chain attacks.
- Criminals will drive victims to use payment apps, digital wallets and peer-to-peer services as part of scams.
- A rise in preventive measures – to better counter cyber-attacks, 2022 is the year that we'll be seeing a rise in AI-based cybersecurity, with the technology becoming more and more sophisticated as machine learning develops to prevent all sorts of conducted attacks.

How to lower the risk of fatal cyber-attacks? embroker.com suggests the following measures:

- Reduce data transfer – keep sensitive data on personal devices
- Download carefully – verify sources and avoid unnecessary downloads
- Improve your passwords
- Update your software regularly
- Monitor for data leaks

Leveraging Social Media During a Disaster

Source: https://www.homelandsecuritynewswire.com/dr20220110-leveraging-social-media-during-a-disaster

Jan 10 – During a disaster, many people turn to social media seeking information. But communicating during disasters is challenging, especially using an interactive environment like social media where misinformation can spread easily.

Now, University of Georgia researchers have developed a social media tool to better help local emergency managers disperse information to community members during a disaster.

Led by recent graduate Dionne Mitcham, a team from the Institute for Disaster Management at UGA's College of Public Health has developed a communication framework that local emergency managers could adopt to support crisis communications.

The proposed framework is a spoke-and-wheel design that utilizes community-based public information officers (PIO), emergency management professionals, and/or trained volunteers to communicate information from the operations team and command and control team to the public, traditional media and other stakeholders.

The framework aims to aid local emergency management agencies that lack access to resources state and federal emergency management organizations typically have, such as risk communicators, social media strategists and full-time PIOs.

"There is a lack of both communication frameworks and guidance on the use of social media as a crisis communication tool that was tailored specifically for use on the local level," said Mitcham. "The framework uniquely leverages local emergency management agencies' close relationships with stakeholders to help amplify the distribution of uniform disaster-related messaging via social media."

Incorporating social media into a local emergency management department's communication plan allows emergency managers and PIOs to directly engage in quick

information sharing with the public. This improves the efficiency of information dispersal and prevents potential misrepresentation of information due to the information being posted directly from the source, said the authors.

Local emergency management departments have a unique opportunity to establish and nurture relationships within a community before disaster strikes. These relationships help to reach the whole community when a disaster happens.

"By collaborating with diverse community organizations, the hub framework assists local governments in understanding and meeting the actual needs of the whole community in real time. Formalizing these partnerships prior to a disaster ensures that all members of the community will receive urgent information," said co-author Morgan Taylor, a doctoral student in the department of epidemiology and biostatistics and research assistant with the Institute for Disaster Management.

There are pitfalls when it comes to using social media. Platforms are not designed to support emergency response and crisis communication: Messages containing critical information can get lost in the influx of messages. False information can spread quickly. Sometimes different community stakeholders can have conflicting messages.

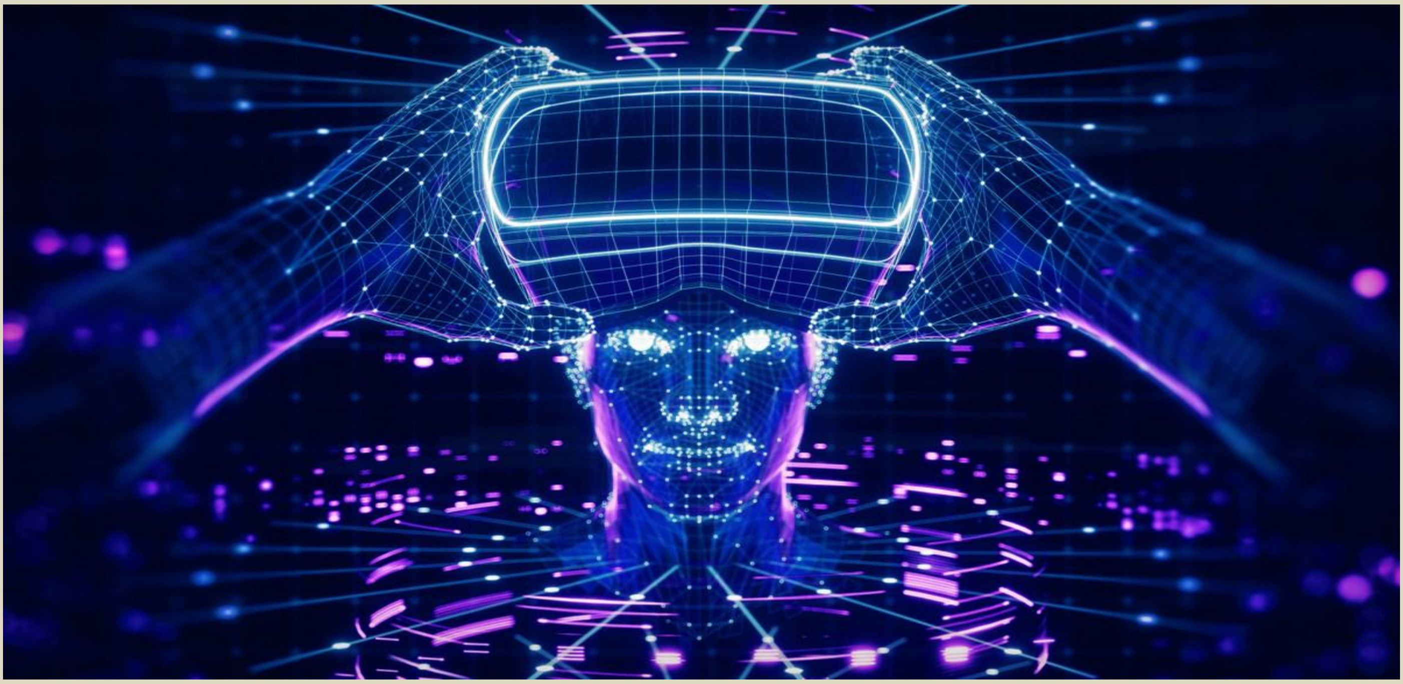
"My co-authors and I hope local emergency managers and their teams use this article as a starting point for considering how to get stakeholders involved in the distribution of crisis communications. In addition, we want to show that uniform distribution of communication messages via social media can be utilized at any level of emergency management – from local to federal," said Mitcham.

●▶ **The full framework is detailed in the team's paper, published in the** International Journal of Environmental Research and Public Health.

The Metaverse Offers a Future Full of Potential – for Terrorists and Extremists, Too

By Joel S. Elson, Austin C. Doctor, and Sam Hunter

Source: https://www.homelandsecuritynewswire.com/dr20220110-the-metaverse-offers-a-future-full-of-potential-for-terrorists-and-extremists-too



Jan 10 – The metaverse is coming. Like all technological innovation, it brings new opportunities and new risks.

The metaverse is an immersive virtual reality version of the internet where people can interact with digital objects and digital representations of themselves and others, and can move more or less freely from one virtual environment to another.It can also involve augmented reality, a blending of virtual and physical realities, both by representing people and objects from the physical world in the virtual and conversely by bringing the virtual into people's perceptions of physical spaces.

By donning virtual reality headsets or augmented reality glasses, people will be able to socialize, worship and work in environments where the boundaries between environments and between the digital and physical are permeable. In the metaverse, people will be able to find meaning and have experiences in concert with their offline lives.

Therein lies the rub. When people learn to love something, whether it is digital, physical or a combination, taking that thing from them can cause emotional pain and suffering. To put a finer point on it, the things people hold dear become vulnerabilities that can be exploited by those seeking to cause harm. People with malicious intent are already noting that the metaverse is a potential tool in their arsenal.

As terrorism researchers at the National Counterterrorism Innovation, Technology, and Education Center in Omaha, Nebraska, we see a potential dark side to the metaverse. Although it is still under construction, its evolution promises new ways for extremists to exert influence through fear, threat and coercion. Considering our research on malevolent creativity and innovation, there is potential for the metaverse to become a new domain for terrorist activity.

To be clear, we do not oppose the metaverse as a concept and, indeed, are excited about its potential for human advancement. But we believe that the rise of the metaverse will open new vulnerabilities and present novel opportunities to exploit them. Although not exhaustive, here are three ways the metaverse will complicate efforts to counter terrorism and violent extremism.

Recruitment

First, online recruitment and engagement are hallmarks of modern extremism, and the metaverse threatens to expand this capacity by making it easier for people to meet up. Today, someone interested in hearing what Oath Keepers founder Stewart Rhodes has to say might read an article about his anti-government ideology or watch a video of him speaking to followers about impending martial law. Tomorrow, by blending artificial intelligence and augmented reality in the metaverse, Rhodes or his AI stand-in will be able to sit on a virtual park bench with any number of potential followers and entice them with visions of the future.

Similarly, a resurrected bin Laden could meet with would-be followers in a virtual rose garden or lecture hall. The emerging metaverse affords extremist leaders a new ability to forge and maintain virtual ideological and social communities and powerful, difficult-to-disrupt ways of expanding their ranks and spheres of influence.

Coordination

Second, the metaverse offers new ways to coordinate, plan and execute acts of destruction across a diffuse membership. An assault on the Capitol? With sufficient reconnaissance and information gathering, extremist leaders could create virtual environments with representations of any physical building, which would allow them to walk members through routes leading to key objectives.

Members could learn viable and efficient paths, coordinate alternative routes if some are blocked, and establish multiple contingency plans if surprises arise. When executing an attack in the physical world, augmented reality objects like virtual arrows can help guide violent extremists and identify marked targets.

Violent extremists can plot from their living rooms, basements or backyards – all while building social connections and trust in their peers, and all while appearing to others in the digital avatar form of their choosing. When extremist leaders give orders for action in the physical world, these groups are likely to be more prepared than today's extremist groups because of their time in the metaverse.

New Targets

Finally, with new virtual and mixed reality spaces comes the potential for new targets. Just as buildings, events and people can be harmed in the real world, so too can the same be attacked in the virtual world. Imagine swastikas on synagogues, disruptions of real-life activities like banking, shopping and work, and the spoiling of public events.

A 9/11 memorial service created and hosted in the virtual domain would be, for example, a tempting target for violent extremists who could reenact the falling of the twin towers. A metaverse wedding could be disrupted by attackers who disapprove of the religious or gendered pairing of the couple. These acts would take a psychological toll and result in real-world harm.

It may be easy to dismiss the threats of this blended virtual and physical world by claiming it isn't real and is therefore inconsequential. But as Nike prepares to sell virtual shoes, it is critical to recognize the very real money that will be spent in the metaverse. With actual money come real jobs, and with real jobs comes the potential for losing very real livelihoods.

Destroying an augmented or virtual reality business means an individual suffers genuine financial loss. Like physical places, virtual spaces can be designed and crafted with care, subsequently carrying the significance people afford things in which they have invested time and creativity building. Further, as technology becomes smaller and more integrated in people's daily lives, the ability to simply turn off the metaverse and ignore the harm could become more challenging.

Preparing for the New (Virtual) Reality

How then to face these emerging threats and vulnerabilities? It is reasonable for corporations to suggest that hate or violence will not be allowed or that individuals engaging in extremism will be identified and banned from their virtual spaces. We are supportive of such

commitments but are skeptical that these are credible, especially in light of revelations about Meta's dangerous behavior on its Facebook, Instagram and WhatsApp platforms. There is profit to be had in hate and division.

If corporations cannot serve as reliable sole guardians of the metaverse, then who can, and how?

Although the arrival of a full-fledged metaverse is still some years in the future, the potential threats posed by the metaverse require attention today from a diverse range of people and organizations, including academic researchers, those developing the metaverse and those tasked with protecting society. The threats call for thinking as much or more creatively about the metaverse as those with malevolent intent are likely to do. Everyone needs to be ready for this new reality.

Joel S. Elson is Assistant Professor of *IT* Innovation, University of Nebraska Omaha.
Austin C. Doctor is Assistant Professor of Political Science, University of Nebraska Omaha.
Sam Hunter is Professor of Psychology, University of Nebraska Omaha.

$400 million worth of crypto stolen to fund North Korean weapons of mass destruction, says report

Source: https://www.windowscentral.com/400-million-worth-crypto-stolen-fund-north-korean-weapons-mass-destruction-says-report

Jan 14 – Last year was a record year for North Korean theft of cryptocurrency, according to a report by Chainalysis. The outlet claims that cybercriminals connected to the North Korean government stole $400 million worth of digital assets, including Ether, Bitcoin, and other cryptocurrencies. Investment firms were the primary victims of the attacks, which came in the form of phishing lures, code exploits, malware, and other methods.

According to Chainalysis, the Democratic People's Republic of Korea (DPRK) laundered the funds to build weapons of mass destruction (WMDs) and ballistic missiles.

Due to the complexity of the attacks, several security experts have classified the cyber actors from the DPRK as advanced persistent threats (APTs). Chainalysis focuses heavily on APT 38, aka "Lazarus Group." That group is reportedly led by the DPRK's primary intelligence agency, the Reconnaissance General Bureau. The Lazarus Group was involved with the Sony Pictures and WannaCry cyberattacks. Since 2018, the APT has stolen sums typically more than $200 million per year.

Chainalysis notes that many of the attacks it covered were likely perpetrated by the Lazarus Group.

In 2021, the number of hacks connected to North Korea rose from four to seven. The value of those attacks grew 40% compared to 2020.

Ether made up 58% of the value of stolen funds. Bitcoin accounted for less than 25% of the value of stolen funds. The trend toward Ether is likely related to the fact that the cryptocurrency's value rose dramatically last year.

The money laundering process required after stealing cryptocurrency is complicated. It involves swapping altcoins for Ether, mixing Ether, and swapping that mixed Ether for Bitcoin. Mixers played an increased role in money laundering in 2021, according to Chainalysis. Over 65% of DRPK's stolen funds were said to have gone through mixers.

Chainalysis goes into more depth regarding the technical process of laundering money. The outlet is bullish in its accusation of the cybercriminals. "These behaviors, put together, paint a portrait of a nation that supports cryptocurrency-enabled crime on a massive scale. Systematic and sophisticated, North Korea's government—be it through the Lazarus Group or its other criminal syndicates—has cemented itself as an advanced persistent threat to the cryptocurrency industry in 2021."

If you're looking for a more legitimate way to obtain cryptocurrency, you can check out the best GPUs for crypto mining.

Ransomware Attacks – Trends for 2022

Source: https://i-hls.com/archives/112649

Jan 15 – Experts expect that the ransomware attacks industry that flourished during 2021 will consolidate around the most sophisticated groups, to automate more of its attacks, and to shift its focus away from critical infrastructure onto corporate targets.

Last year marked a turning point in the fight against ransomware as the collaboration among law enforcement agencies led to high-profile arrests, and the business of ransomware has become riskier for the criminals. Western law enforcement agencies formed dedicated units, such as Europol's Joint Cybercrime Action Task Force or the FBI's National Cyber Investigative Joint Task Force. This led to breakthrough arrests and the seizure of millions of dollars in cryptocurrency.

These efforts are forcing the ransomware ecosystem to change, as Yelisey Boguslavskiy, head of research at security consultancy Advanced Intelligence told techmonitor.ai. But instead of weakening the ecosystem, it may be simply clearing out the less sophisticated groups. "The arrests are clearing the weaker ones, and those who are smart enough not to get arrested, they will keep growing," he said.

This could give rise to a few, highly sophisticated groups that dominate the ransomware business. However, the bigger these groups become, the more of a target they are for law enforcement. As a result, they are diversifying their methods to avoid detection by using a wider variety of attack vectors. Some ot the groups are automating their attacks or reducing their reliance on affiliates, partner organizations that help identify and infect targets with their malware.

Looking forward into 2022, the concentration of ransomware gangs into fewer, more powerful cartels means that companies in the private sector should remain on their guard.

These Targets were Vulnerable to Cyberattacks

Source: https://i-hls.com/archives/112634

Jan 14 – Electric, gas, and water companies are increasingly vulnerable to cyberattacks, according to an annual report reviewing 2021 cybersecurity programs in Connecticut. This may reflect wider emerging trends in the US.

The report by the Public Utilities Regulatory Authority (PURA) found that in 2021, phishing attacks remained the largest source of successful cyberattacks and pose a significant risk to all of the state's critical infrastructure entities.

Phishing attacks are emails claiming to be from reputable companies seeking personal information such as passwords and credit card numbers. Phishing is a type of social engineering attack often used to steal user data.

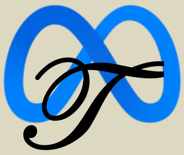
Findings also show these phishing attempts have become more automated, are easier to conduct, and are designed to evade detection.

The lack of multi-factor authentication was the primary cause of many successful phishing hacks of utility vendors and business partners, the report found. For example, malicious cyber actors gained access to the supervisory control and data acquisition system at a water treatment plant to manipulate the water treatment process, PURA said.

These emerging trends, and other wide-reaching phishing and ransomware attacks directed at U.S. companies in the energy and utilities industry, highlight the urgency for Connecticut utilities to continue to refine their existing cybersecurity programs.

Among the security measures already implemented by the Connecticut utilities are requiring multi-factor authentication, enforcing password policies, updating software regularly, establishing protected system back-ups, restricting access to resources, and collecting and retaining audit logs, according to portal.ct.gov.

Terrorism and the Rise of Metaverse



Source: https://i-hls.com/archives/112617

Jan 12 – Through virtual reality headsets or augmented reality glasses, people will be able to live their whole lives in environments where the boundaries between the digital and physical are permeable. The metaverse is an immersive virtual reality version of the internet where people can interact with digital objects and digital representations of themselves and others and can move more or less freely from one virtual environment to another. It can also involve augmented reality.

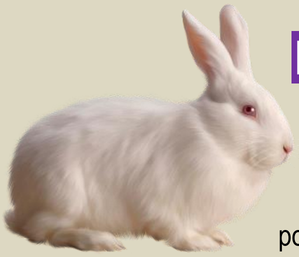
But there is a dark side to the metaverse. People with malicious intent see the metaverse as a potential tool in their arsenal. Terrorism researchers at the US DHS' National Counterterrorism Innovation, Technology, and Education Center (NCITE) in Nebraska assert that the metaverse promises new ways for extremists to exert influence through fear, threat and coercion, and might become a new domain for terrorist activity. The rise of the metaverse will open new vulnerabilities and present novel opportunities to exploit them, complicating counter-terrorism efforts in several ways:

Online recruitment and engagement – the metaverse will make it easier for people to meet up, enabling modern extremism to flourish. The integration of artificial intelligence with augmented reality in the metaverse will enable extremist leaders to meet with their followers, forge and maintain virtual ideological and social communities and expand their spheres of influence.

The metaverse offers new ways to coordinate, plan and execute acts of destruction. With sufficient reconnaissance and information gathering, extremist leaders could create virtual environments with representations of any physical building, which would allow them to walk members through routes leading to key objectives.

Finally, with new virtual and mixed reality spaces comes the potential for new targets. Just as buildings, events and people can be harmed in the real world, so too can the same be attacked in the virtual world. A 9/11 memorial service created and hosted in the virtual domain would be, for example, a tempting target for violent extremists who could reenact the falling of the twin towers.

Preparedness for these emerging threats requires creative thinking about the metaverse as those with malevolent intent are likely to do, according to theconversation.com.



New Ransomware Spotted: White Rabbit and Its Evasion Tactics

Jan 18 – Thrend Micro researchers spotted the new ransomware family White Rabbit discretely making a name for itself by executing an attack on a local US bank in December 2021. This newcomer takes a page from Egregor, a more established ransomware family, in hiding its malicious activity and carries a potential connection to the advanced persistent threat (APT) group FIN8.

Use of a command-line password

One of the most notable aspects of White Rabbit's attack is how its payload binary requires a specific command-line password to decrypt its internal configuration and proceed with its ransomware routine. This method of hiding malicious activity is a trick that the ransomware family Egregor uses to hide malware techniques from the analysis. Read more…

COVID-19: Technology developed to track spread of coronavirus could be abused, privacy campaigner warns

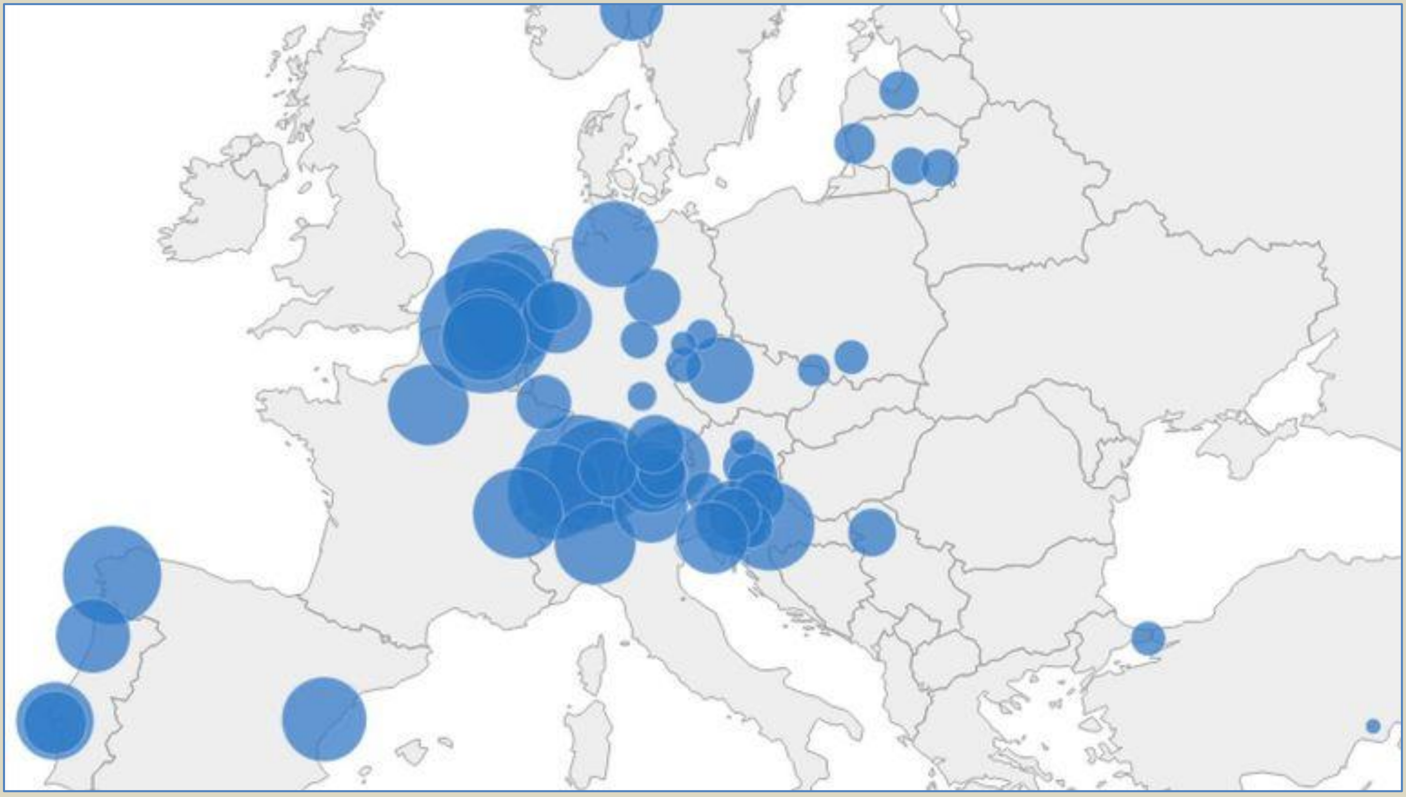
Source: https://news.sky.com/story/covid-19-technology-developed-to-track-spread-of-coronavirus-could-be-abused-privacy-campaigner-warns-12516018

Jan 16 – A medical privacy campaigner says technology developed to track the spread of COVID-19 is a new form of surveillance that could be abused.

Phil Booth, coordinator at MedConfidential, warned that increased monitoring of wastewater from sinks, drains and toilets, which can reveal infections and drug use, needs to be properly regulated.

"The concerns will be raised more by the mission creep, the feature creep, the ways in which these miniaturised technologies might get used and abused beyond the pandemic," he said.

"There needs to be regulation of every sort of technology that can have an effect on people's lives and on individual people."

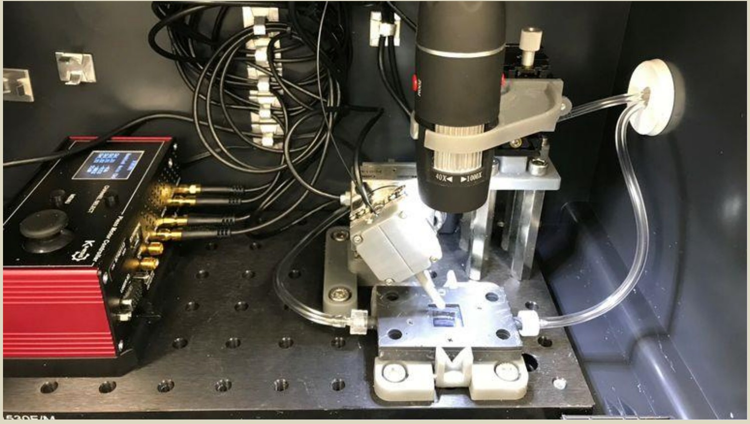


Map shows mean daily cocaine use detected in wastewater in 2020, from the European Monitoring Centre for Drugs and Drug

His claims follow the launch by a biotech company in York of what it calls a "mobile surveillance platform" to detect COVID in sewage from individual buildings.

The suitcase-sized equipment can be connected to any drain to send data remotely to a computer where it is interpreted using artificial intelligence.

The firm, Modern Water, says it has static monitors installed at 3,000 sites in 60 countries and can detect "medicines, pesticides, personal care, [and] hormones" in wastewater.



It began testing its Microtox PD mobile COVID monitoring system in UK municipal sewage treatment works last year.

Paul Ryan, chief business development officer at the firm's parent company, Deepverge, told Sky News he expects the new device to be available for hire within months to monitor COVID in buildings including schools, hospitals and hotels.

Modern Water's new mobile surveillance platform

"This is about surveillance, this is about identifying the presence of COVID and other pathogens ahead of time," he said.

"I think there's a growing consensus that wastewater based epidemiology offers a whole new layer of information which allows national health surveillance."

The testing of raw sewage has been dramatically increased since the discovery in 2020 that it contains remnants of the COVID-19 virus.

Last year the UK government's Joint Biosecurity Centre opened a new laboratory near Exeter which is now testing thousands of samples taken from sewage treatment works and individual drains every week.

A report published in September 2021 said the centre's Environmental Monitoring for Health Protection programme was covering approximately 40 million people in England.

The increased monitoring comes as the identification of illegal drug use from sewage analysis is growing, according to an EU report published last year into monitoring between 2011 and 2020.

The report ranked 80 European towns and cities, none of which are in the UK, for consumption of codeine, amphetamine, methamphetamine and MDMA, based on drug residues found in sewage.

"The results provide a valuable snapshot of the drug flow through the cities involved," it said.

The UK Health Security Agency, which oversees the national wastewater monitoring programme, told Sky News its wastewater programme follows government data protection standards.

"The data provided to local and national decision-makers relating to COVID-19 is not considered personal data," the agency said in an emailed response. "It cannot identify infected individuals or homes as it is designed to provide insights at a community level."

What to Include in a Cybersecurity Disaster Recovery Plan

By Nik Hewitt

Source: https://www.imperva.com/blog/what-to-include-in-a-cybersecurity-disaster-recovery-plan/

Jan 11 – If the unthinkable were to happen to your business, what's your disaster recovery plan? If bad actors were to inject ransomware into your system, what's your process for a return to normal working? Google the words "What do I do if I have a cybersecurity breach" and the first twenty results will start with the words "Refer to your cybersecurity disaster recovery plan (DRP)." The size of your business doesn't matter – some simple work up-front can help you avoid a lot of problems should disaster strike.

Putting the right person in charge

Whether an internal team or an external contractor, it's important to have clear lines of communication between whomever owns the cybersecurity DRP and the overall enterprise DRP.

The person or people that own the cybersecurity DRP should be the first responder in the case of a security breach, and they should know your enterprise DRP inside and out. Their out-of-hours contact details should be at the top of your list of designated respondents (written on Page One of your printed enterprise DRP). Department heads and critical stakeholders will need to support first responders with assistance in cybersecurity disaster recovery plan creation and maintenance. First responders will need help in securing the recognition and attention the plan requires to ensure cooperation and assistance across your organization. Cybersecurity is important, and from top to bottom it needs to be recognized as critical business functionality – and not as just more work or an inconvenience.

When choosing a capable person to head this initiative, it's important to choose an individual who is organized, passionate about what they do, and an expert communicator comfortable liaising with people in different departments across your whole organization that have different levels of technical knowledge. This person needs both the knowledge and capacity to champion the development, analysis, and upkeep of the DRP as a permanent part of their regular workload.

To create an effective cybersecurity DRP, you will need input from all areas of your enterprise to identify departmental essentials, critical tools, and data. You should have dedicated representatives from each area, with your cybersecurity DRP leader coordinating information and requirements. These departmental representatives will also be useful when creating "worst-case scenario" exercises and will be a great help in establishing friction-free lines of communication.

Identify critical tools and data

When working across departments and liaising with team representatives, it's important to find out from them which specific software, applications, information, and systems are critical to the ongoing operational functionality of each of their departments. This information is the key to restoring operations efficiently with minimal downtime.

You should conduct an audit to identify which tools and data are most important for each department to function properly. Plan for individual departments' requirements to be very different. For example, what is important to the dispatch department will be materially different from what's critical to your sales team out on the road, or to the finance department, or to human resources. Some of these requirements may even be time – or seasonally – dependent, with some resources being more important in the run-up to year-end, for example. Payroll data may be more critical in the week before payday. There may even be changes in data usage for some departments in the mornings versus afternoons. Departmental knowledge is invaluable to get the most value from this exercise, and your department representatives will offer important insight. Be sure to identify where backups exist for this critical data, how/where to replace critical tools and software, who requires what levels of access, and the detailed roles of the departmental stakeholders.

It's worth noting that the latest version of any DRP should be printed and stored in a safe place – under lock and key if this includes any major passwords of confidential information. There's no point in having a plan digitally if you can't access it due to your network being compromised.

Knowing the dangers

Department by department, and for the organization overall, create a list of possible cybersecurity disaster scenarios that could affect your operations. Identifying potential weaknesses up-front gives you a window into your vulnerabilities and, therefore, insight into how to mitigate them.

What would you do, for example, if a dissatisfied former employee deletes data before leaving your organization? How would you respond if important data was corrupted by viruses or malware? Even human error and hardware damage could be part of this exercise if you choose to conduct a full IT audit and investigate a backup solution at that time.

Creating this documentation and identifying your weak spots will bring up many issues that you can address now. It's possible, for example, to stop the disruption of supply chain attacks with runtime protection software, protect managed databases with cloud data security solutions, or automate API protection. The first step is knowing your vulnerabilities and identifying and documenting how you would respond.

Create a communications plan

If a cybersecurity breach does occur, especially during off-hours, who needs to know about it and how will you let them know? Curating a prioritized list of those who need to be in the loop, and those whose expertise is critical to operations restoration will be an important part of streamlining recovery efforts.

In addition, if relevant, how will you communicate the existence of a security breach to customers, suppliers, or vendor partners? Who will handle any media queries? How will you inform the general staff? Not every breach will require communication with everyone, but a plan should include how and when these communications should happen as well as who is responsible for that work.

Get around the table

Arrange for some coffee (and biscuits), grab a wad of sticky notes, then get everyone involved around a table – and practice. Take some of your scenarios and walk through how you'd go about recovering from them.

If you can, come up with a few complications and throw them in randomly – making people draw from a deck of possible hurdles to success. What if the designated DRP leader is on holiday in another country? What if your primary backup has also been corrupted? What if a secondary attack is distracting resources with a distributed denial-of-service (DDoS) attack? What other barriers to success can your team come up with and how can you resolve them so that you don't have to think this through in a crisis? This process will allow you to put solutions in place now and you are likely to experience fewer surprises to overcome if a breach does occur. The more you practice, the better and more efficient your team will get and the more prepared you'll be. You may wish to consider Red Team Exercises to take this one step further.

The old adage of "prior planning prevents poor performance" is as true for cybersecurity as it is in any operational area. Having a cybersecurity disaster recovery plan in place, with a well-informed and practiced team behind it, will be critical if the unthinkable happens. Let's hope it never does, but with more and more security breaches happening every day that's probably not a pair of dice you want to roll.

How I Hacked A Nuclear Power Plant

Source: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/how-i-hacked-a-nuclear-power-plant/

March 2021 – In cybersecurity, the worst-case scenario is that malicious hackers might gain access to, or control over, critical infrastructure. In that scenario, criminals or nation state actors might be able to leverage their exploits into a situation where lives are put at risk – in addition to the other severe ramifications. And of course, that worst-case scenario becomes an actual nightmare when we imagine the consequences of a malicious actor gaining access to nuclear power plants or missiles.

While most of us assume – or at least hope – that nuclear power plants are hardened targets that should be protected by the most advanced digital security possible, is that actually the case? In this interview with Charles Hamilton, Principal Security Consultant for Trustwave SpiderLabs, we discuss his experience conducting a penetration testing exercise for a

nuclear power plant. For safety reasons, we won't disclose where and when this exercise was conducted.

Q: Did you actually hack a nuclear power plant?

Charles: Yes, this was part of penetration testing. There are many details that I can't reveal, for obvious reasons. But I've actually tested more than one.

In the test we will talk about today, when I gained access to the plant, posing as a malicious actor, I found out that the management software was actually Windows NT 4.0, far past the time when that would have been appropriate.

The point of the engagement, of course, is to see if an actor can reach the point where they gain control of the reactor. Thankfully, that's rarely possible because there is a physical barrier between the corporate network and the actual power plant. That's purposeful, thankfully, and it should do its job of preventing hackers from being able to trigger a meltdown.

You might remember Stuxnet, a worm that was designed to target the nuclear capabilities of Iran. Whomever designed that exploit built it to account for the physical barrier, which is why they created it to spread by USBs, which they knew were being actually plugged into the reactor environment. But that's the kind of activity that goes above and beyond what a penetration test is designed to discover.

Q: What did you find during your penetration test?

Charles: The first major vulnerability I found was due to contracting work that they had hired out. Sometimes, just like other structures, a nuclear power plant needs to be fixed. In this case, the contractors had set up a WIFI spot which didn't have a strong level of security. Via that avenue, I was actually able to get into the corporate network quite easily.

The reality is that, when I get in, it was just like any other corporate network, with a bunch of Windows and Linux systems, and in this case they were running Windows NT 4.0 as well. I was able to gain direct access to the network and access to some interesting things, like monitoring tools.

In a related example, I tested wind turbine farm and found that it was set up the same way, with layers of networks where the actual system that was physically controlling the turbines wasn't reachable remotely – it would have required direct physical access. So that's something we can all be thankful for.

Q: If you had been a malicious actor, what could you have done with the access you achieved?

Charles: In about one or two hours I had domain level privileged. I could have been able to gain information about how the power plant was performing. If I was involved in spy craft or actual nation state sabotage, I would have been able to see things like pressure rates, etc. In this specific case, the plant was actually shut down at the time, because it was under maintenance. The penetration test was actually part of their efforts to bring it back online, so it was a good thing that they were being proactive and diligent in exposing weaknesses.

Q: Are there key takeaways that organizations should be aware of

Charles: Definitely. Even for companies or organizations that aren't involved in critical infrastructure, the key learning here is that your corporate network is always going to be one of your most vulnerable points. From an external threat actor perspective, phishing exploits will be constant and ongoing. Always assume that your network is as vulnerable as your external perimeters.

Most of the time when we do penetration tests, we find that external perimeters are actually a little bit more secure, because it's publicly facing. Organizations tend to harden it a bit more, and unfortunately leave their internal networks a little bit more exposed.

When you think about incidents like SolarWinds, what's your opinion on how secure the infrastructure grid is in America? The reality is that it's mainly secure because of security through obscurity. When you look at things like SolarWinds, that exploit required a huge amount of time and a fairly large budget. That's not really in the realm of possibility of your average hacker, who's probably out to just make a quick buck.

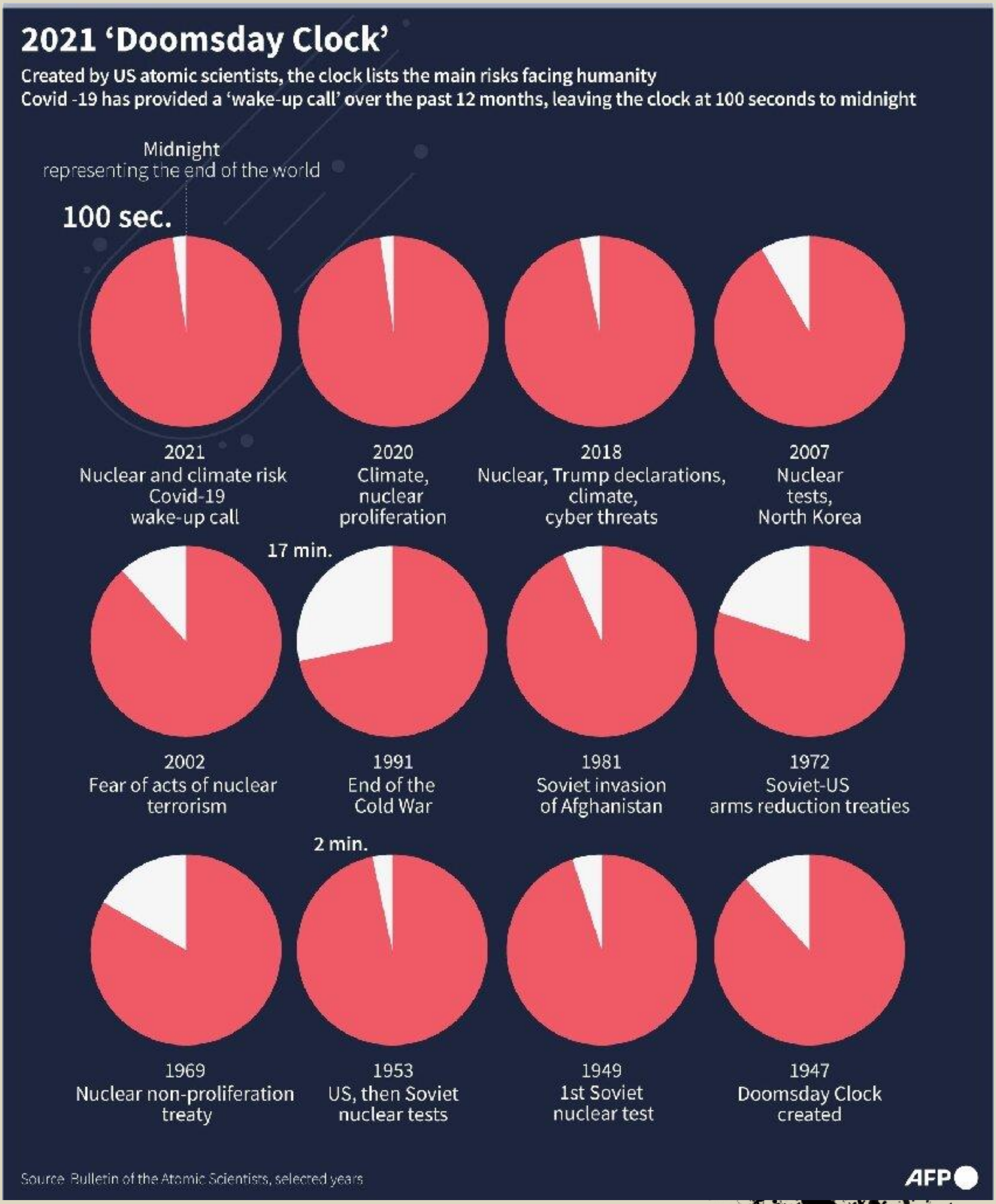
The Doomsday Clock depicts how close humanity is to Armageddon – but where did it come from, how do you read its time, and what can we learn from it?

By SJ Beard (Existential risk researcher)

Source: https://www.bbc.com/future/article/20220119-how-to-read-the-doomsday-clock

Jan 20 – I first became aware of the Doomsday Clock at school in the mid-1990s when a teacher introduced it to me. She told my class about the grand sweep of history, explaining that if everything that had happened on our planet was compressed into a single year, then life would have emerged in early March, multi-cellular organisms in November, dinosaurs in late-December – and humans wouldn't arrive on the scene until 11:30 on New Year's Eve. Then she contrasted this great swathe of history with how short our futures might be, and told us how a group of scientists in the US thought we may only have a few metaphorical minutes left until midnight. It never crossed my mind that someday I might be working on the same problem, as a researcher at the Centre of the Study of Existential Risk at the University of Cambridge.

It's a powerful story, and for many years I thought this is what the Doomsday Clock meant: that its hands represented the time we have left before the end. However, that's not quite accurate.



2021 'Doomsday Clock'

Created by US atomic scientists, the clock lists the main risks facing humanity
Covid -19 has provided a 'wake-up call' over the past 12 months, leaving the clock at 100 seconds to midnight

Source: Bulletin of the Atomic Scientists, selected years

Today, the scientists for the Doomsday Clock at the Bulletin of the Atomic Scientists will publish their annual judgement of how close its hands sit to midnight, for the 75th time. Every year, the announcement highlights the complex web of catastrophic risks facing humanity, including weapons of mass destruction, environmental breakdown and disruptive technologies. And in 2020, the Bulletin's president, Rachel Bronson, solemnly announced that its hands had moved closer to Armageddon than ever before – only 100 seconds. But to understand what that really means, you need to understand the story of the Clock, where it came from, how to read it, and what it tells us about humanity's existential predicament.

Setting the Clock in motion

The speed and violence with which nuclear technology evolved was breathtaking, even to those closely involved in its development. In 1939, world-renowned scientists Albert Einstein and Leo Szilard wrote to the US president about a breakthrough in nuclear technology that was so powerful, and could have such tremendous battlefield consequences, that a single nuclear bomb, "carried by boat and exploded in a port, might very well destroy the whole port". It was a possibility too significant to ignore. This letter led to the establishment of an enormous scientific, military, and industrial collaboration, the Manhattan Project, that a mere six years later produced a bomb much more powerful than the one imagined by Einstein and Szilard, capable of destroying an entire city and its population. Only a few years after that, nuclear arsenals were capable of destroying civilisation as we know it.

The first scientific concern that nuclear weapons might have the potential to end humanity came from the scientists involved in the first nuclear tests. They were concerned that their new weapons might accidentally ignite the Earth's atmosphere. These worries were quickly dismissed and, thankfully for all concerned, proved false.

The Seattle Times
DON'T LET 'EM STICK YOU WITH THE VACCINE, KID, IT'S AN EVIL PLOT TO CONTROL YOUR MIND!
2021
STOP THE STEAL
Q
2022
WOW... YOU SPENT YOUR WHOLE YEAR ON SOCIAL MEDIA, DIDN'T YOU?

ICI International CBRNE INSTITUTE

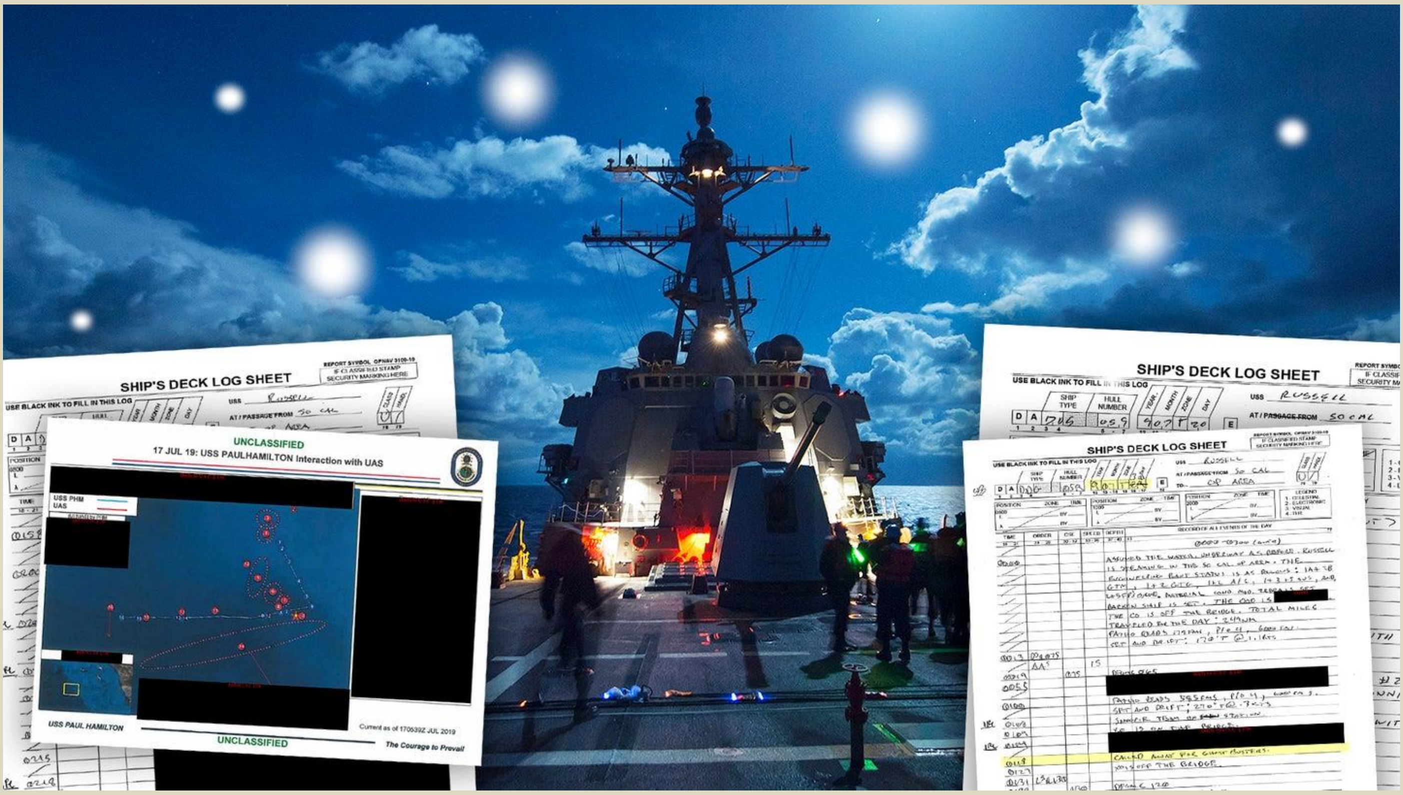
CBRNE-Terrorism Newsletter

C2BRNE DIARY

& Robotic DRONE NEWS

on For Weeks

Source: https://www.thedrive.com/the-war-zone/43561/mysterious-drone-swarms-over-navy-destroyers-off-california-went-on-for-weeks



Dec 17 – Earlier this year *The War Zone* exclusively reported about a series of 2019 incidents that involved unidentified drones stalking US Navy vessels over several nights in the waters off of Southern California. Our initial report also covered the Navy's investigation into the incidents, which appeared to struggle to identify either the aircraft or their operators. Chief of Naval Operations Admiral Michael Gilday later clarified that the aircraft were never identified, and that there have been similar incidents across the service branches and allied militaries.

Newly released documents obtained via the Freedom of Information Act (FOIA) show that the full scope of these drone incursions was greater than it initially appeared, and they persisted well after the Navy's investigation was launched. Deck logs indicate that drone sightings continued throughout the month of July 2019 and included events where drone countermeasure teams were called into action. One notable event involved at least three ships observing multiple drones. Uncharacteristically for unclassified deck logs, the details on this event are almost entirely redacted.

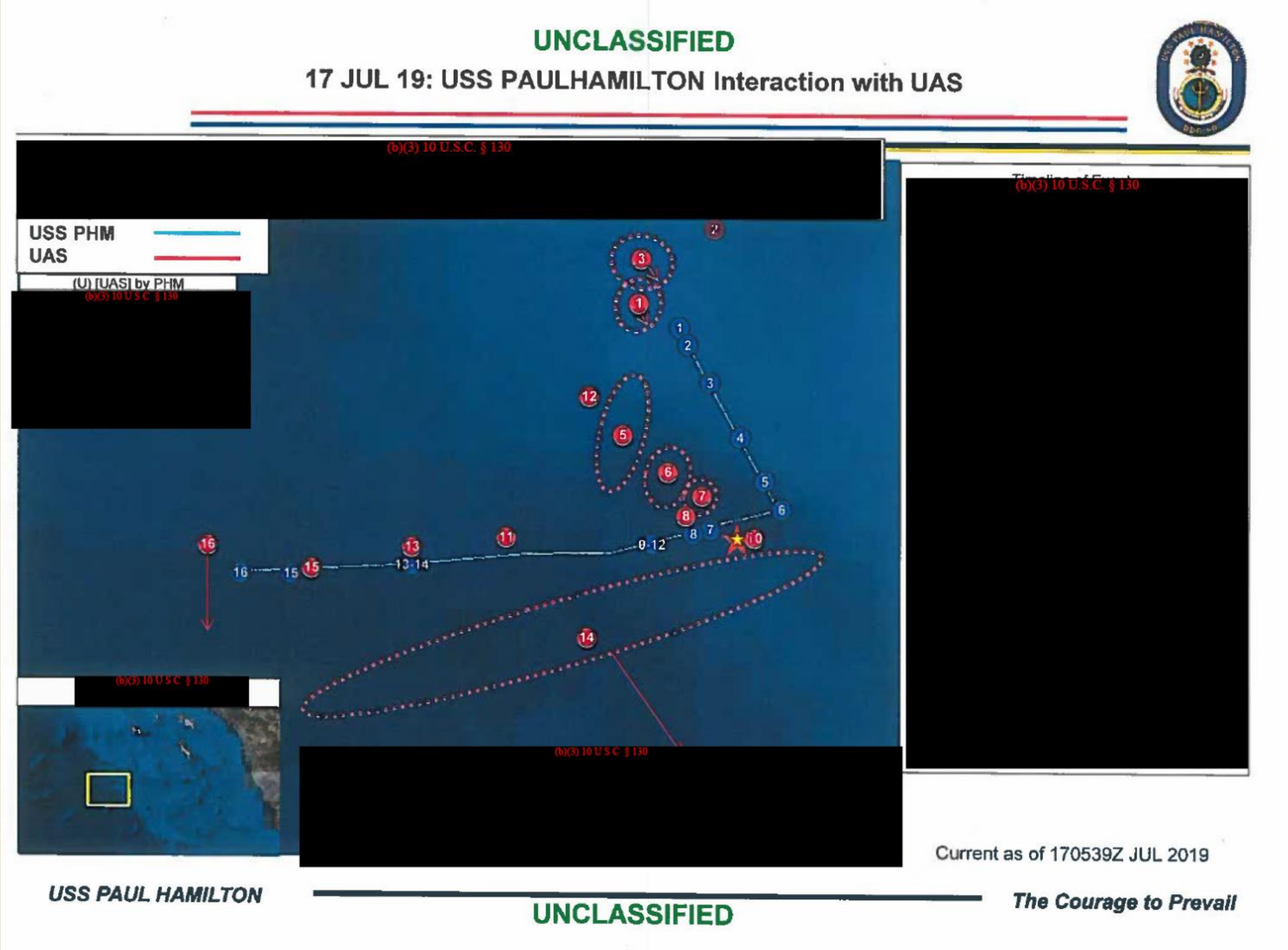
Among the new documents is the map seen below that details the interactions between a drone (denoted on what appears to be a briefing slide as an unmanned aerial system, or UAS) and a Navy *Arleigh Burke* class destroyer, the USS *Paul Hamilton*.

The map depicts *Paul Hamilton* making an abrupt right-hand turn while a drone closely follows the ship. The legends and annotations of the map have been redacted under FOIA exemptions that apply to technical data that have military applications. Though the title of the document reads July 17th, the map appears to refer to drone encounters that occurred in the incidents on July 14th and July 15th.

Intriguingly, one of the position points of the drone is marked with a star, while others show a dashed line around a given area. It is unclear exactly what these indicate without the map legends, though the star suggests at least one particularly notable event. Our previous coverage indicated that the incident involved multiple contacts that maneuvered around the ships in a highly dynamic way, and there may have been uncertainty about the exact location of the drones at times.

The deck logs from the period show that Ship Nautical Or Otherwise Photographic Interpretation and Exploitation (SNOOPIE) teams were deployed frequently during the incidents. SNOOPIE teams consist of sailors specifically trained to enhance situational awareness and to document unknown contacts or other events and objects of interest.

It is highly likely that a number of photographs exist of the drones given the work of the SNOOPIE teams and other onboard sensors. The same document providing the map above also contains a reference to a photograph of the drones, which has been completely redacted under the same technical data exemptions.



UNCLASSIFIED

17 JUL 19: USS PAULHAMILTON Interaction with UAS

(b)(3) 10 U.S.C. § 130 [redacted]

(b)(3) 10 U.S.C. § 130 [redacted]

(U) [UAS] by PHM

(b)(3) 10 U.S.C. § 130 [redacted]

(b)(3) 10 U.S.C. § 130 [redacted]

(b)(3) 10 U.S.C. § 130 [redacted]

Current as of 170539Z JUL 2019

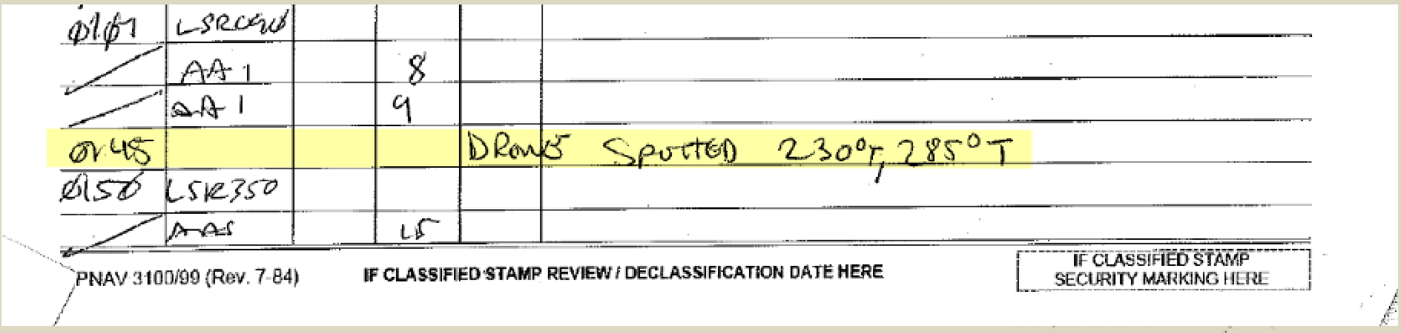
USS PAUL HAMILTON

UNCLASSIFIED

The Courage to Prevail

Map depicts the USS *Paul Hamilton's* interactions with an unknown UAS (US Navy via FOIA)

According to deck logs, the proximity of the drones also led the ships to exercise enhanced “emissions control,” or EMCON, protocols designed to minimize their electronic profile. An extensive analysis by *War Zone* editor Tyler Rogoway explains that drones could play a useful role in provoking reactions from an adversary as a means to capture highly prized electronic intelligence (ELINT) and sensitive operating procedures. Intriguingly, references to EMCON were not universal throughout the encounters, and do not appear to have been as relevant in the newly released documents.



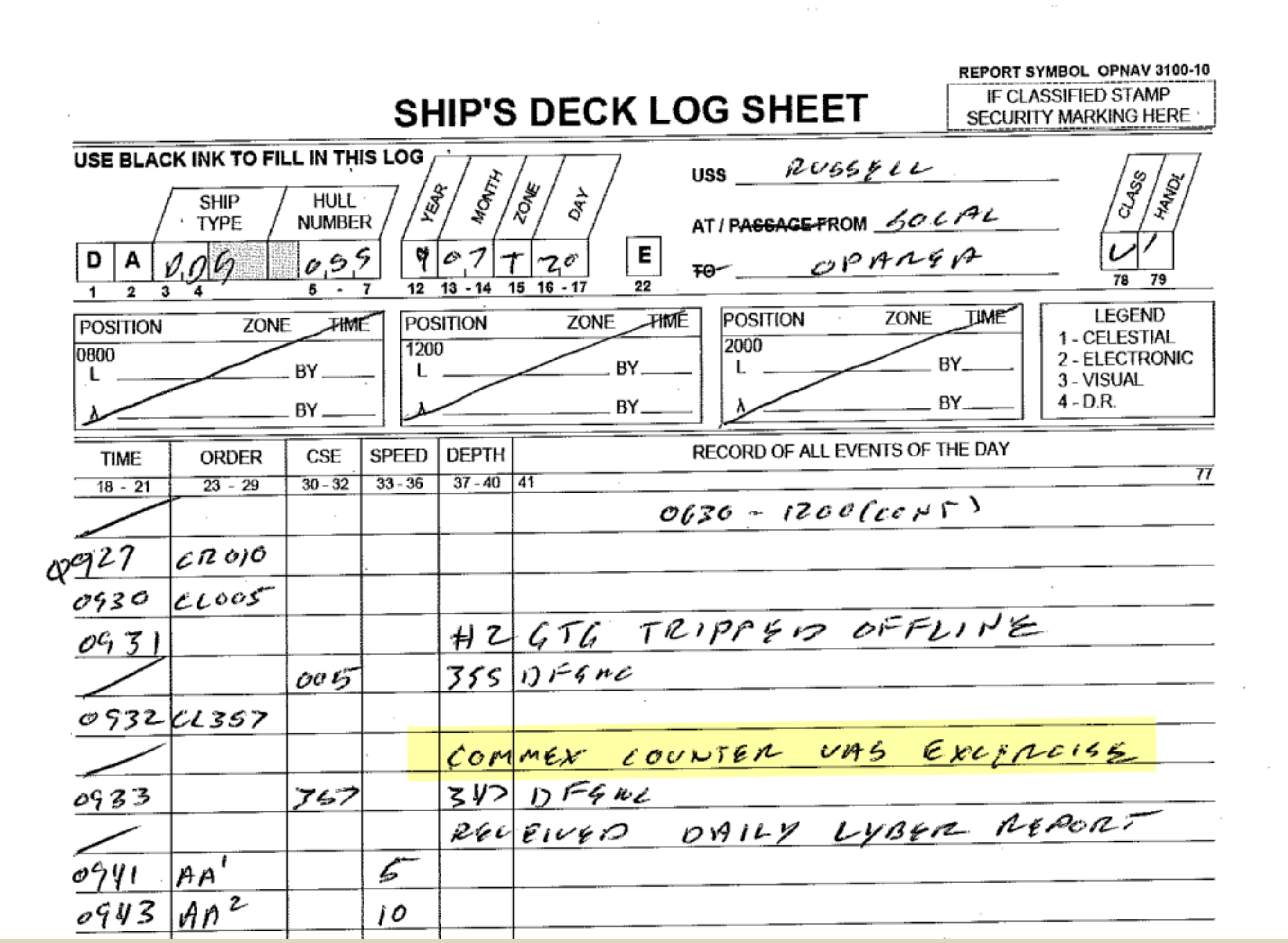
Ø1Ø7	LSRC40				
/	AA 1		8		
/	AA 1		9		
Ø145				DRONES SPOTTED 230°T, 285°T	
Ø15Ø	LSR350				
/	AAS		15		

PNAV 3100/99 (Rev. 7-84) IF CLASSIFIED STAMP REVIEW / DECLASSIFICATION DATE HERE IF CLASSIFIED STAMP SECURITY MARKING HERE

Excerpt from the log of the USS *Russell*. (US Navy via FOIA)

Previously, the majority of available documents suggested that the drone encounters were limited to the evenings of July 15th and July 16th, 2019, with a second, but minor series of

events occurring towards the end of the month. New logs show that sightings persisted sporadically throughout the second half of July with another significant event happening in the early hours of July 30th. Indeed, as early as the morning of July 17th, the *USS Russell*, another *Arleigh Burke* class destroyer, continued to report drone sightings, as seen in the portion of the log below.
It is very noteworthy that several days later, on the 20th, the *USS Russell* conducted an initial counter UAS exercise.



REPORT SYMBOL OPNAV 3100-10

IF CLASSIFIED STAMP SECURITY MARKING HERE

SHIP'S DECK LOG SHEET

USE BLACK INK TO FILL IN THIS LOG

		SHIP TYPE	HULL NUMBER	YEAR	MONTH	ZONE	DAY	
D	A	DDG	055	9	07	T	20	E
1	2	3 4	5 - 7	12	13 - 14	15	16 - 17	22

USS RUSSELL

AT / ~~PASSAGE FROM~~ SOCAL

~~TO~~ OPAREA

CLASS	HANDL
U	/
78	79

POSITION ZONE ~~TIME~~
0800
L ____ BY ____
λ ____ BY ____

POSITION ZONE ~~TIME~~
1200
L ____ BY ____
λ ____ BY ____

POSITION ZONE ~~TIME~~
2000
L ____ BY ____
λ ____ BY ____

LEGEND
1 - CELESTIAL
2 - ELECTRONIC
3 - VISUAL
4 - D.R.

TIME	ORDER	CSE	SPEED	DEPTH	RECORD OF ALL EVENTS OF THE DAY
18 - 21	23 - 29	30 - 32	33 - 36	37 - 40	41 … 77
					0630 - 1200 (CONT)
0927	CR010				
0930	CL005				
0931				#2	GTG TRIPPED OFFLINE
		005		355	DEGRE
0932	CL357				
				COM	MEX COUNTER UAS EXCERCISE
0933		357		347	DEGRE
				REC	EIVED DAILY CYBER REPORT
0941	AA¹		5		
0943	AA²		10		

Excerpt from the log of the USS *Russell*. (US Navy via FOIA)

Later in the same day, the *Russell* conducted another set of counter UAS exercises, this time firing a 5-inch naval gun. Speaking to USNI News, retired Navy officer Thomas Callender explained that 5-inch deck guns have been tested as a counter UAS weapon in the past with limited success, stating "they found that the 5-inch gun took multiple shots to try and hit it because it's not designed for something slow and small." Callender's remarks were in the context of another incident in July 2019 that involved Marines onboard the *Wasp* class amphibious assault ship *USS Boxer* disabling an Iranian drone in the Strait of Hormuz using a vehicle-mounted electronic warfare system. The logs from this period reflect that several shots were fired in the exercise, including at least one misfire.
Three days later, another drone was spotted by a SNOOPIE team at an elevation of about 400 feet. Note that in naval parlance, "calling away" refers to sending sailors to their posts.
A little over an hour later, flares were spotted, though the logs do not remark if these were connected to the ongoing drone sighting. Flares are not uncommon in the training areas off Southern California where the ships were operating.
The following day, a new term is introduced to the logs: "ghostbusters." A log entry reflects an apparently brief counter UAS exercise lasting about eight minutes.
Though official references are hard to come by, "ghostbuster" is a term sometimes used to refer to lower-end counter UAS devices that look similar to rifles.
These anti-drone countermeasures are increasingly being used by security forces around the world. They operate by using highly-directional radiofrequency jammers designed to disrupt communications between drones and their operators. One key limitation of these

devices is that they can only disable drones that are directly controlled by a human operator. Autonomous systems are far more resilient against such countermeasures. Beyond that, their overall effectiveness varies heavily by type and circumstance. Aside from these limitations, they are relatively portable and easily fielded.

An officer test-fires the anti-drone gun known as the DroneDefender. (Battelle)

It is not perfectly clear if the *Russell* had this equipment onboard previously, or if "ghostbuster" devices were brought onboard in reaction to the earlier drone incidents. If so, they would have been among the simplest counter-drone devices to field given their independent man-portable deployability. Our previous reporting did not show any indication of the use of these devices in the earlier incidents, and references to them appear shortly after the counter-UAS exercise, heavily suggesting they may have been introduced in response to the incursions. We are not aware of these systems being widely fielded on surface ships at the time, especially those operating in home waters. Also, only the USS *Russell* reported the use of "ghostbusters" in its logs.

After a relatively quiet period, another incident occurred in the very early hours of July 30th. A SNOOPIE team was activated and "ghostbusters" were called for shortly afterwards.

What follows are uncharacteristically redacted logs. As with the map of the drone movements earlier in this story, the exemptions pertain to technical military data. In the hundreds of pages of ship logs reviewed by us about this matter, these are the first to contain significant redactions and the only ones to reference this particular exemption.

By 3:00 AM on July 30, the pattern of redaction ends. In the same timeframe, at least two other ships nearby noted drone or UAV activity. As previously reported, the *USS Kidd,* another *Arleigh Burke* class destroyer involved in these incidents, deployed its own SNOOPIE team for UAVs at 2:16 AM that day. The log later notes that the SNOOPIE team was recalled by 3:27 AM.

Logs from the *USS Paul Hamilton* also reflect multiple drones spotted off the ship, and their own SNOOPIE team activated around 3:30 AM on July 30.

Later in the morning on the same day, the *Russell* again engaged its SNOOPIE team and the "ghostbusters."

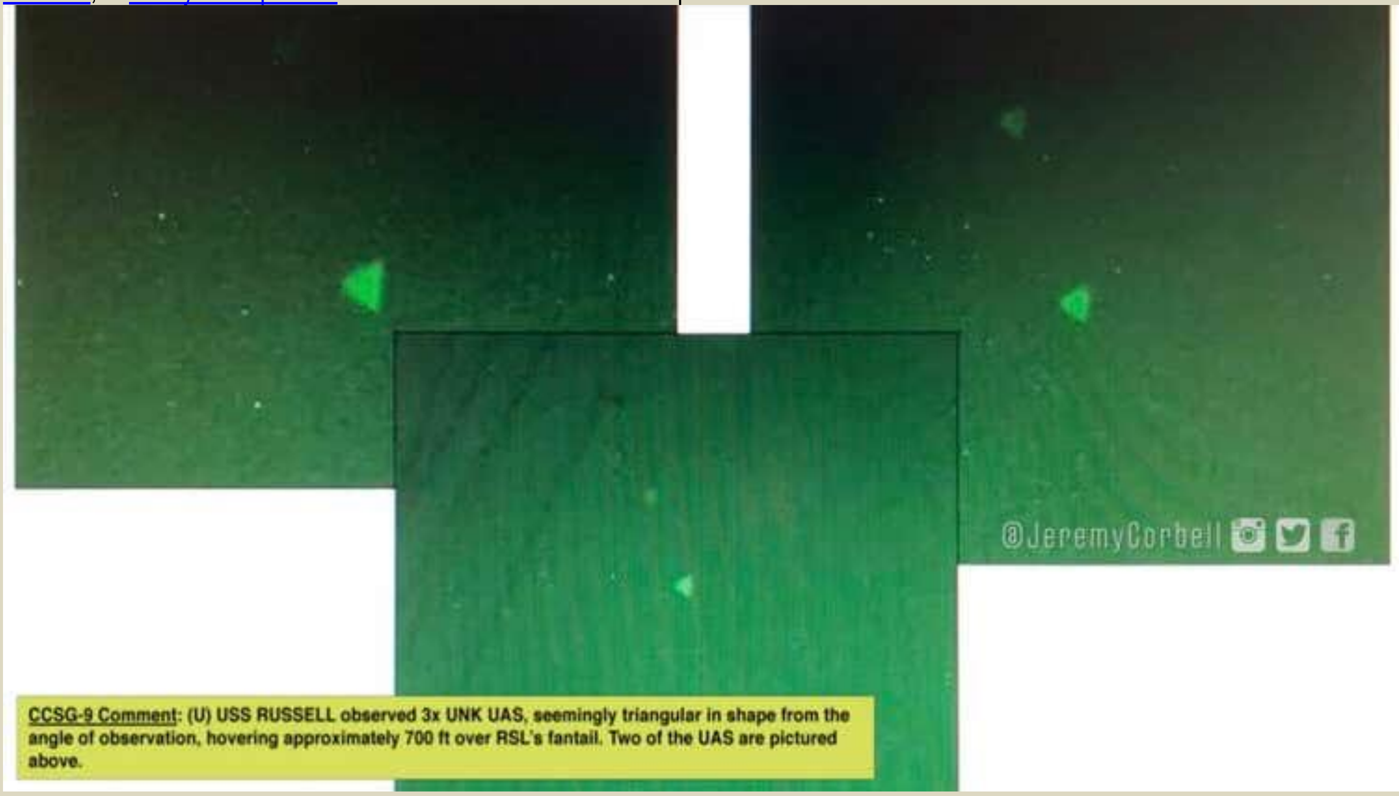
This log entry also has a reference to "SCAT," which likely stands for Small Craft Action Team. Speaking to *Business Insider* last year, Navy Lt. J. G. Frank Smeeks, an anti-terrorism officer, explained that "SCAT is a team consisting of crew-served weapons machine gun operators that provide 360-degree coverage of the ship, an anti-terrorism tactical watch officer and a gunnery liaison officer. They are called away as a pre-planned response to threats the ship may face like a small boat attack or low, slow flyer." Logs from another nearby ship, the *USS Bunker Hill*, also indicate that they manned their own SNOOPIE team and SCAT in the same timeframe. The *Bunker Hill* logs are unclear if the SNOOPIE team was deployed in response to a drone sighting. The simultaneous use of three teams designed for quick reactions to potential threats suggests a high level of alarm well into the morning.

In this same general time period, it appears that the *USS Russell* was visited by an unnamed admiral. Deck logs record an admiral arriving on July 22, just prior to the implementation of counter UAS training exercises and the start of references to "ghostbusters" on the morning of July 24. Logs also remark about an admiral casting off on July 31, but there are few other indicators what the purpose of the visit may have been or if it had any connection to the UAS incidents.

Cumulatively, these records show a sustained, but an intermittent pattern of drone sightings throughout the month of July by Navy ships operating off Southern California. These events seemed to have spurred additional training and the rapid deployment of unique capabilities like the "ghostbuster" counter-UAS equipment. It remains unknown what impact, if any, this training and equipment had on deterring drone operations. At least three ships reported sighting drones in the very early hours of July 30th, with unusual and extensive redactions in the logs of the *USS Russell,* but we do not know what happened the next day, or in the weeks that followed.

It is also noteworthy that these events occurred well after Navy investigators sought to "correlate or rule out operations" with Fleet Area Control and Surveillance Facility (FACSFAC) based in San Diego. Indeed, an investigation began immediately after the initial events on July 16th, with information on the incidents being routed to the Chief of Naval Operations as early as July 18th. Given the progress of the investigation, more prosaic causes like errant US aircraft or civilian activity had already been examined. Whatever the outcome of the July 30th event, it was likely closely scrutinized by Navy leadership.

The lack of concrete identification of the aircraft involved also led to widespread public speculation earlier this year. Leaked photos and videos said to pertain to the July 15th and 16th incident were released this summer by filmmaker Jeremy Corbell. The materials consisted of footage of radar screens showing multiple unknown contacts, video of an object apparently falling into the ocean, and a brief video of a triangular-shaped light flying over the deck of a ship. The apparent triangular shape of the object has been strongly debated, as many have posited it was the result of a common optical artifact.



CCSG-9 Comment: (U) USS RUSSELL observed 3x UNK UAS, seemingly triangular in shape from the angle of observation, hovering approximately 700 ft over RSL's fantail. Two of the UAS are pictured above.

A briefing slide depicts several pictures of a "seemingly triangular" shape recorded by the Russell

The Department of Defense was quick to partially authenticate the material, acknowledging that the videos were taken by Navy personnel. However, to date, the Pentagon has not provided any details that corroborate the location or timeframe of the footage or any clarification on what the objects were. Corbell maintains that the videos depict extraordinarily complex vehicles capable of "transmedium" travel, or the ability to traverse both water and the atmosphere with ease. Chief of Naval Operations Michael Gilday explained in a press briefing earlier this year that while the Navy had not positively identified the aircraft, there were no indications they were extraterrestrial in nature.

There has been significant overlap in the discussion of the mounting threat from lower-end drones and resurgent interest in UFOs in recent years. That overlap is conspicuous in the recent National Defense Authorization Act language, which authorizes an expansive approach to the Pentagon's study of UFOs. The language, introduced by Senator Kirsten Gillibrand, a New York Democrat, creates a requirement for conducting "field investigations," as well as new mandates to scientifically examine UFO reports. An amended version of Gillibrand's proposal was ultimately adopted in the NDAA and awaits President Biden's signature. While many have focused on otherworldly explanations for UFO sightings, Senator Gillibrand told *Politico* that the rationale for her interest encompassed conventional and emerging technology and not only the "unknown." She explained, "you're talking about drone technology, you're talking about balloon technology, you're talking about other aerial phenomena, and then you're talking about the unknown."

The urgency surrounding the drone issue has been a growing focus among defense policymakers as encounters with both civilian and military aircraft have become widespread. In the last five years the Federal Aviation Administration has gathered approximately ten thousand drone incident reports. We have made many of these reports available in an interactive tool that maps the location and descriptions of the incident. Far from being only a domestic issue, drones have also become a matter of grave concern for military leaders. Earlier this year Marine General Kenneth McKenzie Jr. said in a speech to the Middle East Institute that "the growing threat posed by these systems coupled with our lack of dependable, networked capabilities to counter them is the most concerning tactical development since the rise of the improvised explosive device in Iraq." McKenzie also explained that drones "provide adversaries the operational ability to surveil and target U.S. and partner facilities while affording plausible deniability and a disproportionate return on the investment, all in our adversaries' favor."

In the case of the 2019 Southern California incidents, several of these factors appear to be at work. The newly released map clarifies just how closely drones were shadowing Navy ships, likely affording opportunities to gather a variety of valuable intelligence. The lack of positive attribution of the aircraft even today speaks to McKenzie's comments about plausible deniability and disproportionate return. Questions also linger surrounding "dependable, networked capabilities" and countermeasures. For now, it remains unknown if the "ghostbuster" devices and additional counter-UAS training were sufficient to halt the incursions. A highly pertinent question now is when exactly did they end, and how widespread similar incidents have been elsewhere?

The timing of training and potential deployment of counter-UAS capabilities in the weeks after the events of July 15th and 16th also points to the Navy believing these were unidentified drones, not fantastic craft with out-of-this-world abilities. This appears consistent with our previous reporting, which found that the Navy had investigated its own drone flights and questioned civilians known to operate drones in that area. Additionally, countless deck log entries refer to the aircraft not only as UAS or UAV, but also plainly as drones. Finally, asked about our reporting, the Chief of Naval Operations Admiral Michael Gilday himself stated there was no indication that the aircraft were extraterrestrial. Still, since they remain unidentified, we can't say for certain exactly what they were or who they belonged to. We are still far from a full answer. These new documents suggest several avenues for further inquiry, and we expect new information to develop. As we and our expert sources continue to analyze the documents some inferences are bound to change. References to the colorful term "ghostbuster" appear to be new to this story, and we are currently pursuing additional records to clarify exactly what this entailed and what happened in subsequent days and weeks.

What if future war planes can move underwater before a stealth attack by air?

Robots to Replace Warfighters in Subterranean Warfare

Source: https://i-hls.com/archives/112246

Dec 22 – Engaging in subterranean (SubT) environments puts warfighters in dangerous situations with limited visibility and movement, as well as potential environmental risks such as flooding, harmful air quality, etc.

Additional challenges include limited situational awareness and severe communication constraints.

In such situations, deploying autonomy and sensor-enabled robotic systems provide the warfighter a tactical advantage through the ability to perform remote reconnaissance and other specific mission tasks while decreasing overall exposure to risks and lessening physical and cognitive load.

Robotic and autonomous technological advancements for SubT environments were recently demonstrated by the US Army DEVCOM Ground Vehicle Systems Center (GVSC).

Through a project called the **Autonomous Tunnel Exploitation** (ATE), the demonstration exhibited improved situational understanding and tactical advantage by using multi-robot autonomy and sensing in a series of operational tests in a relevant SubT environment.

The technologies developed by the Center included GPS-denied autonomous navigation; 2D/3D spatial mapping; object detection; integrated chemical, biological, radiological, and nuclear sensing; mesh radio communication; and automated after-action reporting, according to dvidshub.net.

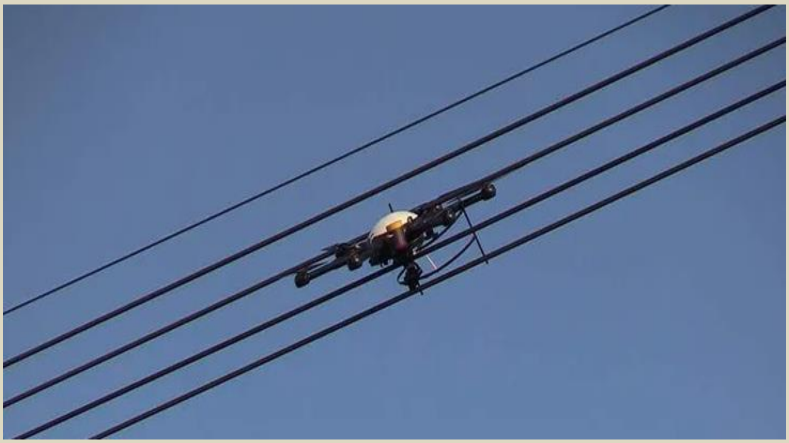
"With the capabilities we developed, warfighters can task unmanned systems to rapidly map, navigate, and exploit underground environments including natural cave networks, tunnel systems, and urban underground infrastructure without stepping a foot inside," said Danny Guerrero, GVSC project manager for Dismounted Robotic Systems.

"The end goal is a fully autonomous robotic solution where a multi-robot team in a highly communication-degraded environment can complete a mission with minimal human supervision," he added.

A project of a drone capable of charging from power lines has been proposed in Russia

Source: https://www.aroged.com/2021/12/25/a-project-of-a-drone-capable-of-charging-from-power-lines-has-been-proposed-in-russia/

Dec 15 – Russian military developers have proposed a project for an unmanned aerial vehicle (UAV) capable of recharging a battery pack from power lines (PTL). This solution is expected to significantly increase the battery life of the drones.



According to RIA Novosti, the concept of the UAV was developed by specialists from the Tyumen Higher Military Engineering Command School named after Marshal of Engineering Troops Proshlyakov of the RF Ministry of Defense. Information about the invention is published on the Rospatent website.

The idea is to equip the drone with a special disconnectable circular magnetic circuit. These are current clamps with which the drone can hook onto power lines to replenish the battery's energy reserve.

For the drone, it is proposed to use the multicopter architecture, that is, a design with multiple rotors. The possibility of recharging from power lines will allow the drone, for example, to carry out reconnaissance of the terrain for a long time and at long distances from the take-off point.

«*It is assumed that such a copter will work as follows: the remote operator of the drone points its "pincers" to the power line and gives a command to close them. The drone then charges upside down. After charging the battery, the copter's engines start – and the "pincers" open the electrical wire, the drone returns to its original position and continues its flight*", – says the publication of" RIA Novosti ".

EDITOR'S COMMENT: Brilliant idea! Amazon had a similar idea to recharge Prime Air drones on street lights.

New Israeli Consortium will Tackle Human-Robot Interaction

Source: https://i-hls.com/archives/112368

Dec 28 – Autonomous robotic platforms currently operate in a "sterile" human-free environment, such as logistics centers and automated production and assembly lines. Integrating robots in a shared workspace environment with human teams will allow the transfer of routine, dull and burnout-inducing tasks to robots and reduce workloads on human teams, thereby increasing crew productivity.

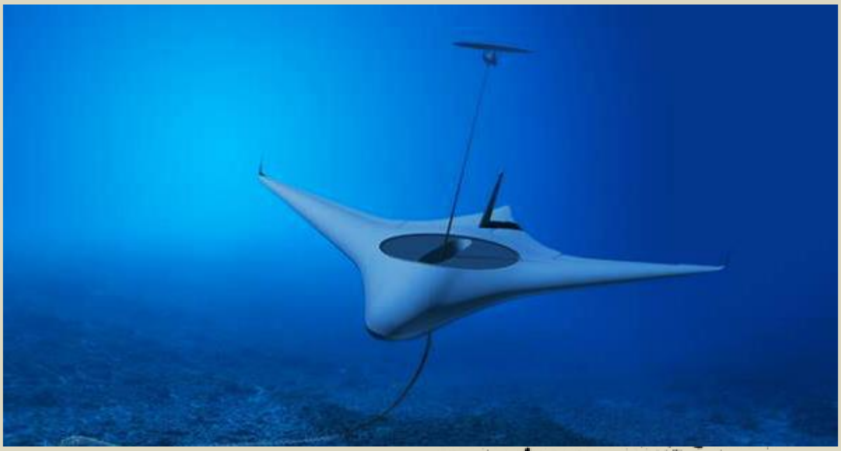
Such integration will only be possible when human crews feel confident and able to communicate naturally with robots, operating in their close environment.

In an attempt to close this technological gap, the Israel Innovation Authority has recently approved the establishment of a new innovation consortium focusing on Human-Robot Interaction.

The consortium is led by Elbit Systems C4I and Cyber, for Human-Robot Interaction (HRI) technologies research and development. It includes leading robotics companies and academic researchers in the fields of Artificial Intelligence, computer science and behavioral sciences, with the goal of developing an innovative HRI infrastructure, addressing the need for close interaction between robotic systems and human users natural communications (verbal & gestures) technologies, according to relevant social codes, robotic platforms level of autonomy methodologies, and more, according to Elbit's announcement.

Manta Ray Project

Source: https://www.darpa.mil/program/manta-ray

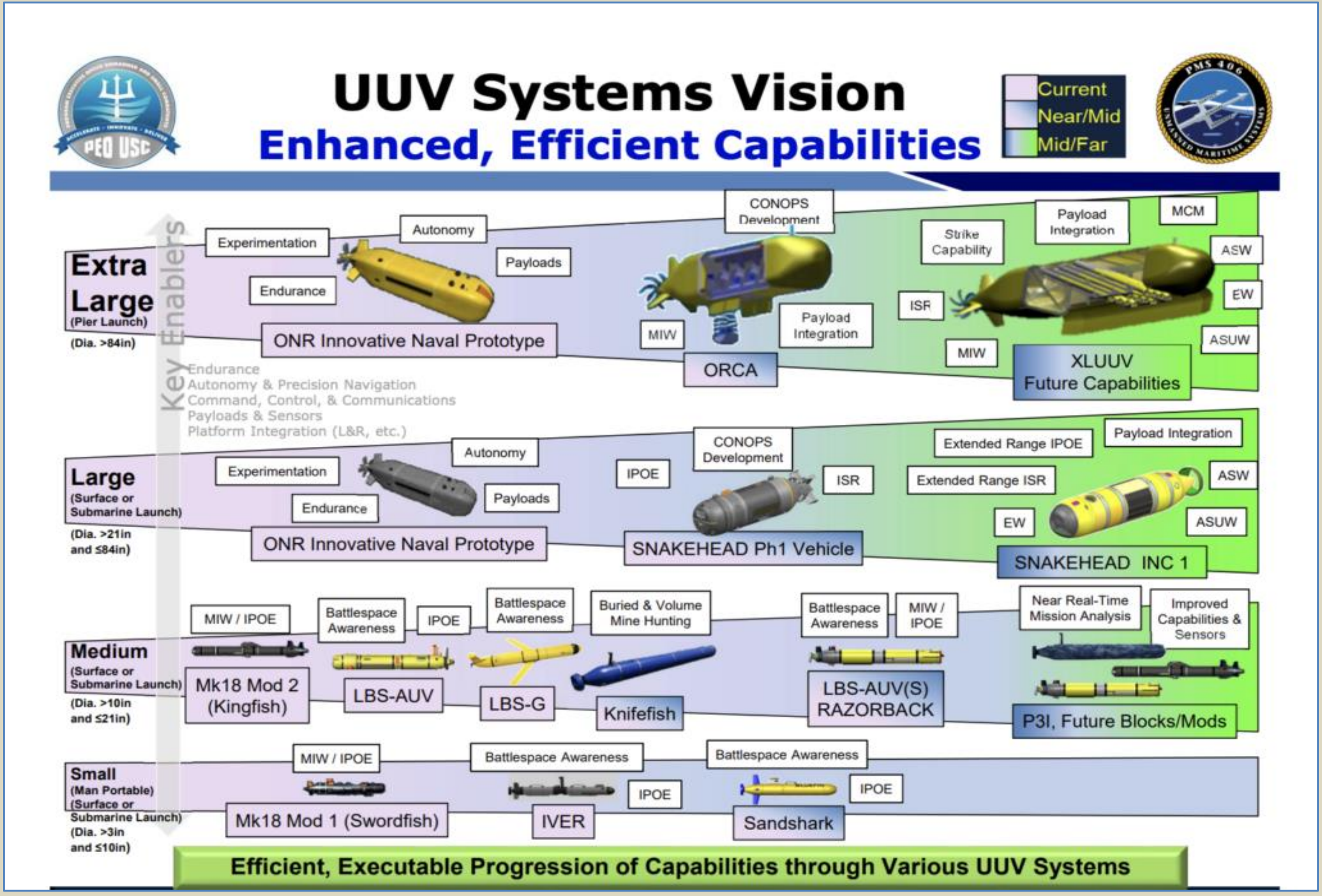


Unmanned undersea vehicles (UUVs) that operate for extended durations without the need for human-present logistic support or maintenance offer the potential for persistent operations in forward environments. Such systems could allow traditional host vessels increased freedom of operational flexibility while providing traditional servicing ports with relief of workload.

The Manta Ray program seeks to demonstrate critical technologies for a new class of long duration, long range, payload-capable UUVs. If successful, this new class of UUV will give the combatant commander an amplification of capacity without disrupting current operations by remaining independent of manned vessels and ports once deployed.

The Manta Ray program plans to advance key technologies that will benefit future UUV designs, including, but not limited to:

- Novel energy management techniques for UUV operations and undersea energy harvesting techniques at operationally relevant depths;
- Low-power, high efficiency undersea propulsion systems;
- New low-power means of underwater detection and classification of hazards or counter detection threats;
- Mission management approaches for extended durations while accounting for dynamic maritime environments;
- Unique approaches for leveraging existing maritime data sets and exploiting novel maritime parameters for high-efficiency navigation and/or C3; and
- New approaches to mitigate biofouling, corrosion, and other material degradation for long duration missions.



UUV Systems Vision

Enhanced, Efficient Capabilities

Current
Near/Mid
Mid/Far

Efficient, Executable Progression of Capabilities through Various UUV Systems

The Department of Defense's Underwater Unmanned Vehicle Systems Vision, showing the various platforms it hopes to field in the near future. (Image Source: The Navy)

Manta Ray is a multi-phase effort that includes at-sea demonstration of critical technologies. The program is using a disciplined systems engineering approach to define demonstration system objectives and identify enabling technologies needed for future systems.

Security Threat Scenarios of Drones and Anti-Drone Technology

By Yeon-Jun Choi (Kwangju Women's University)

Academy of Strategic Management Journal Volume 21, Issue 1, 2022

Source: https://www.abacademies.org/articles/Security-threat-scenarios-of-drones-and-anti-drone-technology-1939-6104-21-1-106.pdf

In the past, drones were only used in the military field, but in the age of the 4th Industrial Revolution, they are used in conjunction with a commercial purpose such as GPS and video transmission where they operate with the integration of terrestrial devices. In addition, they are actively utilized in a diverse range of industries through the fusion with many cutting-

edge technologies such as Artificial Intelligence (AI) and IoT (Internet of Things). Also, with the increase in the output of the drones' motor and battery and better performance coming from the miniaturization of them, they have provided a variety of benefits to society and at the same time, they are setting a new paradigm of living-style. However, with the increase in utilization of drones, which has made it more common-place than before to normal citizens, it has also led to more attacks by dirty drones: we have come to the situation where we need to respond to the onslaught of drones in the field of security in order for the safety of society. As drones are becoming more advanced as time goes past, they are not limited to physical attacks, but instead, they carry out operations such as scouting and information theft. Therefore, this research suggests counter-measurements, utilizing the anti-drone technologies, for the security threat of drones through the analysis of security threat scenarios on illegal footage taking, spoofing and attacks through malicious code and physical attacks of drones.

The Threat of Iran's Drone Swarms

By Seth J. Frantzman

Source: https://www.meforum.org/62921/is-irans-new-drone-swarm-tech-a-game-changer

Dec 26 – Images of a new Iranian drone launcher have appeared online and in Iranian media over the past several days. The drones, dubbed Shahed-136, were combined with missiles in a drill that Iran says took place last week.

Iran's December 20-24 "17th Great Prophet" drill witnessed numerous missile and drone launches

Iran has called these types of drones a "suicide drone," or kamikaze drone. This means they fly into a target and self-destruct.

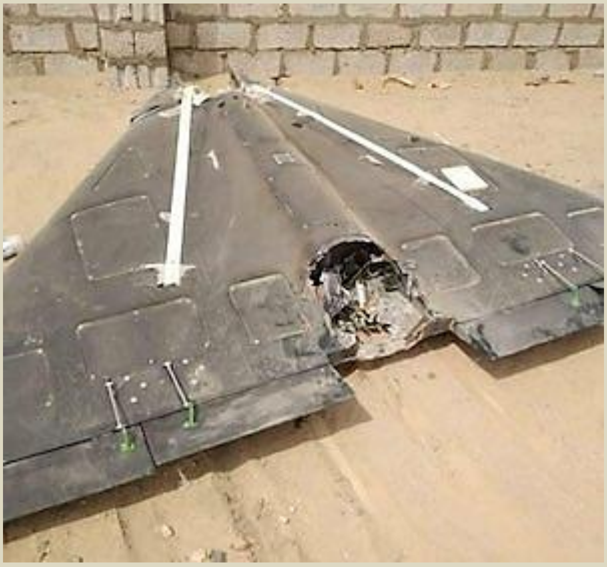
These types of drones have been mentioned before but have not been shown in such close-up detail.

In January, Tom O'Connor wrote in *Newsweek*: "Imagery seen by *Newsweek* and confirmed by an expert who follows Iranian activities in the region indicate the presence of Iranian Shahed-136 loitering munitions, also called 'suicide drones,' deployed to the northern Yemeni province of Al-Jawf, an area of the country controlled by the Ansar Allah, or Houthi, Zaidi Shiite Muslim rebel movement."

This was the first time this type of drone was mentioned in overseas deployment. Prior to this, Iran had built kamikaze drones, but this specific type had not been seen in public military drills.

Based on Tehran's state-run and semi-official media, we now know the Shahed-136 exists and is not only a kamikaze drone but that Iran has created a new way to launch the drones in a kind of multiple-launch, or drone-swarming, format.

Drone swarms are a new technology whereby multiple drones are used to strike at targets. This can overwhelm air defenses and/or wreak havoc. In the past, drones such as the US Predator were not usually used alongside other drones.



Wreckage of a Shahed-136

In addition, drones have not often been used to enter contested airspace, such as the well-defended airspace of Israel or Saudi Arabia. This is because drone technology was mostly dominated by the US, Israel and several other countries up until recently. Iran, China and other drone powers have now entered the game.

Iran has invested heavily in kamikaze drone technology, including the types of drones known as Qasef in Yemen and Hamas's Shehab. These are based on Iranian technology and models. Recent reports from the Alma Research Center have said Hezbollah may have some 2,000 drones – many based on Iranian models.

The new launcher that Iran unveiled in its recent drill appears to have five layers, or racks, on which drones can be fitted before launch. The launcher can be mounted on the back of a truck, so it could be disguised as freight and look like any other commercial truck plying the roads.

Pro-Iranian groups have done this before in Iraq, where they mounted 107-mm. or 122-mm. rockets on the back of trucks. In one documented case, they disguised the rockets under the bed of a normal commercial truck to fire them at a US facility in Iraq. In September 2020, Iran put rockets into a shipping container to hide them.

Iran's new launcher for its Shahed-136 ostensibly gives it the ability to not only hide them but to put five drones in these types of converted trucks. It could conceivably launch dozens of these drones at a target in a kind of "swarm."

Although there is no evidence the drones can communicate with each other or that they have the kind of advanced AI-swarming capability that exists in the West, it does not mean they do not pose a threat. A truck with a secret drone compartment can be used to strike at vulnerable targets or be used to probe air defenses.

Iran did this in 2019 in Saudi Arabia, using drones and cruise missiles to attack Abqaiq, a Saudi Aramco oil facility. Despite radar and air defense, the Saudis did not stop the drones.

Iran's advances since then clearly pose a greater threat now throughout the region. The Shahed-136 is not a very large drone, according to the images, and it contains a warhead, making it a potentially dangerous weapon and possibly not easy to detect because of its size and small radar cross section.

Iran's innovations with the Shahed-136 are not necessarily new. It has based the design of the drone on existing loitering munitions used by other countries. In addition, it is not the first nation to dream up the idea of a multiple drone-launcher system.

Azerbaijan released a music video in April 2018 that included a truck with a launcher on the back that had 12 doors for drones to fly out of. According to reports at the time, the video showed Harop drones, a loitering munition made by Israel Aerospace Industries. Azeri officials praised this drone in September 2020, and according to *Israel Hayom* in October 2020, a report from Armenia said a Harop had crashed in Iran.

"The Armenian Unified Infocenter reported the aircraft was an Israeli-manufactured IAI Harop kamikaze drone that crossed from Azerbaijan to Iranian territory and was shot down by Iranian forces, or crashed in Ardabil, not far from fighting between Armenian and Azerbaijani forces in the Nagorno-Karabakh Region," the report said.

It is not known if Iran used that Harop as a model in 2020 and based its launcher on the Azeri system. The Iranian launch system is different in its positioning and method. However, the overall concept is the same. The concept is to give the forces the ability to launch several drones at the same time.

Newsweek reports this January said the Shahed-136 had a range of some 2,000 km. This is a long range for such a small drone, but it may be possible if Iran has made advances in its technology.

It appears unlikely it can achieve this range, but the reports appeared to coincide with claims that Iran had sent this drone to the Houthis in Yemen. A 2,000-km. radius around Yemen would mean the drone could reach Eilat in southern Israel or threaten shipping in the Gulf of Oman.

The threat of a drone swarm of the type Tehran has now showcased is rising. Iran has experimented with this before, but its new launcher and new drones appear to present a more serious threat than in 2019.

If Iran were to traffic these systems to Iraq, Syria, Lebanon or Yemen with the types of multiple launchers it has built, this would put a new threat in play in any future conflict with Israel.

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

Low-cost warfare: US military battles with 'Costco drones'

Source: https://counteriedreport.com/low-cost-warfare-us-military-battles-with-costco-drones/

Jan 05 – Late in 2019, American military equipment detected an incoming enemy drone over an Iraqi base hosting US forces. The troops were jumpy; their base was vulnerable and exposed.

The detection system gave a grainy picture but indicated the object was getting closer, according to people familiar with events. US forces launched an expensive counter drone missile, which circled the target, missing twice, before being detonated mid-air to avoid a ground explosion. On closer inspection, defence officials later determined the incoming threat was not, after all, a lethally armed drone designed to kill US troops. It was a balloon.

The US has been the pioneer in the use of large killer drones for its global war on terror. Today, much of the conversation about warfare is dominated by extremely sophisticated weapons such as hypersonic, lasers or missile defences that push at the boundaries of the possible. Read more…

Raytheon's counter-UAV Coyote heads toward deployment

Source: https://www.flightglobal.com/military-uavs/raytheons-counter-uav-coyote-heads-toward-deployment/145868.article

October 2021 – Raytheon's Coyote Block 2, an exploding drone intended to down other unmanned air vehicles (UAVs), wrapped up a 10-day test period at the US Army's Yuma Proving Ground in Arizona in August.

The interceptor proved effective at destroying group one-, two- and three-sized UAVs, which range between 9.1kg (20lb) and 599kg. The UAV is headed toward an initial operating capability declaration and deployment overseas by the service soon, Abel Ghanooni, Raytheon's senior director for short-range air defence and rapid development programmes, said on 11 October.

Coyote Block 2 is a jet-powered UAV that uses rocket boosters to launch from a rail. Guided by Raytheon's Ku-720 ground-based radar, the drone uses a radio frequency sensor to trigger its warhead when it gets close enough to its target.

The UAV was developed over the past couple of years under an accelerated timeline, forgoing the conventional US government development and production process so that the US Army could field the defensive weapon sooner. After Iran allegedly used explosive-laden UAVs to attack Saudi Arabia's oil facilities in 2019, the US Army has been hurriedly looking for a way to defend against loitering munition-like weapons.

Coyote Block 2 was given a small jet engine, instead of its predecessor Block 1's propeller, because the US Army wanted something that could get to its target faster, as well as engage at longer ranges. The UAV has a range of at least 5.4nm (10km), although Ghanooni declines to give specifics.

Raytheon also fields a "non-kinetic" Block 3 version of the Coyote. That UAV is powered by a propeller like the original vehicle and uses an electronic warfare payload to down drones. Ghanooni declines to say the type of electronic warfare weapon that is employed.

The Coyote's command and control system uses algorithms to rapidly decide what type of UAV to deploy.

"If you've got something that is flying high or fast, that's larger, you probably want to use a Block 2, just to get out there quicker and get it down," Ghanooni says. "If you've got a few of them coming at you, that are maybe smaller, you probably want to use the Block 3 non-kinetic to go out."

Ghanooni declines to say specifically how many Coyotes the US Army has purchased, but notes the number is in the hundreds. He declines to say where the UAVs will be deployed, other than to say "high-threat" areas.

Smart Shooter releases Smash Dragon for UAS precision

Source: https://www.shephardmedia.com/news/air-warfare/smart-shooter-releases-smash-dragon-for-uas-precis/

Jan 10 – Smart Shooter has unveiled its newest Smash fire control system, the Smash Dragon.

Smart Shooter, a manufacturer of fire control systems that significantly increase the accuracy and lethality of small arms, has revealed the new Smash Dragon, which is configured for use by UASs.

Smash Dragon is an armed drone system that incorporates Smash technology, featured in other products such as the Smash 2000, which ensures precise target elimination.

The Smash Dragon advanced robotic weaponry payload can be mounted on different drones and other UAS.

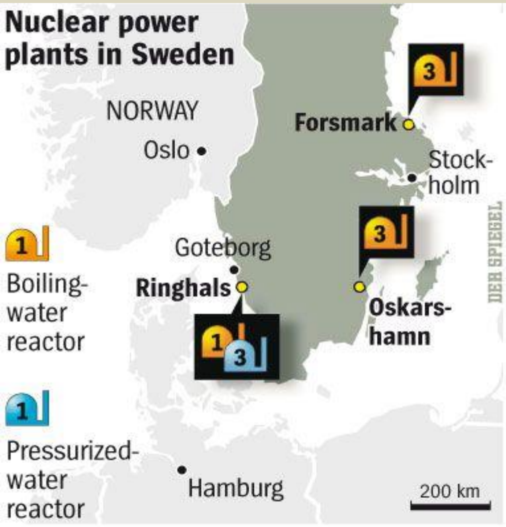
It can incorporate various types of assault rifles, sniper rifles, 40mm and other ammunition.

It features a unique stabilisation concept that enables the system to accurately hit static and moving targets while flying.

It achieves this accuracy through Smash's propriety target acquisition and tracking algorithms as well as advanced computed vision capabilities.

The system has successfully completed live firing tests and is currently under advanced stages of development.

Smart Shooter's Smash family are in use with militaries across the world, including India, Israel and the US.



Swedish police hunt for drone seen flying over Forsmark nuclear plant

Source: https://www.swissinfo.ch/eng/swedish-police-hunt-for-drone-seen-flying-over-forsmark-nuclear-plant/47264626

Jan 15 – Police in Sweden deployed patrols and helicopters to the Forsmark

nuclear plant to hunt for a large drone seen flying over the site late on Friday, but were unable to catch the unmanned vehicle, they said on Saturday.

The incident came a day after Sweden's military started patrolling the main town on the Baltic Sea island of Gotland amid increased tensions between NATO and Russia and a recent deployment of Russian landing craft in the Baltic.

Forsmark, which is Sweden's biggest electricity producer, lies on the Baltic coast about 150 km (93 miles) north of the capital, Stockholm.

Police saw the drone, first spotted by a security guard, moving around the plant before disappearing towards the island of Graso.

"Police continue to try to locate the drone, even with their own (drones), but without success," the police force said in an incident report on its website, adding that there were no signs the drone had dropped anything in the area or landed.

It also cited unconfirmed reports of possible drone sightings at the Ringhals nuclear plant on the country's west coast.

Greek Students Triumph in World Robotics Olympiad

By Theo Ioannou

Source: https://greekreporter.com/2021/11/03/greek-students-triumph-robotics-olympiad/

Nov 03 – The Greek national Robotics team recently won three medals in the Robotics Olympiad, held between June and September.

The "First Global Challenge Team Greece" won one gold, one silver and one bronze medals.

The Robotics Olympiad First Global Challenge called "Discover and Recover 2021" was held from June 27 to September 25, 2021. It was conducted remotely, due to the pandemic restrictions. The First Global Challenge Robotics Olympiad is a robotics, science and technology event.

The Greek team grabbed the gold medal in the field of Health, the silver medal in the "Panacea" project, and the bronze medal for winning third place in the overall classification of the Olympics.

It is the first time that a Greek Robotics Team have won medals in a world event in all competing categories, as well as in the overall world ranking.

Greek Robotics team among 190 Olympiad participants

National teams from 190 countries participated in the "Discover and Recover 2021" Olympiad, with student competitors aged 16-18. It was the second "First Olympic Event" to be held exclusively remotely.

Its goal was to motivate young people around the world to engage in research and propose innovative solutions at tackling the effects of the COVID-19 pandemic in four areas: Health, education, the economy and the environment.

TITAN Eduact
Εκπαιδευτικές Δράσεις για την Καινοτομία
LEGO® Education SPIKE™ Prime
education
Our Future: Built Better Together

The Greek National Team was created by an initiative of the educational non-profit association called “Eduact – Action for Education.” It has been introducing new educational programs for all children in Greece since 2013, through innovative actions cultivating the skills of the future.

A cornerstone of Eduact’s work is the introduction of educational robotics in skill labs. In 2018, Eduact put Greece on the map of the global Robotics Olympiad First Global Challenge.

An open call to Greek students led to a team of 30 children from all over Greece from 14-18 years of age. They were selected based on their programming and robotics skills, their engagement with science and their experience in both national and world events.

Students selected based on robotics and programming skills

All the above were evaluated by a special committee of educational academics and members of the Board of Directors of Eduact. They then made the final selection for the Olympiad entries.

Pupils from Thessaloniki, Attica, Patras, Nafpaktos, Orestiada and Crete worked hard all summer. Their first creation was the “Panacea” robot, an autonomous home nurse which can take patients’ vital signs, inform medical staff and disinfect a small area.

Their second invention was the “Hero” robot, which can move accurately within defined paths, collect and carry objects, throw balls and cubes at a distance, and even lift weights.

Their final achievement was their version of the so-called Cubesat, a small meteorological satellite designed to study atmospheric data and alert the ground station about potential fires.

Three rounds equal three medals for Greek students

The Olympics involved three rounds. In the first round, called the Solutions Challenge Award, the Greek National Team chose the very key sector of health, and developed “Panacea.”

In the second round, the Greek team had to create an alliance with a team from a different continent that had chosen the same theme category. The Greeks chose Canada and started working with students from that country.

They jointly advanced to the third round, called the Solution Grand Challenge Award. They combined their innovative solutions into a joint integrated proposal, which was declared best in the world.

The Greek team was led by Anastasios Kollias, PhD, from the University of Athens. He is also an "O3 Out of the Ordinary" LEGO Education trainer and a research associate of Eduact and the Greek Robotics Team.

Drone attack in Abu Dhabi claimed by Yemen's rebels kills 3

Source: https://apnews.com/article/business-dubai-united-arab-emirates-abu-dhabi-yemen-8bdefdf900ce46a6fd6c7bc685bf838a

In a satellite photo by Planet Labs PBC, Abu Dhabi International Airport is seen on Dec. 8, 2021. A suspected drone attack by Yemen's Houthi rebels targeting a key oil facility in Abu Dhabi killed three people and sparked a separate fire at Abu Dhabi's international airport on Monday, Jan. 17, 2022, police said. (Planet Labs PBC via AP)

Jan 17 — A drone attack claimed by Yemen's Houthi rebels targeting a key oil facility in Abu Dhabi killed three people on Monday and sparked a fire at Abu Dhabi's international airport.

Emirati police identified the dead as two Indian nationals and one Pakistani. Several people were also wounded at an industrial area where Abu Dhabi's state-owned energy company runs a pipeline network and an oil tanker storage facility. The police said they suffered minor to moderate injuries.

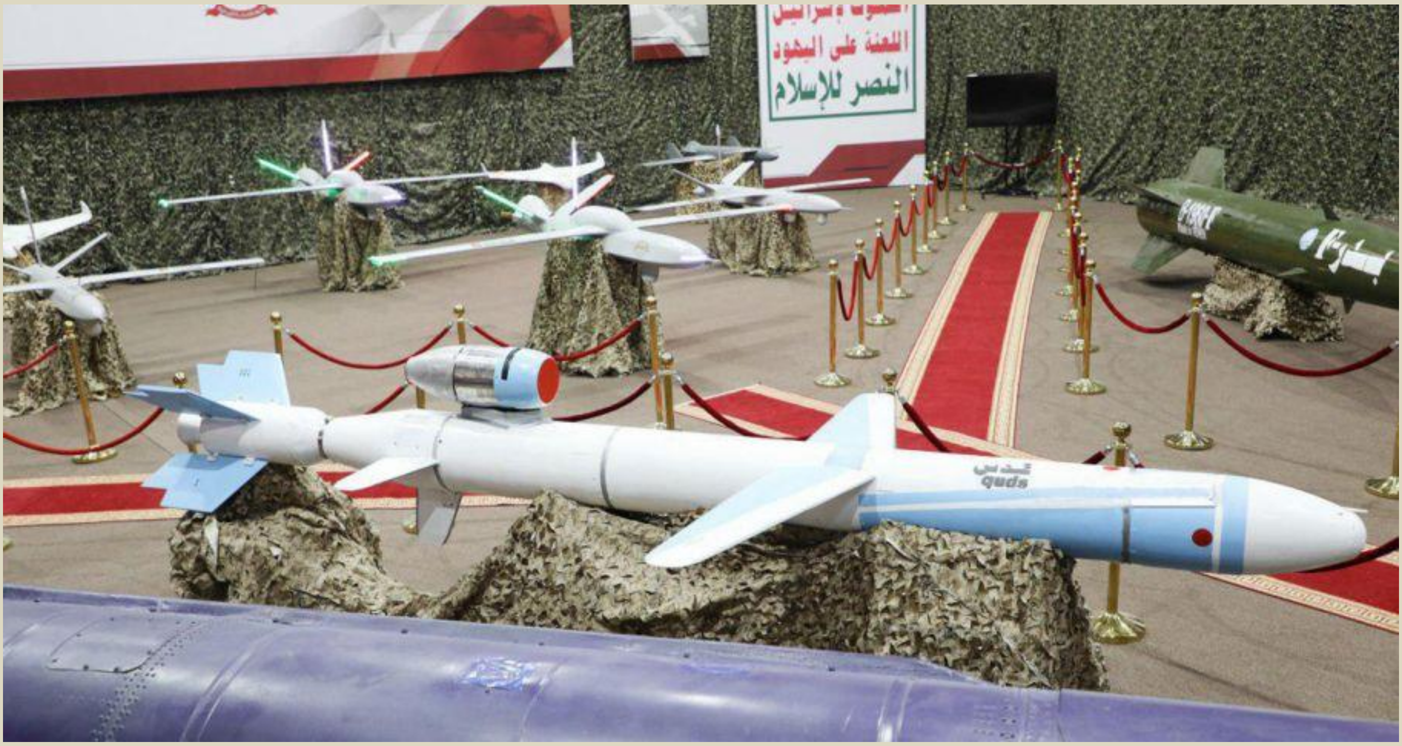
Senior Emirati diplomat Anwar Gargash blamed the Houthis for the attack, saying on Twitter that Emirati authorities were handling the rebel group's "vicious attack on some civilian facilities" in the UAE's capital with "transparency and responsibility."

"The tampering of the region's security by terrorist militias is too weak to affect the stability and safety in which we live," he tweeted.

Three transport tankers caught fire at the oil facility, while another fire was sparked at an extension of Abu Dhabi International Airport.

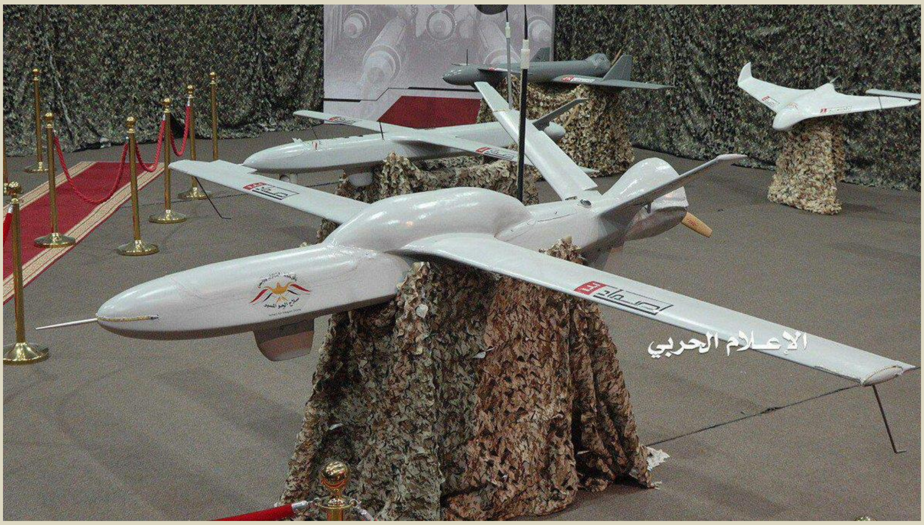
Police said an investigation was underway and that preliminary findings indicate there were small flying objects, possibly belonging to drones, that fell in the two areas and may have

caused the explosion and fire. They said there was no significant damage from the incidents, without offering further details.
Yemen's Iranian-backed Houthi rebels claimed they were behind an attack targeting the United Arab Emirates on Monday, but they did not offer details. Although the UAE has largely withdrawn its own forces from the war in Yemen, it is still actively engaged in the conflict and supports Yemeni militias fighting the Houthis.
The incident comes as the Houthis face pressure and are suffering heavy losses. Yemeni forces, allied and backed by the UAE, have pushed back the rebels in key southern and central provinces, dashing Houthi efforts to complete their control of the entire northern half of Yemen.



Yemeni Quds-2 cruise missiles. The US Navy's recovery of a complete missile from an arms-smuggling ship later that year enabled the UN panel of experts on Yemen to estimate its range at about 800 km.

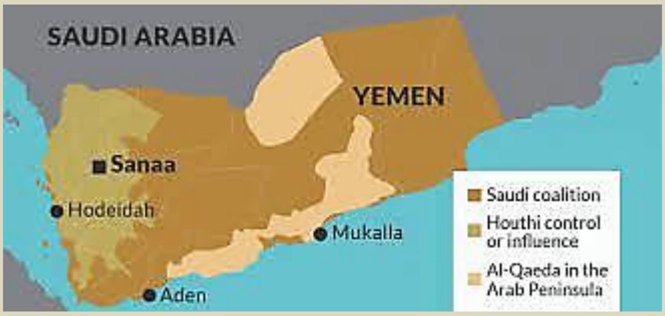
Yemen's government-aligned forces reclaimed the entire southern province of Shabwa from the Houthis earlier this month and made advances in nearby Marib province. They were aided by the UAE-backed Giants Brigades and had help from Saudi airstrikes.



Yemeni Sammad-3 drone

Saudi Arabia condemned Monday's attack targeting Abu Dhabi, describing it as "a cowardly terrorist attack" that shows the dangers posed by the Houthis. Saudi Arabia, as well as the United States, U.N. experts and others have accused Iran of supplying arms to the Houthis.
The UAE was a key member of the Saudi-led coalition that has waged war against the Houthis since 2015, trying to restore the internationally backed government, ousted by the rebels the previous year.
While Emirati troops have been killed over the course of the conflict, now in its eight year, the war has not directly affected daily life in the wider UAE, a country with a vast foreign workforce that is also home to Dubai, a glitzy city of skyscrapers and five-star hotels.

The airport fire in Abu Dhabi was described by police as “minor” and took place at an extension of the international airport that is still under construction. For years, the airport home to Etihad Airways has been building its new Midfield Terminal, but it was not clear if that was where the fire took place.



Etihad Airways said “precautionary measures resulted in a short disruption for a small number of flights” and that airport operations have returned to normal. Abu Dhabi Airports did not immediately respond to a request for comment.

The other blast struck three petroleum transport tankers near a complex for the Abu Dhabi National Oil Co. in the Musaffah industrial area. The company describes it as a pipeline and terminal facility located some 22 kilometers (13 miles) from the center of the city of Abu Dhabi, where 36 storage tanks also supply transport trucks carrying fuel.

It is also a short distance from Al-Dhafra Air Base, a military installation that hosts U.S. and French forces. U.S. Air Force Brig. Gen. Andrew Clark, the Al-Dhafra Air Base commander for American forces, said in a statement to The Associated Press that “no incidents” affected the base amid the attack. “U.S. forces are ready and available to assist and support their Emirati partners if requested,” he said. The location of the ADNOC facility where the tankers caught fire is approximately 1,800 kilometers (1,100 miles) northeast of Saada, the Houthis’ stronghold in Yemen.

The incident comes as South Korea’s President Moon Jae-in is visiting the UAE. During a meeting with Emirati Prime Minister and Dubai ruler Sheikh Mohammed bin Rashid Al Maktoum on Sunday, the two countries reportedly reached a preliminary deal valued at some $3.5 billion sell mid-range South Korean surface-to-air missiles to the UAE.

At an event attended by the South Korean president earlier in the day, Emirati Energy Minister Suhail al-Mazrouei declined to comment on the explosion at ADNOC’s facility, telling the AP only that police would provide updates on their investigation.

The Houthis have used bomb-laden drones to launch crude and imprecise attacks aimed at Saudi Arabia and the UAE. The group has also launched missiles at Saudi airports, oil facilities and pipelines, and used booby-trapped boats for attacks in key shipping routes. Earlier this month, the Houthis seized an Emirati-flagged ship in the Red Sea, a crucial route for international trade and energy shipments. Though there have been civilian deaths in Saudi Arabia from Houthi attacks, there had been no deaths previously reported in the UAE. The overwhelming number of civilian deaths in the conflict have been in Yemen. The war has killed 130,000 people in Yemen — both civilians and fighters — and has exacerbated hunger and famine across the impoverished country.

Torbjorn Soltvedt, an analyst at the risk intelligence company Verisk Maplecroft, noted that while the Houthis have claimed responsibility for an attack on the UAE, Iraqi-based militias have also threatened the UAE in response to alleged Emirati interference in Iraqi politics.

He said the attack highlights the missile and drone threat faced by the UAE and the region’s other main oil producers. He said unless Gulf Arab states find a solution to diffuse wider regional tensions “they will remain vulnerable to attacks.”

EDITOR’S COMMENT: Not a big surprise. Perhaps even expected. The main thing is that next time the target might be a densely populated area with a big number of international victims or a national landmark like Burj Khalifa – both in Abu Dhabi or Dubai. On the other hand, the estimated range of 800km is not enough for Yemeni missiles to reach UAE but since all missile-arsenal is made in Iran there will be no surprise if a more powerful cruise missile is used. UAE urgently needs something like Iron Drone or Scorpius or similar to avoid unpleasant surprises shortly (although the Israelis are reluctant to sell due to the recent rapprochement with Iran).

Death by drone: the robot killers changing the face of modern-day warfare

Source: https://www.thetimes.co.uk/article/death-by-drone-the-robot-killers-changing-the-face-of-modern-day-warfare-d2l7qfszm

Jan 19 – Bomb-toting robotic drones are now winning wars in conflicts around the world. The Iranian-built armed drones used in the strike by Houthi rebels in Yemen against oil tankers in the United Arab Emirates this week demonstrated once again that these weapon systems have the reach and firepower to have a tactical and strategic impact.

Drones with a range of weapons attached have been playing an increasingly deadly role in the eight-year-old conflict in eastern Ukraine while the world waits to see if President Putin will order his army across the border.

●▶ Read the full article at the source’s URL.

Houthi terror attack: what drones do the terrorists have?

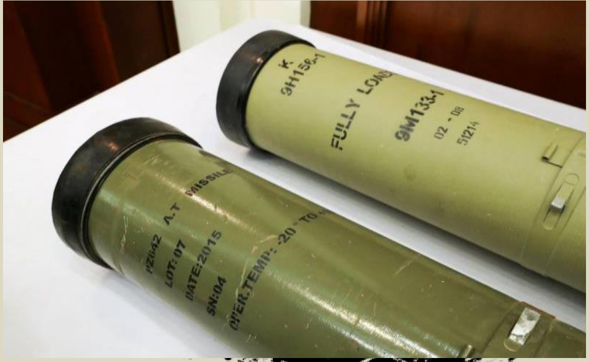
Source: https://www.thenationalnews.com/uae/2022/01/18/houthi-terror-attack-what-drones-do-the-terrorists-have/

Jan 18 – After Monday’s terrorist attack against the UAE, which killed three people and wounded six, international attention is once again focused on low-cost drones: how to stop them, and how to prevent their acquisition by terror groups.

This follows the UAE's announcement that drones were a suspected method behind the attack, but an investigation is ongoing.

Explosive drones, or the “loitering munitions” suspected in this case, have become a challenge to advanced militaries around the world.

But what exactly are these weapons, frequently used by the Houthis and other Iran-backed groups to attack Saudi Arabia and Iraq?



Two anti-tank guided missiles (ATGM). The one on the right is a Russian-made Kornet, and on the left is an Iranian imitation. Markings show they were built in 2015 indicating they were smuggled to Yemen after the UN arms embargo.

Iranian drones

Iran has proliferated unmanned aircraft originally designed for target practice in the 1980s. They typically have a rear-mounted “pusher propeller" system and are constructed from cheap material, sometimes including wooden components.

As cameras evolved, drones such as Iran's Ababil were used for reconnaissance, but in recent years the flimsy looking planes have been rigged with bombs and are sometimes referred to as "Kamikaze drones".

Notoriously, they were used in an attack that shocked the world at Abqaiq in Saudi Arabia in September 2019, when critical oil infrastructure was destroyed.

Drones such as the Houthi Qasef-2K and Sammad 3, propeller-driven aircraft, are slow moving but have a long range.

They have high endurance petrol engines, often made from strong, lightweight material such as titanium and carbon fibre, to reduce weight. The Houthis also have a small cruise missile fitted with turbojet engines, copied from European designs.

Many of these captured and shot down drones, including the Quds-1 missile, were found to have components made in Iran, according to a January 2020 UN Panel of Experts report.

And because of their slow speed, small size, low and unpredictable flight path, they are difficult to detect for ground-based radar systems.

If you have heard the phrase "flying under the radar" – a dangerous job for any pilot – this is roughly the concept used for attack drones, except the risk to a human pilot is removed.

Much of the technology transfer for these aircraft has been sent to Iran through front companies such as Tehran Hobby Ltd, which has illegally obtained engine components from foreign civilian companies.

Indeed, the Qasef drone and similar variants, frequently used to attack Saudi Arabia, is based on the Iranian Ababil drone and built from foreign parts used on commercial drones, plus parts that have been reverse engineered.

These unmanned aircraft are sometimes referred to as "loitering munitions" because they can fly on an unpredictable pattern for long periods and sometimes change course, unlike most missiles that fly on a fixed course.

The concept is often thought of as low tech – and the Iranian designs and Houthi variants often are.

But loitering munitions – as opposed to Iran's target drones such as the Ababil – were first developed by the US in the 1980s.

The most recent variants, such as the Israeli Harop, are far deadlier than Houthi drones, with much more sophisticated guidance systems and autonomous capability.

By contrast, Iran-designed drones should be easy to intercept, but it has proven challenging because modern air defences are designed to shoot down missiles, including ballistic missiles that travel on a predictable arc high in the atmosphere, or enemy aircraft, which have a large radar signature.

These air defense systems are a legacy of the Cold War when many existing systems were developed, including the US Patriot system and the Russian S-300 family of systems.

Russia and America simply did not expect drones to be used in this way — low level kamikazes that fly under the radar horizon—and therefore did not design air defences accordingly.

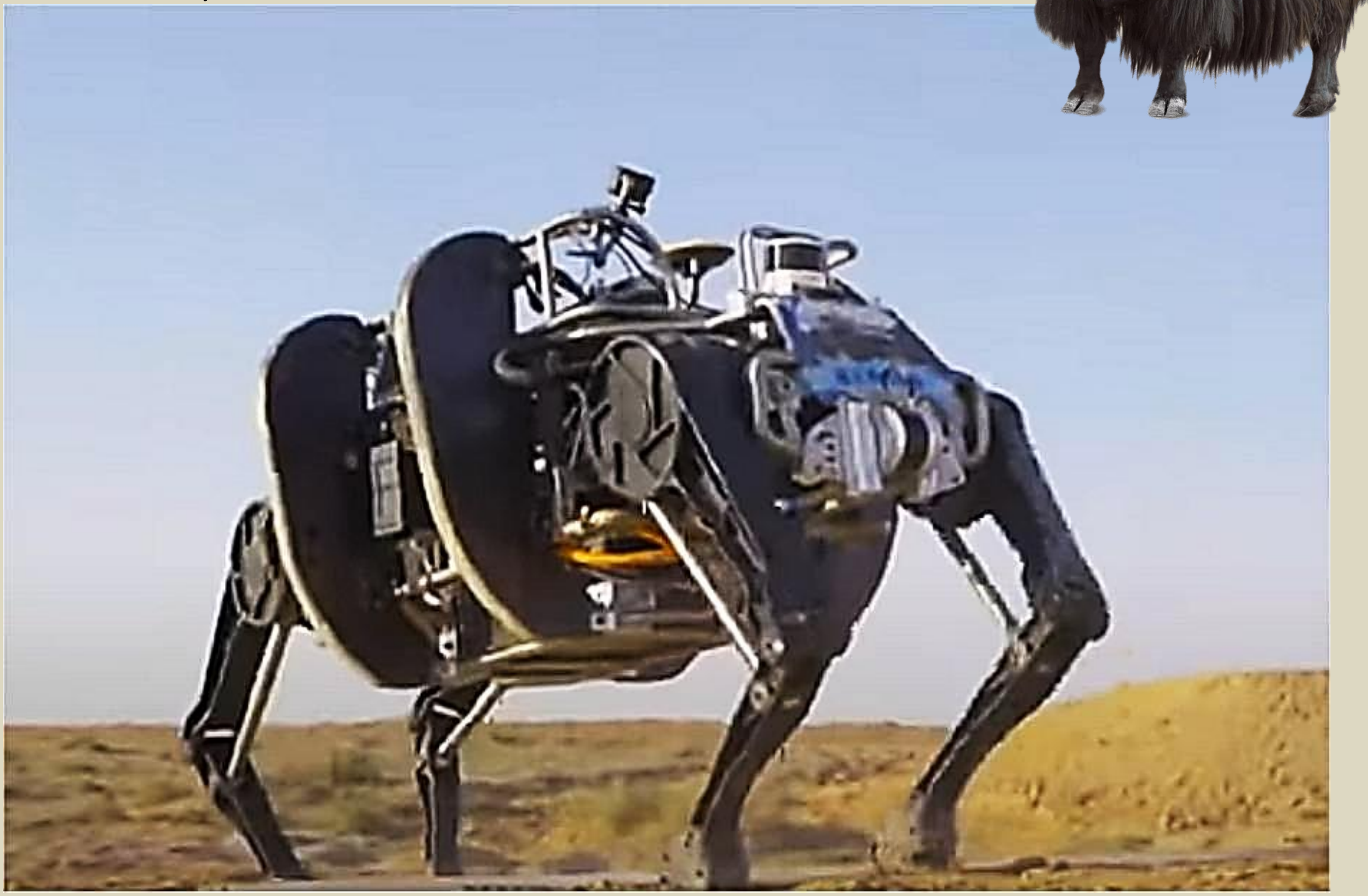
This problem is quickly being solved; the US Patriot missile system PAC-3 variant is designed to shoot down drones with 360-degree radar coverage configured to detect the small objects.

Israel's Iron Dome, which has powerful AI-assisted targeting computers, has proven similarly capable against drones, and the US is now developing a similar system, while Russia's new S-500 system is also designed to take down drones.

Next Robotic Superpower?

Source: https://i-hls.com/archives/112717

Jan 20 – China has developed the world's largest electric-powered quadruped bionic robot, which is expected to join logistics delivery and reconnaissance missions in complex environments that have proven too challenging for human soldiers, including remote border regions and highly risky combat zones, analysts said.



In December, China announced that it would work to become a leading global player in robotics by 2025 under a five-year plan.

The robot (dubbed the "mechanical yak") can carry up to 160 kilograms, and despite its large size, it can run at up to 10 kilometers an hour, CCTV reported. It is equipped with sensors to be aware of the surrounding terrain and environment, and it has displayed a very strong adaptative ability to various types of terrains including steps, trenches and cliffs, not to mention muddy roads, grasslands, deserts and snow fields, the report said.

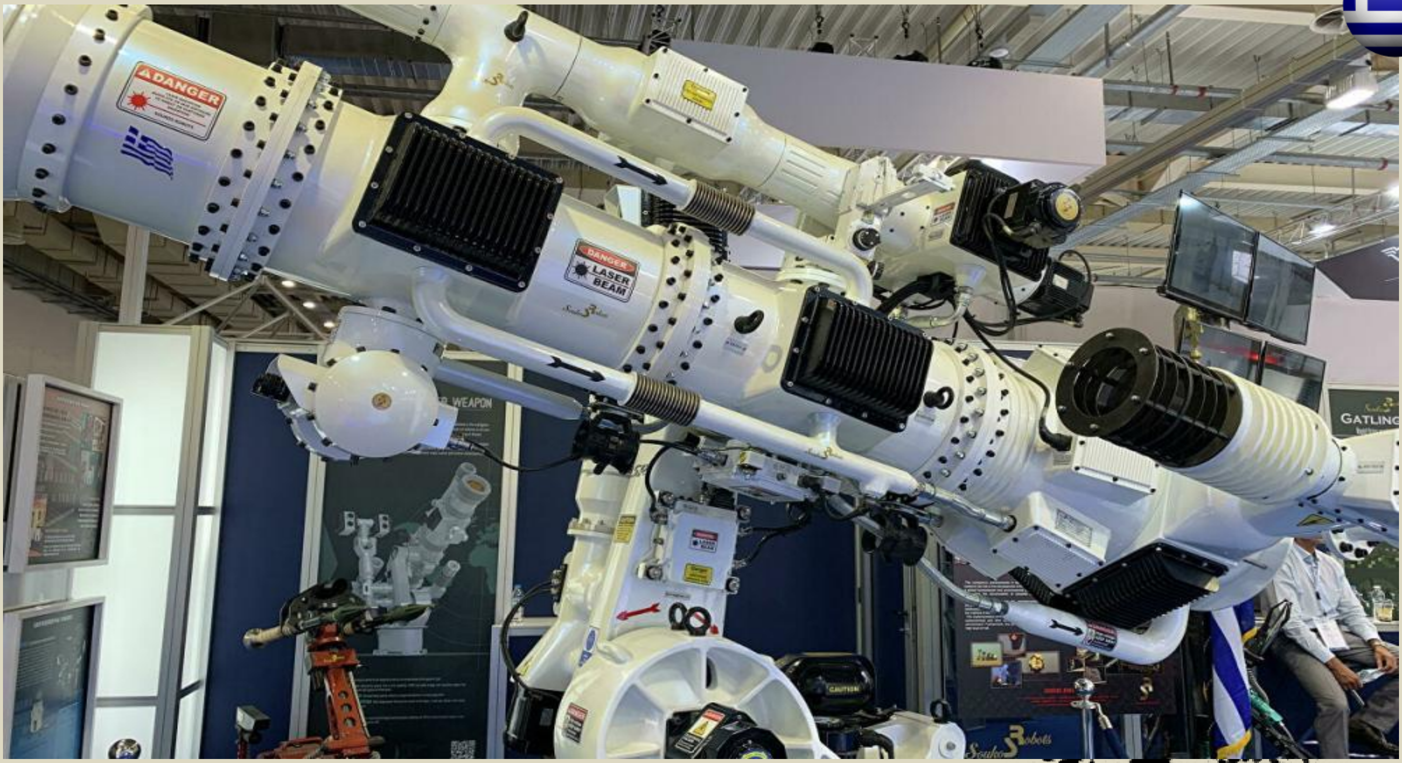
The robot can be deployed to deliver supplies including munitions and food in environments like plateaus, mountains, deserts and forests where normal vehicles have difficult time traversing.

Another potential use is close-in reconnaissance, as it can persistently gather battlefield intelligence and monitor target movements even in complex environments that have proven to be too challenging for human soldiers.

The robot is a very good choice for missions in remote border regions where constant monitoring is needed but conditions do not favor a constant human presence, for example, in high altitude plateaus, icy regions and dense forests, a Chinese military expert who requested anonymity told globaltimes.cn.

Last year, Chinese tech giant Xiaomi had unveiled the "**CyberDog**," a bionic quadruped robot with a high-precision environmental sensing system and 11 high-precision sensors distributed throughout its body. Other Chinese tech companies may have also developed quadruped bionic robots for various applications.

Is this the perfect anti-drone/anti-missile system?



High Energy Laser Weapon by Sukos Robots (Greece)

EMERGENCY RESPONSE

Domestic Preparedness in a Post-COVID-19 World

By Nathan DiPillo

Traditional definitions of domestic preparedness have been influenced by the Cold War and international terrorism. As the 20-year milestone of the 9/11 attack on the United States passed, domestic terrorism also has made its mark on the interpretation of domestic preparedness. It is time for a fresh look, considering pandemics, local human-caused and natural catastrophes, reoccurring threats (like wildfires, earthquakes, and cyberattacks), and crumbling domestic infrastructure. The landscape of emergency response actions and readiness of public and private agencies in a globally interconnected world has left a deep scar on domestic preparedness and how risk is evaluated both nationally and internationally.

Nathan DiPillo currently serves with the California Office of Emergency Services as a Critical Infrastructure Analyst in the State Threat Assessment Center. Prior to state service, he functioned as a Critical Infrastructure Specialist with the Department of Homeland Security and has 25+ years in the emergency management and security industry. In addition, he served as a non-commission officer (E7) with the California State Military Department, Army National Guard with the 223 rd Training Command. He continues to champion the public and private partnerships. He received a Master of Emergency Management/Homeland Security MSEMHS focused on Domestic Security Management and Leadership from National University.

Security Lessons Learned – Part 1, Boston Marathon Bombings

By Daniel Rector

Source: https://www.domesticpreparedness.com/preparedness/security-lessons-learned-part-1-boston-marathon-bombings/

Acts of terrorism continue to affect communities worldwide. As the public tries to retain a semblance of everyday life by attending outdoor events, emergency planners must adapt to new intelligence and learn from past attacks. A review of the 2013 Boston Marathon bombings identifies the event security plans' strengths and shortcomings. Other event planners and public safety officials can use this review and recommendations to plan for large public gatherings within their jurisdictions.

The Boston Marathon typically takes place each spring on Patriot's Day. The Boston Marathon is unique as the 26.2-mile course is run in a straight line and travels through eight separate cities and towns. The race starts in Hopkinton then moves through Ashland, Framingham, Natick, Wellesley, Newton, and Brookline, before finishing in Boston. In comparison, many other marathons are run entirely in a single town or city. The marathon's route dramatically increases the complexity of safety and security for race organizers and public safety agencies.

The 117th running of the race was on 15 April 2013. There were 27,000 registered runners and approximately 500,000 spectators. The race began at 9:00 a.m. with several waves of runners. By the afternoon, all the elite runners had finished, but thousands of spectators were still lining the course cheering on the remaining runners. At 2:49 p.m., the first homemade bomb exploded near the finish line, followed by a second bomb approximately 13 seconds later. The blasts injured 264 spectators and killed three.

Security Strengths

The Boston Marathon planning team does a great job each year coordinating among numerous response agencies to conduct planning for the event. This showed in the immediate response that took place in the aftermath of the bombings. To facilitate this coordination, a safety committee is set up each winter and begins meeting in January. This committee includes representatives from all agencies involved in the event at the local, state, and federal levels. At these meetings, agency representatives work together to update their marathon day plans and procedures using lessons learned from previous years, after-action reviews, and current guidance from intelligence agencies regarding threat assessments.

In addition to these planning meetings, agency leaders participate in a tabletop exercise to improve and test aspects of the plan. The marathon response agencies also work together throughout the year on other events such as the 4th of July, parades, and full-scale public

safety training exercises. This intimate familiarity between officials results in a cohesive and robust working relationship among all parties.

Large gatherings pose challenges for emergency management and law enforcement officials – secure and prevent threats while attendees relax and enjoy the event.

On the day of the event, the organizers set up and staffed a Multi-Agency Coordination Center (MACC), which acted as the hub for health and safety operations along the racecourse. Having a single coordination center was necessary due to how many jurisdictions the race passed through. Representatives from over 80 agencies present at the center provided situational awareness of events along the route and effectively coordinated security, safety, and medical response activities. Agencies that worked together to support the security and safety operations needed for the event included:

- Massachusetts State Police
- Local police from all eight towns along the route
- Massachusetts Bay Transit Authority (MBTA)
- Transit Police
- Boston Regional Intelligence Center
- Boston University Police
- Local fire from all eight towns along the route
- Local ambulance companies providing Emergency Medical Services (EMS) support, including Boston EMS
- Representatives from local hospitals
- The Boston Athletic Association
- The Massachusetts Emergency Management Agency (MEMA)
- The Massachusetts Department of Public Health (MDPH)
- The Massachusetts National Guard (MANG)
- The American Red Cross (ARC)
- The Federal Bureau of Investigation (FBI)
- The Department of Homeland Security (DHS)

Security Weaknesses & Gaps

The Boston Marathon planners have over 100 years of experience organizing the race. Their experience shows in the detailed and thorough security plans put in place for the event each spring. However, even with all the security expertise and due diligence, there was a security weakness present that the terrorist could identify and target.

The weakness they identified was the large crowds who were present along the race route. These crowds were part of the atmosphere, so organizers could not remove them while maintaining the event's allure. To mitigate this, the planners placed law enforcement officials along the route and among the spectators. However, there was no policy in place regarding bags, packages, and the free flow of pedestrian traffic in and out of the spectating areas.

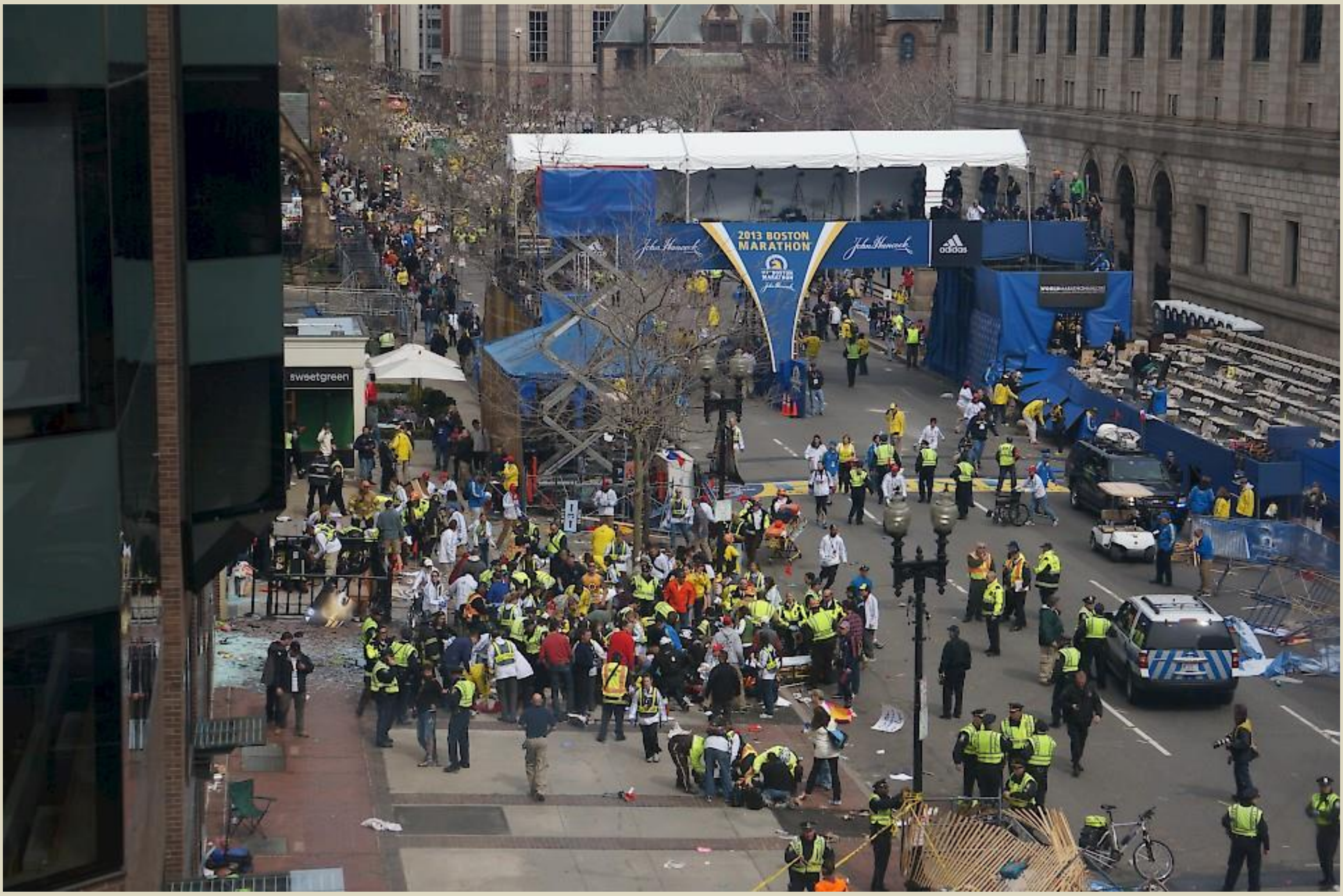
To further complicate security issues, a Boston Red Sox game is played on Patriot's Day each year, which coincides with the marathon. It is a tradition following the game for spectators to walk down the street to the racecourse and join the cheering crowds. This influx of people added security concerns for law enforcement officials, especially those intoxicated from the baseball game.

While the Boston Marathon Security policy was comprehensive, several areas needed improvement. For example, there were too many coordination and operations centers activated. Although the event planners set up the MACC as the central communications hub, each agency also used its own operations center to oversee operations. The event had too many coordination and operation centers active without a correctly identified hierarchy in place.

In addition, though many National Guard service members were present to assist during the race, they acted in more of a crowd control function with little show of force and negligible prevention value. Once the bombings happened, there was no plan to arm them, even though officials often paired them with law enforcement personnel. The marathon team neglected to utilize the National Guard to its full capacity, which resulted in specially trained soldiers essentially acting as crossing guards.

The runners' bags also became a security issue as race officials did not screen them before the race. During many large endurance events, organizers place athletes' personal items in secured bags labeled with their race numbers. These bags are then transported to the finish line for the athletes to pick up after completing the race. Two items many put in these bags are a cell phone and identification card. During the incident, these bags were secured by law enforcement then checked for explosives by Explosive Ordinance Disposal (EOD) teams. However, organizers were not able to return the bags to the runners until the next day. The lack of identification, funds of any kind, and communication added stress on the runners and their families, who were undoubtedly awaiting news of their loved ones.

Lastly, organizers did not have the means in place to notify spectators in real time as the attacks occurred to facilitate proper evacuation and ensure no misunderstanding of information. Federal agencies were not correctly and thoroughly sharing intelligence information with local officials. Congress identified this as a problem linked to the Boston Marathon bombings in the Congressional Report titled *Road to Boston: Counterterrorism Challenges and Lessons from the Marathon Bombings*.



Lessons Learned & Recommended Security Policy for Large Public Gatherings

In the months and years following the events at the 2013 Boston Marathon's finish line, the responding agencies learned many lessons. Although many of the changes recommended in after-action reviews and official reports focus on medical and law enforcement response, there are a few that pertain to security to prevent an attack. The Massachusetts Emergency Management Agency highlighted that their focus has shifted to prioritizing prevention and protection. Since 2013, the number of plainclothes law enforcement officers trained in suspicious behavior detection has dramatically increased. To help facilitate the observation of event attendees, spectators may now be required to pass through "choke" points where these trained professionals can observe them. Supplementing physical security are additional cameras along the race route to monitor the crowds for anything suspicious.

Large public gatherings pose a complicated challenge for emergency management and law enforcement officials. They need to balance security and prevention with the public's desire to relax and enjoy the event. There have been several gaps in the security plans and policies used for large public gatherings in the past. By analyzing past events, these gaps can be identified, and solutions created.

In addition to the items in the Boston Marathon security policies, it would be prudent to add some additional preparedness and prevention measures to increase event security. Event planners and emergency personnel can apply these security policy recommendations to public gatherings of all types:

- Do not schedule multiple major events on the same day – for example, the Red Sox game and the Boston Marathon – due to the influx of spectators. This results in rowdy crowds and adds unnecessary complications to the incident. Having two large events going on simultaneously in such proximity stresses city and state resources. It would be better to host the events on consecutive days.

- Athletes' bags and personal belongings need to be considered as part of the security plan. Runners need to be quickly reunited with their identification cards, communication devices, and monetary funds. By acquiring these items, they can secure lodging if required, procure food and clothing items, communicate with loved ones, and leave the area in a timely manner once approved to do by law enforcement officials.
- EOD should screen all runners' bags as they are loaded into secured buses. Once cleared, the bags need to be kept under guard until they are distributed at the finish line. This practice serves two purposes. First, officials now know these bags are safe and not a threat. Second, if an incident occurs, the bags can be moved under guard to a secondary location until the runners can retrieve them. Although this method requires increased human resources upfront, it would allow a more streamlined collection process. Additionally, it enables the runners to become self-sufficient and more quickly exit the immediate area, thus reducing the strain on local responders and assistance organizations.
- Limit the bags, such as backpacks and purses, that spectators can carry along the course. Organizers should implement rules such as only allowing clear bags along the route. These measures are already in place at many venues worldwide.
- Public address systems must be part of event plans, and equipment should be placed throughout the course or venue. Preplanned emergency messages should be included in the event planning, and officials need to have the ability to record additional messages as required in real-time.
- National Guard soldiers and Airmen acting as law enforcement should be armed in the same way as their law enforcement counterparts. Although there is a hesitancy to arm the National Guard due to public perception, a lack of doing so limits their ability to impose a security presence.
- Federal law enforcement and intelligence agencies need to continue improving their information sharing among themselves and their state and local counterparts. Local officials need to be aware of any potential threats within their jurisdictions as they can add valuable community input to the case and assist with investigations.
- One of the largest sources of prevention can be the public themselves. An aware populous can identify suspicious behavior and alert law enforcement. At the moment of an attack, alert bystanders could also step in and prevent the violence. Public safety professionals still need to redouble their efforts to prevent attacks before an event and to mitigate threats before the public gains knowledge of them.

The attack on the Boston Marathon highlighted the effectiveness of law enforcement and emergency response organizations within the United States. By studying the event, officials can identify opportunities for improvement in planning and tactics. The goal going forward should be to continually improve processes and educate the public on ways to increase their resilience and awareness. It is the responsibility of professionals in these fields to ensure both citizens and response organizations do not become complacent.

Security Lessons Learned – Part 2, Las Vegas Shootings

By Daniel Rector

Source: https://www.domesticpreparedness.com/preparedness/security-lessons-learned-part-2-las-vegas-shootings/

Many of the previous stories and after-action reviews conducted for the 2017 Las Vegas shootings have focused on organizers' and public safety officials' responses in the aftermath of the attack. In contrast, this article focuses on the events' security strengths and weaknesses and then offers recommendations for other event planners and public safety officials to improve their plans for future events.

Each year, thousands of tourists travel to Las Vegas to unwind and relax at the city's various attractions. Las Vegas is home to many hotels and casinos, as well as indoor and outdoor entertainment venues. These facilities host several events each year, including NASCAR races, concerts, and a large New Years' Eve celebration. Local law enforcement, firefighters, and emergency medical providers respond to thousands of calls for assistance from visitors to the city each year.

On 1 October 2017, at approximately 10:05 p.m., a gunman opened fire on concertgoers initiating "the deadliest mass shooting in modern U.S. history." The shooter had reserved a room on the 32nd floor of the Mandalay Bay Hotel specifically because it overlooked the Village Concert Venue, an outdoor event space located in the city where 22,000 people were attending a concert. After more than 10 minutes of gunfire directed at the crowd, 58 people were killed and 546 injured.

Security Strengths

The Las Vegas response agency's security and preparedness policies are in-depth and well-practiced. Regular training exercises and coordination events occur between response agencies throughout the year and focus on various threats and public safety topics. The Las Vegas Metropolitan Police Department (LVMPD) utilized several grants and other forms of federal funding to prepare for various mass casualty events in the years before the attack.

The LVMPD has a mass casualty training section dedicated to teaching officers and other responders to effectively deal with a mass casualty event. The training section used experiences and data from previous attacks around the world to create realistic training scenarios. LVMPD also has a policy to send police captains to local hospitals immediately after an attack to augment security and assist them with the hardening their facilities in anticipation of follow-on attacks. Due to this, responders were well prepared for an active shooter scenario.

Several organizations assisted with the city's event planning, and many were involved in responding to the attack. With the large number of Las Vegas events each year, countless officials know each other well and regularly work together during response missions and training exercises. Agencies involved included:

Event planners and emergency personnel should apply these security policy recommendations to future events that involve public gatherings.

- Mandalay Bay Hotel Security
- Las Vegas Metropolitan Police (LVMPD)
- Henderson Police Department
- Henderson Fire Department
- North Las Vegas Police Department
- Clark County Fire Department
- Live Nation (Event Organizers)
- Contemporary Services Corporation (Event Security)
- Community Ambulance Company
- American Medical Response
- MedicWest Ambulance
- Nevada Highway Patrol
- The North Las Vegas Police & Fire Departments
- Las Vegas Fire & Rescue
- Clark County School District Police Department
- The Boulder City Police Department
- The ATF
- The FBI

Information regarding the organizations involved in the event planning and response was obtained from Smith et al. (2018) and the Federal Emergency Management Agency (2018).

Security Weaknesses & Gaps

Although the emergency response and safety officials within the city have significant experience and skill in planning events, there were some security weaknesses that the shooter was able to identify and exploit to carry out his attack. It appears the shooter chose the location due to the large number of people who would be in attendance. Also, the shooter was able to obtain an elevated position from the nearby hotel to increase his effectiveness and limit law enforcement personnel's ability to interfere. His intent was most likely to kill and injure as many spectators as possible. The fact that the venue did not have enough EMS personnel or transport ambulances onsite to handle a mass casualty event increased his attack's effectiveness.

The most considerable weakness in the city's security was the fact that the shooter was able to bring at least 23 rifles and thousands of rounds of ammunition into his hotel room over several days preceding the event. He was also able to drill holes in his room to install security cameras in the hallway and his door's peephole without alerting hotel staff. In the minutes before the attack, he secured shut both his door and the stairway door with L-brackets. Being able to perform these actions without being noticed by security or staff highlights a severe weakness in the hotels' security measures. The hospitality industry is not required to train and equip its staff to act as intelligence gathering sources. Hotel staff interacted with guests and their belongings multiple times a day but did not identify and report suspicious activity.

Although the preparation for a response to an attack was thorough, mitigation efforts and prevention policies were not as detailed. One concern was that police who were working the concert venue did not have access to their tactical equipment during the event. The officers' gear was in their vehicles, which were parked several blocks away. Officers could have been used as a preventative show of force if they had their tactical gear on them.

Another major security weakness is that of the hospitality and concert industries. Many hotel security professionals believed that there is nothing they could have done to prevent an attack and accepted it as an inevitable possibility. This mindset prevents forward-thinking and preventative actions from being discussed and implemented. Readiness is challenging among the hotel and concert industries due to opinions such as these, which can prevent putting response plans in place or lead to having plans that do not get exercised or are outdated.

The final weakness of the city's security plan is that outdoor venues did not have a way to notify spectators that an emergency was occurring. When the attack began, many people thought it was fireworks. No public service announcement system was in place to broadcast the danger over the venue's network of speakers to advise people to exit.

Lessons Learned & Recommended Security Policy for Large Public Gatherings

Following the events of 1 October 2017, many hotels increased security at elevators, and some even installed X-Ray machines to scan customers' bags as they enter the premises. Many hotels modified "do not disturb" policies to trigger a staff response after the signs have been in place for a predetermined amount of time. For example, if a do not disturb sign was in place for 12 hours, the staff would be required to contact the guest. This policy would ensure that the hotel was in contact with the guest and hopefully act as a deterrent to guests trying to remain hidden.

Any large public gathering introduce challenges for emergency management and law enforcement officials, who need to secure the even and mitigate threats while not detracting from the participants' enjoyment of the event. The following security policy recommendations provide additional preparedness and prevention measures that event planners and emergency personnel can apply to future events that involve public gatherings:

- Events taking place in the open, such as concerts, need plans that include awareness of the high points around the location. Spotters can and should be placed around the perimeter of events if feasible. They can scan the surrounding areas for threats while also observing the crowds.
- Hospitality centers need requirements for checking rooms once "do not disturb" signs have been in place for a specified amount of time. Such policies are now in place at Wynn, Hilton, and Disney hotels.
- Tactical equipment should be made available for police officers to use when they are on patrol at public events. This equipment should include shields, helmets, and additional medical supplies.
- Hospitality and concert industry security professionals who are hired for events should attend mandatory training on prevention and mitigation techniques that they can use to harden their venues. Staff should also participate in behavioral detection training and certification courses to help identify guests who exhibit signs of destructive behavior or malicious intent. Venue operators and event coordinators should seek companies who adhere to these guidelines versus ones that do not.
- The hotel industry should have plans in place to utilize their indoor public service announcement systems during active shooter events.
- While not part of a security plan, high-rise buildings need to look at their windows' weaknesses. Another report or study should look at building code requirements for these buildings to increase the strength of windows to prevent them from being used

as firing positions. Also, current fire codes should be investigated to determine if they are sufficient for mass casualty events.

- Federal, state, and local statues, codes, or laws could be enacted to facilitate efforts to change mindsets of security professionals in the hospitality and concert industries to embrace innovation and prevention.

The public has two choices when it comes to large gatherings and events. They can avoid them, effectively hiding and protecting themselves behind “walls,” or they can continue to enjoy life while increasing their own personal resiliency. Public safety officials, event organizers, and citizens need to continue to revise their security posture in response to new and evolving threats. Security plans must be continuously assessed and updated based on after-action reviews and current threat levels. By working together, the entire community, nation, and the world can move toward more secure outdoor venues and safe entertainment activities.

Daniel Rector, MS, CEM, is a military veteran with 12+ years of experience in homeland security and emergency management operations. He served as a damage controlman in the U.S. Coast Guard and as a survey team chief on a National Guard Weapons of Mass Destruction – Civil Support Team. He currently works for Asfalis Advisors as a business resilience advisor. His career is supported by a Master of Science degree in Emergency Management and current coursework toward a Doctorate of Management with a Homeland Security focus. He has completed multiple courses in CBRN response and detection from the Defense Nuclear Weapons School, Idaho National Laboratory, Dugway Proving Grounds, the U.S. Army CBRN School, and the U.S. Army CCDC Chemical Biological Center, among others. He has completed the FEMA Professional Development Series and the Homeland Security Exercise and Evaluation Program (HSEEP) Course. He is a Certified Emergency Manager (CEM), a licensed HAZMAT echnician, Confined Space Rescue Technician I/II, and EMT-B. He is a recipient of multiple awards for excellence, including being the only National Guard soldier ever named the Distinguished Honor Graduate while simultaneously being nominated by his peers for the Leadership Award at the CBRN Advanced Leaders Course.

Managing a Disaster during the Pandemic
REAL-TIME DATA IS INVALUABLE IN MANAGING CONCURRENT EMERGENCIES
Dataminr

Governor Hochul Announces Completion of More than 600 Counterterrorism Exercises

Source: https://www.hstoday.us/subject-matter-areas/counterterrorism/governor-hochul-announces-completion-of-more-than-600-counterterrorism-exercises/

Dec 31 – New York Governor Kathy Hochul has announced the State Division of Homeland Security and Emergency Services’ (DHSES) Office of Counter Terrorism conducted training exercises at more than 600 locations statewide in 2021. Counterterrorism experts from state and local agencies completed exercises assessing the ability of businesses to recognize and report suspicious activity in nearly every county in the state. More than 4,200

exercises have been conducted across New York since 2016.

"As Governor, I always want to ensure New Yorkers are safe and prepared for any and all risks that threaten our collective security," Governor Hochul said. "These annual exercises are critical to this effort as they not only help ensure businesses statewide know how to spot suspicious activity, but understand their own responsibilities and how to make a report as well."

The Office of Counter Terrorism partnered with more than 360 law enforcement personnel from 76 agencies to conduct the exercises. Teams conducted exercises at a wide range of businesses that offer products or services that could be used in potential terrorist plots. In 2021, teams worked with hardware and building supply stores; hotels and motels; big box retailers; rental vehicle companies; private postal facilities; UAS or drone retailers; agricultural supply stores; grocery stores; beauty and nail supply stores; pool supply stores; self-storage facilities, and gun shops and shows. Teams also assessed 70 critical infrastructure locations that terrorists could exploit or target for an attack. Location examples included malls and shopping centers, colleges and universities, airports, transit hubs, performance venues and other mass-gathering locations.

State Division of Homeland Security and Emergency Services Acting Commissioner Jackie Bray said, "Our Division is committed to helping protect the citizens of New York, as well as the state's critical infrastructure locations, from acts of terrorism. I thank all those involved in these exercises and our partners in law enforcement for helping raise awareness of the key indicators of suspicious activity. I urge businesses and the public to be mindful of their surroundings and to report suspicious activity to the New York State Terrorism Tip Line at 1-866-SAFENYS."

State Police Superintendent Kevin P. Bruen said, "Educating businesses and the public on how to spot suspicious activity and notify law enforcement is a critical part of protecting our communities from the threat of terrorism. We are committed to doing everything necessary to ensure local and state first responders are ready to respond to, and mitigate, any type of emergency situation. Exercises like this help us to better our existing safety protocols and help us prepare to work hand in hand if disaster should strike and ultimately, keeps New Yorkers safe."

In addition to the more than 600 exercises, the Division also partnered with federal, state and local law enforcement agencies in "Operation NY-SECURE" to conduct counterterrorism and incident response details along Amtrak routes and MTA commuter lines. The Operation's goal is to improve coordination and response between the railroad police agencies responsible for each station, and the state and local law enforcement agencies that respond to emergencies at those locations. These visible, proactive details included heightened platform patrols, increased security presence onboard trains, explosive detection canine sweeps and counter-surveillance measures. In 2021, Operation NY-SECURE completed 74 details across the state. Teams conducted 62 single station details across the state, and 12 multi-station exercises at Amtrak and MTA stations along the Empire Line. Since the program's inception in 2018, law enforcement teams have conducted more than 215 details across the state. The details will continue in 2022.

Shipboard Emergencies – 1000 Miles From Nowhere

By Corey Ranslem

Source: https://domprep.com/preparedness/shipboard-emergencies-1000-miles-from-nowhere/

Shipboard emergencies can happen anywhere at any time, and an immediate crew response is critical to a successful outcome. When deployed, crew members of various vessels do not have the same response capabilities or backup as land-based fire and police departments. There are thousands of vessels of all types on the waterways and oceans of the world. Crew members need to be prepared to handle all types of dangers that can threaten their type of vessel – including fires, floods, hazmat incidents, or medical emergencies – regardless of the vessel's location. Because of a ship's changing and often remote location, shipboard emergencies require a quick response that must usually be handled exclusively by crew members.

Crew members of cargo vessels, large yachts, and cruise ships are required to complete a number of safety-related training es based on their own responsibilities on the vessel. Crew members, regardless of vessel type, are required to attend STCW (Standards of Training, Certification, and Watchkeeping) training sessions and refresher training. The International Convention on STCW sets the training standards (through the International Maritime Organization – IMO) for crew members worldwide.

The convention standards were originally adopted in 1978, put into force in 1984, and updated in 1995. Before the major changes incorporated in 1995, fire or flood problems on vessels could rapidly escalate into major disasters, and even small fires could spread quickly through large cargo and cruise ships – frequently causing major damage and the loss of numerous lives.

The newest revision of the convention standards (Manila Amendments) went into effect in January 2012. The new standards expand into areas beyond shipboard safety per se and include work and rest restrictions, security-related training, changes to refresher training and medical training, and new blood alcohol limits. The basic training required for all vessels is typically the same, but there are a number of additional training requirements depending on such variables as the type of vessel, company procedures, and/or union rules and requirements.

Cruise Line & Shore-Side Responses

In many respects, cruise lines are much like floating cities, and are "governed" in accordance with a plethora of crew certification and training requirements – including a number of additional safety and security trainings for cruise-ship personnel. Some of these requirements are mandated exclusively by the U.S. government, while a number of others are designated by foreign governments and the IMO. As a general rule, cruise lines do more non-required training and have more cutting-edge capabilities "than most other types of vessels," according to Ted Morley, the Chief Operations Officer at Maritime Professional Training (based in Fort Lauderdale, Florida) and a Master Unlimited Mariner himself. The ship's personnel "often receive advanced training in medical emergencies, and most ships carry a doctor and a number of nurses. Moreover, the ship's security teams receive advanced training from the Coast Guard, the FBI [Federal Bureau of Investigation], the CBP [U.S. Customs and Border Patrol], local law enforcement, and security specialists. Moreover, the ships carry some of the most advanced medical equipment – and firefighting equipment as well," Morley continued. Finally, he said, "Cruise lines are moving toward mirroring their response operations to an ICS-related model similar to [those used by] shore-side emergency response agencies."

The adaptation of the federally mandated Incident Command Systems (ICS) into shipboard operations also helps facilitate a coordinated shore-side response if an incident on a cruise ship occurs while the ship is in port. "Shore-side response agencies need help from shipboard personnel when they respond to emergencies onboard ship," Morley pointed out, "because the [ship's] personnel know their ship better than the shore-side response agency [does]." Local agencies and shipboard response personnel should coordinate their training to deal more effectively with dangerous emergencies.

Shipboard training requirements have also changed since the major overhaul of the STCW in 1995, according to Amy Beavers, the Managing Director and Vice President of Regulatory Compliance at Maritime Professional Training. "There is more accountability with the training since the changes in 1995," she said. Crew members must now demonstrate the basic skills needed to deal with dangerous incidents. "They had room time and exams before 1995. Now they are also required to demonstrate [that] they understand the concepts. For example, they actually have to don the firefighting equipment in a simulator and fight a fire; they have to don their life jackets and get into the life raft in the [training] pool, which was not required before 1995."

"There are a number of skills they must now demonstrate, whereas before they just sat through lectures," she added. "That was the major change with STCW of 1995 and also a major turning point in ship design and construction."

All evidence suggests that, through improved training requirements and improved ship design and construction standards, the number of fatal ship incidents and major disasters worldwide has decreased significantly since 1995. In short, partially because of better construction, but also because of improved training, modern cargo and cruise ships are more capable than ever before of preventing catastrophic damage and/or a major loss of life due to fires and floods.

An encouraging side effect also worth mentioning is that the number of life-threatening medical emergencies involving crew members has also decreased – on both cargo and cruise ships – partly because of the advanced level of training now available, and required, but also because of the more rigorous screening of potential crew members. "Crew members on cargo vessels receive much better medical screening to determine their level of fitness for sea duty," Beavers commented. By improving the screening methods, and being much more aware of possible medical problems, there are fewer medical issues while a ship is at sea.

Despite several recent groundings and other disasters, shipboard emergencies are not as common today as they were in the early days of maritime operations. Today's ships are better designed, and are built to survive major at-sea disasters that in years past might well have been fatal to all hands and to the ship itself. However, accidents and disasters can still happen. Being able to deal with an emergency situation before it escalates out of control requires that crew members be ready to respond to all potential hazards both quickly and effectively. As equipment and personnel change, all crew members must be trained to ensure that they not only possess the right equipment but also know how to use it. When there is no backup, and/or if the backup response is days away, a well-trained crew that responds quickly is the best and often only way to mitigate the damage and minimize the loss of life.

Corey D. Ranslem, chief executive officer of Secure Waters Security Group Inc. – a maritime-security and consulting firm heavily involved in maritime training, maritime security, and a broad spectrum of other security programs in the maritime field – is the former regional manager of Federal Government Operations for Smiths Detection. He has received numerous awards and citations from the U.S. Coast Guard and other agencies and organizations active in the field of maritime security. He holds a Bachelor's Degree in Communication and Political Science from the University of Northern Iowa and an MBA in International Business from Georgetown University; he has almost 18 years of experience in maritime law enforcement and security.

LIFEBOATS
IT CAN'T HURT TO BE PREPARED.
CA El Niño
Lisa ©2015 10-24 Dist by Wash.Post Writers Group