2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

May 2019

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

DIRTY R-NEWS

Secretive Patrick Air Force Base Lab Watches for Nuclear Explosions Worldwide

Source: https://eu.floridatoday.com/story/news/2019/04/11/secretive-lab-patrick-afb-watches-nuclear-explosions-worldwide-protecting-u-s/3309294002/

The $158 million AFTAC campus at Patrick Air Force Base.

Apr 28 — Inside a secretive Patrick Air Force Base laboratory, Airman 1st Class Cynthia A. Schroll prepares batches of complex chemicals alongside futuristic-looking fume hoods and a white cabinet labeled "Acid" in large red letters.

Wearing blue rubber gloves and a white lab coat, Schroll is a rare breed in the U.S. military: She earned a doctorate in analytical chemistry from the University of Cincinnati. She has written two books. She has a patent in her name.

And Schroll conducts classified lab work at the Air Force Technical Applications Center. The organization detects and analyzes nuclear explosions detonated by foreign countries, utilizing a sprawling network of more than 3,600 sensors deployed around the globe.

"We've got them in space. We've got them at sea. We've got them in the air. We've got them on land on all seven continents, to include Antarctica. And we even work in the cyber domain," said Col. Chad Hartman, who commands AFTAC.

AFTAC is tasked with monitoring nuclear treaty compliance and any "nuclear surprises" from rogue nations or terrorists. Its scientists assessed Iran's nuclear program in 2015 and identified both of North Korea's underground nuclear tests in 2016 — producing reports that made their way to the Oval Office.

The agency also monitored the 1986 Chernobyl nuclear power plant accident in the former Soviet Union; verified North Korea's first nuclear test in 2006; and scrutinized Japan's 2011 Fukushima Daiichi nuclear power plant disaster.

"We're the only government organization whose primary mission is to do that. To be able to go after that problem set requires an incredible amount of equipment, an incredible amount of capability — that's on a global scale," Hartman said.

"And, some of the best and brightest this nation has to offer," he said.

The AFTAC logo is a lithium atom surrounded by the slogan, "In God We Trust: All Others We Monitor."

Classified Laboratory Activities

March marked the five-year anniversary of AFTAC's $158 million campus at Patrick AFB — which was the largest construction project in the Air Force at the time. Officials gave FLORIDA TODAY a rare glimpse inside AFTAC's surreptitious surveillance laboratory.

The tour was the most in-depth media peek since the facility's March 2014 ribbon-cutting ceremony, said Susan Romano, AFTAC's public affairs chief.

Scenes inside AFTAC's state-of-the-art, 38,000-square-foot Ciambrone Radiochemistry Lab resemble settings from a Stanley Kubrick sci-fi movie.

Rotating red lights in hallway ceilings warn that persons without security clearances are present. Technicians wearing white lab coats perform atom-by-atom analyses. Visitors use shoe-cleaning machines and step on white "tacky mats" before entering rooms, ensuring their soles are free of debris.

Charts of the nuclides — resembling periodic tables of elements seen in high school chemistry classrooms — are posted on various walls.

"We use them on a daily basis," said Brett Mapston, flight chief of nuclear measurements.

Aerial filter samples collected by WC-135 Constant Phoenix "nuke sniffer" aircraft enter the lab through an exterior door marked "Caution: Radioactive Materials." Encased in white plastic sleeves marked with bar codes, these samples are routed to various rooms for an array of scientific procedures.

In on room, a futuristic chrome-metal contraption (a thermal ionization mass spectrometer) converts samples into vapor and accelerates them, isolating isotopes of uranium and plutonium. Scientists use these nuclear forensics to collect post-explosion warhead information.

"We can tell you what type it was and what grade it was," said Wesley Schuler, flight chief for mass spectrometry.

Before leaving the Ciambrone Radiochemistry Lab, visitors step inside a Canberra radiation contamination detector for a full body scan. A robotic-sounding woman's voice counts down from 15, then announces, "Clean," when the scan is complete.

'MacGyvers' Repair Aging Sensors

At the AFTAC component repair facility, or CRF, airmen tinker with seismometers inside a large shop equipped with work benches, toolboxes, computers, coils and a cornucopia of electronics and wiring.

Romano nicknames these mechanically adept airmen "MacGyvers" after television's secret agent Angus MacGyver. Oxford Dictionaries defines MacGyver as an informal verb: "make or repair (an object) in an improvised or inventive way, making use of whatever items are at hand."

AFTAC's 709th Technical Maintenance Squadron refurbishes the network's seismometers, both in the workshop and in the field. If these devices detect an underground disturbance, they transmit data to the Space Coast for analysis.

Many were designed during the 1950s and '60s, so replacement parts are scarce or must be custom-built, said Douglas Dale, CRF flight chief.

On top of that, Dale cited Moore's Law, which states the number of transistors on a microchip roughly doubles every two years. Seismometers must fit within narrow bore holes, so airmen labor to keep computerized components up to date.

Master Sgt. Joseph King estimated AFTAC airmen can fabricate about 200 different components. In 2011-12, he trekked to frozen Antarctica to maintain diesel generators, heaters and solar panels at two unmanned sensor sites.

King has also helped install 10 seismometers at AFTAC's array in Morocco, at the edge of the Sahara

Desert in North Africa.

"The young men and women who work in that shop have global responsibilities for maintaining that equipment, all over the world. They go to some of the most remote places on the planet," said Jim Whidden, AFTAC director of staff.

"They are remote because it's important for the sites that we select to be seismically quiet, so that the data has as little background noise as humanly possible. So that what we see is literally just the earth shaking, and we don't have cultural noise. There are no highways or construction activities or railroads nearby," Whidden said.

"And these sites are literally out in the middle of nowhere," he said.

Recruiting and Retaining Scientists

The original AFTAC building at Patrick AFB dated to the 1950s. This outdated, asbestos-ridden structure sat closer to State Road A1A and was deemed vulnerable to attack after the Sept. 11, 2001, terror attacks. Much of the iconic structure — which was fronted by a row of display rockets during the Space Race — fell to the wrecking ball by spring 2016.

Today, Chief Master Sgt. Michael Joseph is AFTAC's command chief. He and Hartman agree on their mission's key challenge amid the digital job market: Recruiting and retaining talent.

"We're competing against the Googles and the Apples of the world. And while we can never come close to offering the financial incentives they will, what we do offer is an incredible purpose. A higher purpose, to be able to come in and attack problems that are incredibly meaningful," Hartman said.

"We have this incredible array of hardware all over the world. But at the end of the day, we're kind of a software company," he said.

What's more, Romano said retired Air Force personnel who return to work at AFTAC as civilians, like Schuler and Dale, provide institutional mission knowledge that newcomers lack. North Korea's twin nuclear tests in 2016 made for the organization's "busiest ops tempo" in the previous 20 years.

"The world is only getting more complex. It's going faster. It's getting more complex and more consequential. So, the challenges they're going to face 10 to 20 years from now are probably going to dwarf some of the things we're dealing with today," Hartman said.

"So, we're trying to make sure we posture ahead, and stay ahead of the curve and equip them for success."

Nuclear weapons might save the world from an asteroid strike – but we need to change the law first

By James A. Green

Source: http://www.homelandsecuritynewswire.com/dr20190424-nuclear-weapons-might-save-the-world-from-an-asteroid-strike-but-we-need-to-change-the-law-first

Apr 24 – The schlocky 1998 Bruce Willis movie Armageddon was the highest grossing film of that year. The blockbuster saw a master oil driller (Willis) and an unlikely crew of misfits place a nuclear bomb inside a giant asteroid heading for Earth, blow it up – and save humanity. Armageddon isn't exactly a documentary: it's packed full of sci-fi nonsense. But, 20 years on, its basic plot – of using a nuclear explosion to avert a cataclysmic asteroid collision – doesn't seem quite as silly as it did at the time.

Major asteroid impact is a low-probability, but high-consequence risk to life on Earth. Large "Near Earth Objects" (NEOs) don't hit Earth often, but it only takes one (just ask the dinosaurs – oh, wait, you can't). Of course, low

probability risks are easily dismissed, however high the consequences of them manifesting might be – and until recently the countries of the world largely viewed the threat posed by NEOs as something best left to Hollywood.

But that's all changed, following the impact (in more ways than one) of the meteoroid that hit Chelyabinsk in Russia in 2013, which injured more than 1,000 people. Suddenly, the NEO threat became "real", and major players – the US, Russia and the EU – all started pumping money into NEO preparedness, and developing formal strategies for response (see, for example, the production of the US's first ever National Near-Earth Object Preparedness Strategy in December 2016).

At the UN, we've recently witnessed the creation of an embryonic international institutional infrastructure to detect and respond to asteroids. As part of all this – and in line with increasing scientific opinion – there is also a notable focus at governmental and intergovernmental levels on the use of nuclear weapons as our best hope. The US and Russia have even mooted working together on a nuclear planetary defense initiative. All of a sudden, it seems Bruce Willis and his team might be put on NASA's speed-dial, after all.

What the law says

As a lawyer I can't help but wonder how these recent developments sit with international law. Not well, it would seem. At the intersection of nuclear non-proliferation law and space law, various Cold War-era treaties would appear to rule out nuclear planetary defense. The legal picture is not always clear – the relevant law was drafted with the superpower arms race in mind, after all, not asteroids. But if a collision-course NEO was identified, it can at least be said that a proposed nuclear response would be very likely to violate international law.

For example, Article IV of the 1967 Outer Space Treaty prohibits stationing nuclear weapons in space, which would apparently rule out nuclear NEO defense, at least if a nuclear defense system was located in space (rather than being launched from Earth).

The 1963 Partial Test Ban Treaty is an even bigger barrier for most states (although, notably, not all of the nuclear powers are party to it – but the US and Russia both are). Article I(1)(a) of that treaty prohibits "any … nuclear explosion … in … outer space". And these are just the key treaties: there are a number of other possible legal hurdles, too.

So what? If it came to a choice between legal niceties and saving humanity from extinction, there wouldn't be much of a choice at all: law shouldn't be a global suicide pact. Indeed, one nuclear power, Russia, has already indicated that – if that asteroid appeared – it likely would opt for "launch first, litigate second".

But ignoring the law is always a dangerous business, and it's not hard to envisage nuclear powers using the vague threat of "asteroids" as a pretext for developing new warheads, or even for launching nukes into space. And if they do so in unapologetic violation of international law, they'll also circumvent all the checks and balances that the law can provide. That threat is maybe more worrying than the threat of some hypothetical space rock.

In a major article just published in the Hastings International & Comparative Law Review, I argue that international law needs to work out a way to thread this needle.

The law has to protect us from states using asteroids as a pretext for dodging nuclear disarmament obligations, or – gulp – nuclear aggression in space, while at the same time providing for a limited, safeguarded exception that would allow for multilateral nuclear planetary defense, should it ever come to pass that we need the "nuclear option" to save ourselves.

A solution?

As such, I propose either treaty amendment (or, more likely, the adoption of additional protocols) to carve out a new, bespoke legal exception for the use of nuclear weapons in space, in instances where a large collision-course NEO was identified and verified, and where the balance of independent scientific option clearly supported a nuclear response.

At the same time, to promote certainty, protect against abuse and increase the chances of success through the pooling of expertise and resources, I also argue for the creation of a new multilateral decision-making and oversight body, composed of all states (or as many states as possible), and which additionally included direct input from independently appointed

scientific experts and organizations.
The aim is that the new body would be equipped both to stop countries misusing the new legal exception to develop militarized nuclear space programs, while at the same time avoiding the deadlock issues associated with existing institutions (such as, for example, the UN Security Council) if humanity has to act quickly to avoid going the way of the dinosaurs.

All of this would be extremely complex (legally, politically and financially) and would take a huge amount of time to set up. But when it comes to the "asteroid threat", time is not an issue. Until it is. So, I suggest we get started now.
The political and scientific context has changed since 2013 but the legal context is still stuck in the thinking of the 1960s – and we need to update it. If we don't, we really could risk Armageddon.

James A Green *is Professor of Public International Law, University of Reading.*

Qatar calls for nuclear weapons-free zone

Source: https://www.gulf-times.com/story/630659/Qatar-calls-for-nuclear-weapons-free-zone

May 05 – Qatar has affirmed its belief that a 'zone free of nuclear weapons and other weapons of mass destruction and their means of delivery' represents a regional and practical approach to resolving the problem of the spread of such weapons in a region rife with military conflicts and political crises. Speaking at the Preparatory Committee for the 2020 Nuclear Non-Proliferation Treaty (NPT) Review Conference, Chairman of the National Committee for the Prohibition of Weapons, Brigadier-General Hassan Saleh al-Nisf, said Qatar considers this approach to be a collective solution to the Iranian nuclear issue, to the use of chemical weapons in the region, and to Israel's exclusive possession of nuclear weapons in the Middle East.
Al-Nisf referred to Qatar's endorsement of the statements of the Arab Group and the Non-Aligned Movement on the establishment of a zone free of nuclear weapons and other weapons of mass destruction in the Middle East and to the Arab working paper on the same subject.
"We have no other chance before 2020, so we would like at the outset to demand that we stop any futile debate over whether review conferences are the right forum to discuss this issue or not," he said.
"The 1995 Middle East decision was an inseparable part of the deal of the indefinite extension of the Treaty and will remain an essential part of the review process as long as it is not implemented. "We wish to recall that the conferences of 2000 and 2010 emphasised the importance of the decision and that it will remain in force until its objectives are achieved," he added.
He suggested instead of repeating the previous positions that obstruct the implementation of the decision "to start a real dialogue on how to implement it", stressing the readiness of Qatar to fully interact with any serious proposals to break the stalemate in this issue.
The Chairman of the National Committee for the Prohibition of Weapons expressed his astonishment at the promotion of some that the states have become tired of this subject dominance on the review process, stressing that countries that support the efforts to free the Middle East from these weapons are those of the Non-Aligned Movement and the majority of African and Asian countries, and the majority of European countries and some nuclear countries support – at least in theory – this initiative.
Therefore, the way out of the stalemate is to move forward positively towards its implementation and not back down.
He pointed out that the 2010 conference was a shining sign and an important turning point, as a clear mechanism and practical steps were put in place to begin negotiations on the establishment of a zone free of these weapons in the Middle East.
The conference also clarified that the parties to the Treaty are responsible for implementing the resolution and its mechanisms along a particular responsibility on the three depositories of the Treaty and the Secretary-General of the United Nations.
Therefore, if there is a default, it is the responsibility of those who have not fulfilled the obligations and mandates to which they have committed themselves.

He added that the delay in the implementation of the Middle East decision is one of the most important factors that eroded the credibility of the Treaty as a whole and is problematic in a review cycle.
Since the postponement of the 2012 conference, in violation of the text and spirit of the mandate issued in 2010, the Arab countries have tried to break the impasse in the process and presented various proposals and ideas and some of which have been rejected without alternative proposals, noting that the first and second preparatory committee did not make any progress on the subject and did not make a positive discussion of any proposals, and this third preparatory committee has the last opportunity to make effective recommendations to the NPT Review Conference in 2020.
In this regard, he proposed a recommendation to the Review Conference to 'repeat demand that Israel accedes to the Treaty on the Non-Proliferation of Nuclear Weapons as a non-nuclear-weapon state without conditions, and to subject its nuclear facilities to the comprehensive safeguards system of the International Atomic Energy Agency to invite Israel, Iran and the Arab countries to participate effectively and in good faith at any negotiating conferences organised by the United Nations to establish a treaty for the establishment of a zone free of such weapons'.
He also proposed to call on 'all states parties to the Treaty, especially the nuclear states, to cease any nuclear co-operation or technological exchange with Israel until it accedes to the Treaty on the Non-Proliferation of Nuclear Weapons and with any state that refuses to participate in the process of negotiations to be initiated in order to create a real incentive among the countries of the region to start a serious process towards the establishment of the zone and request the Secretary-General of the United Nations to brief the review conferences and their preparatory committees on developments in this area'.
Concluding, al-Nisf said Qatar affirms the collective responsibility of all the states and the geographical and political groups to create the appropriate conditions and effective incentives for the implementation of the Middle East decision and all its obligations at the subsequent review conferences, adding "this is our vision and our proposals, and we are ready and exited to hear specific views and proposals from all states parties."

Ohio School Closed After Enriched Uranium Discovered Inside

Source: https://www.newsweek.com/ohio-school-closed-enriched-uranium-discovered-radiation-cancer-1424704

May 14 – An Ohio school has been forced to close for the remainder of the academic year after enriched uranium was discovered inside. **Neptunium 237**—a byproduct of nuclear reaction and plutonium production—was also detected inside Zahn's Corner Middle School in the town of Piketon, about 80 miles east of Cincinnati, WLWT reported.

Both substances are radioactive, and extended exposure to them can cause cancer.

The middle school serves about 320 students, and officials have been working to determine the source of the contamination and establish its extent. They have not ruled out a longer school closure.
Scioto Valley Local School District Superintendent Todd Burkitt made the decision to close the school on Monday. "Even the last couple of hours have been very hectic. There's just not a playbook in how we deal with this. We're kind of writing the script as we go. We're not going to take any chances on someone's child. We just won't do that," Burkitt told WLWT.
The state department of education said that the affected students had already fulfilled their necessary classroom hours for the year, so would not need to make up the missed days once the uranium issue had been addressed.
The source of the enriched uranium remains unclear. According to WLWT, some local residents suggested that the nearby Portsmouth Gaseous Diffusion Plant—located 2 miles from the school—might be responsible. The facility previously produced enriched uranium,

including weapons-grade uranium, for the United States Atomic Energy program and for use in U.S. nuclear weapons. Uranium enrichment at the site ended in 2001.
The site is now subject to an environmental cleanup under the supervision of the Department of Energy. Department officials told WLWT, "Routine air samples in the area of DOE Portsmouth Gaseous Diffusion Plant in Piketon revealed trace amounts of two radiological isotopes that were more than one thousand to ten thousand times below the established threshold of public health concern. DOE treats all detections seriously—even those that are at such low levels."
The statement said the department was "committed to the safety, health and protection of our workforce, the general public and the environment at all our sites." Officials said the Department of Energy is planning to commission an "independent third party to perform an additional analysis of the air and ground readings to properly assess the situation." The statement noted that the department was "confident that those findings will allay any cause for further concern."
Regardless, the development came as a shock to the local community. Jennifer Chandler, a councilwoman for Piketon, told WLWT: "We aren't prepared for something like this, that's for sure… We, at this point, don't know how far the contamination has reached. That will be part of the ongoing investigation." She noted that homes and bodies of water had tested positive for enriched uranium and neptunium.

Iran officially begins unlimited production of enriched uranium, heavy water

Source: http://www.homelandsecuritynewswire.com/dr20190515-iran-officially-begins-unlimited-production-of-enriched-uranium-heavy-water

May 15 – **Iran has officially ended its compliance with several commitments under the 2015 nuclear accord,** an informed official in the country's atomic energy body told local media channels on Wednesday.
The source from the Atomic Energy Organization of Iran told the semi-official ISNA news agency that the country has stopped "programs related to compliance with the ceiling for production of enriched uranium as well as the unlimited production of heavy water at the Arak facility."
Under the nuclear accord, Iran had limits imposed on the quantities of uranium and heavy water it can produce, set at 300 kilograms and 130 tons, respectively. Moving forward, the official said, the Islamic Republic will no longer adhere to limitations regarding the production of enriched uranium and heavy water.
However, the official insisted that the change in policy doesn't violate the terms of the Joint Comprehensive Plan of Action (JCPOA).
Iran notified China, Russia, France, Germany, and Britain of its decision to scrap some commitments under the nuclear accord, a year after the United States withdrew from the agreement and re-imposed sanctions.
On 8 May, Iranian President Hassan Rouhani warned world powers that unless they shield the country's collapsing economy from crippling U.S. sanctions within 60 days, Iran would start enriching uranium at higher levels.
"If the five countries join negotiations and help Iran to reach its benefits in the field of oil and banking, Iran will return to its commitments according to the nuclear deal," Rouhani said.
While EU foreign ministers insisted that they were still committed to the nuclear deal, they rejected any ultimatums from Tehran. The U.S. imposed further sanctions on Iran following those threats, this time on the country's metals industry.
Iranian Supreme Leader Ayatollah Ali Khamenei said on Tuesday that Tehran would not negotiate with the United States on another nuclear deal. On Wednesday, Iran's Minister of Defense, Ami Hatami, vowed that the country will "defeat the American-Zionist front," referring to the United States and Israel.


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

Deadly gases may be starting to leak from Europe's World War weapons cemeteries

Source: https://www.washingtonpost.com/world/2019/05/03/deadly-gases-may-be-starting-leak-europes-world-war-weapons-cemeteries/

May 03 — After World War I and World War II, officials decided to dump hundreds of thousands of metric tons of munitions into the oceans around Europe, which at the time appeared to be the most easily accessible disposal ground. Some of those weapons — including mines containing mustard gas — were simply dropped into the Baltic and North seas in the heart of Europe rather than being taken to faraway dump sites near the Arctic Circle.

But the hidden legacy of those world wars may come to haunt the continent for decades to come.

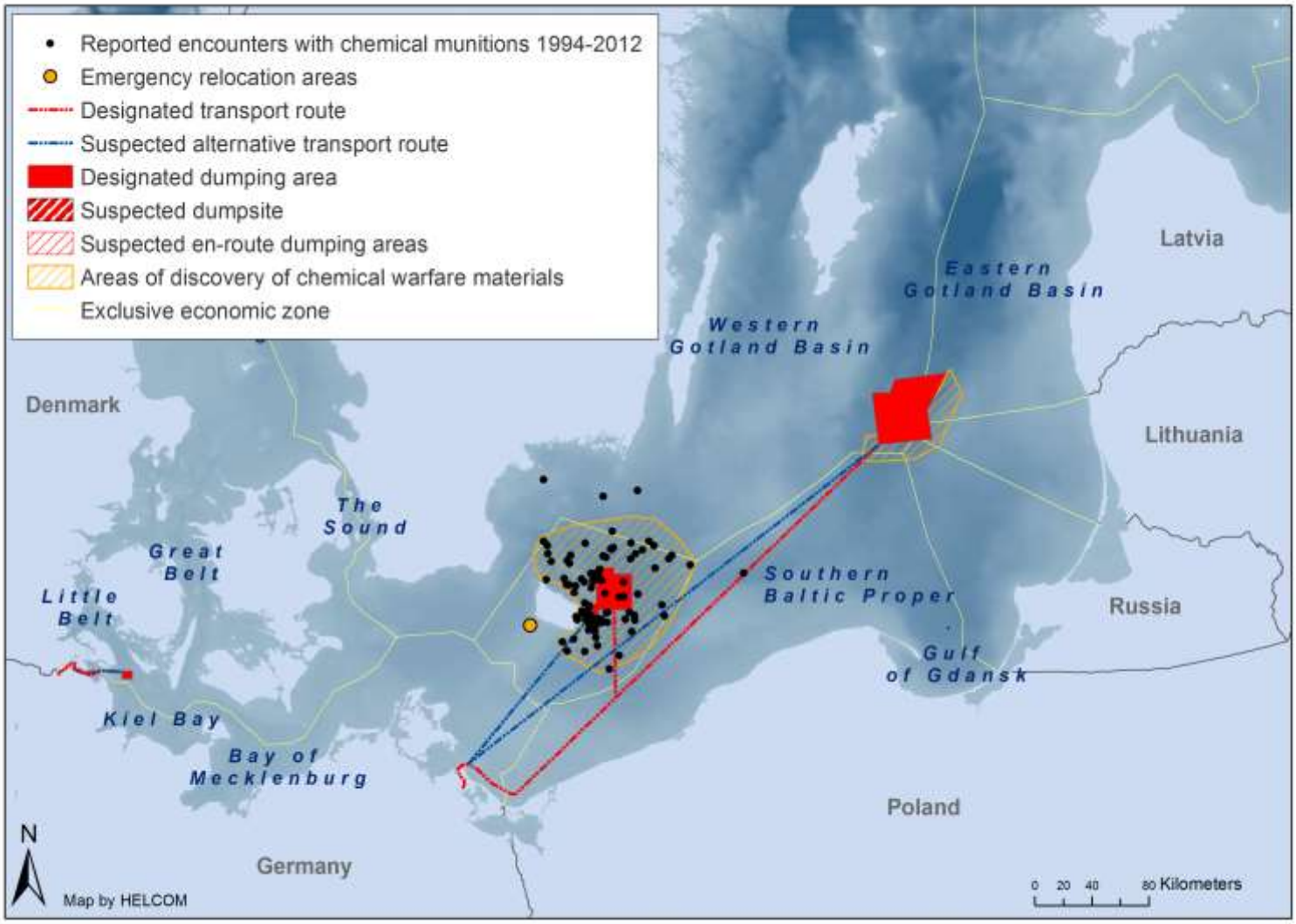
This week, the Belgian newspaper Het Laatste Nieuws reported that officials have grown concerned that one of those dump sites — close to the Belgian coastal municipality of Knokke-Heist — has started to leak. At the site, two out of 23 probed locations showed signs of contamination, the paper said. The revelation followed months of official inquiries into what authorities' fear could be a mounting public safety threat.

Used as a potentially deadly chemical agent during World War I, mustard gas can burn victims' skin, respiratory tract and eyes.

If confirmed, the leaks would hardly come as a surprise to other officials around Europe. They see themselves in a race against time to prevent the leaking of deadly gases and other hazardous substances, but they have struggled to have their concerns heard.

While mustard gas leaks from Europe's underwater weapons cemeteries were long considered a worst-case scenario, officials also are expressing alarm over leaks of explosives such as TNT from dumped land mines or sea mines. While those substances have been contained inside metal cases for eight decades in the case of World War II, and about a century in the case of World War I munitions, the metal has rusted and become porous.

In the 1920s and 1940s, that may have seemed like a distant threat amid the still-vivid horrors of some of the deadliest conflicts in world history. But in more recent years, such leaks have posed a growing environmental threat. Activists have blamed the leaks in part for decreasing biodiversity in the Baltic Sea.



The problem extends far beyond the "weapons cemeteries" that are now making headlines.

In the neighboring Baltic Sea, more than 80,000 mines are believed to be beneath the surface. Unlike the North Sea's mass dump sites, the locations of single mines are more difficult to track down. There are only vague maps of where the mines might be hidden — and most of them appear to be spread out across hundreds of miles.

Reminders of their potentially deadly impact have mounted.

In 2005, three Dutch fishermen were killed after they accidentally caught an American-made World War II bomb in their fishing net. Similar discoveries regularly trigger mass evacuations — for instance, last August in the Polish resort city of Kolobrzeg, where three bombs were discovered in the nearby bay.

European navies help out with remote-controlled vehicles and clearance divers within their own territorial waters. But in some areas, the density of explosives is believed to be so high that fishing is still prohibited there a century later.

Pipeline construction companies often hire private mine-clearance contractors to do the job if there is no way around it and when the explosives are found far out at sea, where European navies do not claim responsibility.

"It's unbelievable how many mines there still are," Cmdr. Peeter Ivask, the head of Estonia's navy, told a visiting reporter late last year.

"Our mission here will last decades," Ivask said.
And, likely, it will never be complete.

What consequences have bombs and mines left over from wars?

Source: https://vietnamnews.vn/opinion/519652/it-could-take-100-years-to-be-free-of-explosives-official.html#Cfy4r5FKkyTVLwUS.97

May 09 – It is estimated that bombs and explosives are left from the wartime in all 63 provinces and cities nationwide. In some districts in the central provinces of Quảng Bình and Quảng Trị, the contaminated areas have been reported to account for 80 per cent of the area.

Since peace returned to Việt Nam in 1975, more than 40,000 people have been killed while some 60,000 others have been maimed by explosions from remnant explosives, particularly bombs and mines.

Though Việt Nam has done its best to clear the contaminated land from the remaining bombs and mines, some 6.1 million hectares are still suspected of being contaminated with bombs and mines.

What has Việt Nam been focusing on to tackle this problem?

There are many activities we have been doing, including educating and supporting victims from explosions of bombs or mines.

On the part of VNMAC, we have focused our efforts on helping victims of explosions and launching communication campaigns to help the public understand the danger of bombs and mines, including activities to support victims during and after the war.

In April 2018, VNMAC had completed a map on land contaminated with bombs and mines in all Việt Nam. In the map, VNMAC also indicated areas which are seriously contaminated.

What are the main challenges Việt Nam has faced in the work?

In Việt Nam, only army engineers or sappers are the forces involved in mine-clearing activities. A big challenge that the Vietnamese sappers are facing is that they don't have up to date equipment to perform their jobs. Meanwhile, bombs and mines in Việt Nam are made by many countries and they are buried deep under the ground with different topography.

This is a challenge for Vietnamese sappers. The Vietnamese People Army has launched many campaigns to clear the land of bombs and mines. Yet, many bombs and mines are still buried under the

ground – a headache for the Vietnamese Government and the general public. Under Vietnamese law, all costs incurred during de-mining activities are paid for by the State budget.

In 2010 the Government approved the very first Việt Nam National Mine Action Plan for 2010-2025. How many hectares of land contaminated with bombs or mines have since been cleared?

In that programme, the Government set a target that in 15 years – from 2010-2025, each year, at least from 30,000-50,000 ha should be de-contaminated.

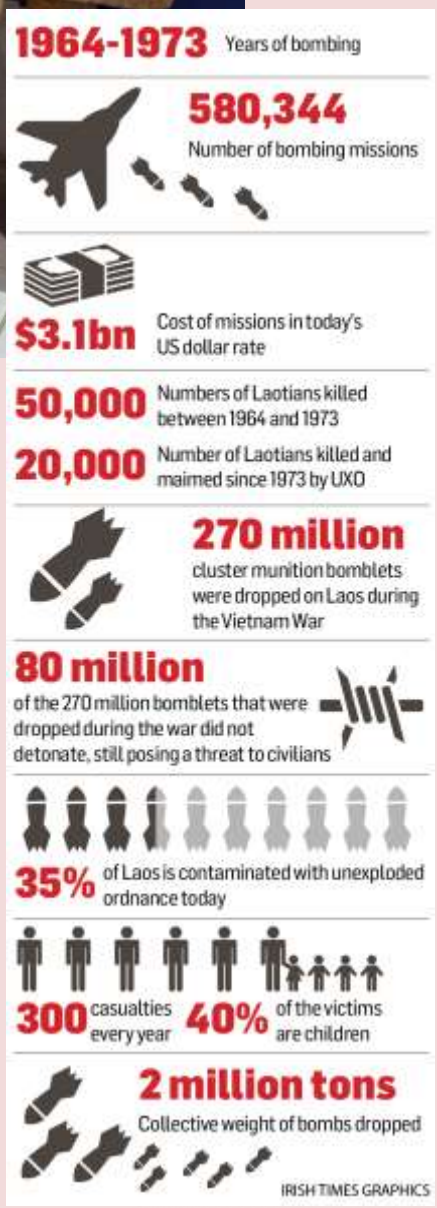
If that goal was realised, it would take Việt Nam 20 years to clean 1 million ha which have been contaminated with bombs or mines. But, in Việt Nam, we have more than 6.1 million ha which are contaminated or suspected of contamination with bombs and mines. So it would take the country more than a hundred years to do the job.

Over the past more than eight years, on an average each year, Việt Nam was able to clear about 30,000 ha per year,

Of course, while performing our task, Việt Nam has received financial support from friends far and near. For example, the Republic of Korea has granted Việt Nam US$20 million to do the bombs/mines clearance and support victims in the two southern provinces of Bình Định and Quảng Bình and to help Việt Nam to develop its national data system on bombs and mines left over in war for national independence.

For Việt Nam, the biggest challenge is financial. Since the launching of this national action plan, we have received a lot of support from friends far and near, ranging from financial support to human resources training and others.

With official development support from foreign countries and organisations, one of the tasks that the VNMAC will focus on in a near future is to decontaminate bombs and mines in the five provinces of Hà Giang, Lào Cai, Cao Bằng, Quảng Trị and Quảng Nam.




WHAT HAVE WE HERE?
LOOKS LIKE WE NEED
A PLAN...
MINISTERIAL
MEETING 2018
HELCOM

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

CYBER NEWS

What does Google know about me?

By Gabriel Weinberg, I run a search engine (Duck Duck Go)
Source: https://www.quora.com/What-does-Google-know-about-me/answer/Gabriel-Weinberg

Updateyd Sep 12, 2018 · Upvoted by Cole Duncan, A Google Staff Manager at Google (2015-present) and Yongzhen Chen, former Student Ambassador at Google (2014) · Author has 93 answers and 625.4m answer views

May 03 – Did you know that unlike searching on DuckDuckGo, when you search on Google, they keep your search history forever? That means they know *every* search you've *ever* done on Google. That alone is pretty scary, but it's just the shallow end of the very deep pool of data that they try to collect on people.

What most people don't realize is that even if you don't use any Google products directly, they're still trying to track as much as they can about you. Google trackers have been found on 75% of the top million websites. This means they're also trying to track most everywhere you go on the internet, trying to slurp up your browsing history!

Most people also don't know that Google runs most of the ads you see across the internet and in apps – you know those ones that follow you around everywhere? Yup, that's Google, too. They aren't really a search company anymore – they're a tracking company. They are tracking as much as they can for these annoying and intrusive ads, including recording every time you see them, where you saw them, if you clicked on them, etc.

But even that's not all…

If You Use Google Products

If you do use Google products, they try to track even more. In addition to tracking everything you've ever searched for on Google (e.g. "weird rash"), Google also tracks every video you've ever watched on YouTube. Many people actually don't know that Google owns YouTube; now you know.

And if you use Android (yeah, Google owns that too), then Google is also usually tracking:

- Every place you've been via Google Location Services.
- How often you use your apps, when you use them, where you use them, and whom you use them to interact with. (This is just excessive by any measure.)
- All of your text messages, which unlike on iOS, are not encrypted by default.
- Your photos (even in some cases the ones you've deleted).

If you use Gmail, they of course also have all your e-mail messages. If you use Google Calendar, they know all your schedule. There's a pattern here: For all Google products (Hangouts, Music, Drive, etc.), you can expect the same level of tracking: that is, pretty much anything they can track, they will.

Oh, and if you use Google Home, they also store a live recording of every command you've (or anyone else) has ever said to your device! Yes, you heard that right (err… they heard it) – you can check out all the recordings on your Google activity page.

Essentially, if you allow them to, they'll track pretty close to, well, *everything you do on the Internet.* In fact, even if you tell them to stop tracking you, Google has been known to not really listen, for example with location history.

You Become the Product

Why does Google want all of your information anyway? Simple: as stated, Google isn't a search company anymore, they're a tracking company. All of these data points allow Google to build a pretty robust profile about you. In some ways, by keeping such close tabs on everything you do, they, at least in some ways, may know you better than you know yourself.

And Google uses your personal profile to sell ads, not only on their search engine, but also on over three million other websites and apps. Every time you visit one of these sites or apps, Google is following you around with hyper-targeted ads.

It's exploitative. By allowing Google to collect all this info, you are allowing hundreds of thousands of advertisers to bid on serving you ads based on your sensitive personal data. Everyone involved is profiting from your information, except you. You are the product.
It doesn't have to be this way. It is entirely possible for a web-based business to be profitable without making you the product – since 2014, DuckDuckGo has been profitable without storing or sharing any personal information on people at all. You can read more about our business model here.

The Myth of "Nothing to Hide"
Some may argue that they have "nothing to hide," so they are not concerned with the amount of information Google has collected and stored on them, but that argument is fundamentally flawed for many reasons.
Everyone has information they want to keep private: Do you close the door when you go to the bathroom? Privacy is about control over your personal information. You don't want it in the hands of everyone, and certainly don't want people profiting on it without your consent or participation.
In addition, privacy is essential to democratic institutions like voting and everyday situations such as getting medical care and performing financial transactions. Without it, there can be significant harms.
On an individual level, lack of privacy leads to putting you into a filter bubble, getting manipulated by ads, discrimination, fraud, and identity theft. On a societal level, it can lead to deepened polarization and societal manipulation like we've unfortunately been seeing multiply in recent years.

You Can Live Google Free
Basically, Google tries to track too much. It's creepy and simply just more information than one company should have on anyone.
Thankfully, there are many good ways to reduce your Google footprint, even close to zero! If you are ready to live without Google, we have recommendations for services to replace their suite of products, as well as instructions for clearing your Google search history. It might feel like you are trapped in the Google-verse, but it is possible to break free.
For starters, just switching the search engine for all your searches goes a long way. After all, you share your most intimate questions with your search engine; at the very least, shouldn't those be kept private? If you switch to the DuckDuckGo app and extension you will not only make your searches anonymous, but also block Google's most widespread and invasive trackers as you navigate the web.
If you're unfamiliar with DuckDuckGo, we are an Internet privacy company that empowers you to seamlessly take control of your personal information online, without any tradeoffs. We operate a search engine alternative to Google at http://duckduckgo.com, and offer a mobile app and desktop browser extension to protect you from Google, Facebook and other trackers, no matter where you go on the Internet.
We're also trying to educate users through our blog, social media, and a privacy "crash course" newsletter.

Will the next cyberattack be in the hospital?

By Brian Blum
Source: http://www.homelandsecuritynewswire.com/dr20190516-will-the-next-cyberattack-be-in-the-hospital

May 16 – What's your stereotype of a hacker: a malicious millennial intent on hijacking your computer, deleting your files and demanding a ransom? A corporate criminal stealing sensitive data from Sony or Yahoo? Or a rogue programmer attacking connected cars and electrical, water and telecommunications grids?

You may not think of hackers targeting hospitals, but this is where our wired world may be most vulnerable, and the results could be deadly.

Most medical devices such as drug-infusion monitors, kidney-dialysis units and ventilators were built when Internet connectivity was still new and IT professionals never imagined a hacker could change the drip rate in an IV or stop an ICU patient's breathing machine.
That chilling prospect was at least one of the reasons why Israeli startup Cynerio was able to raise $7 million for its technology

designed to protect medical devices from cyberattacks.

"Every cyber company has two elements," Daniel Brodie, Cynerio's CTO, tells ISRAEL21c. "There's a bit of the fear story – what would the worst-case scenario look like – as well as a real business ability to provide solutions for customers."

Cynerio addresses what's become known as the "Internet of Medical Things" – a play on words for the better-known "Internet of Things" which describes devices such as smart refrigerators and thermostats that are Internet-connected.

Zion Market Research estimates that the global market for the Internet of Medical Things is growing 11 percent a year and could reach $14.7 billion by 2022.

The benefits of smart medical devices are clear. They're "good for doctors [who] can make decisions based on real-time data," explains Cynerio CEO Leon Lerman.

Consider a hospital's radiology department, for example. When a patient is admitted to the hospital, a new digital record is created in the main computer system. If the patient is subsequently sent for a CT scan, the patient's information is already queued up. The results of the scan are automatically sent to the hospital's imaging server, which later updates the patient's EMR (electronic medical record).

That makes for efficient medical care, but a determined hacker could enter at multiple points in the process. "These systems are not secure," Lerman laments, "and a large number of these devices are operated by old systems and don't even have anti-virus installed."

Protecting hospital networks

In 2017, a ransomware attack called WannaCry targeted computers running Microsoft Windows. Although
the hack was generic, in the UK it hit the country's NHS-operated hospitals the hardest, forcing them to turn away patients and cancel some 19,000 appointments.

Staff had to use pen and paper and their own mobile devices after the attack affected key systems including telephones. The UK Department of Health estimated the damage at more than $100 million.

Hackers who get into a hospital's computer systems via a medical device can also steal personal data that can be used later for identity theft. A group of hackers known as the Dark Overlord stole and then leaked the phone numbers and addresses of several Hollywood celebrities who were clients of a Beverly Hills, Calif. plastic surgeon.

Because there are so many possible medical devices with different vulnerabilities, creating cybersecurity patches specific for each would be an impossibly large task, Brodie tells ISRAEL21c. So Cynerio is working with hospitals' IT departments to protect the network as a whole.

"We take the metadata – such as what types of messages are being uploaded – and do machine learning across the hospital, in order to understand the behavior of the facility in general," Brodie explains. "We know that MRI machines don't talk to patient monitors, for example."

This kind of insight helps Cynerio guard against attacks while delivering a low number of false positives, he adds.

Cynerio uses the tools a hospital already has, such as firewalls and Network Access Controls, Brodie says. **"Our main added value is the learning."**

Cynerio also educates hospital staffers who don't always know how to use the tools they have and – because equipment can sometimes be purchased by individual departments rather than a central buying facility — may not even know how many medical devices they have at the facility.

Cynerio provides hospitals with visibility (which devices are communicating on the network); assessment (which devices are vulnerable); detection (identifying anomalies in real time within a medical context); and protection (improving security).

Because Cynerio's tech is not attached to the equipment, it will not "interfere with the routine operations of the device in providing medical treatment," Lerman adds.

What makes Cynerio unique

Brodie and Lerman launched Cynerio in 2017 in Ramat Gan outside Tel Aviv. The company's cybersecurity software is now running at hospitals in Israel including Tel Aviv Sourasky Medical Center and Rambam Health Care Campus in Haifa.

The new financing from Accelmed, RDC and MTIP will allow Cynerio to expand to the United States and hire 10 people there. Lerman is moving to the US to head up the sales arm of the company.

Cynerio is not the only company providing cybersecurity to hospitals.

"A few generic IT solutions have shifted into healthcare," Brodie points out. "Our uniqueness is that we're not looking only at the medical devices but the entire ecosystem around them. Not just a specific patient monitor, but the servers that aggregate all the patient monitors in the hospital."

We go to great lengths to seek out the top hospitals and health professionals. Keeping those facilities safe from hackers is the latest twist in the quest for top-notch medical care in the twenty-first century.

***Brian Blum** writes about startups, pharmaceutical advances, and scientific discoveries for Israel21c.*

The radio navigation planes use to land safely is insecure and can be hacked

Source: https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

May 15 – Just about every aircraft that has flown over the past 50 years—whether a single-engine Cessna or a 600-seat jumbo jet—is aided by radios to safely land at airports. These instrument landing systems (ILS) are considered precision approach systems, because unlike GPS and other navigation systems, they provide crucial real-time guidance about both the plane's horizontal alignment with a runway and its vertical angle of descent. In many settings—particularly during foggy or rainy night-time landings—this radio-based navigation is the primary means for ensuring planes touch down at the start of a runway and on its centerline.

Like many technologies built in earlier decades, the ILS was never designed to be secure from hacking. Radio signals, for instance, aren't encrypted or authenticated. Instead, pilots simply assume that the tones their radio-based navigation systems receive on a runway's publicly assigned frequency are legitimate signals broadcast by the airport operator. This lack of security hasn't been much of a concern over the years, largely because the cost and difficulty of spoofing malicious radio signals made attacks infeasible. Now, researchers have devised a low-cost hack that raises questions about the security of ILS, which is used at virtually every civilian airport throughout the industrialized world. Using a $600 software defined radio, the researchers can spoof airport signals in a way that causes a pilot's navigation instruments to falsely indicate a plane is off course. Normal training will call for the pilot to adjust the plane's descent rate or alignment accordingly and create a potential accident as a result.

One attack technique is for spoofed signals to indicate that a plane's angle of descent is more gradual than it actually is. The spoofed message would generate what is sometimes called a "fly down" signal that instructs the pilot to steepen the angle of descent, possibly causing the aircraft to touch the ground before reaching the start of the runway.

The video (https://www.youtube.com/watch?v=Wp4CpyxYJq4) shows a different way spoofed signals can pose a threat to a plane that is in its final approach. Attackers can send a signal that causes a pilot's course deviation indicator to show that a plane is slightly too far to the left of the runway, even when the plane is perfectly aligned. The pilot will react by guiding the plane to the right and inadvertently steer over the centerline.

The researchers, from Northeastern University in Boston, consulted a pilot and security expert during their work, and all are careful to note that this kind of spoofing isn't likely to cause a plane to crash in most cases. ILS malfunctions are a known threat to aviation safety, and experienced pilots receive extensive training in how to react to them. A plane that's misaligned with a runway will be easy for a pilot to visually notice in clear conditions, and the pilot will be able to initiate a missed approach fly-around.

Another reason for measured skepticism is the difficulty of carrying out an attack. In addition to the SDR, the equipment needed would likely require directional antennas and an amplifier to boost the signal. It would be hard to sneak all that gear onto a plane in the event the hacker chose an onboard attack. If the hacker chose to mount the attack from the ground, it would likely require a great deal of work to get the gear aligned with a runway without attracting attention. What's more, airports typically monitor for interference on sensitive frequencies, making it possible an attack would be shut down shortly after it started.

In 2012, Researcher Brad Haines, who often goes by the handle Renderman, exposed vulnerabilities in the automatic dependent surveillance broadcast—the broadcast systems planes use to determine their location and broadcast it to others. He summed up the difficulties of real-world ILS spoofing this way:

If everything lined up for this, location, concealment of gear, poor weather conditions, a suitable target, a motivated, funded and intelligent attacker, what would their result be? At absolute worst, a plane hits the grass and some injuries or fatalities are sustained, but emergency crews and plane safety design means you're unlikely to have a spectacular fire with all hands lost. At that point, airport landings are suspended, so the attacker can't repeat the attack. At best, pilot notices the misalignment, browns their shorts, pulls up and goes around and calls in a maintenance note that something is funky with the ILS and the airport starts investigating, which means the attacker is not likely wanting to stay nearby.

So if all that came together, the net result seems pretty minor. Compare that to the return on investment and economic effect of one jackass with a $1,000 drone flying outside Heathrow for 2 days. Bet the drone was far more effective and certain to work than this attack.

Still, the researchers said that risks exist. Planes that aren't landing according to the glide path—the imaginary vertical path a plane follows when making a perfect landing—are much harder to detect even when visibility is good. What's more, some high-volume airports, to keep planes moving, instruct pilots to delay making a fly-around decision even when visibility is extremely limited. The Federal Aviation Administration's Category III approach operations, which are in effect for many US airports, call for a decision height of just 50 feet, for instance. Similar guidelines are in effect throughout Europe. Those guidelines leave a pilot with little time to safely abort a landing should a visual reference not line up with ILS readings.

"Detecting and recovering from any instrument failures during crucial landing procedures is one of the toughest challenges in modern aviation," the researchers wrote in their paper, titled Wireless Attacks on Aircraft Instrument Landing Systems, which has been accepted at the 28th USENIX Security Symposium. "Given the heavy reliance on ILS and instruments in general, malfunctions and adversarial interference can be catastrophic especially in autonomous approaches and flights."

What happens with ILS failures

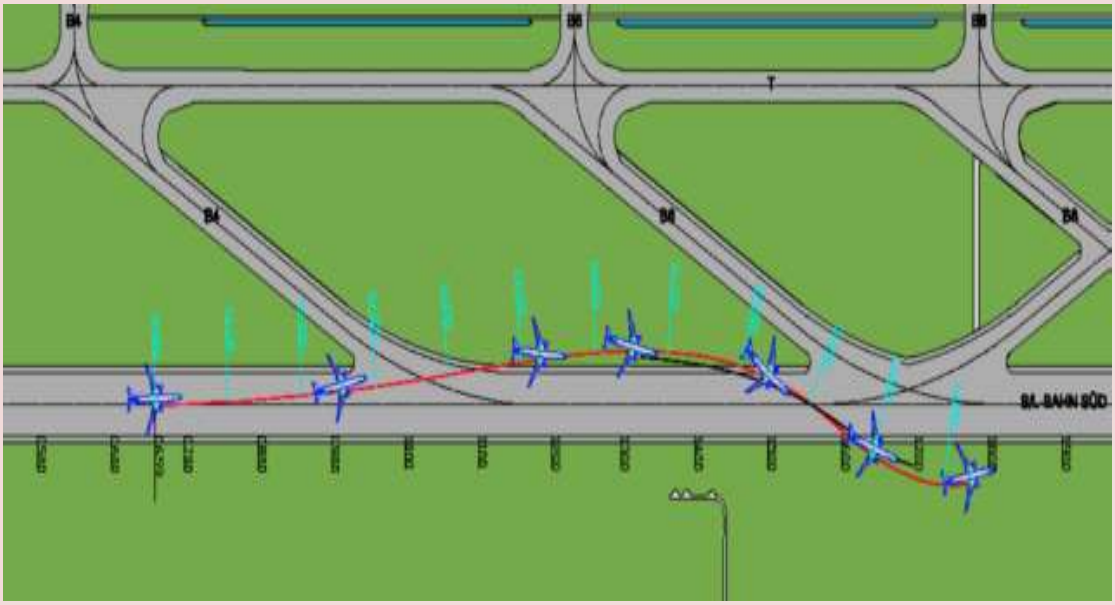
Several near-catastrophic landings in recent years demonstrate the danger posed from ILS failures. In 2011, Singapore Airlines flight SQ327, with 143 passengers and 15 crew aboard, unexpectedly banked to the left about 30 feet above a runway at the Munich airport in Germany. Upon landing, the Boeing 777-300 careened off the runway to the left, then veered to the right, crossed the centerline, and came to a stop with all of its landing gear in the grass to the right of the runway. The image directly below shows the aftermath. The image below that depicts the course the plane took.

An instrument landing system malfunction caused Singapore Airlines flight SQ327 to slide off the runway shortly after landing in Munich in 2011.

An incident report published by Germany's Federal Bureau of Aircraft Accident Investigation said that the jet missed its intended touch down point by about 1,600 feet. Investigators said one contributor to the accident was localizer signals that had been distorted by a departing aircraft. While there were no reported injuries, the event underscored the severity of ILS malfunctions. Other near-catastrophic accidents involving ILS failures are an Air New Zealand flight NZ 60 in 2000 and a Ryanair flight FR3531 in 2013. The following video helps explain what went wrong in the latter event.

Vaibhav Sharma runs global operations for a Silicon Valley security company and has flown small aviation airplanes since 2006. He is also a licensed Ham Radio operator and volunteer with the Civil Air Patrol, where he is trained as a search-and-rescue flight crew and radio

communications team member. He's the pilot controlling the X-Plane flight simulator in the video demonstrating the spoofing attack that causes the plane to land to the right of the runway.
Sharma told Ars:



The path Singapore Airlines flight SQ327 took after landing.

This ILS attack is realistic but the effectiveness will depend on a combination of factors including the attacker's understanding of the aviation navigation systems and conditions in the approach environment. If used appropriately, an attacker could use this technique to steer aircraft towards obstacles around the airport environment and if that was done in low visibility conditions, it would be very hard for the flight crew to identify and deal with the deviations.
He said the attacks had the potential to threaten both small aircraft and large jet planes but for different reasons. Smaller planes tend to move at slower speeds than big jets. That gives pilots more time to react. Big jets, on the other hand, typically have more crew members in the cockpit to react to adverse events, and pilots typically receive more frequent and rigorous training.
The most important consideration for both big and small planes, he said, is likely to be environmental conditions, such as weather at the time of landing.
"The type of attack demonstrated here would probably be more effective when the pilots have to depend primarily on instruments to execute a successful landing," Sharma said. "Such cases include night landings with reduced visibility or a combination of both in a busy airspace requiring pilots to handle much higher workloads and ultimately depending on automation."
Aanjhan Ranganathan, a Northeastern University researcher who helped develop the attack, told Ars that GPS systems provide little fallback when ILS fails. One reason: the types of runway misalignments that would be effective in a spoofing attack typically range from about 32 feet to 50 feet, since pilots or air traffic controllers will visually detect anything bigger. It's extremely difficult for GPS to detect malicious offsets that small. A second reason is that GPS spoofing attacks are relatively easy to carry out.
"I can spoof GPS in synch with this [ILS] spoofing," Ranganathan said. "It's a matter of how motivated the attacker is."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

The expected unexpected that happened

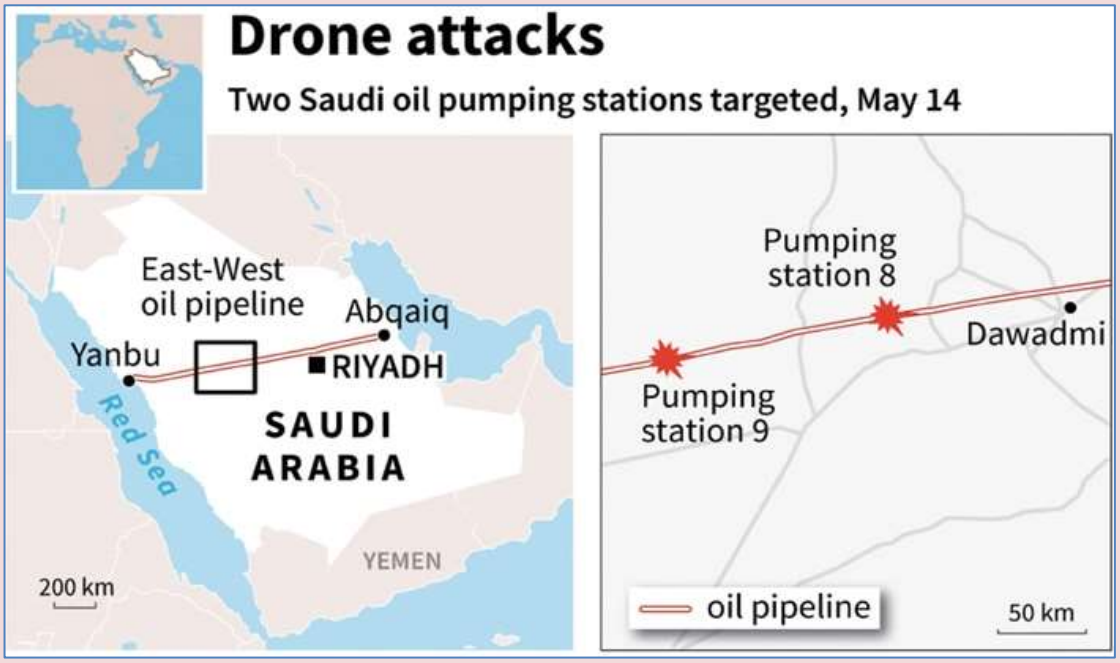
Oil prices jump as Saudi energy minister reports drone 'terrorism' against pipeline infrastructure

Source: https://www.cnbc.com/2019/05/14/oil-jumps-as-saudi-energy-minister-reports-drone-terrorism-against-pipeline.html

May 14 – Oil prices rose sharply Tuesday morning on reports of a drone attack at oil pumping stations in Saudi Arabia.

The incident is an "act of terrorism," Saudi Energy Minister Khalid al-Falih said according to the Saudi state news agency SPA, describing attacks on two oil pumping stations near Riyadh for the country's East-West pipeline carried out with bomb-laden drones.

Brent crude futures were up 1.7% at $71.39 a barrel. U.S. West Texas Intermediate (WTI) crude futures settled at $61.86 per barrel, up 1.2%.



The fire has since been contained, according to the SPA. Al-Falih asserted that oil production was not interrupted. State oil company Saudi Aramco said that its oil and gas supplies to Europe have not been affected, and that no one was injured.

"This act of terrorism and sabotage in addition to recent acts in the Arabian Gulf do not only target the Kingdom but also the security of world oil supplies and the global economy," the SPA described al-Falih as saying.pected that

No one has yet been directly accused of carrying out the attack, but a Yemeni Houthi-run TV channel announced on Tuesday morning it had launched drone attacks on several Saudi installations.

The channel Masirah TV, citing a Houthi military official, reported that "seven drones carried out attacks on vital Saudi installations."

Al-Falih, according to the SPA statement, said: "These attacks prove again that it is important for us to face terrorist entities, including the Houthi militias in Yemen that are backed by Iran."

Yemen's Houthi rebels, who are supported by Iran, have been fighting Saudi Arabia in their country since the kingdom launched an offensive against it in early 2015 in defense of its internationally-recognized government, which the Houthis had overthrown. The more than four-year long conflict has been deemed by the UN as the world's worst humanitarian crisis.

'Sabotage attacks' and tensions with Iran

Saudi Arabia's main stock index, the Tadawul, was down 3.8%.

The exchange, which joined the MSCI emerging markets index this year as part of the country's economic diversification agenda, dropped 2.7% on Monday on government reports that two Saudi oil tankers were among four vessels targeted in an unspecified "sabotage attack" off the United Arab Emirates coast of Fujeirah.

Fears over potential for accidental conflict

The series of incidents have ramped up tensions in the oil-rich region, where the reported sabotage attack on the commercial vessels Sunday has spiked fears of possible conflict with regional rival Iran. The escalation could threaten the Strait of Hormuz, a critical choke point for some 30% of the world's seaborne oil.

The news also follows a week of increasingly provocative language exchanged between Washington and Tehran.

Citing "very real" threats coming from Iran, but withholding specific details, Secretary of State Mike Pompeo emphasized during an interview with CNBC on Sunday that all options — military and otherwise — were on the table in case Iran "makes a bad decision."

Tehran announced last week that it would return to higher levels of uranium enrichment, breaching the 2015 Iranian nuclear deal, if Europe did not protect it from the impact of U.S. sanctions, which have crippled Iran's economy.

This followed the White House pushing news of a U.S. strike group carrier in the Gulf to send an "unmistakable" message to Iran. Although the ship was on a routine deployment, the administration's announcement signaled its preparedness for confrontation.

With the growing volume of military hardware occupying the Persian Gulf, analysts and foreign officials fear a miscalculation or misunderstanding could spark a serious conflict.

British Foreign Minister Jeremy Hunt told reporters on Monday: "We are very worried about the risk of a conflict happening by accident with an escalation that is unintended."

Bomb-carrying drone from Yemen rebels targets Saudi airport

Source: https://www.marketwatch.com/story/bomb-carrying-drone-from-yemen-rebels-targets-saudi-airport-2019-05-21

Illustrative: The remains of an Iranian Qasef-1 Unmanned Aerial Vehicle, used as a one-way attack UAV to dive on targets and then detonating its warhead, which was fired by Yemen's Iran-backed Houthi rebels into Saudi Arabia, according to then-US ambassador to the UN Nikki Haley during a press briefing at Joint Base Anacostia-Bolling, December 14, 2017, in Washington. (AP Photo/Cliff Owen)

May 21 – Yemen's Iranian-allied Houthi rebels said Tuesday they attacked a Saudi airport and military base with a bomb-laden drone, an assault acknowledged by the kingdom as Mideast tensions remain high between Tehran and the United States. There were no immediate reports of injuries or damage.

The attack on the Saudi city of Najran came after Iran announced it has quadrupled its uranium-enrichment production capacity, though still a level far lower than needed for atomic weapons, a year after the U.S. withdrew from its nuclear deal with world powers.

Underlining the tensions, Iranian President Hassan Rouhani is seeking expanded executive powers to better deal with "economic war" triggered by the Trump's administration's renewal and escalation of sanctions targeting the Islamic Republic, the state-run IRNA news agency reported Tuesday.

By increasing production, Iran soon will exceed the stockpile limitations set by the nuclear accord. Tehran has set a July 7 deadline for Europe to set new terms for the deal, or it will enrich closer to weapons-grade levels in a Middle East already on edge. The U.S. has deployed bombers and an aircraft carrier to the Persian Gulf over still-unspecified threats from Iran.

In the drone attack, the Houthis' Al-Masirah satellite news channel said early Tuesday they targeted the airport in Najran with a Qasef-2K drone, striking an "arms depot." Najran, 840 kilometers (525 miles) southwest of Riyadh, lies on the Saudi-Yemen border and has repeatedly been targeted by the Iran-allied Houthis.

A statement earlier on the state-run Saudi Press Agency quoted Saudi-led coalition spokesman Col. Turki al-Maliki as saying the Houthis "had tried to target" a civilian site in Najran, without elaborating.

Al-Maliki warned there would be a "strong deterrent" to such attacks and described the Houthis as the "terrorist militias of Iran." Similar Houthi attacks in the past have sparked rounds of Saudi-led airstrikes on Yemen, which have been widely criticized internationally for killing civilians.

Civilian airports throughout the Middle East often host military bases.

The New York Times last year reported that American intelligence analysts were based in Najran, assisting the Saudis and a U.S. Army Green Berets deployment on the border. Lt. Col. Earl Brown, a spokesman for U.S. Central Command, said there were "no U.S. personnel involved nor present at Najran" at the time of the attack.

Last week, the Houthis launched a coordinated drone attack on a Saudi oil pipeline amid heightened tensions between Iran and the U.S. Earlier this month, officials in the United Arab Emirates alleged that four oil tankers were sabotaged and U.S. diplomats relayed a warning that commercial airlines could be misidentified by Iran and attacked, something dismissed by Tehran.

In its nuclear program announcement Monday night, Iranian officials made a point to stress that the uranium would be enriched only to the 3.67% limit set under the 2015 nuclear deal with world powers, making it usable for a power plant but far below what's needed for an atomic weapon.

Iran said it had informed the International Atomic Energy Agency of the development. The Vienna-based U.N. nuclear watchdog did not respond to a request for comment. Tehran long has insisted it does not seek nuclear weapons, though the West fears its program could allow it to build them.

President Donald Trump, who campaigned on a promise to pull the U.S. from the Iran deal, has engaged in alternating tough talk with more conciliatory statements —a strategy he says is aimed at keeping Iran guessing at the administration's intentions. Trump also has said he hopes Iran calls him and engages in negotiations.

But while Trump's approach of flattery and threats has become a hallmark of his foreign policy, the risks have only grown in dealing with Iran, where mistrust between Tehran and Washington stretches four decades. While both sides say they don't seek war, many worry any miscalculation could spiral out of control. A Trump tweet Monday warning Iran would face its "official end" if it threatened the U.S. drew sharp rebuke from Iranian Foreign Minister Mohammad Javad Zarif on Twitter, who used the hashtag #NeverThreatenAnIranian.

In Iran, it remains unclear what powers Rouhani seeks. In Iran's 1980s war with Iraq, a wartime supreme council was able to bypass other branches to make decisions regarding the economy and the war.

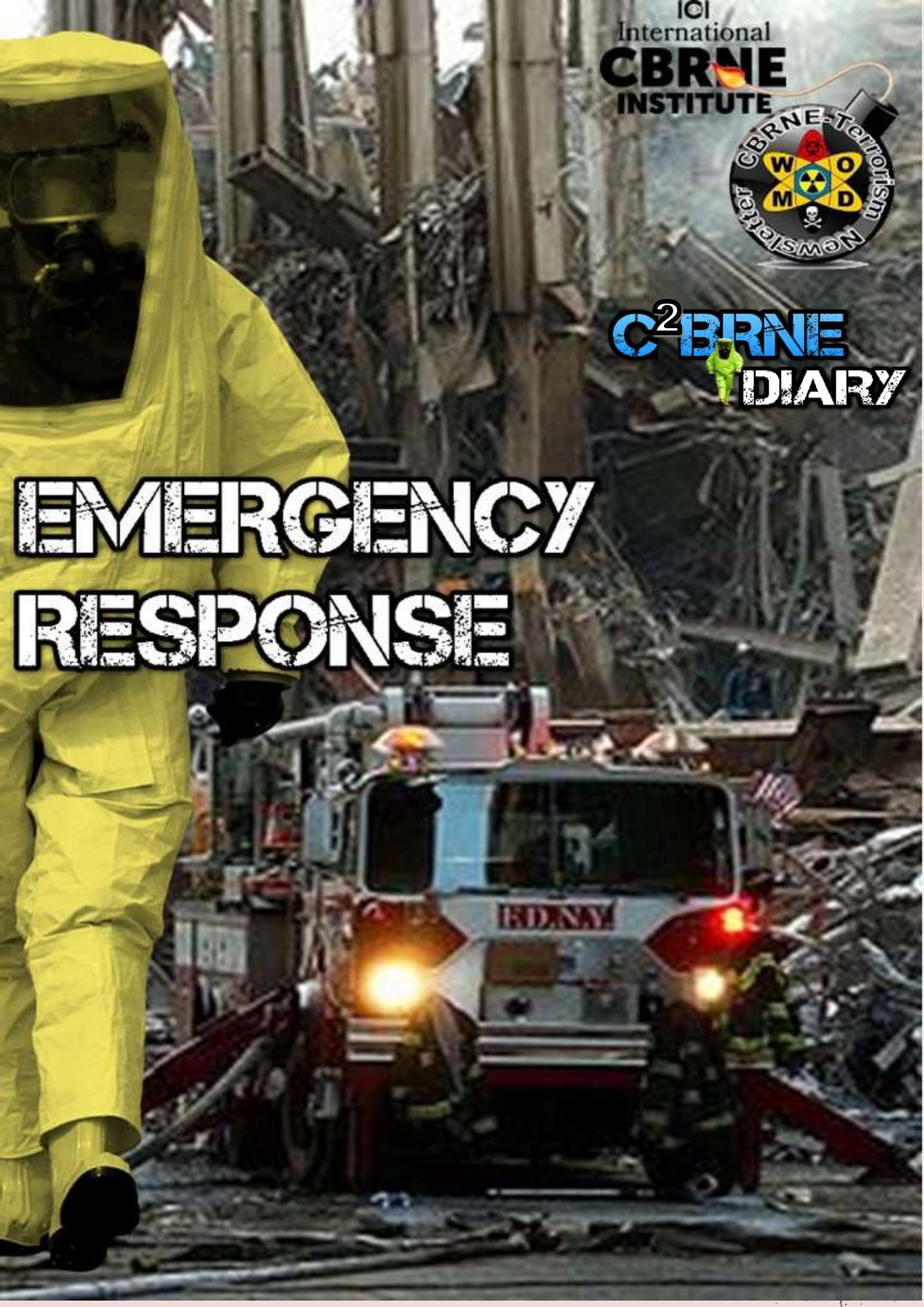
"Today, we need such powers," Rouhani said, according to IRNA. He added that country "is united that we should resist the U.S. and the sanctions."

Meanwhile, former U.S. Secretary of Defense Jim Mattis told an audience in the United Arab Emirates on Monday night that America "needs to engage more in the world and intervene

militarily less." While "Iran's behavior must change," he urged the U.S. not to engage in unilateral action and that American "military must work to buy time for diplomats to work their magic."

"I will assure you no nation will be more honest with you than America," the retired Marine Corps general said, according to a report in the state-linked newspaper The National. "America will frustrate you at times because of its form of government, but the UAE and America will always find their way back to common ground, on that I have no doubt."

Mattis abruptly resigned in December after clashing with Trump over withdrawing troops in Syria. He spoke at a previously unannounced speech before a Ramadan lecture series in honor of Abu Dhabi's powerful crown prince, Sheikh Mohammed bin Zayed Al Nahyan.


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

How FEMA Could Lose America's Next Great War

Lucie, Quinton. "How FEMA Could Lose America's Next Great War." Homeland Security Affairs 15, Article 1 (May 2019).
Source: https://www.hsaj.org/articles/15017

The United States lacks a comprehensive strategy and supporting programs to support and defend the population of the United States during times of war and to mobilize, sustain and expand its defense industrial base while under attack from a peer or near- peer adversary. These legacy programs were disbanded and broken up over 25 years ago, and without a reinvestment in these activities by the Federal Emergency Management Agency (FEMA) and the Department of Homeland Security (DHS), America risks losing its next great war. FEMA is currently responsible for advising the President on the coordination, mobilization, and sustainment of the U.S. industrial and manpower base in times of war, and to protect and assist in the recovery of its population from enemy attacks. Developing a framework based around Civil Defense, the mobilization and sustainment of the nation's manpower and defense industrial base, protecting and sustaining its morale and political institutions, and support to the Department of Defense (DOD) efforts to deploy forces overseas while contested domestically by its adversaries, may provide a way to shape future preparedness efforts and a taxonomy to organize them. This nation's failure to do so may end its next great war before it even begins.


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

Scaling the levels of war: The strategic major and the future of multi-domain operaions

By Heather Venable and Jared R. Donnelly

Source: https://warontherocks.com/2019/05/scaling-the-levels-of-war-the-strategic-major-and-the-future-of-multi-domain-operations/

May 10 – It takes less than 24 hours after a *Game of Thrones* episode airs before the armchair emerge, eagerly dissecting the show's latest events, including failures of strategic thinking. Yet those same military professionals often begin at the tactical level when contemplating future warfare, as is the case for the solution *du jour* — multi-domain operations, which began as the more tactically-focused multi-domain battle. Although this shift up the levels of war represents a step in the right direction, some commentators disagree. By contrast, we suggest the need for a more strategic approach to multi-domain operations at a moment when it seems the United States struggles to develop a strategy for global competition.

In many ways, multi-domain operations represent a more sophisticated conceptualization of joint operations, but it is also context agnostic in that it is not meant to be a response to a specific strategic challenge. In late 2011, then chairman of the Joint Chiefs of Staff, Gen. Martin Dempsey, asked the Military Education Coordination Council "What's after joint?" Concerned that joint warfare, the backbone of how the U.S. military fights, might no longer be enough in the face of dramatic technological change, Dempsey asked this group of military educators how the United States would fight in a future where its traditional dominance on land, sea, and in the air might no longer suffice. The answer was slow in coming, but many suggest that war will need to be fought simultaneously across traditional warfighting environments as well as space and the electromagnetic spectrum. The concept is still nascent and the services have only recently begun exploring combining their individual efforts on multi-domain operations. Yet momentum is building as the concept spreads throughout the U.S. military. It now appears that multi-domain operations will change how the U.S. military fights at the operational level of war if it can overcome several significant challenges to enable the services to cooperate more seamlessly.

A recent *War on the Rocks* article by Maj Gen. (ret.) Robert H. Scales — certainly no armchair general — challenges the direction in which multi-domain operations are going, arguing that they should be more tactical in focus. Scales appears to be skeptical of this concept and clearly finds the rhetoric overblown. But, far from representing a "flurry of self-congratulatory prose," as Scales contends, *The U.S. Army in Multi-Domain Operations 2028* — one of the most

recent articulations of the concept — promises no easy answers. Nor does the U.S. Air Force, which has even established a new career field to tackle the "wicked-hard" problem of multi-domain operations. The tone of *Army in Multi-Domain Operations in 2028*particularly represents a major departure from much of the previously unrealistic rhetoric that has characterized multi-domain operations' supporters, noting that in a war against an opponent equipped with nuclear weapons it is an "unlikely expectation to hope for a vanquished opponent." Scales furthermore takes *Army in Multi-Domain Operations in 2028* to task for being a "slogan" rather than a doctrine. This is somewhat unfair, as from the first page it acknowledges it is attempting to take the "first step in doctrinal evolution."

The thesis of multi-domain operations presented in Scales' article maintains that "emerging technologies have added new dimensions to the traditional combined and joint layers of warfare: artillery, infantry, armor and air power." These developments center largely on the electromagnetic, space, cyber, and information domains.

Scales, by contrast, challenges these relationships by putting infantry and "tactical art" at the tip of the spear and everything else in a support role. This represents his true challenge to multi-domain operations, and that is where he gets it wrong. What the Army proclaims is the "central idea" of multi-domain operations is the "rapid and continuous integration of all domains of warfare" in the context of the challenges of "layered stand-off" posed by adversaries. Scales might be viewing future challenges through a lens honed by his participation in the Close Combat Lethality Task Force, which focuses on leveraging technology to create the best small unit maneuver forces possible. As a result, the retired artilleryman has enthroned a new "king of battle": infantry, with the assumption being that small units of close combat infantry will have enough battlespace awareness to run the operation. Although it is unclear how infantry will penetrate through layered stand-off, the author envisions it operating – indeed orchestrating – all domains of warfare. This infantry-centric approach removes the principal of combined arms warfare that long has been essential to how the Army wages war. Furthermore, this setup would neglect the complex and extremely challenging task of synchronizing effects in other domains at the tactical and operational levels to enable the infantry's maneuver.

Scales' focus on tactical maneuver, also moves "[t]raditional supporting enablers such as fires, intelligence, [and] medical aid" further back on the battlefield. Indeed, these tactical units – i.e. infantry – will be required to "increasingly fend for themselves." Their principle purpose, though, is not primarily to "win the close fight." Rather, their main job is to "work as human sensors, decisional 'gatekeepers,' and facilitators responsible for translating killing power residing at a distance into killing effects on the enemy." Because technology such as F-35s and tanks are on the verge of obsolescence, according to this argument, the infantry is left with a "fires app" from which they can rapidly acquire "precision mortars, precision grenade launchers, and immediate access to cheap, proliferated precision delivered from artillery and aircraft."

Scales envisions these units being protected by an undefined "cone of impunity" and "surrounded by a constellation of unmanned vehicles" as they communicate with higher headquarters via applications similar to Facebook and Twitter. What is missing is an understanding of the extreme vulnerability of these units via the electromagnetic spectrum. U.S. soldiers and their unmanned vehicles will be emitting signatures that cannot be hidden; the more these troops and their unmanned aerial vehicles communicate the easier they are to target. American adversaries have demonstrated the capability to track electromagnetic signatures and exploit them with devastating effect. The military's reliance on the electromagnetic spectrum is significant and growing, as demonstrated in some of the technologies being developed in the Close Combat Lethality Task Force, yet the military's understanding of the accompanying risks is lagging. The only way for such a well-connected unit to arise is if the United States first gains electromagnetic superiority. The reality is the U.S. military will likely be forced to fight in a communications degraded environment. Mission command, coupled with secure communication limited to only the most essential information, will play an integral role in multi-domain operations conducted in a contested, degraded, and operationally limited environment.

Multi-domain operations, at the core, recognize the six domains the military operates in – the electromagnetic spectrum, space, air, land, maritime, and the human domain – and the vulnerabilities and opportunities that exist in each. They call for a holistic understanding of these domains and the synchronization of effects in two or more domains towards mission

objectives. Because of advances in technology in every domain, war has become even more complex. As a result, the established paradigms of combined arms and joint warfare alone are not enough to deal with this complexity.

This is also where a strategic perspective is essential. Indeed, despite Scales' emphasis on the tactical, he does acknowledge that good tactics cannot overcome bad strategy. And one of the most compelling elements of this concept may be the least appreciated and understood. Multi-domain operations forces planners and commanders to think higher in the levels of war because it requires the synchronization of effects far outside their component, service, and domain. The capabilities that provide multi-domain effects reside throughout the instruments of national power, within the private sector, as well as within coalition partner instruments of national power. Therefore, all future multi-domain strategies should be built with the coordination of all of the services and government agencies.

This requires a strategic perspective that is challenging to acquire. As Jeff Reilly explains, strategic design's focus goes far beyond a region or joint operations area. The primary reason for this geographical spread is that the problem and/or solution may exist far outside the confines of a distinct region or area of operations. Strategists must be able to recognize global system linkages, understand the effective use of the national instruments of power, and evaluate actions that impact the long-term attainment and preservation of national security interests.

For example, a multi-domain operation where the objective is to disrupt an adversary's command-and-control network could combine synchronized actions in the electromagnetic, air, land, sea, space, and human domains, which would require a host of entities to work together at a very high level. A cyber-attack on the adversary's power grid, using access points developed months in advance, might require assets from the National Security Agency. Space assets that maneuver to be co-orbital with enemy communication satellites and disrupt their signals would need to be coordinated at the highest levels of the Department of Defense with Space Command and possibly civilian agencies. Naval underwater unmanned vehicles could be used to cut or degrade sea cables connecting the mainland with nearby islands containing early warning radars. Air Force F-35s could be used to slip through the gaps in the enemy's radar coverage to strike elements of their integrated air defense system on the mainland, enabling fourth-generation fighters to perform strikes on command-and-control centers. Special Forces elements on the ground could sow confusion throughout the local defense by targeting the enemy's tactical communications. Each of these actions are significant efforts on their own. The coordination required to ensure that each action occurs at the right time and delivers the desired effect would be herculean in the current decision-making structure – not to mention the authorities an operation like this would require. Such an operation would require the strategic vision to leverage capabilities across domains and throughout the government. This is why each service cannot have its own version of multi-domain; the employment of service-centric concepts to a whole-of-government problem will fail. That is how multi-domain operations answer Dempsey's query "What's after joint?" and that is where a tactically focused approach to how the United States will fight and win a future near-peer conflict falls short.

While the technological and logistical challenges of small unit maneuver on the future battlefield are significant, the U.S. military has a tendency to focus on the tactical as quickly as possible. This is understandable, for many senior leaders had their formative experiences at the tactical level as captains and lieutenants. They are most comfortable in the cockpit, in the battalion tactical operations center, or on the bridge of the frigate. When faced with the extremely challenging problem of fighting a near-peer conflict in an anti-access/area denial environment, solving the tactical level of war is easier than providing solutions at the operational and the strategic levels. Yet, that is where the United States must get it right. The United States has plenty of recent experience in achieving tactical and even operational success in wars that were strategic blunders. Those experiences were costly enough; a bad strategy in a near-peer fight could have catastrophic consequences, and yet recent commentators have questioned the extent to which even the *National Defense Strategy* constitutes a real strategy.

Tomorrow's battlefield may look quite different to the 18-year-old with a rifle, but Scales' vision of an extremely well-connected soldier with a host of capabilities at their fingertips and a constellation of drones ready to do their bidding cannot become reality without a complete understanding of how the warfighting domains interact and well-executed multi-domain operations. And

meet national aims at the strategic level. Let's get strategy right first to understand fully how to fight in a multi-domain environment.

***Heather Venable, PhD**, is an assistant professor of military and security studies at the U.S. Air Force's Air Command and Staff College and teaches in the Department of Airpower. She has written a forthcoming book entitled* How the Few Became the Proud: Crafting the Marine Corps Mystique, 1874-1918.
***Jared R. Donnelly, PhD**, is an assistant professor of military and security studies in the Multi Domain Operational Strategists concentration at the U.S. Air Force's Air Command and Staff College.*