2 CBRNE DIARY

Dedicated to Global First Responders

CBRNE-Terrorism Newsletter

September 2019

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

DIRTY R-NEWS

HBO hit 'Chernobyl' spread myths about nuclear power, says UAE expert

Source: https://www.thenational.ae/uae/hbo-hit-chernobyl-spread-myths-about-nuclear-power-says-uae-expert-1.908329

Sep 09 – Delegates at the World Energy Congress say more needs to be done to inform public of environmental benefits

The nuclear power industry has been urged to do a better job of promoting itself after public fears about the energy source were fuelled by the hit HBO series *Chernobyl*.

Mohamed Al Hammadi, chief executive of the Emirates Nuclear Energy Corporation, said the mini-series, which catalogued a series of mistakes leading to the tragic 1986 nuclear plant meltdown and the devastating aftermath, had spread "myths" about nuclear power.

He said assertive public information campaigns were needed to educate people about the benefits of nuclear power, revealing that Enec had launched its own successful PR drive after the 2011 Fukushima disaster.

Despite the reputation of nuclear power generally taking a hit after the Japanese accident, Mr Al Hammadi said that in the UAE, which is building its first nuclear plant, outlook on nuclear energy had been improved on the back of the organisation's efforts.

"Recently, HBO published a mini-series," Mr Al Hammadi said. "From a public viewership, it had more [viewers] than *Game of Thrones,* which is one of the most popular TV shows. It had a lot of myths, and none fact-based stories about what happened in Chernobyl. That needs public education … that this is a safe, clean reliable, abundant source of energy."

On Monday, at a panel discussion at the World Energy Congress about the future of nuclear energy, a string of experts cited public opinion as the major barrier to the further development of new reactors. An impromptu audience poll found that more than half believed public acceptance was the main barrier to development of nuclear power, after they were presented with five options which included factors such as cost and the length of time it takes for projects to be built.

Industry experts insisted that nuclear should be seen as a vital clean resource which would be key to fighting climate change. However, in many countries it remains highly controversial, with opponents citing the creation of radioactive waste and the potential for a disaster if something goes wrong.

Mr Al Hammadi told how he had convinced his own environmentally-conscious 17-year-old daughter of the merits of nuclear after he informed her of its benefits in reducing emissions.

"[I said] imagine a solution that will be environmentally clean, an abundant source of energy," he said. "That's what your father is doing, working on a project that will

eliminate 20 million tonnes of CO2 emissions on an annual basis.

"She said that's an even greater solution than what she's thinking about, about not buying plastic bags. That was her mission in life.

"We have a young generation very interested in trying to save the world and sustainability. I see a golden opportunity for our technology to be marketed, and put in the right position, for a younger generation."

Mr Al Hammadi has led the project to build Al Barakah Nuclear Power Plant since 2008, which is now close to completion. He told how the project had survived the financial crisis, due to the UAE government's commitment to it, as well as the Fukushima disaster which led to other administrations abandoning or curtailing their civilian nuclear programmes.

He said he had been abroad when the Japanese disaster happened, but quickly launched a PR campaign which ensured the public remained supportive.

"We checked, and in the Arabic language, if you go on Google at that time, search nuclear, it's all about not civilian use of nuclear, but bombs, war happening, and all that," he said.

"So we said that's an opportunity for us. Why don't we translate the facts and the science, and everyone is interested to listen. We put that for the public, a couple of days later, I was on TV talking about hard, scientific facts.

"We got a lot of attention from the Arab world, not just the UAE. We went from 67, 68, per cent of public acceptance, to around 82, because we saw it as an opportunity to educate the public. With nuclear technology we cannot sit back and say, 'the public is not accepting it and we don't have an option'."

Other panelists backed Mr Al Hammadi's call for more effective promotional campaigns.

Xavier Ursat, executive director of energy giant EDF, said that France had successfully overcome public opposition to a major nuclear energy programme in the 1970s and '80s.

"The biggest fight we have in front of us is against climate change," he said. "And we are not winning the battle. We need to decarbonise our economies and we need low carbon electricity. There are two ways to produce low carbon electricity, renewables and nuclear.

"One issue is public acceptance. It's not easy to speak about nuclear. Everyone can feel the wind on their face, see the water dropping, feel the sun. But what is nuclear? It is difficult to understand.

"We have to work together, very carefully, on the way we speak about nuclear. We have a brilliant explanation about nuclear, but most of the time, you need to have a degree in physics or mathematics. We do not speak to the heart of people, we speak to their brain.

"Most of the time, in public debates, the media field, the political field, we are dealing with nuclear as if it was a religion or ideology. We need to show people who work in nuclear, it needs to have a visible face, not any more this mysterious energy that people don't know how it is produced."

Chinese nuclear forces, 2019

By Hans M. Kristensen and Matt Korda, June 30, 2019

Source: https://thebulletin.org/2019/06/chinese-nuclear-forces-2019/

A Chinese intercontinental ballistic missile at a 2015 military parade in Beijing. China may be a source for other governments wishing to buy missiles. (Photo credit: Voice of America via Wikimedia Commons.)

The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Matt Korda, a research associate with the project. The Nuclear Notebook column has been published in the *Bulletin of the Atomic Scientists* since 1987.

This issue's column examines China's nuclear arsenal, which includes about 290 warheads for delivery by ballistic missiles and bombers. This stockpile is likely to grow further over the

next decade, and we estimate that China will soon surpass France as the world's third-largest nuclear-armed state.

China's nuclear arsenal includes about 290 warheads for delivery by ballistic missiles and bombers and is likely to grow over the next decade,

▶▶ **Read more:** Chinese nuclear forces, 2019 | Nuclear arsenals of the world

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 research associate for the Nuclear Information Project at the Federation of American Scientists. Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Korda received his MA in International Peace & Security from the Department of War Studies at King's College London, where he subsequently worked as a research assistant on nuclear deterrence and strategic stability. He also completed an internship with the Verification, Training and Information Centre (VERTIC) in London, where he focused on nuclear security and safeguards. His research interests and recent publications focus on nuclear deterrence, missile proliferation, gender mainstreaming, and alliance management, with regional concentrations on Russia and the Korean Peninsula.*

Why India wants to break its decades-old nuclear pledge

Source: https://www.bbc.com/news/world-asia-india-49354185

Aug 22 – India's defence minister recently suggested that the country may re-evaluate its "no first use of nuclear weapons" doctrine, raising the stakes at a time of high tension with its nuclear-armed neighbour Pakistan. Analysts Christopher Clary and Vipin Narang examine the implications for peace and security in South Asia.

Defence Minister Rajnath Singh recently reaffirmed a long-standing tenet of India's nuclear weapons doctrine: that it would not be the

first to use the devastating weapons in a conflict. But he subsequently questioned how much longer that commitment would remain. He told the media that while India had "strictly adhered to" the doctrine thus far "what happens in future depends on the circumstances".

He was signalling that India's "no first use" commitment is neither absolute nor permanent, and implying that in a conflict, nothing would compel India to abide by it. His statement came after India revoked the special constitutional status of the part of Kashmir it controls - prompting a furious reaction from Pakistan, which, like India, claims the entire territory.

These were not off-the-cuff remarks. Mr Singh was speaking at Pokhran, the site of India's nuclear weapons tests in the late 1990s. He tweeted the seemingly scripted remark from his official account and the government's Press Information Bureau put out a press release quoting the statement.

As such, it was the most official signal to date that India's "no first use" doctrine might give way to something more ambiguous. The implication was that one day India might decide that it would have to use nuclear weapons first to safeguard its security.

What is the 'no first use' doctrine?

During the Cold War, the US, the Soviet Union, France, and the United Kingdom all reserved the right to use nuclear weapons first in a severe conflict. There were two classical scenarios for first use:

(1) that a country in danger of conventional military defeat on the battlefield would employ so-called tactical nuclear weapons against adversary military forces to forestall that defeat, or

(2) that a country fearing an adversary would attack it with nuclear weapons would pre-empt that attack with a nuclear first strike designed to destroy as much of the adversary's nuclear arsenal as possible.

When India announced its nuclear status with weapons tests in 1998, it rejected the idea of "nuclear war fighting". It would design its nuclear forces for "retaliation only" and as a consequence, it said, it could have a more limited arsenal.

India joined China in offering a no first use doctrine.

When China first tested nuclear weapons in 1964, it declared it would "never at any time and under any circumstances be the first to use nuclear weapons". The fact that India never fully believed China's commitment was one ironic reason behind India's own decision to overtly test nuclear weapons in 1998.

Except for China, no other country besides India currently offers a no first use declaration.

North Korea at one point floated one, but few believed it, given that Pyongyang's stated motivation to pursue nuclear weapons included defeating a combined South Korean and American invasion through nuclear first use.

While periodically the US has considered the wisdom of a no first use pledge as a means to lower Russian and Chinese fears in a hypothetical crisis, and as part of a general commitment to reducing the political salience of nuclear weapons, it has refused to do so to date.

India's most likely adversary, Pakistan, explicitly preserves the right to use nuclear weapons first. It has threatened to use battlefield nuclear weapons to forestall a conventional military defeat at the hands of the Indian army - a deterrent threat that has so far constrained India's ability to retaliate to a stream of terrorist and militant violence in India that Delhi has blamed on Islamabad.

Why is India reconsidering no first use now?

Mr Singh's statement was hardly the first sign of internal debate about the wisdom of the two decade-old policy, but coming from a sitting defence minister it was the most authoritative signal to date.

Shortly after India tested nuclear weapons in May 1998, senior Indian officials declared India would follow a no-first-use doctrine.

In 2003, India revised that commitment in releasing a revised official doctrine that explicitly maintained the option to retaliate with nuclear weapons in the event of a chemical or biological weapons attack. While many noted that India's move to "no first use of weapons of mass destruction" was a less expansive commitment than it had originally made, it was not regarded as a major shift.

In 2016, India's then-defence minister Manohar Parrikar wondered why India should "bind" itself by declaring no-first-use. Better, Mr Parrikar argued, for adversaries not to know

what India might do, though he subsequently clarified that these were only his personal views. Mr Singh, by contrast, has made no such clarification.

Meanwhile, India began developing the technological elements that might make first use attractive as a means to disarm an adversary.

In 1998, India had only a handful of ballistic missiles, limited intelligence capabilities, and a modest set of precise conventional air-dropped munitions. Today, it has a much wider array of ballistic and cruise missiles, several space-based imagery satellites as well as similar sensors aboard manned and unmanned aircraft, and a growing range of precision-guided munitions, many of them capable of being launched at targets some distance away.

Additionally, India has invested in developing indigenous ballistic missile defences and acquiring expensive Russian- and Israeli-origin missile defence systems, which could theoretically be used to intercept any "residual" forces that the pre-emptive first strike failed to destroy.

While unlikely, it is no longer impossible to imagine a leader in Delhi concluding that with concerted effort, India might be able to pre-empt any first strike by an adversary and meaningfully limit the damage to Indian cities by doing so.

Why does this matter?

Mr Singh stressed that "India attaining the status of a responsible nuclear nation is a matter of national pride". Part of that reputation was built through careful messaging about Indian restraint and the choices it could have taken but did not.

Now critics, such as retired Lt Gen Prakash Menon, argue that abandoning that high-ground "taints India's image as a responsible nuclear power". The Pakistani state, somewhat unhinged in recent rhetoric emanating from the office of Prime Minister Imran Khan, has taken to questioning "the safety and security of India's nuclear arsenal in the control of the fascist, racist Hindu supremacist [Prime Minister] Modi".

The real impact of India's eroding no first use pledge will not be in the realm of symbolism or rhetoric, however. Rather, it will be in Pakistan's material response. Pakistan's nuclear stewards have stressed privately in the last week that they never believed India anyway - but this rhetoric shift, combined with growing Indian capabilities, will heighten Pakistani interest in making more nuclear weapons, dispersing them in a crisis, and using those weapons before India can destroy them on the ground.

The nuclear option will be on the table much quicker during a time of crisis, and Pakistan's peacetime posture may have to be prepared for more rapid use.

The net effect on safety and security, accidents and potential misunderstandings will not be clearly understood for some time, but it's likely that South Asia will be unable to fully avoid the costly and dangerous arms races that characterised the Cold War competition.

__Christopher Clary__ is an assistant professor of political science at the University at Albany, State University of New York. Vipin Narang is an associate professor of political science at the Massachusetts Institute of Technology and a member of MIT's Security Studies Program.

Data May Point to Second Blast at Russian Test Site

Source: http://www.homelandsecuritynewswire.com/dr20190823-data-may-point-to-second-blast-at-russian-test-site

Aug 23 – Researchers at a Norwegian institute believe that there may have been two explosions, not one, at the Russian naval test site on the White Sea earlier this month, an incident that killed at least five people and raised new questions about Russia's weapons research.

The conclusions were published on August 14 by the Norsar Research Institute, based on seismographic and acoustic readings taken the day of the deadly incident, but had gone largely unnoticed.

Anne Lycke, the institute's chief executive, told RFE/RL in an interview on August 23 that the institute's monitoring stations first detected seismographic readings on August 8 at around 9 a.m. local time in Arkhangelsk, a major city on the White Sea.

The readings, she said, pointed to an explosion that occurred somewhere close to the Earth's surface, either on ground or on water.

Around two hours later, at 11 a.m., a different sensor designed to pick up infrasound, or low-frequency sound, registered another, different acoustic event, Lycke said.
Researchers concluded that that was likely an explosion that occurred in the air, some height above the ground, she said.
"Yes, it appears that two explosions took place, based on our findings," Lycke said.
The institute's findings, which were first reported by the newspaper Afternposten on August 22, add to a growing body of publicly available evidence about the August 8 incident that took place at the Nyonoksa naval test site, a range on the White Sea that has been used for decades by Soviet and Russian military planners.

Contradictory Information
Russian authorities have released scattered and sometimes contradictory information about the mishap, which has added to anger among Russians about what exactly happened and whether there was any danger.
The Defense Ministry revealed the incident the same day it happened, saying two people had been killed, but gave no details. Two days later, the state-run nuclear agency Rosatom revealed that five of its scientists had been killed while they were conducting "technical-engineering oversight" of a test of "radioactive isotope fuel for a liquid-fueled rocket engine."
The following day, on August 11, managers at the state research institute where the five were employed revealed in a video interview that the researchers had been investigating, among other things, "the creation of small-scale sources of energy using radioactive fissile materials."
In the communities near Nyonoksa, including the cities of Severodvinsk and Arkhangelsk, many Russians have been angered by the lack of clear information from authorities. In the hours after the incident, many of Severodvinsk's pharmacies were sold out of iodine drops. Iodine is often taken in the aftermath of a nuclear incident as a way to protect the thyroid gland from radiation.
Residents of the region also took to social media to discuss radiation levels and share videos of Geiger counters registered ambient radiation levels. Local sensors initially reported a brief spike in radiation in Severodvinsk, but the information quickly disappeared from official websites.

"Important Work"
Earlier this week, at a news conference alongside Finnish Prime Minister Antti Rinne in Helsinki, Russian President Vladimir Putin was asked about the incident.
"Unfortunately, the tragedy in the White Sea took the lives of our experts," he said. "This is work carried out in the military sphere, work on prospective weapon systems. We are not concealing this. The people who were injured or died were performing very important work for Russia's security."
Adding to anger in the region are reports that doctors and medical staff who treated the initial victims of the explosion, which included three survivors, had no information about what the incident was exactly, and that there was a risk of radiation exposure. Doctors have complained on social media, and in interviews, that they were given no protective equipment as they treated victims.
While nearby residents have worried about whether it was safe to eat fish or berries and mushrooms, Western analysts have scrambled to figure out what exactly was being tested at Nyonoksa.
Several analysts have suggested that it may have been a nuclear-powered cruise missile dubbed the Burevestnik in Russian. That's a weapon which President Putin himself boasted was under development last year.
And U.S. President Donald Trump added to the speculation by posting a Tweet that stated outright that it was the Burevestnik, known to NATO analysts under the name Skyfall.
Other analysts said it might not be a nuclear-propelled, super-fast cruise missile, but a "radioisotope thermoelectric generator" used to generate power for a missile and its components.

"Doomsday Machine"
Still others have speculated it could be a new underwater nuclear drone — dubbed the "doomsday machine" — that is reportedly under development, or a hypersonic anti-ship missile known as the Tsirkon.

Lycke told RFE/RL that the institute's sensors detected the apparent airborne explosion, but they don't have enough data to conclude that it was caused by an exploding missile.
"We could see the explosion, but what it comes from, we can't tell," she said.
On August 15, one week after the mishap, another Norwegian facility, the Norwegian Radiation and Nuclear Safety Authority, reported tiny amounts of airborne radioactive iodine were detected by monitors, but they were unable to link the iodine to the Arkhangelsk incident.

Located in Kjeller, just northeast of the capital Oslo, the Norsar institute is independent of the government and operates sensors in six locations, including in the Finnmark region bordering Russia, and the Spitsbergen islands, near Russia's Novaya Zemlya test site on the Barents Sea.
The institute is charged with, among other things, helping to monitor compliance with the Comprehensive Test Ban Treaty, a nonbinding agreement that restricts nuclear tests worldwide.
The Norsar monitors are part of a global network of monitors that record and transmit data to the Vienna-based organization known as the Comprehensive Test Ban Treaty Organization (CTBTO), which monitors global compliance with the treaty.
Earlier this week, the organization reported that four Russian monitoring stations designed to detect radiation had stopped transmitting data in the days after the August 8 explosion.
A spokeswoman for the CTBTO declined to comment on whether the organization had received data pointing to a possible second explosion at the Arkhangelsk site.

The Unlikely Possibility of an 'American Hiroshima'

Source: https://worldview.stratfor.com/article/unlikely-possibility-american-hiroshima

2005 – The publisher of online newspaper World Net Daily alleged in an Aug. 2 interview with daily political magazine FrontPageMagazine.com that al Qaeda has nuclear weapons within the United States and is preparing to unleash an "American Hiroshima." Publisher Joseph Farah claims al Qaeda has been planning a large-scale nuclear attack for years, and that at least some of its nuclear weapons have been smuggled into the United States over the Mexican border with the help of local criminal gangs. In the same interview, however, Farah contradicted himself, claiming the devices were smuggled into American cities by the Soviet Union during the Cold War. Although it is known that al Qaeda has long been interested in acquiring or developing weapons of mass destruction (WMD), the likelihood that the network possesses functional nuclear weapons is remote. From time to time, various groups or individuals have made the assertion that al Qaeda, or groups such as Chechen militants possess nuclear weapons, possibly in the form of "briefcase nukes," compact, portable nuclear devices that supposedly were developed by the United States and the

Soviet Union during the Cold War. The premise here is that these groups have acquired nuclear weapons from Soviet-era stockpiles. Given Russia's questionable ability to maintain nuclear surety during and after the Soviet period, it would not be impossible for militant groups to have acquired such devices. Russian security sources, however, say Chechen militants and other groups lack the training to properly operate and maintain such weapons. They are, in fact, more intricate than larger missile warheads. More

importantly, because of the potentially devastating consequences, the longer the terrorists held on to such a weapon, the greater the chance it would be discovered by authorities and destroyed. In the United States, Immigration and Customs Enforcement has devoted a huge proportion of its recourses to the investigation and interdiction of WMD, even to the extent of failing to fully assess other possible threats. Detection capabilities for potential WMD have greatly improved since the Sept. 11 attacks, with detection systems installed in major U.S. cities and issued to first responders. Furthermore, the FBI's Joint Terrorism Task Force and major police departments check storage facility sites and run name checks on storage-space renters, which also helps reduce the probability of nuclear devices being assembled or stored at these sites. Although these checks are mainly an effort to interdict conventional bombs, they could easily uncover the existence of a nuclear device.

Of course, some cities are better prepared than others, with New York perhaps the most vigilant of all. Al Qaeda has often said it is engaged in an all-out war with the United States, and that any and all U.S. interests — from military personnel to civilian non-combatants — are fair game for attacks. Furthermore, al Qaeda tried to acquire a nuclear capability for many years prior to Sept. 11 — as Osama bin Laden publicly acknowledged in a Dec. 23, 1998 interview. "I would say that acquiring weapons for the defense of Muslims is a religious duty … If I have indeed acquired these weapons, then this is an obligation I carried out and I thank god for enabling us to do that ... But how we could use these weapons, if we possess them, is up to us." In light of such statements, security regarding WMD has been tightened considerably since Sept. 11 — suggesting it would have been easier to acquire such weapons before September 2001. If al Qaeda had had WMD at that time, it would have used them instead of airplanes. The idea that these devices are pre-positioned in American cities and that al Qaeda is awaiting a significant date to unleash them is simply preposterous. First, dates and anniversaries are not particularly important to al Qaeda. Second, such a weapon would be its crown jewel — and the network would never run the risk of it being discovered by leaving it hidden for long periods. Considering all the resources that would have to be expended and the risk associated with using a nuclear weapon, a terrorist group would get a much higher return from carrying out more conventional attacks, similar to the Madrid train bombings or the London Underground bombings. Farah's theory is that al Qaeda might have sub-contracted the delivery and operation of its nuclear weapons to Mara Salvatrucha criminal gangs and former Soviet KGB agents and Spetznats commandos. If al Qaeda possessed such weapons, however, they certainly would be the most valuable physical assets controlled by the network — and their operation would be closely coordinated with the core leadership, perhaps even with the direct knowledge of bin Laden. The operatives assigned to deliver and operate the weapon would be drawn from al Qaeda's most trusted inner circles, chosen for their loyalty and commitment to the cause. Because of this, custody and operation of the weapons would probably not be trusted to infidel criminal gangs and former enemies. The very existence of "briefcase nukes" also is questionable. Some have claimed that perhaps 100 such weapons from the former Soviet arsenal are unaccounted for. With so many of these devices supposedly on the loose, it is logical to assume that some trace of at least one of them would have been uncovered by either Russian, U.S., British, French, German, or Israeli intelligence. To date, this has not happened. It is important to keep in mind that these are complex devices that require a great deal of regular, careful maintenance. They do not have an indefinite shelf life. Speculation about terrorists possessing and using nuclear weapons has been making the rounds for years. Because of the exponentially increasing risk associated with holding onto a nuclear device, however, any group that possesses one would use it sooner, rather than later. If al Qaeda had a nuclear device, it would have used it by now.

The Unlikely 'Atomic Suitcase' Scenario

Source: https://worldview.stratfor.com/article/unlikely-atomic-suitcase-scenario

Self-exiled Russian tycoon Boris Berezovsky said Feb. 8 he helped foil a plot by Chechen separatists to sell an "atomic suitcase" on the international arms black market, and that the rebels have a number of nuclear weapons at their disposal. Berezovsky's claims raise serious doubts. If the Chechens had nuclear weapons to sell, it seems likely they would have used at least one in their separatist struggle against Moscow. The premise here is that the Chechens have acquired nuclear weapons from Soviet-era stockpiles. Given the questionable ability of the Russians to maintain nuclear surety during and after the Soviet period, it would not be impossible for the Chechen militants to have acquired such a device. Russian security sources, however, say the Chechens lack the training to properly operate and maintain such a weapon. Sources in the Russian Defense Ministry and other Russian government ministries deny Berezovsky's claim, though if they did have reason to believe the Chechens had nuclear weapons they would not admit it — wanting to avoid blame should the rebels actually use one. More

important, because of the potentially devastating consequences, the Russian hunt for such a weapon would be sophisticated and relentless. The longer the Chechens held on to it, the more likely it would be found — and destroyed. Berezovsky's motives for making such a claim are unclear. He is living in self-imposed exile in London and has been indicted in Russian courts on a variety of economic crimes. His political enemies in Moscow also have accused him of everything from supporting Ukrainian President Viktor Yushchenko's campaign to collaborating with the Chechens, including notorious warlord Shamil Basayev. It is possible, then, that he is attempting to curry favor with the West by telling the CIA, Britain's MI5 and British newspapers that he helped foil the atomic suitcase sale. Perhaps the most compelling evidence refuting Berezovsky's claims is the fact that the Chechen militants have not used a nuclear weapon against Russia. In just the recent past, Chechen militants have carried out devastating attacks against civilian targets in Moscow and southern Russia, including schools, theaters, hospitals and apartment complexes. They also likely blew up two Russian airliners in flight Aug. 24, 2004, killing hundreds. It seems apparent, therefore, that they would have no compunction about using a nuclear weapon. This, combined with the dangers associated with holding such a weapon in reserve, suggests the Chechens would have used it sooner rather than later.

Saudi Arabia Wants Uranium Production, Enrichment Capability for Nuclear Power Programme – Minister

Source: https://www.globalsecurity.org/wmd/library/news/saudi/saudi-190909-sputnik01.htm

Sep 09 – Earlier this year, after discovering that the Department of Energy had greenlit six authorisations to allow US companies to assist Saudi Arabia with its nuclear programme, a bipartisan group of lawmakers in the US Senate attempted to put together a bill to block Washington from providing funding for the transfer of US nuclear technology to Riyadh.

Saudi Araiba wants to achieve the capability to produce and enrich uranium for its peaceful nuclear programme, energy minister Prince Abdulaziz bin Salman has announced.

"We are proceeding with it cautiously...we are experimenting with two nuclear reactors," the minister said, speaking at a conference in Abu Dhabi in the United Arab Emirates on Monday, his remarks quoted by Reuters.

Saying his country wanted to create a full cycle nuclear programme, including uranium production and enrichment capabilities, the official made reference to Riyadh's plans to issue a tender for the kingdom's first two nuclear power reactors. The tender is expected to be made next year, with US, Chinese, Russian, South Korean and French companies thought to be involved in preliminary talks about the project, said to be worth billions of dollars.

Abdulaziz bin Salman was appointed energy minister on Sunday by royal decree, becoming the first royal ever to hold the position.

US lawmakers recently voiced concerns over Riyadh's pursuit of nuclear technology, saying US financing via the US Export-Import Bank for the transfer of nuclear technology to the kingdom should be contingent on a commitment from the Saudis not to engage in uranium enrichment.

Last month, US Secretary of Energy Rick Perry indicated that Washington would have to assist Saudi Arabia with its nuclear ambitions, since the alternative would be having "the Russians" or "the Chinese," who allegedly "have zero interest in non-proliferation," helping Riyadh. Perry promised that the US would be looking to reach a "very strong" agreement with Saudi Arabia to ensure US interests are safe-guarded.

Under US nuclear technology transfer standards adopted in 1954, recipient countries must adopt a so-called "gold standard" of regulations designed to ensure the non-proliferation of nuclear weaponry and the peaceful use of nuclear technology, complete with inspections by the UN's nuclear watchdog. Riyadh has so far refused to adopt the standard, with this factor becoming a stumbling block in negotiations.

In April, US Secretary of State Mike Pompeo warned that Washington would "never" allow Saudi Arabia to become a nuclear power, saying such a development would threaten its own security and that of Israel.

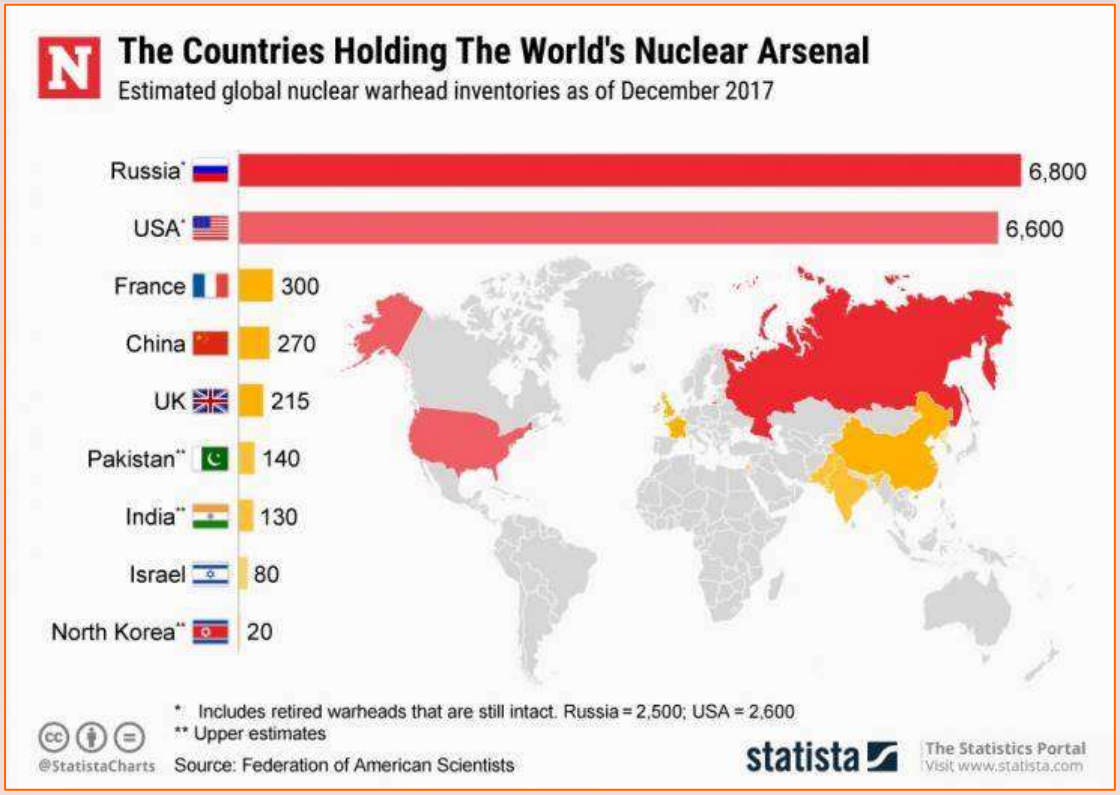
Riyadh has sought to build nuclear power plants as a means to diversify its power-generation capabilities and to move away from

dependence on fossil fuels under its "Vision 2030" programme, but has made no indication that it would seek to pursue nuclear weapons.
Earlier this year, US nuclear specialists told media that the country was close to completing the construction of its first nuclear reactor at the King Abdulaziz City for Science and Technology facility in Riyadh. According to former International Atomic Energy Agency director Robert Kelley, the 30-kilowatt research reactor would be prepared for operations within a year's time. The reactor was said to have been designed by an Argentinian company, but completed by Saudi specialists.
Along with Saudi Arabia, several other countries in the Middle East are pursuing peaceful nuclear power technology, including the United Arab Emirates, Qatar and Kuwait. The idea of countries in the region having access to nuclear technology has been frought with risks, with Israel, which is thought to have a nuclear weapons programme despite not using the technology for power generation, bombing an Iraqi nuclear reactor in 1981, and attacking and destroying a Syrian facility suspected of being a nuclear reactor in 2007. Syria dismissed claims that the facility was a 'nuclear site'. Iran, Saudi Arabia's regional rival, has its own peaceful nuclear programme, and signed a commitment guaranteeing its peaceful nature in 2015. In recent months, Tehran announced plans to increase its nuclear enrichment activities until the 2015 nuclear deal's other signatories fulfil their commitments, but has continued to maintain that it will not pursue nuclear weapons.

Turkey Has U.S. Nuclear Weapons, Now It Says It Should Be Allowed to Have Some of Its Own

Source: https://www.newsweek.com/turkey-us-nuclear-weapons-its-own-1457734

Sep 04 – Turkish President Recep Tayyip Erdogan has argued that his country should be allowed to develop nuclear weapons as other major powers have.
Addressing the Central Anatolian Economic Forum in the central province of Sivas, Erdogan lauded the expansion of the Turkish defense industry, especially recent conversations with the United States and Russia, while hinting at future talks with China. He then recalled how "some countries have missiles with nuclear warheads" and "not just one or two."
"But I cannot possess missiles with nuclear warheads? I do not accept that," Erdogan said. "Right now, nearly all the countries in the developed world have nuclear missiles."
The U.S. currently has an estimated 50 of its nuclear weapons deployed to Turkey as part of the NATO Western military alliance's nuclear sharing policy, according to an accidentally-released NATO report published in July by Belgian newspaper *De Morgen*. The weapons, located at Incirlik Base, are under U.S. control, but some have raised concerns as to their safety there amid regional instability and political differences.
In 1980, Turkey signed the Non-Proliferation Treaty (NPT) opposing nuclear weapons in the hands of countries other than "recognized powers" that include Russia, the U.S., France, the U.K. and China. Still, other powers such as India, Pakistan, North Korea and Israel were all believed to have developed and be in possession of such weapons of mass destruction.
Though a member of NATO since 1952, Turkey has strained ties with other members of the Cold War-era defense pact by shoring up relations with Russia, against whom the nuclear sharing agreement was conceived. Ankara recently defied Washington's warnings by accepting Moscow's state-of-the-art S-400 surface-to-air missile system, which the Turkish Defense Ministry said Wednesday its personnel had started training on in the Russian town of Gatchina.
President Donald Trump hit back at Turkey's acquisition in July by suspending the country's planned participation in the advanced F-35 fifth-generation fighter jet program, but Russian President Vladimir Putin responded by showing off his nation's own fifth-generation Su-57 and modernized Su-35 during Erdogan's visit last week to the International Aviation and Space Show (MAKS) at the Zhukovsky International Airport outside Moscow.
After inspecting the Su-57, Erdogan asked if it was for sale and Putin said "yes, you can buy it" as they both laughed.



A graphic depicts global nuclear weapons arsenals as estimated by the Federation of American Scientists as of December 2017. STATISTA

Turkey has continued to display interest in U.S. weapons too, however, and Erdogan also said Wednesday he would discuss buying the Patriot surface-to-air missile system — designed primarily to take out ballistic missiles, not aircraft as well, unlike the dual-use S-400 — with Trump at the upcoming United Nations General Assembly. He said, however, he would only buy the system "under the same conditions" offered to him by Russia during the S-400 purchase.

Ankara also worked alongside both Washington and Moscow in Syria, where all three nations have competing interests. Turkey has remained the last major foreign sponsor for insurgents once backed by the U.S. and a number of its regional allies in a bid to unseat Syrian President Bashar al-Assad, but has at the same time joined Assad allies Russia and Iran as part of a trilateral peace process.

Following a phone call Wednesday with White House nationals security adviser John Bolton, Turkish spokesperson Ibrahim Kalin said his country had "completed its preparations to put into action without delay" a proposed safe zone designed to allow the withdrawal of U.S.-backed Kurdish forces, some of which were designated terrorist organizations by Ankara, from the Syrian border with Turkey.

EDITOR'S COMMENT: What a surprise! Turkey is becoming a global problem and the West does not have the Bs to deal with it – see S-400; F-35; Syria; refugees and illegal immigrants' tsunami flooding Europe. And soon we will all be sorry!

Strangelove Redux: U.S. Experts Propose Having AI Control Nuclear Weapons

Source: http://www.homelandsecuritynewswire.com/dr20190904-strangelove-redux-u-s-experts-propose-having-ai-control-nuclear-weapons

Sep 04 – In an article in *War on the Rocks* titled, ominously, "America Needs a 'Dead Hand,'" U.S. deterrence experts Adam Lowther and Curtis McGiffin propose a nuclear command, control, and communications setup with some eerie similarities to the Soviet system

referenced in the title to their piece. The Dead Hand was a semiautomated system developed to launch the Soviet Union's nuclear arsenal under certain conditions, including, particularly, the loss of national leaders who could do so on their own. Given the increasing time pressure Lowther and McGiffin say US nuclear decision makers are under, "[I]t may be necessary to develop a system based on artificial intelligence, with predetermined response decisions, that detects, decides, and directs strategic forces with such speed that the attack-time compression challenge does not place the United States in an impossible position."

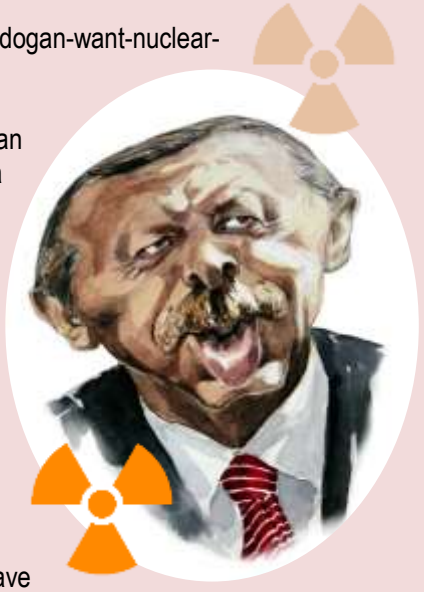
Matt Field writes in the *Bulletin of the Atomic Scientists* that we should think long and hard before considering the Dead Hand idea. History is replete with instances in which it seems, in retrospect, that nuclear war could have started were it not for some flesh-and-blood human refusing to begin Armageddon. Perhaps the most famous such hero was Stanislav Petrov, a Soviet lieutenant colonel, who was the officer on duty in charge of the Soviet Union's missile-launch detection system when it registered five inbound missiles on Sept. 26, 1983. Petrov decided the signal was in error and reported it as a false alarm. It was. Whether an artificial intelligence would have reached the same decision is, at the least, uncertain.

One of the risks of incorporating more artificial intelligence into the nuclear command, control, and communications system involves the phenomenon known as automation bias. Studies have shown that people will trust what an automated system is telling them. In one study, pilots who told researchers that they wouldn't trust an automated system that reported an engine fire unless there was corroborating evidence nonetheless did just that in simulations. (Furthermore, they told experimenters that there had in fact been corroborating information, when there hadn't.)

University of Pennsylvania political science professor and *Bulletin* columnist Michael Horowitz, who researches military innovation, counts automation bias as a strike against building an artificial intelligence-based nuclear command, control, and communications system. "A risk in a world of automation bias is that the Petrov of the future doesn't use his judgment," he says, "or that there is no Petrov," he told Field.

Why does Erdogan want nuclear weapons?

Source: https://www.al-monitor.com/pulse/originals/2019/09/turkey-why-does-erdogan-want-nuclear-weapons.html



Sep 10 – In an unprecedented move, Turkish President Recep Tayyip Erdogan declared his desire to obtain nuclear weapons, flouting Turkey's obligations as a signatory of the Non-Proliferation Treaty (NPT). Speaking at an economic forum in the central Anatolian city of Sivas Sept. 4, Erdogan praised the advancement of Turkey's defense industry and then said, "It's all fine and well, yet some countries have missiles with nuclear warheads, not one or two. But I don't have missiles with nuclear heads. This I cannot accept."

Erdogan's use of the singular first-person pronoun was, of course, meant to denote Turkey and not himself. His statement reflects his mistrust in the nuclear umbrella of NATO, to which his country belongs. Indirectly, it also indicates that he attributes no deterrent significance to the American B61 tactical nuclear weapons deployed at the Incirlik Air Base, in southern Turkey, as part of NATO's nuclear program.

In further remarks, Erdogan claimed that "all developed countries in the world" have nuclear weapons and recounted an anecdote about how the former president of an unnamed nuclear country grumbled about restrictions on him. Erdogan said, "When I was on a visit there, he told me, 'They tell us this and that, yet I have about 7,500 nuclear warheads at present, but Russia and America have 12,500 or 15,000. I, too, will make [more].'"

Signaling that he does not object to nuclear arms races, Erdogan commented, "Look at them. Look at what they are competing over. But when it comes to us, they say, 'Don't do it!'" In arguing why Turkey's acquisition of nuclear arms would be legitimate, he pointed to Israel, which is believed to be a nuclear state but maintains a policy of "nuclear ambiguity," neither confirming nor denying whether it has nuclear weapons. "There is Israel just beside us. Do

they have [nuclear weapons]? They do," he said, describing Israel's possession of nuclear arms as a tool for "bullying" the region.

As he wrapped up the topic, Erdogan made a crucial remark. "We are currently working on it," he assured the audience, suggesting that Turkey is engaged in activities to acquire a nuclear capability. If that is indeed the case, open sources are, of course, unavailable on what those activities entail and how much they have progressed.

The Turkish Foreign Ministry, meanwhile, maintains the page "Arms Control and Disarmament" on its website, which emphasizes Turkey's "active participation in international efforts in these areas, adherence to relevant international instruments and their full implementation." It lists the multilateral agreements that Turkey has joined to become part of international control regimes against the proliferation of nuclear weapons and ballistic missiles. That this ministry is bound to a president who "cannot accept" not having nuclear weapons is an inexplicable paradox.

Turkey became party to the NPT in 1979 and to the Comprehensive Test Ban Treaty in 2000. It is a founding member of the 1996 Wassenaar Arrangement on export controls of dual-use equipment and technologies, which can be used both for civilian purposes and the development of nuclear arms. In 1997, Turkey joined the Missile Technology Control Regime, which aims to prevent the proliferation of chemical, biological and nuclear-tipped ballistic missiles. Finally, Turkey has been party to The Hague Code of Conduct Against Ballistic Missile Proliferation since its inauguration in 2002.

Given this background, the question is inevitable: Has Turkey under Erdogan decided to backtrack and acquire nuclear weapons? The question is not baseless. It is hard to believe that Turkey's leaders have never discussed the option of nuclear armament. What is unprecedented, however, is that an inclination toward nuclear armament has been proclaimed so openly, directly and at the highest level.

In the years since the end of the Cold War, there had been only one previous occasion on which a Turkish official had spoken publicly on the issue. It occurred in August 2006 when military chief of staff Gen. Hilmi Ozkok referred implicitly to the nuclear option at the end of his tenure. Speaking at a ceremony marking his retirement, Ozkok began by expressing Turkey's concern over the proliferation of weapons of mass destruction. "The presence of countries possessing or suspected of possessing weapons of mass destruction on the axis from North Korea all the way to the Middle East is a serious and determining threat for our country today," Ozkok said.

He went on to allude to Turkey's nuclear option, using very careful language: "If the problem [of the proliferation of weapons of mass destruction] cannot be resolved despite the intense diplomatic efforts of the international community, I see a strong likelihood that we will face some important decision stages in the near future. Otherwise, we will face the prospect of losing our strategic superiority in the region."

The threat perception Ozkok outlined could have stemmed from Iran's reactivation of its nuclear program under President Mahmoud Ahmadinejad, a radical adversary of the West and Israel elected in 2005, replacing the Reformist administration, which had suspended the country's nuclear program. Israel is unlikely to have fueled Turkey's concerns, as its nuclear arsenal was already well known, and bilateral ties had not yet plunged into crisis.

The difference is glaring between Ozkok's remarks 13 years ago and Erdogan's Sept. 4 statement. While the chief of staff made do with insinuations, Erdogan's assertion of ongoing work in the context of nuclear-tipped missiles is clear and explicit, leaving no room for interpretation. It is also a gesture of defiance.

Remarkably, a decade ago in remarks to Qatar's Al Jazeera, Erdogan had called for "no nuclear weapons in the region." At the time of the interview, Nov. 25, 2009, the Mavi Marmara flotilla crisis between Turkey and Israel had not yet unfolded, but bilateral ties were already in turmoil, and Erdogan was aware of Israel's nuclear arsenal. He even told Al Jazeera, "Pressuring Iran is unfair and unjust while others have [nuclear weapons]," a reference to Israel, but he did not use Israel's case to advocate Turkey's right to nuclear weapons.

So, what has changed in a decade to lead Erdogan to defiantly ask why he cannot have nuclear missiles? Why is he pointing to Israel now, given that Israel was not an argument for justifying a nuclear option for Turkey a decade ago? Moreover, there are the well-known examples of how India and Pakistan became nuclear powers. Unlike Erdogan, their leaders never declared to the world their intentions to acquire nuclear weapons and related ballistic missiles, keeping their programs state secrets until their first back-to-back nuclear tests in 1998. Why is Erdogan

doing the opposite? What is his purpose in declaring his inclination so prematurely, given that Turkey is not even a nuclear-threshold country at this point?
The answers might lie in the geopolitical bottleneck in which Turkey currently finds itself.
Turkey's security issues have only grown more complicated with Erdogan's acquisition of the S-400 air defense systems from Russia, a move he made against the existential threat he perceives from the United States, which, he believes, backed (either passively or actively) the failed coup attempt against him in July 2016. Because of the S-400 purchase, Turkey is now deprived of the F-35 warplanes it had paid for in addition to having been expelled from the F-35 co-production program and facing the threat of further US sanctions.
Meanwhile, the United States is backing Israel and Greece in their drive to build energy corridors in the eastern Mediterranean, shutting Turkey out, and the risk of confrontation in the region growing. Moreover, Turkey's loss of the F-35s means that its air force, the country's main source of deterrence, will weaken with time, and closing the gap by purchasing warplanes from Russia does not seem possible at present. On top of all this, Turkey is literally squeezed between Russia and the United States in Syria.
Faced with these predicaments, Erdogan is brandishing his nonexistent "nuclear card" to warn the forces he views as threatening him that he will move to create more instability and disorder unless they ease the pressure on him. By advocating Turkey's right to nuclear weapons, he is sending the message that he will not step back against these forces, but will forge ahead, upping the ante.
If Erdogan's message is taken seriously, the reactions it will spawn can hardly help Turkey extricate itself from its geopolitical bottleneck. On the contrary, all the countries and alliances that might see a nuclear Turkey as a threat would, no doubt, begin to scrutinize it closer and with more suspicion. With this framework of mistrust, increasing direct or tacit pressure, isolation and threats of sanctions against Turkey will obviously lead to more instability and disorder both in Turkey and the broader region.

Kadri Gursel *is a columnist for Al-Monitor's Turkey Pulse. He focuses mainly on Turkish foreign policy, international affairs, press freedom and Turkey's Kurdish question as well as Turkey's evolving political Islam and its national and regional impacts. He wrote a column for the Turkish daily Cumhuriyet from May 2016 to September 2018 and for the daily Milliyet from 2007 to July 2015. Gursel also worked for Agence France-Presse from 1993 to 1997. While with AFP, he was kidnapped by Kurdish militants in 1995. He recounted his misadventures at the hands of the PKK in the book "Dağdakiler" (Those of the Mountains).*

Indonesian militants planned 'dirty bomb' attack - sources

Source: https://www.reuters.com/article/us-indonesia-security/exclusive-indonesian-militants-planned-dirty-bomb-attack-sources-idUSKCN1B51FW

August 2017 – Indonesian militants planned to detonate a radioactive dirty bomb, security sources said, highlighting the rising ambitions of extremists to wreak destruction in the world's largest Muslim-majority nation.
But experts cast doubt on their expertise, equipment and chances of success.
The plot was foiled when police raided homes and arrested five suspects in Bandung, West Java, last week, the sources with direct knowledge of the plot said. After the raids, police spoke of a plan to explode a "chemical" bomb but provided no other details.
The plot comes as Indonesia grapples with an influx of militants deported from other countries and the fallout from the Islamic State-led siege in the southern Philippines city of Marawi that regional leaders and analysts worry has energized militants across Southeast Asia
The three counter-terrorism sources, speaking on condition of anonymity, said the militants had hoped to **transform low-grade radioactive Thorium 232 (Th-232) into deadly Uranium 233 (U-233).**
The highly radioactive uranium would be combined with the powerful home-made explosive triacetone triperoxide (TATP) to create a "nuclear bomb", according to an instruction manual used by the militants and reviewed by Reuters.
In fact, the device would be, at best, a radiological dispersal device or dirty bomb that could spray radioactive material when the conventional bomb exploded.

A spokesman for Indonesia's national police, Inspector General Setyo Wasisto, declined to confirm or deny the plot to construct the device, but said it would have been more potent than the two bombs made from TATP that killed three police in Indonesia's capital Jakarta in May.

Anti terror policemen stand beside goods seized from a house of suspected Islamist militants in Bandung, West Java province, Indonesia August 15, 2017 in this photo taken by Antara Foto. Antara Foto/Agus Bebeng via REUTERS/File Photo

"If this bomb was finished, it would have had a more destructive impact than the bomb made from 'Mother of Satan'," he said, using the nickname for TATP.
"It could burn anything and make it hard for people to breathe."
Thorium-232 can be transformed into Uranium-233 but requires the Thorium to absorb a neutron, a process that needs powerful irradiation, generally from a nuclear reactor, according to three analysts contacted by Reuters and the website of the World Nuclear Association, which represents reactor vendors and nuclear engineers, among other industry stakeholders.
The militants' manual advised an X-Ray machine or microwave be used instead.
"X rays would not have enough punch to overcome the binding energy of the Thorium atoms," said Peter Hayes, an expert in radiological devices from the Nautilus Institute, in an email.
"And, no, you can't cook Th-232 to make U-233 in a microwave and, if you could, you would have a painful and rapid death from the radioactive nature of the co-present U-232 produced alongside U-233."
One senior Indonesian counter-terrorism source said the Bandung-based cell had bought a large amount of a household item and had begun to extract the Thorium. Reuters has chosen not to name the item.
"They needed three weeks. It was still only one week (into the process when police raided)," the source said.

"A Muslim's duty"

Indonesia has suffered a series of mostly small attacks by extremists over the past 18 months, although police have disrupted many more.
Indonesian terrorism analyst Rakyan Adibrata fears militants have been inspired by the events in Marawi, where IS fighters continue to occupy part of the city despite a three-month offensive by Philippines force to re-take it.

"They don't have the ability to occupy a city like has happened in Marawi, but they want to do something big that pleases their bosses in Islamic State," said Adibrata.
A radiological bombing could fit the bill, although Adibrata said that it was highly unlikely that the Bandung cell had either "the equipment or the knowledge" to succeed.
Most of Indonesia's recent attacks have involved members of Jamaah Ansharut Daulah (JAD), a pro-IS alliance of Indonesian militants. Many have been directed from Syria by an Indonesian national and JAD leader Bahrun Naim, according to police.

Naim is identified as the author on the front page of the 47-page Indonesian-language bomb instruction manual - named **"Nuclear for Dummy"** (sic) - and posted on a blog that has since been taken down.
"Mastering weaponry is essentially every Muslim's duty," it says.
"This paper, we hope, also can motivate the Muslim mujahideen to learn nuclear science easily and apply it."
Last week, police said the militants had been working off Naim's manual, but did not disclose its contents.
According to police, the suspected Bandung plotters were members of JAD and were considering targets like the presidential palace in Jakarta and police headquarters in Bandung and the capital.
Two of the five suspects are Indonesian migrant workers deported from Singapore and Hong Kong this year for posting radical Islamist material on social media.
They spent a month or less in a deradicalization shelter before joining up with the other militants, sources told Reuters.
About 177 Indonesian militants have been deported from other countries this year, according to Adibrata, citing the Ministry of Foreign Affairs. **The Malaysian police have recorded no less than 20 cases involving radioactive and nuclear materials which have "gone missing" over recent years.**

Qatar – Scientific knowledge affecting public policy now required for Georgetown's future policymakers

Source: https://menafn.com/1099002648/Qatar-Scientific-knowledge-affecting-public-policy-now-required-for-Georgetowns-future-policymakers

Sep 14 – What do the social sciences and humanities have to do with nuclear physics? According to **Dr. Kai-Henrik Barth**, the professor teaching Georgetown University in Qatar's first required natural science course this semester, the answer is 'everything.
His course, Nuclear Know-How for Presidents, gives students majoring in economics, history, culture, and politics, an introduction to the science behind nuclear weapons and an understanding of why that knowledge matters for policy makers, not just for scientists.
'From the Iran deal and North Korea's nuclear weapons programme, to Fukushima and Chernobyl, it's clear that nuclear technologies continue to shape international politics. Now more than ever, global leaders need to be able to understand scientific arguments in order to make informed decisions on issues that will have a tremendous impact on our world, explains Dr. Barth, who studied nuclear physics in his homeland of Germany, before receiving his Ph.D. in the History of Science and Technology from the University of Minnesota.
'I am really pleased that through this course, students will gain a broad understanding of nuclear science and technology, in both military and civilian applications, so they are better prepared to engage in discussions and debates on the complex issues surrounding nuclear weapons and nuclear energy, said Dr. Barth, who is also the Senior Assistant Dean for Research Support at GU-Q.

Ayesha Iqbal, a second-year student majoring in International Politics, had considered a career in physics before a love of politics brought her to GU-Q. With required readings including books by nuclear physicists, the curriculum is rigorous enough to challenge, without being overly technical. 'I didn't expect to go this deeply into technical concepts of nuclear physics, so I'm really enjoying it.
With hopes of pursuing a career in security studies and defence policy, she says the science has helped

her understand the stakes involved. 'Studying the amalgamation of nuclear physics and politics has made me take any headline I see on CNN or BBC about nuclear programs or nuclear threats far more seriously. These aren't just abstract diagrams and concepts in my physics coursebook anymore. The threat is real, and leaders are gambling with something that has the capacity to cause incalculable harm.
This course isn't GU-Q's only foray into the issue of nuclear technology. Dr. Barth also spearheads the university's partnership with the Qatar Ministry of Defence's National Committee for the Prohibition of Weapons (NCPW), a joint initiative that raises student awareness about the dangers of weapons of mass destruction (WMDs). And the school is exploring possibilities of expanding its natural science offerings in the future as well. 'For students in the social sciences and humanities, says Dr. Barth, **"scientific literacy is a life skill".**

Where Would America Be If It Never Invaded Saddam Hussein's Iraq?

No ISIS?

By Robert Farley
Source: https://nationalinterest.org/blog/buzz/where-would-america-be-if-it-never-invaded-saddam-husseins-iraq-80481

Key point: America would have saved trillions and thousands of lives.

Sep 14 – Every player of the popular video game Civilization knows to hit the save button before engaging in the risky, stupid invasion of foreign country. In the case of the 2003 invasion of Iraq, it became apparent after the first few months that the war was not working out as its framers had envisioned. The failure to find weapons of mass destruction was only the icing,

so to speak, on the disaster of failed reconciliation, state collapse, and executive incompetence.
What if we had "saved game" before we invaded Iraq? What would America's strategic options look like today?

The Middle East

In 2003, we spoke of the policy of "dual containment" as a problem that needed a solution. How could the United States manage a pair of hostile countries right next to one another? Today, the wiser among us recognize that "dual containment" was, in large part, a solution to its own problem. The animosity of the Hussein regime and the Islamic Republic of Iran meant that neither could achieve overarching influence in the Gulf.

In the wake of the Iraq War, "dual containment" has become "basket case management," as Iraq has ceased to exist as a relevant strategic actor, and Iranian influence has grown in Iraq, Syria, and Lebanon. While the U.S. no longer has to worry about Hussein, it has been forced to devote its military and political attention not only to the maintenance of the shaky Baghdad government, but also to the resistance of Iranian power in the region.

The impact of the Iraq War on the Arab Spring is more difficult to sort out. The framers of the war hoped that the establishment of a democratic Iraq would spur anti-authoritarian reactions around the region, although they also hoped that U.S. clients (including Egypt, Saudi Arabia, and the Gulf states) would be spared. Something along these lines did indeed happen in 2011, but only well after most in the region had concluded that the invasion of Iraq was a disastrous failure.

And indeed, the fruits of the Arab Spring have been limited at best. Tunisia represents the clearest case of success, while Libya has fallen into chaos, authoritarian forces have reasserted themselves in Egypt, and Syria has become an unending cauldron of violence and brutality. In Iraq itself, the legacy of the invasion of 2003 seems to be an inability to escape obligations to the new Iraqi government; the United States continues to act as the Iraqi air force, and continues to struggle to train reliable Iraqi army forces.

Was dual containment manageable in the long run? The U.S. has spent far more in blood and treasure since 2003 than it did between 1991 and 2003, so from a purely military and financial standpoint the answer is clearly "yes." And while dual containment would have left the dreadful Hussein regime in power, it likely would have avoided the worst of the several civil wars that Iraq has endured in the past twelve years.

Russia and China

Did Russia or China take advantage of the U.S. invasion of Iraq to advance their interests? This question demands the follow up "How would Russian or Chinese behavior have changed if the U.S. had avoided the Iraqi quagmire?" The answer, probably, is "not much."

The Iraqi campaign surely occupied U.S. attention and used up American capabilities, but the likelihood of U.S. military intervention in a campaign involving either Russia or China was vanishingly small in any case. The only conflict of note that the U.S. might have played a part in was the 2008 South Ossetia War. Although the Georgians desperately sought American intervention, the Bush administration wisely limited its support to rhetoric.

The rise of China and the increased belligerence of Russia owe more to geopolitical factors than to anything specifically associated with the Iraq War. At best, we might find some association between the rise of oil prices in the wake of the invasion of Iraq and the strength of the Russian state (China did not benefit from higher oil prices. However, the increase in oil prices after 2003 owes at least as much to the growth of the Chinese and Indian economies as it does to the decision to invade.)

Russia and China have surely enjoyed soft power benefits from the U.S. invasion of Iraq. Moscow regularly responds to U.S. criticism of its actions in Ukraine by referring to the 2003 invasion, although it also points to the 1999 Kosovo War and the 2011 Libya intervention. Beijing regularly questions American pretensions to maritime husbandry in the South China Sea, fueled to some extent by lingering unhappiness about the invasion of Iraq. But the long-term impact of this soft power boost is uncertain.

Afghanistan

The invasion of Iraq affected Afghanistan in two ways. First, it

diverted U.S. government resources away from Afghanistan at a time when the Taliban was clearly suffering from a devastating defeat. Second, it undermined the legitimacy of the Afghanistan war by presenting the operation merely as one of (potentially) several invasions of Muslim countries, rather than as a uniquely necessary effort to destroy a uniquely horrible regime.

It goes too far to claim that more attention to Afghanistan in the middle of the last decade would have led to the complete destruction of the Taliban, and an end to the war. The roots of the Taliban's survival are more complex, and more difficult to dig out, than a simple diversion of resources would suggest. At the same time, it is equally hard to argue that additional attention would not have made Afghanistan at least somewhat more secure. In particular, a strong U.S. commitment to Afghanistan (made impossible by the Iraq War) could have limited the degree to which Pakistan sought to make mischief in the region.

Domestic

The biggest effects of the Iraq War, and the most enduring limitations, may have come in how the conflict affected the U.S. military, and changed the attitudes of Americans toward the use of force.

With respect to the former, the Iraq War undoubtedly slowed research and development of advanced weapon systems within the U.S. Department of Defense. Without Iraq, the United States might have a much larger fleet of F-22s, for example. The U.S. Navy might expect additional Zumwalt class destroyers, and the Army's Future Combat Systems might never have died an ignominious death. In addition to specific platforms, DoD might have taken advantage of the 2000s to pursue a variety of "disruptive" technologies that would have left it farther ahead of Russia and China than it now sits. Secretary of Defense Rumsfeld certainly made pursuit of such technologies a priority, at least before Iraq derailed his plans.

But available technology rarely dominates strategic decision-making. Extra Raptors and Zumwalts could enhance American freedom of action at the margins, but would hardly have changed the trend lines of relative power in East Asia. Similarly, Future Combat Systems would not have given the United States much more in the way of political options for resisting Russian encroachment into Ukraine. And it is clearly wrong to believe that the money and attention devoted to Iraq would unproblematically have shifted over to research and development if the Bush administration had decided against intervention.

Moreover, the demands of the Iraq War (as well as the Afghanistan conflict) undoubtedly drove some technological development. The Iraq War revealed significant problems with how the Army and Air Force, in particular, viewed the future of warfare, leading to technological and doctrinal innovations that have improved U.S. warfighting capabilities.

The bigger domestic change may have come in terms of the public's attitude towards war. In the fifteen years after the end of the Cold War, the U.S. public became more tolerant towards the use of force than it had been in the post-Vietnam era. The Iraq War changed that, dramatically; today, few serious candidates for President support even a limited land war against ISIS.

President Obama won the 2008 Democratic primary because of his opposition to the Iraq War in 2003, and whatever one's attitude towards the drone war, the Obama administration clearly favors a less interventionist policy than its predecessors. This preference seems to accord with public and elite opinion about the use of force.

Does this reticence limit U.S. strategic options? America assisted France, the United Kingdom, and Libyan rebel forces with the deposition of the Gaddafi regime in 2011, notwithstanding any reluctance to use force. The U.S. continues to carry out a drone-and-special-forces war against Al Qaeda, across the Middle East. However, the reluctance to use force has surely played some role in the Obama administration's reaction to the Syria conflict, which has raged with minimal American intervention for the last four years.

Dr. Robert Farley, a frequent contributor to TNI, teaches at the Patterson School of Diplomacy and International Commerce at the University of Kentucky. He is the author of the Battleship Book and can be found at @drfarls. The views expressed are those of the author and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government.

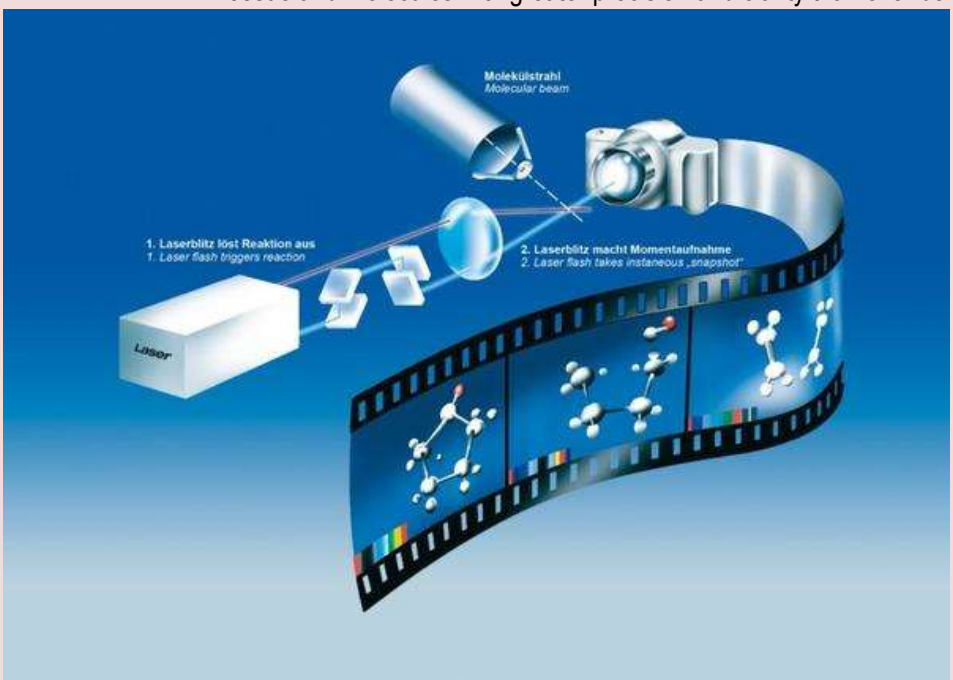
EDITOR'S COMMENT ON THE KEYPOINT: So, why they did it? Why they keep on taking similar decisions? I have some possible answers at hand

Scientists develop technique to observe radiation damage over femtoseconds

Source: https://www.sciencedaily.com/releases/2019/09/190919100209.htm

Sep 19 – Scientists at Nanyang Technological University, Singapore (NTU Singapore) have developed a technique to observe how radiation damages molecules over time-frames of just one quadrillionth of a second -- or a femtosecond.

The technique involves dissolving organic molecules in water to simulate the state molecules are found in biological tissue. This allows the research team to see radiation damage occur in biological tissue and molecules with greater precision and clarity than ever before.



Nuclear or "ionising" radiation can damage our bodies by altering DNA and other biological molecules as it disintegrates the chemical bonds holding molecules together.

Using their new technique, the scientists watched the vibrations generated by collisions of ionising radiation particles with an organic molecule, which eventually caused it to break apart after undergoing violent stretching, bending, and twisting motions. These vibrations only occurred when the molecules were dissolved in water, which represents a significant advance on previous studies.

Associate Professor Zhi-Heng Loh, an Assistant Chair at NTU's School of Physical & Mathematical Sciences who led the research, said, "This is the first time anyone has observed ionisation-induced molecular dynamics in aqueous solutions on femtosecond time scales. In previous studies, scientists were only able to observe the products of ionisation after the molecule had already been broken apart."

Although the hazards of radiation have been widely recognised since the 1930s, when Marie Curie died from anemia caused by her long-term exposure to radioactivity, the exact processes by which ionising radiation alters molecules are still not completely understood.

The study used methods from femtochemistry, to capture how atoms and molecules behave at ultra-short time scales, as in the formation or breaking of chemical bonds that take a few quadrillionths of a second, or femtoseconds.

Femtochemistry uses lasers that emit extremely brief pulses of light and each pulse creates a snapshot of the chemical reaction. These can then be stitched together like the frames of a video, to watch ultra-fast chemical processes from start to end.

Uncovering how radiation alters molecules

Assoc Prof Loh and his team set out to understand how ionising radiation affects biological molecules. As a starting point, they focused their attention on the phenoxide ion, a relatively simple organic molecule that contains many of the same types of chemical bonds that are found in the proteins that make up living tissue.

High-resolution spectroscopy had previously been used to study phenoxide in its gaseous form, and from it researchers had observed a relatively simple behaviour: when struck by ionising radiation, each phenoxide molecule vibrates at a single frequency, like a bell ringing in a single clear tone. However, this method could not be used to study organic molecules dissolved in water, which is similar to the state molecules are found in biological tissue.

Using a pulsed-laser apparatus, the NTU team was able to record how radiation damages phenoxide molecules dissolved in water. The team identified multiple vibrational frequencies, distinct from the single frequency observed in gaseous phenoxide. They discovered that when radiation causes the molecules to eject an electron, the molecule vibrates in a highly complex pattern, more akin to the sound of a cymbal or gong than a ringing bell.

"In the future, we will build on this to investigate how radiation affects larger and more complicated molecules, such as proteins and nucleic acids, which are the building blocks of life," said Assoc Prof Loh. "Our research group specialises in femtochemistry, and once we got interested in the topic, it turned out to be relatively simple to adapt our femtochemistry methods to studying the vibrational motion of ionised molecules dissolved in water. To our surprise, no one had ever tackled this particular problem before," he added.

Journal Reference: *Tushar Debnath, Muhammad Shafiq Bin Mohd Yusof, Pei Jiang Low, Zhi-Heng Loh.* ***Ultrafast structural rearrangement dynamics induced by the photodetachment of phenoxide in aqueous solution***. Nature Communications, *2019; 10 (1) DOI: 10.1038/s41467-019-10989-1*

Copyright by Signe Wilkinson


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

Liquid restrictions to end at UK airports thanks to new technology

Source: https://news.sky.com/story/liquid-restrictions-to-end-at-uk-airports-thanks-to-new-technology-11793561

Aug 25 – **Air passengers will no longer have to take liquids and laptops out of their carry-on bags under new rules coming into force for UK airports to upgrade their security scanners.**

Similar to CT scanners used in hospitals, the new technology will provide a detailed picture of a bag's contents and allow images to be visually rotated and dissected.

Heathrow has already invested millions in the equipment and the government will now force all other UK airports to change their systems by December 2022.

The upgrades should mean the end of the 100ml limit on liquids, with passengers no longer required to use plastic bags for their toiletries and cosmetics.

Ministers are advising travelers to continue to separate liquids and electronics for now as the new technology will not be introduced straight away.

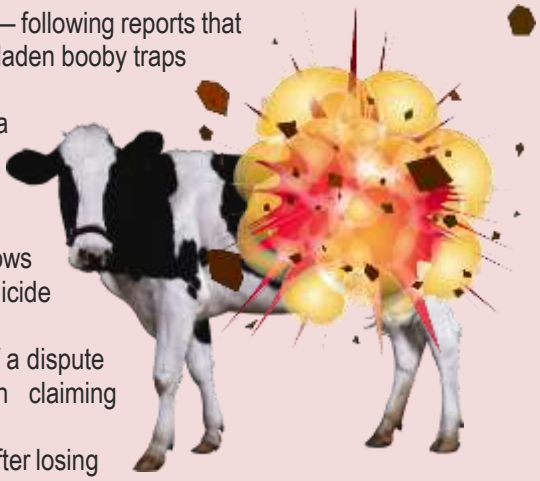
Transport Secretary Grant Shapps said the upgrades will mean "no more intrusive pulling out your socks and your underwear, having to separate all your liquids and take your laptop out, all that can just stay in the bag and be able to go through".

Airport bosses estimate the scanners will mean passengers clearing security 50 to 60 times faster than is currently the case.

ISIS is now weaponizing cows with explosives

Source: https://nypost.com/2019/09/03/isis-is-now-weaponizing-cows-with-explosives/

Sep 03 – Add animal rights activists to the ever-growing list of ISIS haters — following reports that the fiends had weaponized a pair of cows by turning them into explosives-laden booby traps that killed a civilian.



The bovines were strapped with explosive belts and were headed toward a military checkpoint in Diyala province when Iraqi soldiers opened fire and "blew them up," killing a bystander, according to a report on the Kurdish language Rudaw news website, the Independent reported.

A local official, Sadiq Husseini, told the Kurdish outlet that the incident "shows that the group has lost the ability to recruit young people and would-be suicide bombers, instead they are using cattle."

Diyala province is home to Kurds, Sunnis and Shias and is at the heart of a dispute between the Kurdistan Regional Government and Iraq, with both claiming ownership, Fox News reported.

ISIS has taken advantage of the dispute and worked to re-establish itself after losing most of the territory it had held under its so-called caliphate.

ISIS holds a "durable support zone" and has "increased its attack tempo against security forces, local tribal figures and commercial sites," according to the Institute for the Study of War.

Terrorists have used animals to carry out their cowardly attacks in the past.

In November 2003, more than a dozen rockets were fired from donkey carts that slammed into Iraq's Oil Ministry and a pair of Baghdad hotels.

Other rocket launchers mounted on donkey carts were found in Waziriya, a neighborhood north of downtown, and in all, weaponized donkeys have killed 14 people.

Emerging Threats to Rail Infrastructure – Freight

By Joseph Trindal

Source: https://www.domesticpreparedness.com/commentary/emerging-threats-to-rail-infrastructure-part-i-freight/

There is a desire for some bad actors to target rail systems, especially the hazardous materials freight rail network. This threat underscores the need for the rail transportation industry to maintain and strengthen partnerships with federal, state, and local authorities. With over 140,000 miles of infrastructure, there are difficult security challenges. For example, the U.S. rail system moves over 1.8 billion tons originated/year of freight, petroleum, chemicals, and military assets, making it a vital lifeline. A recent roundtable examined current issues and progress regarding this important topic from government and private sector experts.

Analysis of terrorist attack and plot trends targeting transportation infrastructure in developed countries demonstrates a growing interest in rail systems. Over the past 13 years, European rail systems infrastructure have been the increased focus of successful terrorist attacks, failed attempts, and disrupted plots. Examples include:

- The March 2016 suicide bombing on board a metro train at a station in the center of Brussels, Belgium, part of a coordinated operation that targeted the city's international airport, killed 32 people and wounded more than 300 others;
- The March 2010 coordinated suicide bombings in Moscow, Russia, subway killed 40 and injured more than 100;
- The July 2005 coordinated suicide bombings on three underground trains and a double decker bus in London, UK, public transport killed 52 people and injured over 700 more;
- The March 2004 coordinated bombings over a period of about four minutes on four commuter trains operating on the same line in Madrid, Spain, killed 192 people and injured over 1,800 others.

Noteworthy terrorist failures include the September 2017 attempt to detonate an improvised explosive device on board a London Underground train at Parsons Green station and the attempt to execute a mass shooting on board a high-speed train operating in northeastern France in August 2015. In the United States, numerous plots envisioning attacks on domestic rail systems have been disrupted, the most advanced being a plan to detonate suicide explosives on board New York City subway trains foiled in September 2009. More recently,

a plot to target a VIA Rail passenger train in the Toronto, Canada, area during the September 2012 to April 2013 period was disrupted by the combined efforts of a joint investigation. The Royal Canadian Mounted Police and the Federal Bureau of Investigation (FBI) monitored the two main plotters and the timely reporting of pre-attack surveillance observed by a conductor on a passing train operating on the targeted rail line.

Certainly, the interest of terrorist groups in targeting rail systems has persisted. In August 2017, al-Qaida published issue 17 of its *Inspire* online publication that focused on inciting attacks against both passenger and freight rail systems in the United States and Europe. On 10 October 2017, Domestic Preparedness moderated a roundtable discussion entitled "Emerging Threats to Freight Rail Infrastructure." The panel was comprised of distinguished speakers representing a board range of stakeholders in the freight rail transportation sector. Representatives from the following agencies and organizations contributed to this discussion on emerging threats and mitigation strategies in the freight rail transportation sector: Transportation Security Administration (TSA), Threat Analysis Division; TSA, Office of Security Policy and Industry Engagement; the FBI's Rail Security Program; the U.S. Department of Defense (DoD) TRANSCOM; National Protection and Preparedness Directorate (NPPD), Protective Security Coordination Division; Amtrak Police, Criminal Intelligence Unit; the Association of American Railroads (AAR); and the Secure Technology Alliance. Many interesting and relevant points were discussed during this important roundtable event.

Holistic Perspectives on Threat Mitigation

The panel acknowledged that, although the trends in terrorists' actions and priorities continuously evolve, so too are integrated measures to disrupt, detect, and mitigate threats to the freight rail industry. Recent events indicate a terrorist focus on the rail sector, but predominately target passenger and commuter rail systems. Attacks such as 2017 Parsons Green bombing in London and the 2016 Brussels bombings targeted urban commuter rail infrastructure during peak hours. TSA's officials made clear that the risks of attack on the freight rail sector are low. The FBI pointed out that their investigative activities still include cargo thefts by criminal actors and gangs, as well as disruptive activities targeting freight rail by environmental activists. The panel identified cyberthreats as an emerging challenge, a common public and private sector threat across customer facing, business, and operational systems.

The panelists agreed that defeating every threat is practically unattainable. However, disrupting plots and creating difficult environments that thwart attacks are key elements of a shared strategy for narrowing risks. It was pointed out during the discussion that, if some of the early indicators of the Parsons Green and Brussels attacks as well as other successful terrorist operations against passenger trains and stations had been recognized, reported, and acted upon, these plots may have been disrupted before the attacks were launched. According to a 16 September 2017 BBC news report, London's Metropolitan Police commissioner, Cressida Dick, stated that police had interdicted six "significant plots" in the months leading up to the Parsons Green attack. A shared challenge across the rail sector is recognition and early identification of threat indicators.

The TSA and FBI both noted that public and private stakeholders in the rail industry work closely together in developing broad understandings of threat indicators. TSA's Threat Analysis Division assesses data collected from a wide array of sources, domestically and abroad, to produce threat analysis products that are disseminated to stakeholders in both the public sector and throughout the rail industry in the United States and Canada. Although the discussion panel included representation from many organizations, the panelists knew one another well. Many panelists stated that they talk with one another on a daily basis.

Strength in Partnerships

Developing and maintaining a holistic threat understanding requires constant coordination among the stakeholders, both internal within government and external with the private sector. Thriving partnerships share certain common goals and understandings that weather the test of time. The 9/11 attacks caused significant economic impact across several levels of the aviation industry as well as disrupting many nation-state economies. For both public and private sectors, a unifying common thread is the shared understanding of economic consequences of terrorist plots that target critical infrastructure.

In the rail sector, the railroad police agencies have a long history of working with local public sector police agencies in investigating cargo thefts and rail asset vandalism. Today there is close interaction among federal, local, and railroad agencies, with the FBI's Rail Security Program and their local field offices taking a proactive role. The FBI frequently supports local law enforcement and railroad police agencies in nonterrorist criminal matters with intelligence and investigative support.

State, local, federal, and railroad partnerships are strengthened through a national network of local-based task forces, such as the FBI-led Joint Terrorism Task Forces (JTTFs). Numbering over 80 JTTFs nationwide, law enforcement representation includes railroad police in many locations.

The American Association of Railroads (AAR) is a nonprofit industry group representing the Class I freight railroads, Amtrak, and some regional railroads. The AAR expressed the strength by which the railroads collaborate with the federal and local government partners. The AAR member railroads have a long history of working with state and local first responders on both safety and security matters. Within the freight railroad industry, AAR leads its members in developing and maintaining unified security plans that are current and inclusive. The AAR unified security plan model focuses on five key areas: (1) train operations, (2) critical infrastructure, (3) hazardous materials, (4) military transport, and (5) cyber and communications. In implementing the plan, the AAR serves as the security information center for the railroad industry and facilitates preparedness exercises jointly, involving railroads and government officials across the United States and Canada. These regular, recurrent, structured exercises are designed to place plans and procedures under stress in realistic terrorism and cyberthreat incident scenarios, develop lessons learned in areas for improvement, and apply those lessons to strengthen future capacities for all participating organizations.

Relationships among federal, state, local, and tribal government agencies are stronger through the establishment of intergovernmental points of contact across jurisdictions. The growth of state and locally operated fusion centers has generated a network of intergovernmental collaboration. Operating under a National Network of Fusion Centers with unifying guidelines, intelligence, advisories, and lessons learned are rapidly and securely communicated. Private sector representatives with proper clearances and bone fide "need to know" are integrated into the National Network of Fusion Centers.

The Rail Sector Coordinating Council, stemming from the National Infrastructure Protection Plan, is the rail industry principal liaison forum of coordination between the railroads, stakeholder organizations, and the government. An important coordination strategy for AAR members is to achieve the goals of the National Infrastructure Protection Plan and sector-specific plans by proactively and collaboratively planning, training, exercising, sharing information, and assessing capacities against risks. The railroad industry supports the threat awareness of fusion centers through sharing of advisories on matters pertaining to terrorism, cyberthreats, and measures to mitigate risk.

U.S. Department of Homeland Security's (DHS) Protective Security Coordination Division fields Protective Security Advisors (PSAs) across the country to engage the 16 critical infrastructure sectors, which include the Freight Rail sub-sector. The PSAs' primary mission is to protect critical infrastructure. The five mission areas are: (1) plan, coordinate, and conduct security surveys and assessments; (2) plan and conduct outreach activities; (3) support National Special Security Events and Special Event Activity Rating Level I and II events; (4) respond to incidents; and (5) coordinate and support improvised explosive device awareness and risk mitigation training. PSAs are security subject matter experts who engage with state, local, tribal, and territorial government mission partners and members of the private sector stakeholder community to protect the nation's critical infrastructure. PSAs serve as regional DHS critical infrastructure security specialists, providing a local perspective to and supporting the development of the national risk picture by identifying, assessing, monitoring, and minimizing risk to critical infrastructure at the regional, state, and local levels.

In addition, there is a network of railway enthusiasts, called "rail buffs," who make a recreational hobby out of observing and noting railroad activity. Many rail buffs are well known to railway engineers and workers; some even on a first name basis. These rail buffs tend to be very familiar with their railway areas of interest and can easily spot suspicious behavior or activity. The rail buff network is loosely connected through the Railfan Network. Local railroad and law enforcement collaboration with rail buffs is an example of grassroots connectivity.

A collaboration challenge from some organizations is continuity of principal points of contact. For some agencies and organizations, personnel assigned to key collaborative positions change every few years. Relationships are built over time and, when personnel change with promotions or reassignments, it can be disruptive. At the very least, a degree of institutional knowledge and expertise needs to be re-learned. This matter tends to be more of an issue with some of the federal agencies than local and railroad organizations.

Through the network of government, private, and citizen collaboration around the freight rail industry, terrorists' ability to prepare an attack is made more difficult, takes longer and provides much greater risk of detection and interdiction. Collaborative success is demonstrated in the high volume of thwarted terrorist plots in recent years.

State of Rail Sector Information Sharing

Networks of collaboration are only useful and sustainable if they provide value to the network stakeholders. Meaningful information sharing – distilled from data and intelligence analysis – is critical to keeping ahead of evolving terrorist threats. Within the federal agencies, there are verticals of information sharing between agency headquarters and the agency's field personnel. More important is the information flow that spans across agencies and includes private sector stakeholders.

The federal agencies with responsibilities for freight rail security today are closely integrated in sharing information across common networks and direct collaborative relationships. For example, the FBI information-sharing network goes beyond headquarters to the field, as the FBI oversees 84 JTTFs with representation across numerous federal, state, and local agencies. The FBI's Rail Security Program engages with railroads and other federal agencies at various levels, with multilateral information sharing. The FBI and TSA also collaborate with trusted international partner countries drawing on intelligence, incident analysis, and lessons learned. Collectively, the network of public and private information analysis, intelligence development, and sharing improves stakeholder threat awareness.

Agencies and private sector information sharing takes many forms. The joint government-industry coordinated Rail Intelligence Working Group (RIWG), is an example of public and private sector collaboration in action for information sharing. The group is comprised of representatives from the FBI, TSA, Amtrak, the American Public Transportation Association, and AAR – a partnership that remains unique across critical infrastructure sectors. Recently, the RIWG analyzed the video and the August 2017 *Inspire* edition. These materials urged supporters to target trains, particularly emphasizing so-called "Train Derail Operation" with lengthy instructions on building a "homemade derail device" for this purpose. The RIWG developed and disseminated informational awareness advisories through various rail industry and public sector networks, including the AAR's Railway Alert Network. These materials highlighted both the complexities of the actions advocated and the lack of understanding reflected in the magazine articles of the rail transportation system and its safety and security capacities. This cooperative effort reflects a joint commitment to sharing timely and useful security information across government and industry for security enhancement.

Complementing this work, the AAR publishes the Rail Awareness Daily Analytic Report (RADAR) as well as focused awareness advisories through the Railway Alert Network, keeping railroad and government stakeholders continuously informed on matters of relevance to rail security. Similarly, both TSA and the U.S. Department of Transportation produce and disseminate informational, intelligence, and alert products. Recipients of the governmental and Railway Alert Network products include officials with numerous federal agencies in the United States and Canada, state and regional fusion centers in the United States, and law enforcement and physical and cybersecurity leads for freight and passenger railroads in the United States and Canada.

The FBI's Tripwire Program has proven highly effective as a means for actionable information sharing. Described as "See Something, Say Something with focus," the Tripwire Program educates industry stakeholders on key trends and potential indicators of criminal terrorist preparation. Stakeholders are encouraged to report any suspicious activity with relevant details to local law enforcement or the FBI Field Office. The FBI conducts a structured assessment of Tripwire reports, some of which have led to preliminary investigations with a few resulting in criminal investigations and prosecution before planned attacks materialized.

Effective rail industry-centric information management ensures that priorities are aligned, and timely action is taken, in a concerted effort to create conditions to prevent bad outcomes. AAR pointed out three elements of the railroad industry's security strategy. First, understand that prevention is attainable. Second, worry less about what is not known and learn what can be known as thoroughly as possible. Third, avoid self-inflicted wounds through actions that ease adversaries' ability to achieve their disruptive, destructive, and event lethal purposes. Gaining continuous situational awareness from reporting by railroad operators while providing these operators with relevant threat intelligence and related security information is advantageous for developing a results-oriented preventive posture.

Through effective information sharing that creates a climate of relevant awareness and response, threats can be either blunted or significantly mitigated in potential effects. AAR also stressed the need to ensure that information-sharing structures avoid inadvertently facilitating the preparation of criminals and terrorists. Rail operations and security information must be shared only with those who have a valid need to know. Government information-sharing networks are only accessible by credentialed personnel who have been vetted and meet agency standards for physical and logical access to systems and information. Similarly, railroads control access to security information received from all sources.

Cyberthreats, vulnerabilities, and attacks are increasing. Threats and attacks are focusing on public facing, business, and operational enterprise systems and devices, including person and nonperson tractions, personal and support staff, and third-party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. These threats have implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems, in addition to known ICS/SCADA weaknesses and vulnerabilities.

Public and private sector leaders are working together to address this threat. Cybersecurity is the fastest growing focus of railroads, government agencies, and DoD. DoD's reliance on commercial rail infrastructure has been long established. Today, DoD TRANSCOM's surface deployment mission is supported in large part by commercial railroads. DoD's rail deployments are closely synchronized with mission commands and the railroad industry, where movement information must be secure. Currently, DoD is working with the Critical Infrastructure Resilience Institute, a DHS Science and Technology center of excellence operated by the University of Illinois at Urbana-Champaign, to develop a refined cyberrisk scoring metric.

Similarly, AAR member railroads have elevated cybersecurity at the top of their priority lists. As freight rail systems become more automated and integrated, railroad investment in securing information technology networks – including those in development for the Positive Train Control system, which includes design to mitigate the risk of exploitation by cyberthreats. Amtrak pointed out that they have invested and continue to invest in securing their cyber systems. Nearly 85% of Amtrak's ticket sales take place on the internet. Amtrak police vigorously investigate growing volume of cyber and financial crimes involving their ticketing system.

A major challenge in top-down information sharing is the security classification of the information. The federal government Code of Federal Regulations (CFR) establishes requirements for managing unclassified but sensitive information. The term "Sensitive Security Information" (Title 49, CFR, Part 1520) is applied to information that falls short of meeting the National Security Classification regulations, but if disseminated it would be detrimental to the transportation security. TSA's sharing of Sensitive Security Information provides an important intermediate level for broader dissemination with regulatory safeguards and information security standards.

Freight Rail Security Regulatory Influence

Both DHS and U.S. Department of Transportation provide federal regulatory oversight of freight rail security matters. Additionally, some states apply regulations that impact freight rail security. The TSA Rail Transportation Security Rule (Title 49, CFR, Parts 1520 and 1580), promulgated in 2006, is among the federal regulations designed to strengthen rail industry security and reduce risk associated with the transport of security-sensitive materials. The Rail Security Rule developed into regulatory requirements practices that most railroads had already implemented. For example, the rule requires secure chain of custody of security-sensitive materials, which

most railroads had already performed pursuant to agreed, voluntary security actions with TSA as a prudent business practice. The rule further requires regulated railroads to designate a rail security coordinator and mandates security concern reporting to TSA. The rail security coordinator requirement does enhance consistency in public and private sector coordination with the regulated railroads.

Regulations, at both state and federal levels, have generated linear reporting mandates and prescribed standards. However, regulatory reporting standards tend to be reactive and cannot replace stakeholder driven initiatives to build strong, functional relationships. As one TSA official stated, "Our success has been built on collaboration, not regulation."

Many on the panel pointed out that regulation alone does little to enhance rail security and may, in some instances, produce the self-inflicted damage that should be avoided. The U.S. Department of Transportation requirement for railroads to report to states detailed information on the routes used, and frequencies of operations on those routes each week, by trains transporting high volumes of crude oil and other flammable liquids has resulted in publication of those schedules. Open-source publication of the operations of hazardous shipments unnecessarily releases security and safety information outside the first responder and community emergency planning agencies – and needlessly exacerbates risk.

Regulatory oversight by government inspectors and reporting regimes strain the railroads' personnel resources. In some situations, rail security coordinators and other railroad personnel are drawn away from performance based rail security matters to address report legibility or formatting. Security regulatory development and implementation should be collaborative between public and private sectors – as the private sector best practices often exceed regulatory standards.

Key Takeaways

The current and future state of freight rail security continues to change. The panel addressed a number of key strengths and some challenges for securing the nation's freight rail infrastructure. Some of the salient points from the Emerging Threats to Freight Rail Infrastructure roundtable discussion include:

- **Threats are dynamic** – There is significant evidence that threat trends involving the freight rail transportation infrastructure are changing. Intelligence assessments and extremists' propaganda and threats reflect a continuing interest of terrorists in targeting rail systems. Cyberthreats are increasing as well, which has implications for business and operations networks of railroads. Generally, the threat to rail systems is low but, as one participants stated, "Low does not mean 'no'."
- **Cyberthreats are increasing** – This includes attacks on public facing, business, and operational enterprise systems, including person and nonperson tractions, personal and support staff, and third - party vendors and service providers. The continued expansion of the internet of things and smart connected transactions are creating new and ever-increasing exploitation opportunities. This has implications for the freight rail infrastructure, especially given the evolution and integration between rail operation and business enterprise systems.
- **Criminal activities overshadow terrorist threat** – The federal, state, local, and railroad police agencies investigate far more cargo theft, vandalism, and disruptive criminal activity, including trespass and blockades by protesters, than terrorist plots involving the freight rail sector.
- **Stakeholder partnerships are strong** – The coordinated effort among federal, state, local, and private sector agencies and organizations is stronger than ever before. Through rail sector focused task forces, fusion centers, working groups and interagency networks, collaboration for planning, information sharing, training, outreach, response, and recovery are based on common goals of enhancing security.
- **Public and private partnerships are collaborative** – Stakeholder organizations in the public and private sectors have designated points of contact and established functional structures to promote collaboration and coordination around rail system security. Effective practices for elevating prevention and response capacities are widely shared among the railroads and with public sector agencies.
- **Information sharing is multi-lateral and relevant** – Intelligence and security information sharing occurs continuously among freight and passenger railroads, federal government agencies, state and regional fusion centers, and law enforcement agencies through a variety of networks. This extensive effort develops and sustains a current and relevant understanding of threat indicators and informs reporting capacities among stakeholders

in industry and government. Enhancing security through constant emphasis on effective information sharing remains a common focus with public and private sector organizations. All involved apply appropriate protections based on need-to-know and access controls.

- **Freight railroad security focus and capacities are strong** – The Class I railroads, as well as most others, maintain strong security capabilities. AAR provides uniform and consistent guidance and support for its railroad members. The railroad industry's unified security plan in use by all Class I railroads and many others is an industry standard. AAR supports security awareness training through products disseminated to freight and passenger railroads via the Railway Alert Network and facilitates preparedness exercises for the railroad industry, which includes public sector agencies in the United States and Canada. The railroads actively engage with federal, state, and local investigative and intelligence agencies to ensure continued access to relevant information and analysis.
- **Information security challenges remain** – Some information and intelligence obtained by federal agencies is highly classified and has limited distribution in its raw form. Agencies have developed standards for redacting or recasting classified information into unclassified intelligence products while still maintaining security protocols. TSA's Sensitive Security Information is an example of unclassified but sensitive information, which can be shared and managed in accordance with federal regulations. Representatives of state and local agencies as well as designated private sector employees, with bone fide need-to-know, may be sponsored for security clearance to receive classified briefings and intelligence products.
- **There are three key risk mitigation points** – (1) Understand that prevention is attainable; (2) learn as much as possible about what can be known; and (3) avoid self-inflicted wounds. Many potential threats and security risks can be avoided or substantially mitigated by acting on timely and actionable information. Develop thorough practical understanding of security threats at the right levels and align resources and capabilities accordingly. Recognize that resources are finite; partnerships based on common priorities and practical information can be effective in actionably preventing most risks. Avoid inadvertently making the terrorists' or criminals' planning and preparedness easier to put into action. Maintain informational and operational security over sensitive information that could be useful to terrorists and criminals.
- **Railroads are prioritizing cybersecurity** – As the industry moves toward greater reliance on integrated cyber systems, railroads recognize the economic returns for investing in secure system designs. Cybersecurity is a high priority throughout the railroad industry.
- **Railroad regulations have limitations** – Regulations levied on the freight rail industry have increased over the years. Many of the regulatory requirements codify and establish government oversight over best practices that had already been established by freight and passenger railroads. Some regulations between jurisdictions undermine strong security measures. Regulations alone do not create collaboration. Greater alignment between regulatory rule making and the railroads would go a long way to harmonizing best practices and achieving the shared goals between the public and private sector.

Conclusion

Western railroad system infrastructure continues to be an evolving terrorist target of interest. Expressed terrorist organizations' desires to sow economic harm through attacks involving critical infrastructures – for example, passenger *and* freight rail systems – is publicized in their global outreach to affiliated and non-affiliated groups as well as lone actors seeking recognition. Although the proliferation of global, web-based outreach by certain terrorist groups to unaffiliated groups and lone actors may indicate the effectiveness of multinational counterterrorist operations, it also creates new challenges for pre-attack detection and interdiction.

In the United States, the continued strengthening of public and private partnerships in the freight rail sector creates extreme difficulties for terrorists and criminals to succeed in executing attack plots. Intergovernmental cooperation and information sharing continue to improve with actionable lessons learned and pre-attack indicators shared bilaterally between local personnel and national agencies. Similarly, the daily interaction between the rail industry and government officials, at all levels, enhances situational awareness such that terrorist pre-attack and plot

indications are more likely detected and proactively thwarted. Joint federal, state, and local interdiction and prosecution of terrorist plotters are indications of the successes stemming from public and private partnerships.

Challenges remain for private sector and government agencies in the freight rail sector. As demonstrated by the security and safety initiatives implemented by railroad companies and standardized by private industry organizations like the AAR, the private sector's economic interests drive innovation that stay ahead of government regulations. Many of the railroad companies' security procedures exceed regulatory minimum requirements, whereas some regulations even divert private sector resource priorities in counterproductive ways. Intergovernmental regulations and policies need greater alignment in developing cohesion between federal, state, and private sector shared objectives for freight rail security and safety. With emerging cyberrisks and the growing need for information security in the global digital age, all stakeholders in the rail transportation sector need to examine ways to deny terrorist plotters and attackers access to open source information and resources. Creating greater difficulties for terrorists and criminals is a universally shared public and private sector sustainable goal.

***Joseph W. Trindal, PPS**, is a career homeland security professional with over 40 years of experience in both public and private sector. He has been a contributing writer to DomPrep for over 10 years. Having served for two decades with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal, he answered an invitation to contribute in creating the U.S. Department of Homeland Security (DHS) as regional director of the Federal Protective Service for the National Capital Region. During his service as an executive at DHS, he led a select team developing the Chemical Facility Anti-Terrorism Standards regulations, DHS's first legislated regulatory authority. Since his retirement, with over 30 years of government service, he continues executive service, now in the private sector security industries. A past president of the FBI's InfraGard, he led the transformation of the National Capital Region Chapter into a leader in public-private partnership initiatives. Currently, he is president and chief operating officer with the Akal Group of Companies, leading over 2,000 employees serving in 22 countries with a $250M portfolio of U.S. government and private sector contracts. Living in Virginia, and a veteran of the U.S. Marine Corps, he holds degrees in police science and criminal justice.*

IOI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C²BRNE DIARY

CYBER NEWS

It was sensitive data from a U.S. anti-terror program – and terrorists could have gotten to it for years, records show

Source: https://www.latimes.com/science/sciencenow/la-sci-biowatch-20190402-story.html

Aug 25 – The Department of Homeland Security stored sensitive data from the nation's bioterrorism defense program on an insecure website where it was vulnerable to attacks by hackers for over a decade, according to government documents reviewed by The Times.

The data included the locations of at least some BioWatch air samplers, which are installed at subway stations and other public locations in more than 30 U.S. cities and are designed to detect anthrax or other airborne biological weapons, Homeland Security officials confirmed. It also included the results of tests for possible pathogens, a list of biological agents that could be detected and response plans that would be put in place in the event of an attack.

The information — housed on a dot-org website run by a private contractor — has been moved behind a secure federal government firewall, and the website was shut down in May. But Homeland Security officials acknowledge they do not know whether hackers ever gained access to the data.

Internal Homeland Security emails and other documents show the issue set off a bitter clash within the department over whether keeping the information on the dot-org website posed a threat to national security. A former BioWatch security manager filed a whistleblower complaint alleging he was targeted for retaliation after criticizing the program's lax security.

The website shared information among local, state and federal officials. It was easily identifiable through online search engines, but a user name and password were required to access sensitive data.

A security audit completed in January 2017 found "critical" and "high risk" vulnerabilities, including weak encryption that made the website "extremely prone" to online attacks. The audit concluded that there "does not seem to be any protective monitoring of the site," according to a Homeland Security report summarizing the findings.

An inspector general's report published later that year said sensitive information had been housed on the BioWatch portal since 2007 and was vulnerable to hackers. The report recommended moving the data behind the government's firewall and said Homeland Security officials had agreed to do so.

It is unclear how valuable the data would have been to a terrorist group or enemy state. Scientists have warned that the BioWatch technology is unreliable. The system recognizes only a narrow range of microbes, and it struggles to differentiate between typical environmental bacteria and dangerous threats.

Still, several biodefense experts said it was disturbing that Homeland Security officials failed to adequately secure sensitive information from one of the nation's anti-terrorism programs.

"Advertising your vulnerabilities is never a good thing. Letting your adversaries readily access your vulnerabilities — that's a national security risk, in my judgment," said Tom Ridge, who as the nation's first secretary of Homeland Security oversaw the 2003 launch of BioWatch but has since denounced the program as ineffective. "Every American citizen would wonder, 'What else is so easily accessible by the rest of the world?'"

James F. McDonnell, an assistant secretary appointed by President Trump to oversee Homeland Security's new Countering Weapons of Mass Destruction Office, which includes BioWatch, said the data that were housed outside the secure government firewall were not important enough to cause a national security threat, but he said officials have taken steps to strengthen cybersecurity across the department. He noted that the problem predated his appointment.

"What happened before, happened before. You can't put the genie back in the bottle," he said. "There's been a real ramping-up on concerns about cybersecurity."

Long list of troubles

The security problems add to a long list of troubles for BioWatch.

The program, which has cost taxpayers more than $1.6 billion, was launched two years after letters laced with anthrax spores killed five people and sickened 17 others shortly

after the Sept. 11, 2001, terrorist attacks. BioWatch became part of Homeland Security's Office of Health Affairs in 2007.

A 2012 Times investigation identified serious shortcomings, including false alarms and doubts about whether BioWatch could be relied on to identify a bioterrorism event. In 2015, a Government Accountability Office study concluded that the program could not be counted on to detect an attack and said BioWatch generated 149 false alarms from 2003 through 2014.

Each day, public health workers across the country collect filters from the air samplers and run tests on the contents, searching for signs of dangerous pathogens in the air. In some cases, reports of suspicious lab findings are uploaded to the BioWatch portal for review by other officials.

Some local officials objected to storing these and other sensitive documents on a federal server that other government officials could access without their knowledge or consent, according to the inspector general's report. As a result, the report said, the Office of Health Affairs decided against moving the portal inside the Department of Homeland Security's firewall.

Alarms over security

In August 2016, Harry Jackson, who worked for a branch of Homeland Security that deals with information security, was assigned to the BioWatch program. Three months later, he said in an interview with The Times, he learned about biowatchportal.org and demanded the agency stop using it, arguing that it housed classified information and that the portal's security measures were inadequate.

Two other department officials tasked with monitoring how sensitive information is handled echoed the concerns in emails to BioWatch managers, according to records reviewed by The Times.

BioWatch officials pushed back. Michael Walter, the program's manager, said in a conference call with other Homeland Security officials that information about the location of the network's air samplers would not undermine its effectiveness since it was designed to detect a massive biological warfare attack. The samplers are in plain sight, he said, according to a recording of the call made by Jackson and reviewed by The Times.

Larry "Dave" Fluty, then Health Affairs' principal deputy assistant secretary, argued during the same call that the agency had previously decided that treating the information as classified — and therefore triggering stricter access guidelines — would require security clearances for some 1,000 local officials who are involved in gathering and analyzing data from the air-collection units.

"It was determined from a policy standpoint that that can't happen," he said.

Weeks after the conference call, Steven Lynch, then chief of Homeland Security's special security programs division, wrote in a memo reviewed by The Times that the agency planned to move the portal onto a dot-gov site behind the secure federal firewall. Still, he said, experts concluded there was "no evidence of criminal or suspicious activity" involving the dot-org portal and "minimal to no risk of unauthorized access."

But a complaint made to the inspector general hotline had already triggered an internal audit of biowatchportal.org.

The audit turned up 41 vulnerabilities, and a scan detected a possible attempt by a hacker to access the portal. The auditing team was unable to validate the scan's finding, and the team recommended that the contractor overseeing the site investigate. It is unclear whether that was done.

The contractor, Logistics Management Institute, declined to provide a comment. Walter, Fluty and Lynch did not respond to emails or phone calls from The Times.

'DHS will never know'

In January 2017, Jackson published his concerns about the portal in the Journal of Bioterrorism & Biodefense. His article detailed what he called "negligent" security that required only single-factor authentication to access the website.

Department of Homeland Security officials removed BioWatch from Jackson's portfolio, then suspended his security clearance and later placed him on administrative leave. They notified him that he had not sought the proper approval to publish his article and that it included information that should not have been made public. They also cited his recent conviction for drunk driving.

Jackson filed whistleblower complaints with several federal

agencies, alleging he was the victim of retaliation for criticizing the program's security. In one, he wrote that a successful hacker could "monitor the system, manipulate data, and create false flags so as to stake out federal, state and local response to a possible incident." The complaint continued: "To this date, DHS will never know the harm that has resulted from this because there is no intrusion detection capability."

The inspector general's report published later that year said no classified information was found on the BioWatch portal, but it confirmed that "critical and high risk vulnerabilities" could allow an attacker to access sensitive information on the site.

In October 2017, Homeland Security reinstated Jackson's security clearance but issued him a warning. A letter notifying him of the decision did not address his whistleblower claim. He left the agency a few weeks later.

No federal agency has agreed to investigate Jackson's complaints. In May, he filed an appeal with the Office of the Intelligence Community Inspector General. He is awaiting a response.

North Korea Denies Making $2bn from Cyber-Attacks

Source: https://www.infosecurity-magazine.com/news/north-korea-denies-cyber-attacks/

Sep 03 – **North Korea has denied allegations that it obtained $2bn by carrying out state-sponsored cyber-attacks on banks and cryptocurrency exchanges.**

Claims that the one-party republic had used "widespread and increasingly sophisticated" cyber-attacks to steal money to fund the development of weapons of mass destruction (WMDs) were made in a confidential United Nations report submitted to the UN Security Council North Korea Sanctions Committee in July this year.

As reported by news agency Reuters in August, the report stated: "Democratic People's Republic of Korea cyber actors, many operating under the direction of the Reconnaissance General Bureau, raise money for its WMD (weapons of mass destruction) programs, with total proceeds to date estimated at up to two billion US dollars."

On Sunday, North Korea's state-controlled news agency KCNA reported that a spokesperson for the National Coordination Committee of the Democratic People's Republic of Korea (DPRK) for Anti-Money Laundering and Countering the Financing of Terrorism said: "The United States and other hostile forces are now spreading ill-hearted rumors that we have illegally forced the transfer of $2bn needed for the development of WMD programs by involving cyber actors."

The spokesperson went on to liken "the fabrication of such a sheer lie" to "the same old trick as Hitler fascist propagandists used to cling to."

Chief among the allegations against North Korea is a claim that the country is deeply connected to hacking group Lazarus, which has been linked to an $81m cyber-heist that targeted the Bangladesh central bank in 2016. The group was also accused by the U.S. Federal Bureau of Investigation of hacking into Sony Pictures in 2014.

According to the NCC spokesperson's statement, the DPRK's accusers fabricated the cybercrime allegations to justify the use of sanctions against the country.

The spokesperson said: "Such a fabrication by the hostile forces is nothing but a sort of a nasty game aimed at tarnishing the image of our Republic and finding justification for sanctions and a pressure campaign against the DPRK."

Internet content of terrorists detected, deleted faster than ever: UN official

Source: https://www.devdiscourse.com/article/headlines/658522-internet-content-of-terrorists-detected-deleted-faster-than-ever-un-official

Sep 04 – Although terrorists have become skilled at manipulating the Internet and other new technologies, artificial intelligence or AI, is a powerful tool in the fight against them, a top UN

counter-terrorism official said this week at a high-level conference on strengthening international cooperation against the scourge.

Co-organized by Belarus and the United Nations Office of Counter-Terrorism (UNOCT), "Countering terrorism through innovative approaches and the use of new and emerging technologies" concluded on Wednesday in Minsk.

The internet "expands technological boundaries literally every day" and AI, 3D printing biotechnology innovations, can help to achieve the Sustainable Development Goals (SDGs), said Vladimir Voronkov, the first-ever Under-Secretary-General for the UN Counter-Terrorism Office.

But it also provides "live video broadcasting of brutal killings", he continued, citing the recent attack in the New Zealand city of Christchurch, where dozens of Muslim worshippers were killed by a self-avowed white supremacist.

"This is done in order to spread fear and split society", maintained the UNOCT chief, warning of more serious developments, such as attempts by terrorists to create home-made biological weapons.

He pointed out that terrorists have the capacity to use drones to deliver chemical, biological or radiological materials, which Mr. Voronkov said, "are even hard to imagine."

But the international community is "not sitting idly by", he stressed, noting that developments in this area allow the processing and identification of key information, which can counter-terrorist operations with lightning speed.

"The Internet content of terrorists is detected and deleted faster than ever", elaborated the UNOCT chief. "Fifteen to twenty minutes is enough to detect and remove such content thanks to machine algorithms".

Crediting quantum computing coupled with the use of AI, he explained that accelerated information processing enables terrorist tracing.

Mr. Voronkov added that the use of blockchain registration – a growing list of records, or blocks, that are linked using cryptography – is also being explored to identify companies and individuals responsible for financing terrorism.

"It is necessary to increase the exchange of expert knowledge on technologies such as 3D printing, synthetic biology, nanotechnology, robotics, the synthesis of the human face and autonomous weapons", he underscored. "This will help to better identify and respond to risks before it is too late".

The two-day conference was divided into three themed sessions that focused at global, regional and national levels on the misuse of new technologies and AI by terrorists; approaches and strategies to counteract terrorist propaganda; and the misuse of scientific innovations.

Insurance Companies Are Fueling Ransomware Attacks

Source: http://www.homelandsecuritynewswire.com/dr20190904-insurance-companies-are-fueling-ransomware-attacks

Sep 04 – Ransomware is proliferating across America, disabling computer systems of corporations, city governments, schools and police departments. This month, attackers seeking millions of dollars encrypted the files of **22 Texas municipalities**. Overlooked in the ransomware spree is the role of an industry that is both fueling and benefiting from it: insurance. In recent years, cyber insurance sold by domestic and foreign companies has grown into an estimated **$7 billion to $8 billion-a-year market in the U.S. alone**, according to Fred Eslami, an associate director at AM Best, a credit rating agency that focuses on the insurance industry. While insurers do not release information about ransom payments, *ProPublica* has found that they often accommodate attackers' demands, even when alternatives such as saved backup files may be available.

Renee Dudley writes in *Defense One* that the FBI and security researchers say paying ransoms contributes to the profitability and spread of cybercrime and in some cases may ultimately be funding terrorist regimes. But for insurers, it makes financial sense, industry insiders said. It holds down claim costs by avoiding expenses such as covering lost revenue from snarled services and ongoing fees for consultants aiding in data recovery. And, by rewarding hackers, it encourages more ransomware attacks, which in turn frighten more businesses and government agencies into buying policies.

"The onus isn't on the insurance company to stop the criminal, that's not their mission. Their objective is to help you get back to business. But it does beg the question, when you pay out to these criminals, what happens in the future?" said Loretta Worters, spokeswoman for the Insurance Information Institute, a nonprofit industry group based in New York. Attackers "see the deep pockets. You've got the insurance industry that's going to pay out, this is great."

That Pill Is Watching You - Privacy and Hackability Of Ingestible Electronic Sensors

By Dr. Elizabeth Fernandez

Source: https://www.forbes.com/sites/fernandezelizabeth/2019/09/03/that-pill-is-watching-youprivacy-and-hackability-of-ingestible-electronic-sensors/#57ff1e7a405e

Sep 03 – What if, like in "Fantastic Voyage", your doctor could shrink down and enter your body, fixing whatever ailed you from the inside-out? Technology might not be that far behind. But instead of swallowing your doctor, you can swallow a tiny sensor, just the size of a pill, which can monitor all sorts of issues from within your body. These ingestible electronic sensors (IESs) may help to transform healthcare.

These sensors can then give a medical care team direct information about their patient, from whether they are taking the medicines correctly to their physical or mental state. Sensors like this can provide dramatically better care. However, whenever there is a digital aspect involved, there is also the potential for a lot to go wrong - from hacking to privacy issues. A recent commentary in Nature Electronics by Sara Gerke and collaborators urge the community to look at these ethical and legal issues associated with IESs.

IESs are small sensors. Once they enter the patient's stomach, they communicate with another sensor called a "Patch" on the skin. They can collect all sorts of data - from heart rate to body position to whether or not the patient is taking their medicine correctly. Sometimes they are used for patients of mental illness, such as schizophrenia, to assure that they are taking their medication, or can even help monitor something as simple as irritable bowel syndrome by monitoring different gas levels in the gut.

But Gerke and collaborators say there are several ethical issues to think about. Firstly, there are privacy concerns. In these cases, sensitive health data is being collected. It's not always clear who owns or can access the data. "The availability of this data in the hands of third

parties might have implications on life insurance premiums, employment opportunities, and even personal relationships," Gerke and collaborators point out.
It's also possible that the patient may feel "watched". They might not have a choice whether or not to use this technology. Their insurance might demand it, a family member might insist upon it.
Many patients aren't even really aware of the issues surrounding this technology. How many times have you just clicked accept in a user agreement? Patients may ignore it or not understand this user agreement, even when has to do with their own private, sensitive medical data. Clarity is needed.
There are other issues too. Some of these IESs make use of an app on the patient's cell phone. What happens when a patient can't afford a cell phone? And whenever there is wireless transmission of data, hacking is possible. Corrupt or hacked information could lead to doctors recommending treatments that are unsafe, and possibly even deadly, for the patient.
IESs have great potential to transform healthcare, but these ethical questions should not be an afterthought. "Privacy protection, cybersecurity, accountability, transparency, explainability, fairness, and robustness are of pivotal importance," Gerke says.

Dr. Elizabeth Fernandez *is the host of SparkDialog Podcasts, which covers the intersection of science and society. She has a PhD in astrophysics from the University of Texas at Austin and has worked around the world in both astronomy and in science and society. She currently specializes in how science and technology are impacting our lives.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

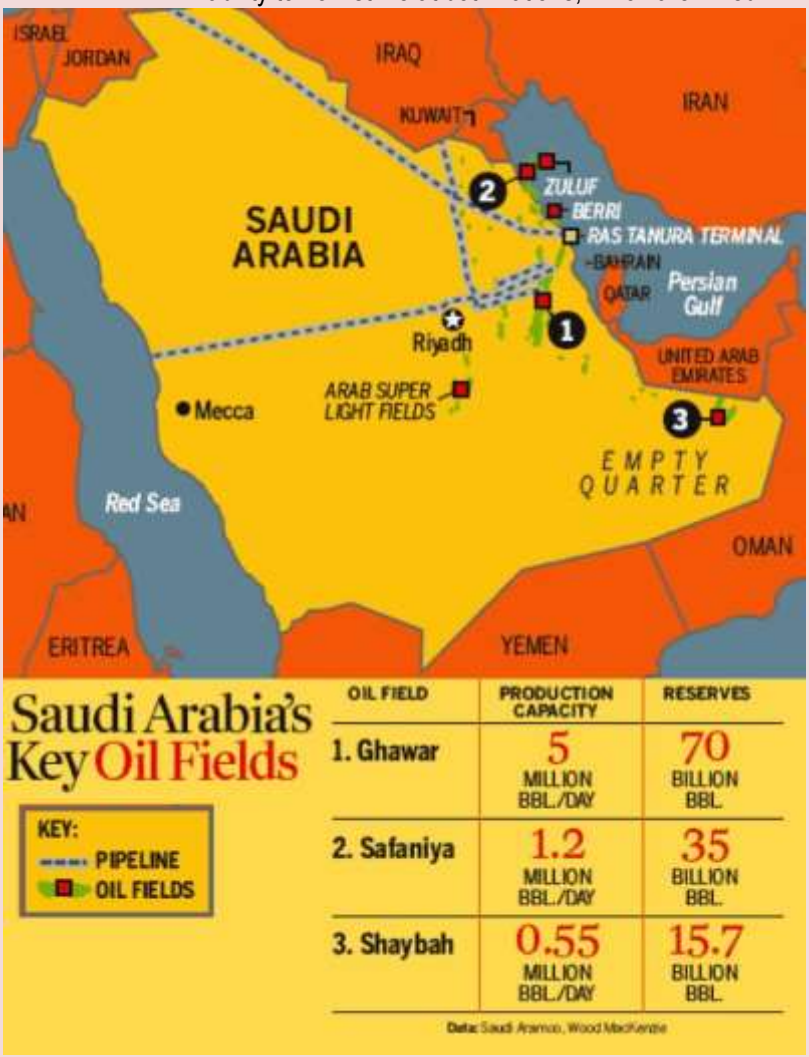
Yemen rebel drone attack targets remote Saudi oil field

Source: https://www.israelhayom.com/2019/08/18/yemen-rebel-drone-attack-targets-remote-saudi-oil-field/

Aug 18 – Saudi Arabia describes the damage as a "limited fire" in the second such recent attack on its crucial energy industry. Houthi spokesman says rebels launched 10 bomb-laden drones targeting the field in their "biggest-ever" operation; threatens more attacks coming.

Drones launched by Yemen's Houthi rebels attacked a massive oil and gas field deep inside Saudi Arabia's sprawling desert on Saturday, causing what the kingdom described as a "limited fire" in the second such recent attack on its crucial energy industry.

The attack on the Shaybah oil field, which produces some 1 million barrels of crude oil a day near the kingdom's border with the United Arab Emirates, again shows the reach of the Houthis' drone program. Shaybah sits some 1,200 kilometers (750 miles) from Houthi-controlled territory, underscoring the rebels' ability to now strike at both nations, which are mired in Yemen's years-long war.



Saudi Arabia's Key Oil Fields

KEY: PIPELINE, OIL FIELDS

OIL FIELD	PRODUCTION CAPACITY	RESERVES
1. Ghawar	5 MILLION BBL./DAY	70 BILLION BBL.
2. Safaniya	1.2 MILLION BBL./DAY	35 BILLION BBL.
3. Shaybah	0.55 MILLION BBL./DAY	15.7 BILLION BBL.

Data: Saudi Aramco, Wood MacKenzie

The drone assault also comes amid heightened tensions in the Mideast between the US and Iran, whose supreme leader hosted a top Houthi official days earlier in Tehran.

State media in Saudi Arabia quoted Energy Minister Khalid al-Falih as saying production was not affected at the oil field and no one was wounded in the attack on Saturday. The state-run Saudi Arabian Oil Co., known widely as Saudi Aramco, issued a terse statement acknowledging a "limited fire" at a liquid natural gas facility at Shaybah.

A satellite image obtained by The Associated Press showed black smoke rising just west of the natural gas facility that wasn't seen in images from prior days. The facility is just north of the airstrip that Saudi Aramco built to fly staffers into the remote region.

The Saudi acknowledgment of the attack came hours after Yahia Sarie, a military spokesman for the Houthis, issued a video statement claiming the rebels launched 10 bomb-laden drones targeting the field in their "biggest-ever" operation. He threatened more attacks would be coming.

"This is in response to their aggression toward us and our people in Yemen," Sarie said.

Al-Falih linked the attack to a May assault by Houthi drones that targeted the kingdom's crucial East-West Pipeline, a 1,200-kilometer-link between its eastern oil fields and the Red Sea. He also mentioned recent explosions on oil tankers near the Strait of Hormuz that the US blames on Iranian-planted limpet mines. Iran denies being behind those attacks.

"This act of terrorism and sabotage is only an extension of those acts that have recently targeted the global oil supply chains, including oil pipelines in the kingdom, and oil tankers," al-Falih said.

"This cowardly attack once again highlights the importance of the international community's response to all terrorist actors who carry out such acts of sabotage, including the Houthi militias."

The oil field at Shaybah is in the Arabian Peninsula's Empty Quarter, a sea of sand where temperatures routinely hit 50 degrees Celsius (120 degrees Fahrenheit). Saudi Aramco on its website refers to the field as "the most remote treasure on Earth," home to reserves of 14.3 billion barrels of oil and 25 trillion cubic feet of natural gas.

The field's distance from rebel-held territory in Yemen demonstrates the range of the Houthis' drones. UN investigators have said that the Houthis' new UAV-X drone, found in recent months during the Saudi-led coalition's war in Yemen, likely has a range of up to 1,500 kilometers (930 miles). That puts Saudi oil fields, an under-construction Emirati nuclear power plant and Dubai's busy international airport within their range.

Unlike sophisticated drones that use satellites to allow pilots to remotely fly them, analysts believe Houthi drones are likely programmed to strike a specific latitude and longitude and cannot be controlled once out of radio range. The Houthis have used drones, which can be difficult to track by radar, to attack Saudi Patriot missile batteries, as well as enemy troops.

Saudi Arabia and the UAE launched their war against the Houthis in March 2015 to back the country's internationally recognized government. The UAE recently began withdrawing troops from the conflict while UAE-allied separatists recently seized the city of Aden, further complicating a war that is seen as the world's worst humanitarian crisis.

Jihadi killed when his drone bomb ran low on battery and flew back

Source: https://www.nzherald.co.nz/world/news/article.cfm?c_id=2&objectid=12262933

Aug 29 – An Isis fighter was killed by his own drone bomb when the hapless jihadi forgot to charge the device's batteries - sending it straight back to him when its power ran low.

His death came during the Battle for Mosul and has been revealed after a security source came forward to share the story.

The source told the Sun: "We learned this idiot had wired up his drone with explosives but was killed when its batteries ran low and it flew home."

"With a weak signal for some reason it detonated over his head."

Isis used drones frequently during the fight for control of the northern Iraqi city of Mosul, which officially ended in 2017.

British troops remain in the area training Iraqi troops and still face drone attacks.

The improvised aerial weapon is made by turning small, inexpensive drones into flying bombs or adapting them to drop grenades.

The sourced added: "Drone warfare is hugely effective for insurgents.

"They can see where we are operating, choose targets then launch a coordinated attack from up to three miles away."

"This caused quite a laugh for us but the drone threat is very real. The fighter killed himself last year due to his own ineptitude, but is still keeping morale high today."

Egozi: Explosive Drones are Small but Dangerous

Source: https://i-hls.com/archives/94245

Aug 26 – During recent years, the drone threat has evolved at a record rate. Cheap, small drones which can be easily turned into lethal systems. Some of the solutions are still under development, but the threat has been growing from day-to-day.

On Saturday, 24/8, IDF Spokesperson reported that the Israeli Air Force had attacked targets in the vicinity of Damascus, thwarting in the field a terrorist attempt by the Iranian Quds force. According to the IDF, the terrorist attack was supposed to be operated by attack drones, and was planned to be launched from Syria against Israeli targets.

IDF Spokesperson, Brig. Gen. Ronen Manelis, said that combat aircraft had attacked several terrorist targets at the village of Akrabe, South of Damascus: "Recently, we have been tracking these operational preparations led by Qasem Suleimani, directed at the perpetration of this attack via the launch of several attack drones towards northern Israel. We attacked several targets in Akrabe, where Iranian and Shi'ite militia activists are operating, including the equipment that was supposed to be used in this terrorist attack."

It was also reported that "the unit tried to perpetrate this attack already on Thursday, but we succeeded in thwarting it."

Apparently, improved models have reached Syria, capable of operating a "swarm attack".

The Iranians have also developed the capability of swarm drone attacks involving a large number of drones, a method that makes it difficult for detection systems to detect all drones within the timeframe that enables their interception.

The danger has not gone away. According to all estimations, Iran will bring to the region more Iranian-made drones and UAVs.

As said, Israel is equipped with detection and neutralization systems, but these do not solve the problem, and further development is required in response to this growing danger.

Israeli drone dropped incendiary substance in border forest - Lebanon army

Source: https://www.euronews.com/2019/09/01/israeli-drone-dropped-incendiary-substance-in-border-forest-lebanon-army

Sept 01 – The Lebanese military said an Israeli drone, which violated Lebanon's airspace, dropped incendiary material and sparked a fire in a pine forest by the border on Sunday.

The fires near the border in Lebanon "originate with operations by our forces in the area," the Israeli military said in a statement without elaborating.

The Lebanese army statement said it was following up with U.N. peacekeepers but gave no further details.

Residents and security sources at the border in south Lebanon say Israel has in recent days fired flare bombs into the Israeli-occupied Shebaa farms along the border.

Lebanese state news agency NNA said Israeli forces fired flare bombs there on Saturday – a tactic sometimes used to burn away brush to prevent an ambush.

Israel's military said on Saturday it had ordered extra forces to deploy near the border, amid rising tensions with Lebanon's Hezbollah movement.

The leader of Iran-backed Hezbollah, Sayyed Hassan Nasrallah, said his field commanders were prepared to retaliate to a drone attack in Beirut's suburbs a week ago, which he has blamed on Israel.

The two old enemies last fought a deadly month-long war with each other in July 2006.

Lebanese soldiers, who do not have air defence systems, opened fire at Israeli drones in southern Lebanon earlier this week.

Israeli aircraft regularly enter Lebanese airspace, but it is rare for Lebanon's army to target them. Beirut has sent several complaints to the United Nations before about Israeli drones and jets breaching its airspace.

Cyprus – Unmanned Turkish aerial vehicles disrupting Paphos Airport's flight paths

Source: http://en.protothema.gr/unmanned-turkish-aerial-vehicles-disrupting-paphos-flight-paths/

Sep 04 – Authorities on Wednesday confirmed reports that the presence of Turkish unmanned aerial vehicles (UAVs) is forcing aircraft to and from the Paphos airport to change their course.

But they said the situation is under control.

The confirmation follows an article in daily Philelefthеros on Wednesday reporting that Turkish UAVs have been flying frequently off Paphos in the area where the Turkish drillship Fatih is operating, and as a result air traffic controllers have been forced on several occasions to ask aircraft that are either landing at or taking off from Paphos airport to change their course.

According to the paper the flights of these UAVs – Bayraktar TB2 type – had increased during July and August. The Turkish vessels fly for long periods of time in circles over the area where the Fatih is located.

The head of the civil aviation's Nicosia Area Control Centre, Haris Antoniades said there are Turkish UAVs flying between Antalya and Paphos but that the situation was "manageable".

Terror accused plotted lone UK army barracks drone attack

Source: https://www.bbc.com/news/uk-england-manchester-49645627

Sep 10 – An Islamic State supporter plotted to attack an Army barracks with a modified drone, a court has heard. Hisham Muhammad, 25, wanted to use the remote-controlled aerial vehicle to drop a projectile or harmful device, the Old Bailey was told.

When police raided his house in Bury, Greater Manchester, they found diagrams and materials for the homemade drone attachment, jurors heard. Mr Muhammad denies engaging in conduct in preparation for acts of terrorism.

Prosecutor Anne Whyte QC said Mr Muhammad had steeped himself in barbarous Islamic State propaganda. A number of knives were among the suspicious items found in Hisham Muhammads house.

Prosecutors allege he planned to launched a lone wolf attack on Castle Armoury Barracks in Bury, which he visited before his arrest last June. The court heard he planned to attack a military or police target in a drone and knife attack.

Mr Muhammad's home in Victoria Street, Whitefield, was raided by police after landlord Onkar Singh came across several "suspicious" items including knives, a soldering iron and a tub of wires. Officers found a stash of weapons, including a tomahawk, a machete and

bear-claws, jurors heard. They also found red lollipop sticks attached to an electrical component with black tape and various wires, described in court as a prototype of the drone attachment.
Police also seized two Japanese ninja eggs – shells containing crushed chilli seeds and shards of glass.
Hisham Muhammad allegedly wanted to target Castle Armoury Barracks in Bury, Greater Manchester.

Mr Muhammad, who is originally from Bermuda and moved to Britain in 2013, had allegedly researched other Army and police bases.

EDITOR'S COMMENT: (1) Always so pissed when criminals and terrorists are addressed as "Mr.X"! (2) This time intel worked just fine. But there will be a next time if commercial drones continue to be available to the public. **Control drone market or be sorry**. Very sorry! Soon!

Saudi Arabia oil facilities ablaze after drone strikes

Source: https://www.bbc.com/news/world-middle-east-49699429

Sep 14 – Drone attacks have set alight two major oil facilities run by the state-owned company Aramco in Saudi Arabia, state media say.
Footage showed a huge blaze at Abqaiq, site of Aramco's largest oil processing plant, while a second drone attack started fires in the Khurais oilfield.
The fires are now under control at both facilities, state media said.

A spokesman for the Iran-aligned Houthi group in Yemen said it had deployed 10 drones in the attacks.
The military spokesman, Yahya Sarea, told al-Masirah TV, which is owned by the Houthi movement and is based in Beirut, that further attacks could be expected in the future.
He said Saturday's attack was one of the biggest operations the Houthi forces had undertaken inside Saudi Arabia and was carried out in "co-operation with the honourable people inside the kingdom".
Saudi officials have not yet commented on who they think is behind the attacks.
"At 04:00 (01:00 GMT), the industrial security teams of Aramco started dealing with fires at two of its facilities in Abqaiq and Khurais as a result of... drones," the official Saudi Press Agency reported.
"The two fires have been controlled."
There have been no details on the damage but Agence France-Presse quoted interior ministry spokesman Mansour al-Turki as saying there were no casualties.

Abqaiq is about 60km (37 miles) south-west of Dhahran in Saudi Arabia's Eastern Province, while Khurais, some 200km further south-west, has the country's second largest oilfield.
Saudi security forces foiled an attempt by al-Qaeda to attack the Abqaiq facility with suicide bombers in 2006.

An attack method open to all

Jonathan Marcus, BBC defence and diplomatic correspondent

This latest attack underlines the strategic threat posed by the Houthis to Saudi Arabia's oil installations.
The growing sophistication of the Houthis' drone operations is bound to renew the debate as to where this capability comes from. Have the Houthis simply weaponised commercial civilian drones or have they had significant assistance from Iran?
The Trump administration is likely to point the finger squarely at Tehran, but experts vary in the extent to which they think Iran is facilitating the drone campaign.
The Saudi Air Force has been pummelling targets in Yemen for years. Now the Houthis have a capable, if much more limited, ability to strike back. It shows that the era of armed drone operations being restricted to a handful of major nations is now over.
Drone technology - albeit of varying degrees of sophistication - is available to all; from the US to China, Israel and Iran... and from the Houthis to Hezbolllah.

Markets await news from key facilities

Analysis by BBC business correspondent Katie Prescott

Aramco ranks as the world's largest oil business and these facilities are significant.
The Khurais oilfield produces about 1% of the world's oil and Abqaiq is the company's largest facility - with the capacity to process 7% of the global supply. Even a brief or partial disruption could affect the company, and the oil supply, given their size.
But whether this will have an impact on the oil price come Monday will depend on just how extensive the damage is. Markets now have the weekend to digest information from Aramco and assess the long-term impact.
According to Richard Mallinson, geopolitical analyst at Energy Aspects, any reaction on Monday morning is likely to be muted, as markets are less worried about supply than demand at the moment, due to slower global economic growth and the ongoing trade war between the US and China.
However, there are concerns that escalating tensions in the region could pose a broader risk, potentially threatening the fifth of the world's oil supply that goes through the critical Strait of Hormuz.

Who are the Houthis?

The Iran-aligned Houthi rebel movement has been fighting the Yemeni government and a Saudi-led coalition.
Yemen has been at war since 2015, when President Abdrabbuh Mansour Hadi was forced to flee the capital Sanaa by the Houthis. Saudi Arabia backs President Hadi, and has led a coalition of regional countries against the rebels.
The coalition launches air strikes almost every day, while the Houthis often fire missiles into Saudi Arabia.
Mr Sarea, the Houthi group's military spokesman, told al-Masirah that operations against Saudi targets would "only grow wider and will be more painful than before, so long as their aggression and blockade continues".
Image copyright EPA Image caption Saudi-led coalition air strikes regularly target Houthis in Yemen
Houthi fighters were blamed for drone attacks on the Shaybah natural gas liquefaction facility last month and on other oil facilities in May.
There have been other sources of tension in the region, often stemming from the rivalry between Saudi Arabia and Iran.
Saudi Arabia and the US both blamed Iran for attacks in the Gulf on two oil tankers in June and July, allegations Tehran denied.
In May, four tankers, two of them Saudi-flagged, were damaged by explosions within the UAE's territorial waters in the Gulf of Oman.

Saudi Arabia and then US National Security Adviser John Bolton blamed Iran. Tehran said the accusations were "ridiculous".
Tension in the vital shipping lanes worsened when Iran shot down a US surveillance drone over the Strait of Hormuz in June, leading a month later to the Pentagon announcing the deployment of US troops to Saudi Arabia.

Terrorists' Use of Drones Promises to Extend Beyond Caliphate Battles

By Anne Speckhard and Ardian Shajkovci
Source: https://www.hstoday.us/subject-matter-areas/terrorism-study/terrorists-use-of-drones-promises-to-extend-beyond-caliphate-battles/

March 2019 – Unmanned and remote-controlled aircrafts, i.e. drones, continue to change the character of contemporary warfare.[i] It was satellites and drones, alongside a good deal of human intelligence, that located Osama bin Laden in Afghanistan in 2000[ii] and later, right up to the minute of the raid, helped to zero in on his compound in Abbottabad, Pakistan.[iii]
Drones in the hands of governments have raised considerable controversy as the unmanned aircrafts were excessively relied upon during the Obama administration to carry out targeted assassinations against terrorist leaders in Somalia, Yemen and Northern Pakistan, to name a few. Their increased usage, by both the U.S. military and CIA, caused complaints that drone kills carried out by the CIA were illegal, that drone kills of terrorists in their homes also killed innocent family members visiting or residing with them, and that killing versus arresting terrorists sacrificed valuable intelligence that could be otherwise gathered in a capture operation.
Controversy also arose over the usage of drones by governments to target their own citizens serving in terrorist organizations. In 2015, Reyaad Khan, a UK citizen who had joined ISIS, was killed in a drone strike. British Prime Minister Theresa May defended drone usage in targeted killings on the grounds that they are "necessary and proportionate" to ISIS' use of violence.[iv] Likewise, Americans Adam Gadahn and Ahmed Farouq, two senior al-Qaeda operatives, were also killed by drones in 2015, although the extent to which they were deliberately targeted remains debatable.[v] Similarly, U.S. drone strikes led to the killing of Anwar al-Awlaki, an American-born radical cleric and imam, in Yemen in 2011.[vi] More disturbingly, al-Awlaki's American son, 16-year-old Abdulrahman al-Awlaki, was also killed in a drone strike two weeks later, raising serious ethical concerns about the use of drone kills against U.S. citizens, particularly minors.
The use of drones by non-state actors has been documented as well. Both Hamas and Hezbollah used Iranian-manufactured drones to conduct surveillance over Israeli-controlled territories.[vii] In addition, drones had become central to ISIS' military operations, in varying capacities, since at least 2014.[viii] The group had managed to take advantage of drone usage in recent years, namely to utilize them from gathering intelligence through aerial photography, to making aerial video recordings of their attacks for use in their propaganda films, to geographic mapping, to border control surveillance and delivery of explosive, chemical and biological weapons.
Research shows that, generally speaking, ISIS had been able to develop its drone programs without any support from state actors, although many of its drones were, according to our interviews and other sources, transferred into Syria via Turkey by non-state terrorist actors. ISIS was also able to magnify their usage and impact by studying guides and following instructions on drone modification and weaponization.[ix] In addressing the use of drones by the Islamic State, some researchers have noted: "The Islamic State is a group known for doing things a bit differently, for its capacity for innovation, and for its many 'firsts.' The first occurred in October 2016 when the group used a bomb-laden drone to kill, after the explosive hidden within the drone killed two Kurdish Peshmerga soldiers who were investigating the device. Another 'first' happened in January 2017 when the Islamic State released a propaganda video that showed nearly a dozen examples of the group releasing munitions on its enemies from the air with a fair degree of accuracy via quad copter drones it had

modified. And it wasn't long before the group's bomb-drop capable drones would go on to kill, too.[x]"
In January 2019 a YPG media representative told ICSVE researchers that she and her media group had been forced to flee the ISIS front (near Hajin, Syria, at the time) as an ISIS drone locked in on and bombed them from the air, pursuing them as they took shelter in a nearby building.
In February 2019, ICSVE researchers had the opportunity to view firsthand some of the captured arsenal of ISIS utilized and manufactured drones, both weaponized and non-weaponized, used against Iraqi and enemy forces. In addition to bomb components, snipers, laptops, and pistols used in public executions, among others, which were displayed as war trophies in the war against ISIS in a museum in Baghdad, Iraqi military and security forces also paraded dozens of drones seized by the Islamic State following a number of decisive and breakthrough battles against the terrorist group (See pics 1 and 2).

Sky Hunter: estimated payload 4-50kg

Modified DJI drone for payload delivery

While ISIS has lost most of its territories it once held in Iraq and Syria, the use of drones and emerging technologies by terrorists and their supporters remains worrisome. In September 2018, Danish authorities arrested two individuals suspected of buying drones and attempting to ship them via Turkey, to the Islamic State in Iraq and Syria. They were believed to be a part of a much larger network. [xi]
The dangers emanating from unmanned aircraft has been also documented in a recent attempt to assassinate Venezuelan President Nicholas Maduro. Moreover, some researchers have cited "off-the-shelf technology and tactical flexibility" associated with drones, coupled with state sponsorship of terrorist groups, as potential factors increasing the likelihood of terrorist drone attacks in the future.[xii]
FBI Director Christopher Wray has also warned of the potential for drone attacks against U.S. citizens, given their availability and ease of use. [xiii] Given that attacks by terrorists and violent extremist groups involving drones are likely to become more common in the future, we must not underestimate their efficacy in the hands of terrorists in both perpetrating direct attacks and serving as effective surveillance tools to gather intelligence that could facilitate the planning and commission of attacks by other means.

***Anne Speckhard, Ph.D.**, is Director of the International Center for the Study of Violent Extremism (ICSVE) and serves as an Adjunct Associate Professor of Psychiatry at Georgetown University School of Medicine. She has interviewed over 600 terrorists, their family members and supporters in various parts of the world including in Western Europe, the Balkans, Central Asia, the Former Soviet Union and the Middle East.*
***Ardian Shajkovci, Ph.D.**, is the Director of Research and a Senior Research Fellow at the International Center for the Study of Violent Extremism (ICSVE). He has been collecting interviews with ISIS defectors and studying their trajectories into and out of terrorism as well as training key stakeholders in law enforcement, intelligence, educators, and other countering violent extremism professionals on the use of counter-narrative messaging materials produced by ICSVE both locally and internationally. He has also been studying the use of children as violent actors by groups such as ISIS and how to rehabilitate them. He has conducted fieldwork in Western Europe, the Balkans, Central Asia, and the Middle East, mostly recently in Jordan and Iraq.*

Drones as weapons

By the Editor of C²BRNE Diary

What we have so far world wide:

Conventional attacks or attempts:

- **UK 1:** Commercial unarmed drones greatly disturbed Heathrow and Gatwick airports. If interfered to the landing or take-off phase of an airliner they could shoot-down the airplane (London, 2019).
- **UAE:** An armed group (Houthis?) claimed to have sent an armed drone to attack the international airport in Abu Dhabi (2018). A commercial drone disrupted operations at Dubai's International Airport (2019).
- **UK2:** Attempted plot to attach military barracks (Manchester, 2019).
- **Cyprus:** Turkish military drones endangered civilian flishts at Paphos airport (2019).
- **Saudi Arabia:** Houthis drones attacked several oil facilities and airports (2019).
- **Lebanon:** Israeli drones accused for setting forest fires in the borders with Lebanon (2019).
- **USA:** Commercial drone landed inside the garden of the White House (Washington, DC. 2015).
- **France & Belgium:** Suspicious drone flights over French and Belgian nuclear facilities (2014). Greenpeace drone crashed over nuclear power station near Lyon, France (2018).
- **Afghanistan:** US armed drones used in many occasions against Taliban and al Qaeda leading terrorists – in fact the birthplace of armed drones' use.
- **Syria and Iraq:** ISIS armed commercial drones used against regime and coalition forces (2018) – first time a terrorist organization added explosive payloads on drones.
- **Venezuela:** two drones detonated explosives near Avenida Bolívar, Caracas, where Nicolás Maduro, the President of Venezuela, was addressing the Bolivarian National Guard in front of the Centro Simón Bolívar Towers and Palacio de Justicia de Caracas (2018).
- **Libya:** Turkish armed drones attacked Haftar's regime (2019).
- **Yemen:** Armed US drones were used many times against local insurgents[1].
- **Mexico:** Mexican cartel attaches bomb to drone (2017).

Asymmetric (non-conventional/CBRN) attacks or attempts

- **Japan:** A commercial drone carrying a vial with radioactive material landed on the roof of the building where the office of the Japanese Prime Minister is (2015).

Possible (future) targets

- Oil tankers passing hot/conflict zones;
- Cruisers (anywhere – i.e. in the Mediterranean Sea launched from Libya);
- Qatar's oil/gas facilities (member of the KSA-led Arab coalition fighting Houthis) – same for UAE (and Kuwait/Bahrain even they are more distant); also, members of the coalition;
- Nuclear power plants (existing or under construction);
- Military camps and airbases/warships (i.e. the Anad Base drone strike near Aden);
- Critical infrastructure facilities (power grid, chemical plants, dams);
- Random attacks against populated cities;
- Airports and Ports;
- Pyroterrorism operations (Northern Europe; Russia);
- Landmarks attacks in major European (but not exclusively) capitals;
- Drones spraying a bioterrorism agents or chemical warfare agents over specific areas or crops (agroterrorism);
- Flying radiological dispersal drone against civic targets
- Cargo/freight trains with hazardous chemicals or radiological waste.
- Passenger trains and subway/metro (surface)

[1] https://www.justiceinitiative.org/voices/human-cost-secret-us-drone-strikes-yemen

- Schools and universities (civilian and military)
- Churches and mosques
- VIPs[2]

Payloads

- The drone as it is – big enough to cause injuries or destroy an airplane's turbine[3];
- Equipped with high explosives detonated remotely;
- Equipped with grenades (i.e. thermite type);
- Equipped with shrapnel to enhance the explosive potential;
- Equipped with a radiological source – preferably a gamma emitter;
- Equipped with a chemical warfare agent – detonation on impact or spraying over densely populated areas;
- Equipped with spore forming bacteria targeting the inhalation route but also can survive on the ground for long;
- Equipped with a high-power laser targeting the cockpit of commercial airliners from a close distance;
- Fly inside buildings with a machinegun adjusted and activated – "slaughterbots" (for the time being still a video[4] but…)

Worst case scenario (one out of many)

UAVs are now used to record mega events, thus the likelihood of a "rogue" drone (or more) blending in without raising suspicion cannot be ruled out[5].

In conclusion

It is obvious that drones are asymmetric weapons and can be used in a variety of ways and targets. If commercial drones continue to be in the market without any control and reasoning, then sooner or later a big bloody incident will follow. Not to mention the drone taxis and passenger drones[6] that can be used for targeted attacks or that multiple drones may attack simultaneously in a so called "drone swarm attack" (e.g. a swarm consisting of 13 drones attacked two Russian bases in Syria; another UAE swarm attacked Tuskish UAV personnel in Libya). But even if commercial drones are not available to buy anymore, there is always the 3D printing solution that can construct almost anything. Predictions show that the number of COTS (Commercial off-the-shelf) UAVs in 2035 will be higher than that of manned aircrafts[7]. As one of the Editorial Team (M.H.) of the newsletter said "*the water is already out of the jar on that one. They are readily available throughout most of the world, and components even more so. I'm afraid now we have to look at mitigation*." So, it is not "how" anymore but "when" (urban attack)!

[2] https://arstechnica.com/information-technology/2013/09/german-chancellors-drone-attack-shows-the-threat-of-weaponized-uavs/

[3] https://www.nytimes.com/2017/10/17/world/canada/canada-drone-plane.html

[4] https://money.cnn.com/2017/11/14/technology/autonomous-weapons-ban-ai/index.html
Video: https://www.youtube.com/watch?v=9CO6M2HsoIA&t=

[5] https://www.theatlantic.com/international/archive/2014/10/the-flag-flying-drone-that-sparked-a-soccer-brawl/381479/

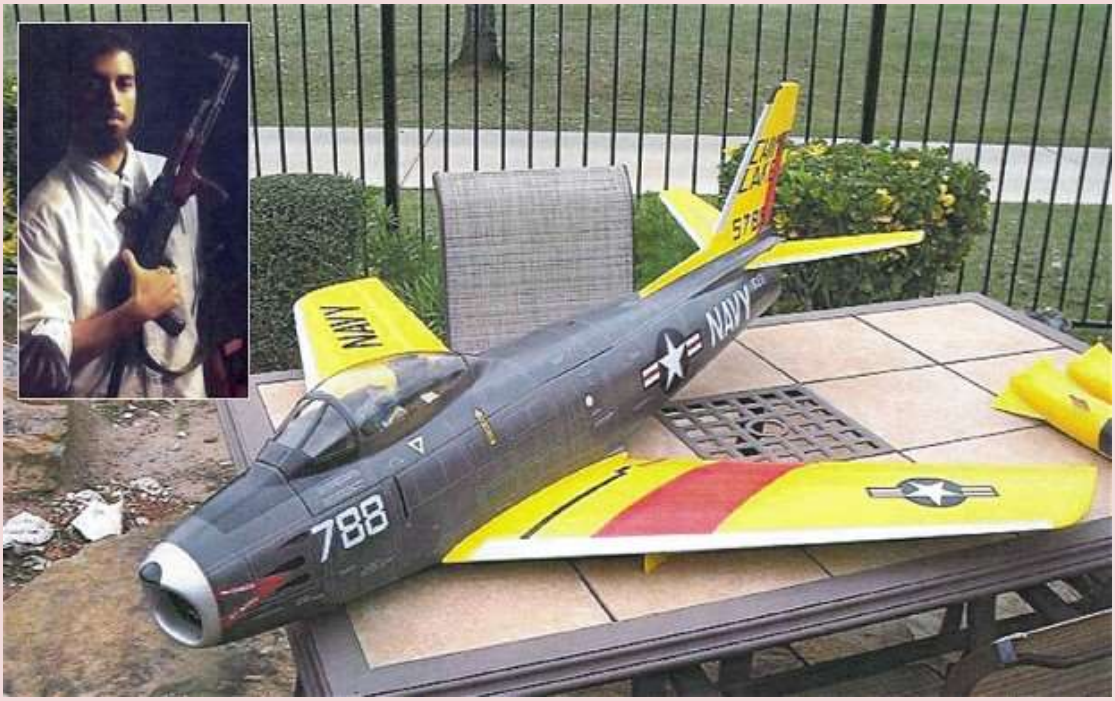
[6] https://blog.dronetrader.com/top-passenger-drones-helicopters-drone-taxis/

[7] https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/apr/Commercial_Drones.pdf

Also, do not forget this category

RC Model Airplanes

A new term in our vocabulary: Joystick terrorism



Jihadist jailed for Pentagon remote-control plane plot (2012)[8]

[8] https://www.telegraph.co.uk/news/worldnews/al-qaeda/9650194/Jihadist-jailed-for-Pentagon-remote-control-plane-plot.html

'Automated *vs.* Autonomous' Technologies – What is the Difference?

Source: https://i-hls.com/archives/94658

Sep 12 – Security technologies are often described as either "automated" or "autonomous." These words sound similar but have very different meanings. Both types of systems can provide immense value if used appropriately.

An automated drone system increases efficiency by eliminating the need for a drone operator, while providing seamless access to routine, frequent and real-time data. An autonomous drone, on the other hand, entails the absence of an operator that is responsible for the technology. Even at their most autonomous, however, drones still require an individual to preprogram their flight paths. A human set the objective, the machine can then decide between a number of approaches based on other situational data it may have collected and the current status of the objective.

Darkreading.com explores the differences between them, and while it focuses on IT environment, the differences can relate to other fields as well.

Autonomous Solutions – An autonomous system learns and adapts to dynamic environments and makes decisions (or takes actions) based on ever-changing data. Such systems use machine learning (ML) and artificial intelligence (AI) to learn from data, and the more data they ingest, the better they learn. In certain applications, autonomous systems eventually will become more reliable than humans and will perform tasks at an efficiency level not humanly possible.

Automated Solutions run within a well-defined set of parameters that consistently execute the steps as defined. The decisions made or actions taken by an automated system are based on predefined rules, and the system will perform those decisions/actions perfectly every time, eliminating the possibility of human error.

The concern about autonomous systems stems from the fact that they might be deployed for the wrong purpose. For example, if you're building a system that's highly predictable and performs the same function repeatedly, then an automated system provides value because it is simpler, easier to maintain, and requires fewer resources to continue working. Leveraging autonomous systems for these types of solutions may wind up being overly complex relative to the job being performed and introduces unnecessary risks, such as the systems learning incorrectly and performing the wrong action in the future.

Autonomous solutions are best used when the full spectrum of possible scenarios is unknown, and therefore there are no predefined rules for how to respond to new situations. Self-driving cars are the go-to example of why autonomous solutions are necessary, because there are too many different variants for a rules-based approach.

In the world of cybersecurity, these solutions are important because hackers are constantly coming up with new attack methods. Suspicious activity that has never been seen before (and therefore no rules exist for it) could slip by an automated system, but this is what autonomous solutions are built to identify and respond to.

Use cases include the detection of anomalous activity in very large, complex data streams, the identification of unknown threats, etc.

Automated systems are best used in highly predictable scenarios and tasks for which a best practice already exists.

Warning Over Terrorist Attacks Using Drones Given by EU Security Chief

Source: https://www.forbes.com/sites/zakdoffman/2019/08/04/europes-security-chief-issues-dire-warning-on-terrorist-threat-from-drones/#b6309a47ae41

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

This is not new news—the threat from a drone attack on a crowded space in the West has been focusing security minds for some time now. And the real fear from a drone attack is that a chemical or biological payload could be delivered into the midst of a crowded space with relative ease. The challenge with such attacks has always been delivery. A drone takes that challenge away.

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

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

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

Last year, at a closed meeting with one of the U.K.'s leading soccer clubs, the stadium's security director told the room "there are two things that terrify us: a large vehicle driven at speed at thousands of fans as they head home after a match, and, of course, drones." The meeting room overlooked a stadium where 50,000 plus people gather 25 plus times a year, the threat from drones did not require elaboration.

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

Islamic State propaganda posters have already depicted a drone attack on the Eiffel Tower in Paris and

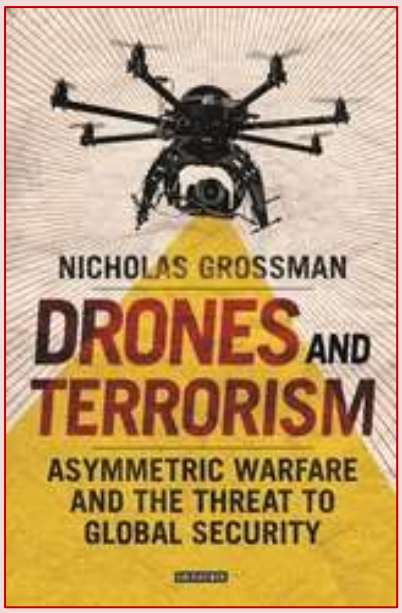
New York City, and former U.S. Secretary of Homeland Security, Kirstjen Nielsen has warned that the threat from drones "is outpacing our ability to respond… terrorist groups such as the Islamic State aspire to use armed drones against our homeland and US interests overseas… We have already worked with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

Remember, IS operatives have extensive drone experience from the Middle East. As U.K. police counter-terror lead Neil Basu pointed out, drones "have been used on the battlefield and what's used on the battlefield will eventually be adapted to be used on domestic soil."
The relative ease of availability and execution to mount a drone attack terrifies security agencies worldwide, and the context is that payload risk. The amount of explosive that can be carried by a commercial drone remains somewhat limited. A targeted attack on a high-profile location or an aeroplane in-flight would be possible but challenging to execute. In a crowded space it would generate headlines but limited damage. But a rudimentary attack using a non-explosive payload into an unprotected public space...
King's latest comments echo a similar warning in Europe from U.K. Defence Secretary Ben Wallace, who said last year that "terrorists continue to explore new ways to kill us on our streets: chemical and biological weapons are marching in closer. They have developed and worked on a better arsenal. We have to be prepared for the day that might come to our streets here."

EDITOR'S COMMENT: Why nobody listens to the alarms? But always listen the noise of the blast?

Drones and Terrorism

Source: https://www.bloomsbury.com/us/drones-and-terrorism-9781784538309/



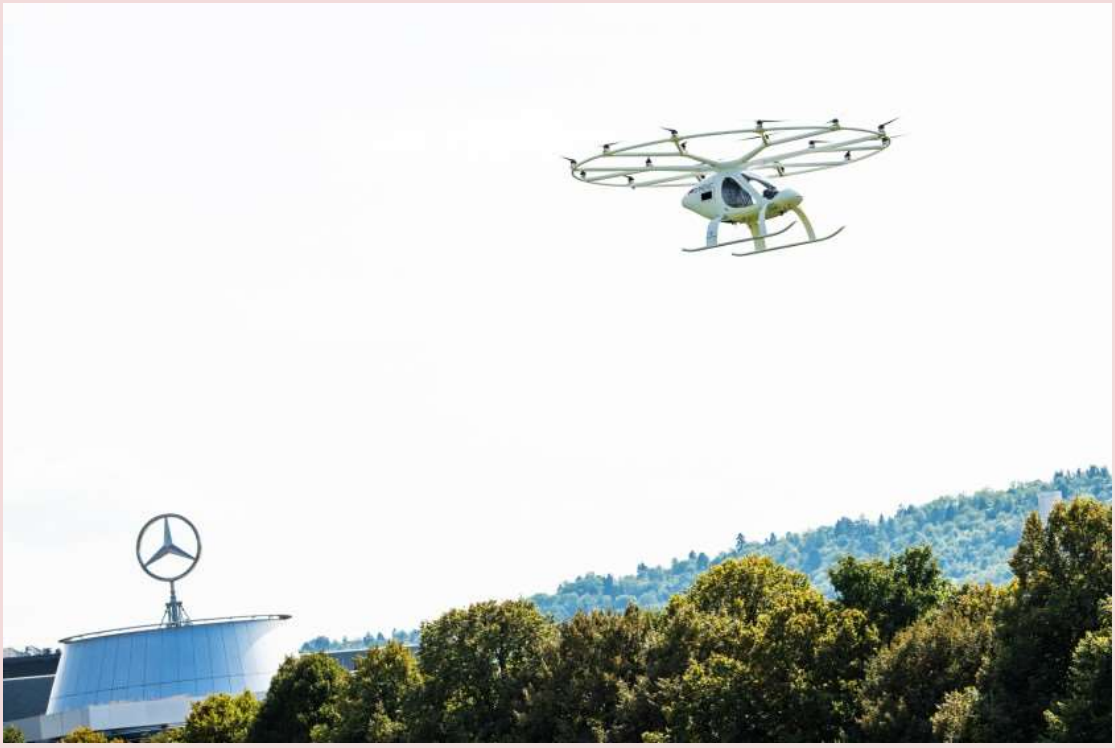
In warzones, ordinary commercially-available drones are used for extraordinary reconnaissance and information gathering. They can also be used for bombings - a drone carrying an explosive charge is potentially a powerful weapon. At the same time asymmetric warfare has become the norm - with large states increasingly fighting marginal terrorist groups in the Middle East and elsewhere. Here, Nicholas Grossman shows how we are entering the age of the drone terrorist - groups such as Hezbollah are already using them in the Middle East. Grossman will analyse the ways in which the United States, Israel and other advanced militaries use aerial drones and ground-based robots to fight non-state actors (e.g. ISIS, al Qaeda, the Iraqi and Afghan insurgencies, Hezbollah, Hamas, etc.) and how these groups, as well as individual terrorists, are utilizing less advanced comm ercially-available drones to fight powerful state opponents. Robotics has huge implications for the future of security, terrorism and international relations and this will be essential reading on the subject of terrorism and drone warfare.

Volcopter completes its first city demo flight in Europe

Source: https://newatlas.com/aircraft/volcopter-completes-city-demo-flight-europe/

Sep 15 – The team at Volocopter has ticked off another first, this time sending its 18-rotor unmanned aircraft into the skies over Stuttgart as part of its first urban demonstration flight in a European city center. The short jaunt follows a string of other recent demo flights as the aviation startup looks to make real inroads with its audacious flying taxi in the latter parts of the year.
In the world of flying taxis, Volocoper is certainly among the busier players on the scene. Its aircraft has previously flown as part of demonstrations in Dubai, at CES and in Germany, and has also attracted big name investors such as Daimler. In the last year alone, we've seen the company expand to Singapore, introduce a new, more powerful version and fly it amid airport traffic for the first time.

This latest outing for the Volocopter was part of a two-day event called Vision Smart City, which centers on a research project out of the Stuttgart University of Applied Sciences and explores the future of mobility. This includes an exploration of self-driving cars, connected cities and more environmentally friendly forms of transport, with Daimler-owned Mercedes-Benz among the exhibitors.



The unmanned flight only lasted a few minutes and didn't see the aircraft covering any kind of distance, it being restricted to the airspace above the sports fields from which it took off and landed. But it gave the large nearby crowd an idea of the kind of noise such aircraft are likely to bring to cities in the not-too-distant future.

"Our Volocopter air taxis open up a completely new dimension in urban mobility," said Florian Reuter, CEO of Volocopter GmbH. "As Stuttgart has seen today, they fly safely, quietly and are fast approaching the implementation stage. Volocopter air taxis are able to ease traffic congestion in major cities around the world, also here in Germany."
We have seen the Volocopter take flight in Germany before, but in the relative safety of airfields away from populated areas. This flight is billed as the first to take place within an urban area in Europe, and having set up shop in Singapore the company is planning to build its first flying taxi station in the city and kick off test flights by year's end.

EDITOR'S COMMENT: Nice! Just another threat in the sky! What is the purpose for these aerial vehicles? In a few years, we will be able to "beam" people from one place to another (like in the Star Trek" – so, all these flying machines will be usefull ☺

Trump Awaits Orders from Saudis; and Why the Houthis Could Have Done It

By Juan Cole
Source: https://www.globalresearch.ca/trump-awaits-orders-saudis-why-houthis-could-have-done-it/5689487

Sept 16 – Trump actually said that he was waiting on the Saudis to determine the guilty party and to tell him what to do!
We all kept saying it is dangerous to have an erratic person like Trump in the White House in case there was a major global crisis. This might be it, folks.
The responsibility for the ten drone strikes on the Abqaiq and Khurais facilities is in dispute, with the Israelis ~~and Secretary of State Mike Pompeo~~ fingering Shiite militias in Iraq, whereas the Houthi rebels of north Yemen claimed they sent the drones.
One anonymous Trump official even told ABC on Sunday that Iran directly launched drones and cruise missiles on Saudi Arabia. We await forensics, but this allegation should be provable from forensics. It hasn't been, and sounds Gulf of Tonkinish to me. If it is true, buy an electric car quick.
One of the arguments for the Iraqi or Iranian provenance of the drones is that the Houthis were not known to have this capability before now. This allegation is not true. As I discussed in May, the Houthis used drones to hit Aramco pumping stations in al-Duwadimi (853 miles from Sana'a) and Afif (764 miles from Sana'a). The Houthis only had to go another hundred miles or so to reach Abqaiq from their stronghold at Saada (about 1,000 miles).
In May, the Houthis must have used Iran's Shahed 129 UAV (unmanned aerial vehicle) or something very

like it, which has a range of 1100 miles and has been used for similar strikes by Iranian forces in Syria. The advantage of drones for smuggling weapons to the Houthis by Iran is that they could simply be flown to them from a vessel offshore in the Red Sea.

If the drone can go 1,100 miles, there is no advantage to taking off from Iraq or Iran rather than Yemen.
In murder mysteries we look at means, motive and opportunity. The Houthis have the most motive of any of these actors, since the Saudis have dropped thousands of bombs on them for nearly four and a half years. Moreover, the Houthis have nothing to lose. They are already being hit as hard by the Saudis as they can be hit, and they have no resources that the Saudis can destroy.
In contrast, the Iraqi Shiite militias may not like the Saudis one little bit, but they don't have anywhere near the same degree of motive as the Houthis. Moreover, they benefit mightily from Iraq's oil facilities at Basra, which you wouldn't think they would want to put at risk of a Saudi counter-strike.
For the same reason, Iran would have been foolish to plan or direct this attack, since its own oil facilities are vulnerable to a counter-attack. Neither Iran nor Iraq did this kind of damage to one another's oil facilities in the Iran-Iraq war of 1980-88, operating under a constraint of mutual assured destruction.
Finally, I think we should be suspicious of Israeli and Neoconservative intelligence on this matter. Israel has not been involved in the Yemen War and there is no advantage to it if the Houthis did it. Israel has developed a fear of the Iraqi Shiite militias, which are close to Iran and operating in Syria near Israel, and has struck them in Iraq several times with drones. It would be awfully convenient for Tel Aviv if the full force of the United States and the Saudis could be turned on the Iraqi Shiite militias, and even better if it could be turned on Iran itself.
Look, I'm no hardware expert and it is all the same to me whether the drones were launched from Basra or from Saada, so I have an open mind. But the argument that the Houthis absolutely couldn't have done it makes no sense to me as a layperson, given the recent al-Duwadimi operation.
In the meantime, we Americans apparently must wait patiently for our marching orders from Riyadh. Or maybe, you know, the Saudis will bankrupt Trump by ceasing to rent all those rooms in the Trump Tower from him.

First photos from the Aramco drone attack

EDITOR'S COMMENT: There are still no adequate info about the drones used for this operation. Were they commercial drones with explosive payloads? Highly unlikely. Were they military drones equipped with missiles? Most probably. Was is a combination of drones and cruise missiles. Possible. Of course, fire resulted contributed to the disaster caused. The fact is that incident will change the war parameters as it used to be. Asymmetry got another point and all nations should consider this seriously. This was not an isolated case; many similar attacks with many different players will happen in the near future and not only in the fragile Middle East region.

If U.S. Claims of How the Saudi Oil Attack Went Down Are True, Then the Failure to Prevent It Is a Huge Embarrassment

Source: http://www.homelandsecuritynewswire.com/dr20190917-if-u-s-claims-of-how-the-saudi-oil-attack-went-down-are-true-then-the-failure-to-prevent-it-is-a-huge-embarrassment

Sep 19 – It has yet to be definitively established how the massively disruptive attacks this past weekend on a crucial Saudi oil facility took place.

The version of events being advanced by U.S. officials, however — that most of the damage was from cruise missiles launched from Iran — raises the embarrassing question of why the U.S. military was unable to do anything about it.

Mitch Prothero writes in *Business Insider* that the airspace around Iran and Saudi Arabia is some of the best-defended and most intensively monitored on earth, thanks to the decades-long buildup of U.S. assets there. But on Saturday those defenses failed to prevent what U.S. officials have said were at least 17 separate strikes.

Based on information made public about the strikes, defense insiders were left wondering how the U.S. military had fared so poorly in one of its primary missions in the region.

One former U.S. Navy officer, who deployed to the Persian Gulf region twice to operate air-defense systems, said it would be nearly impossible for the U.S. not to notice the attack as it happened or attempt to intercept the weapons.

"It's very hard to imagine a salvo of 17 shots from Iranian territory not being picked up via some land and sea radars," said the former officer who asked not to be identified discussing U.S. military capabilities in the region.

"Over the Persian Gulf is hard to comprehend … in that there'd be a lot of radars to detect it. There may be ships in-port [in] Bahrain whose air-defense radar would pick it up."

The attack Saturday struck two key oil facilities in the energy-rich eastern part of Saudi Arabia and knocked out about 5 percent of the world's oil production.

Life-Saving Mission at Battlefield – Blood drone

Source: https://i-hls.com/archives/94766

Sep 15 – Transporting blood resupply to the battlefield matches the strengths and constraints of small uncrewed aerial systems. Medical researchers at Johns Hopkins already determined in 2015 that small vials of blood could be transported as safely by drone as by car. A 2016 demonstration with a hexacopter showed that blood could be transported from ship to shore by drone, a valuable tool for both relief work and possibly contested beach landings. Later research showed that not just blood samples but whole bags of blood for transfusion could be carried by small flying robot, meeting not just testing needs but promising immediate delivery to a human in need.

In May 2018, the US Defense Innovation Unit DIUx put out a request for a drone capable of delivering 5 pounds of blood over 60 miles. That already exists in the civilian and aid world, from drone delivery companies like Zipline, and it is coming close to a reality for military models, too.

The Vapor all-electric drone series, designed by Pulse Aerospace before it was acquired by Aerovironment, have similar airframes and characteristics across the brand. While the payload of the Vapor 35 is likely going to be used up with sensors, the **Vapor 55's** greater payload capacity, reports Janes360.com, is useful for "troop-in-contact resupply, blood drops, and the like."

The range of the miniature helicopter-bodied Aerovironment Vapor drones is not the full 60 miles that DIUx was looking for, though at 35 miles it is more than halfway there.
The all-electric operation likely means the drones are quieter than internal combustion-powered alternatives, which could prove useful if the drones need to fly relatively unnoticed to get their blood or other vital payload where it needs to be.
Blood resupply by robot may become as routine in the 2020s as surveillance by drone was for the 2010s, according to c4isrnet.com.

Polish Quadcopter Capable of Versatile Strikes

Source: https://i-hls.com/archives/94787

Sep 16 – A Polish company has recently unveiled a new quadcopter attack drone designed for urban warfare and capable of carrying a warhead in order to conduct precision strikes against lightly armored targets.

The Polish Company WZL 2 has presented its **Dragonfly UAV**. The Dragonfly opens a new use for military quadcopters. With its ability of vertical takeoff and landing, the quadcopter can be launched from practically anywhere and used to to assist foot soldiers with taking out hostile armored threats.

With its maximum takeoff weight of five kilograms, the Dragonfly can be fitted with different payloads. Depending on the payload, the quadcopter can be used for precision strikes of targets or for clearing areas up to ten kilometers away.
The quadcopter was designed for both open area combat and urban warfare, making the Dragonfly an incredibly versatile attack system.
The Dragonfly can be equipped with daytime or nighttime cameras, as well as fragmentation, cumulative, thermobaric, or training warheads.

Uasvision.com reports that the quadcopter has a maximum flight time of 25 minutes at speeds of up to 80 kilometers an hour. It can reach a maximum altitude of 1,600 feet and a max range of 10 kilometers while maintaining line of sight with the command station.

This Drone Can Swim and Glide in the Air

Source: https://i-hls.com/archives/94894

Sep 20 – Hybrid drones, capable of both swimming underwater and flying in the air, are becoming a thing of the near future. Researchers at the Imperial College London's Aerial Robotics Lab have succeeded in developing a concept for a drone capable of swimming and gliding, similar to flying fish.

The AquaMAV drone utilizes combustible powder and the water it floats in order to propel itself. The

drone creates acetylene gas by mixing calcium carbide powder with water. The gas is then funneled into a combustion chamber where it is ignited alongside water and air. Once ignited, the water is blasted out of the combustion chamber allowing the drone to propel itself out of the water and glide. The drone is capable of gliding up to 26 meters in the air.

The AquaMAV drone utilizes combustible powder and the water it floats in order to propel itself. The drone creates acetylene gas by mixing calcium carbide powder with water. The gas is then funneled into a combustion chamber where it is ignited alongside water and air. Once ignited, the water is blasted out of the combustion chamber allowing the drone to propel itself out of the water and glide. The drone is capable of gliding up to 26 meters in the air.

The AquaMAV has some possible military applications. Potentially, the drone could pave the way for a novel form swarm attack, where drones fitted with explosive warheads could sneak the water and propel themselves to attack coastal targets.

Engadget.com mentions that the AquaMAV can also be used for collecting water samples in floods and dangerous waters.

New Solution Against GPS Jamming

Source: https://i-hls.com/archives/94824

Sep 18 – Unintended or intentional GPS/GNSS signal jamming or spoofing can disrupt defense and commercial operations. Moreover, it can be virtually impossible to know if a critical system is affected without specially designed detection capabilities. Many of these incidents have been documented, according to armyrecognition.com.

Orolia, specializing in Resilient Positioning, Navigation and Timing (PNT) solutions, has unveiled its new for **GPS/GNSS denied environments**.

"The risks associated with the sudden inability to navigate, communicate or react in critical situations (or even realize that you've lost control of your systems) are serious for any industry," said Orolia VP Resilient PNT Systems Rohit Braggs. "But when it comes to national security, the ability to conduct unhindered military operations is critical."

The company introduced its latest advanced GNSS simulator, GSG-8. A military-grade, software-defined simulator that can accommodate dozens of algorithms to conduct system testing and simulation, GSG-8 is designed for military, space and other specialized customers who require complex capabilities for harsh, high-risk environments. GSG-8 can be programmed to simulate operations with multiple GNSS constellations such as GPS and Galileo and to incorporate the use of encrypted or proprietary signals. It may also be configured for Wavefront and Anechoic chamber simulation protocols to test anti-jam antennas and complete systems, to serve the most sensitive and challenging program requirements.

The new Simulation and IDM portfolio offers a comprehensive array of GNSS spoofing and jamming simulation, detection, suppression, and countermeasures technologies.

These capabilities are based on the company's PNT solutions, together with two key acquisitions completed this year: Skydel Solutions and Talen-X – GNSS testing and simulation companies which had demonstrated US and Allied Forces Simulation and IDM experience.

Orolia's expertise ranges from strategies to protect military bases, government facilities and other fixed site locations to lightweight, software-defined technologies to thwart enemy spoofers and jammers on the mobile battlefield, whether on land, at sea or in the air.

Orolia CEO Dr. Jean-Yves Courtois said: "In Europe, there's no longer a question that GNSS jamming and spoofing is real and affecting both military and commercial operations." "We must now go beyond acknowledging the problem of putting real-world solutions in place quickly."

Many current military systems are operating on older platforms that would require more expensive, long term improvements to achieve integrated GNSS signal protection. Orolia's approach offers a cost-effective solution that can be retrofitted to provide effective GNSS signal protection now.

Two flights diverted as suspected drone spotted near Dubai International Airport

Source: https://www.thenational.ae/uae/transport/two-flights-diverted-as-suspected-drone-spotted-near-dubai-international-airport-1.913502

Sep 22 – Dubai International Airport closed on Sunday for 15 minutes due to suspected drone activity in the area.

Two incoming Emirates flights from Brisbane and Delhi were diverted to Dubai World Central and Sharjah International Airport.

"Dubai Airports can confirm that flight arrivals were briefly disrupted at Dubai International from 12.36pm to 12.51pm UAE local time this afternoon due to suspected drone activity resulting in the diversion of two flights," a airport spokesman said.

"Safety is our top priority and Dubai Airports is working closely with authorities and service partners to ensure normal operations and minimise inconvenience to our customers."

Emirates said EK433 from Brisbane via Singapore and EK511 from Delhi returned to Dubai International Airport once the airspace reopened.

"Emirates will assist affected passengers with alternative rebooking options and hotel accommodation where required," an Emirates spokeswoman said.

"Emirates regrets any inconvenience caused but the safety of our passengers and crew is of utmost importance and will not be compromised."

The incident is the latest drone activity to affect international flights.

In February, operations were temporarily shut-down at Dubai International, causing delays of almost an hour on some flights.

Drones forced the airspace around Dubai International to close on three occasions in 2016, leading to strict penalties by the country's General Civil Aviation Authority.

In December, major disruption was caused at London's Gatwick airport after drones were spotted near the airfield, raising concerns globally about the vulnerability of airports to unmanned aerial vehicles.

Anyone found operating a drone without a licence in the UAE or any restricted airspace can be hit with a Dh20,000 fine. The devices cannot be flown within 5 kilometres of an airport.

A variety of measures have been tested at airports around the world to improve safety in airspace occupied by aircraft at low altitudes during take-off and landing.

Police in Holland were the first to utilise the use of falcons and eagles, trained to intercept and down unauthorised drones.

London Heathrow is also reported to have developed 'signal jammers' to incapacitate drones flown illegally in its airspace.
Climate change protesters threatened to fly drones in Heathrow area this month to cause widespread disruption to one of the world's fourth busiest airport, behind Atlanta, Beijing and Dubai.

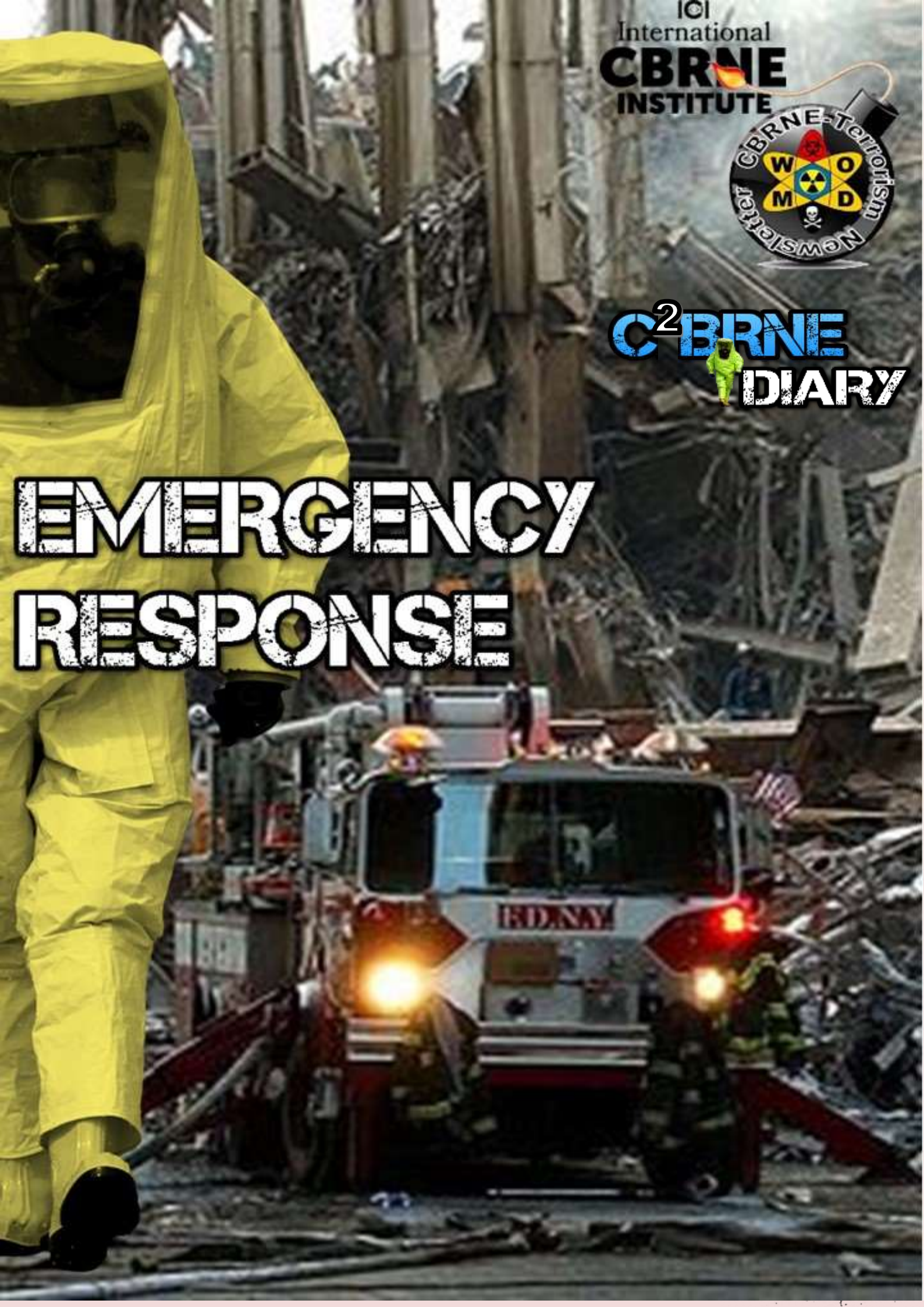
EDITOR'S COMMENT: Dh20,000 fine is about 5.000 euro. Rediculous fine! Why don't they make it Dh 200,000 (~50,000 euro) plus 3 years of community service for antisocial behavior, plus 6 months in jail with no right to appeal and the obligation to report the conviction to all future employees (if local) or deported if being a non-Emirati. By caressing offenders, they will continue having fun with their drones and a future airliner tragedy cannot be excluded.

The Attack on Saudi Arabia's Oil Facility. The Patriot Air Defence System Failed. Why?

Failure of the Air Defense System? Or Was the Patriot System "Disabled" on September 14?

By Prof Michel Chossudovsky
Source: https://www.globalresearch.ca/the-attack-on-saudi-arabias-oil-facility-the-patriot-air-defence-system-failed-why/5689779

Michel Chossudovsky *is an award-winning author, Professor of Economics (emeritus) at the University of Ottawa, Founder and Director of the Centre for Research on Globalization (CRG), Montreal, Editor of Global Research. He has taught as visiting professor in Western Europe, Southeast Asia, the Pacific and Latin America. He has served as economic adviser to governments of developing countries and has acted as a consultant for several international organizations. He is the author of eleven books including The Globalization of Poverty and The New World Order (2003), America's "War on Terrorism" (2005), The Global Economic Crisis, The Great Depression of the Twenty-first Century (2009) (Editor), Towards a World War III Scenario: The Dangers of Nuclear War (2011), The Globalization of War, America's Long War against Humanity (2015). He is a contributor to the Encyclopaedia Britannica. His writings have been published in more than twenty languages. In 2014, he was awarded the Gold Medal for Merit of the Republic of Serbia for his writings on NATO's war of aggression against Yugoslavia.*


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

When Disaster Strikes, a Search Website for First Responders Will Save Lives

Source: https://www.domesticpreparedness.com/updates/when-disaster-strikes-a-search-website-for-first-responders-will-save-lives/

(Released 20 August 2019) When Mount Vesuvius erupted almost 2,000 years ago, it took hours for a single message from Pompeii to reach rescuers 18 miles away. Today we have the opposite problem during disasters: too much rapid information from many sources, with consequences just as fatal for some people.

Engineers at the University of California, Riverside, are working to change this with a tool that searches real-time text, photo and video from social media and surveillance cameras alongside data from sensors, like fire detectors and security alarms. With the tool, for example, firefighters could search the terms "fire" and crowds" in a particular location and time and receive data from multiple sources.

The research, supported by a $1.2 million National Science Foundation grant, aims to develop a single search interface across all potential sources. The group's goal is to make a functional tool—a website similar to Google—that can search keywords.

But while Google can only search websites and images, the UC Riverside tool will be also be able to search space and time.

From left: Vagelis Hristidis, Vassilis Tsotras, Amit Roy-Chowdhury, Vagelis Papalexakis, Konstantinos Karydis.

"If police or firefighters have drones to photograph an area, this technology could guide them to where they have to go," said Vagelis Hristidis, a professor of computer science and engineering in the Marlan and Rosemary Bourns College of Engineering.

In addition to locating and analyzing information, the new tool will also collect it to constantly update databases. With a more integrated and holistic view of the situation, first responders can better allocate their resources.

Work has already been done searching individual sources. But to date, there is no way to search multiple sources at the same time said Hristidis, who leads a team that includes four of his Bourns College colleagues: Vassilis Tsotras, Amit Roy Chowdhury, Evangelos Papalexakis, and Konstantinos Karydis.

"The question is how to be more active in increasing the coverage," Hristidis said. "We're trying to get the best out of existing sources and cover gaps in order to get the big picture of an event."

One challenge is how to represent all sources (text, image, social relationship) in a common format. Another challenge is how to convert the sources into vectors, or numbers, so that computers can understand them. The group has done some preliminary work using advanced mathematical concepts like tensors—an algebraic way to map objects across multiple dimensions—to convert data sources to numbers.

"This project will require us to address a set of very challenging problems which will undoubtedly push the boundaries in representation learning forward," said Papalexakis, an assistant professor of computer science and engineering.

The search tool could also provide better security at concerts, sports, commencements, events that draw large crowds, and improve the safety of students on college campuses with live monitoring as potentially dangerous situations unfold.

Hristidis stressed that the search tool will only be able to access public information, like public Facebook posts or Tweets, and security apparatus like surveillance cameras and sensors

that police and fire departments can already access. It will not have access to social media posts with privacy restrictions, personal surveillance cameras, or other sensors in homes.

▶▶ Released by University of California Riverside. Click here for source.

Preparing for the Unexpected Disaster

Source: http://www.homelandsecuritynewswire.com/dr20190912-preparing-for-the-unexpected-disaster

Sep 12 – When thinking of earthquakes in the U.S., California often comes to mind. But what if a massive earthquake suddenly struck Middle America? Would first responders and emergency managers have the tools to swiftly secure infrastructure and ensure public safety? Would every level of government, as well as stakeholders at non-governmental organizations or in the private sector, know how to properly communicate and share resources? The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) asked itself these questions, and they were the driving force behind S&T joining the Federal Emergency Management Agency (FEMA) and others for FEMA's 2019 Shaken Fury exercise.

Although you seldom hear about earthquakes in the central U.S., the threat is real along the New Madrid Seismic Zone, which crosses eight states: Illinois, Indiana, Missouri, Arkansas, Kentucky, Tennessee, Oklahoma and Mississippi. An earthquake there could cause catastrophic physical and economic loss, which makes bringing stakeholders together in one place so critical for preparation. From soil degradation to identifying alternate transportation routes, from power generation to destroyed pipelines—the need to coordinate and deliver relief is of utmost importance.

S&T says that under the guise of a fictional 7.7 magnitude earthquake, S&T deployed teams and technologies to several Shaken Fury exercise locations in the region to improve response and recovery capacities and assist state and local organizations with the adoption of new technologies and protocols. Throughout a week in late May and early June, S&T and FEMA Urban Search and Rescue Program, the Central United States Earthquake Consortium (CUSEC), U.S. Department of Defense, the National Guard, state and local government agencies, NGOs, and the private sector coordinated response efforts and resources across what in a real emergency would be a nearly unimaginable expanse of need.

"The importance of Shaken Fury is that it provided S&T with an opportunity to get our technology in front of the folks that potentially will be using it to manage disaster response—expose them to it, and train them on it," said S&T Program Manager Ron Langhelm. "This way, if they have an event next week, they're better prepared to utilize the tools that they have available."

In the year and a-half it took to plan the exercise, S&T determined that the primary objectives would be to:

- Leverage S&T's research and development portfolio to enhance information sharing and urban search and rescue practices;
- Demonstrate a "whole community" approach to adjudicating and allocating critical resources;
- Integrate real-time field reporting capabilities in emergency operation centers.

"Our role in Shaken Fury was to bring in science and technology capabilities to enhance not only resilience, but also to foster a stronger culture of innovation within the first responder space," said Colin Murray, Senior Exchange Officer from Canada to S&T. By bringing new technology and approaches to bear on challenges, such as finding disaster survivors in rubble or ensuring a shared understanding of the situation on the ground in multiple states, S&T showcased a range of solutions and tools to help responders remain safer and more effective.

S&T Technologies Deployed at Shaken Fury

Information Sharing

In many disasters, particularly in a constantly-evolving situation like the aftermath of an earthquake, one of the biggest hurdles to overcome is communication—not simply the ability

for agencies to speak to one another, but also the challenge of getting the information they need, when they need it, in a form that's useful. For the past several years, S&T has partnered with CUSEC to develop tools for automated sharing of situational data across different platforms. For Shaken Fury, S&T developed data dashboards linking to FEMA's seven community lifelines (pdf, 280.75 KB, 1 page), which are indispensable services, and developed links to seamlessly share information between civilian and Department of Defense elements responding to the disaster. The dashboards were integrated into Shaken Fury play at emergency operations centers in Kentucky and Tennessee.

"The primary information sharing tool we deployed is the Regional Information Sharing Portal (RISP). And essentially, that is the backbone of all the information sharing systems that we have," said Langhelm. "We had information both feeding into it as well as flowing back out it into other applications. For the folks working the field on the ground, this supported their decision-making in everything from where to move commodities to mitigating power outages. You know, where they could best utilize resources and deploy those resources in the field."

Michael Dossett, Director of the Kentucky Division of Emergency Management and CUSEC Chairman, attested to RISP's usefulness. "I can look at the level of damage and the predicted recovery time, and that gives me some idea… of how to prepare for what's coming toward us," he said.

"We can now pull-down layers from just about everything, whether it be sheltering, transportation, energy, health. The ability to pull all those resources together, leverage technology to move the information, and then allow folks at my level to make critical decisions—I submit to you, this is the foundation of a process that you will see go on for the next decade in terms of more timely, tested data in the hands of state emergency managers that allows us, quite frankly, to make life-saving decisions."

Josh Wickham, Planning Branch Administrator for the Tennessee Emergency Management Agency, agreed. "One thing we really liked about RISP is that it is tied into our existing resource tracking board. With this tool, we can change a few of our processes to create a dashboard that can identify resource status based on region or county, filter by FEMA Lifelines, and create automated maps to see which counties are activated for which Lifeline. This is one of my favorite tools because it is just one button that creates all this information that we haven't had before."

The ability to share critical emergency information at the tribal, local, state, and federal levels is not lost on FEMA, either. "Platforms like what DHS S&T has developled are so important to the whole community because we're all seeing the same things," said FEMA Region IV Administrator Gracia Szczech. "We are all looking at, assessing and singing off the same sheet of music… that's why it's so important to have these types of platforms… so that we can all be together and make those decisions together."

Urban Search and Rescue (USAR)

Under the Shaken Fury umbrella, S&T staff also deployed to the Muscatatuck Training Center in Indiana for Unified Response, the largest-ever US&R exercise hosted in the U.S. The multi-national exercise included 13 US&R teams from the U.S., Canada and Australia, the State of Illinois, as well as six FEMA task forces, the Department of Defense and National Guard. S&T demonstrated and integrated both existing and emerging technologies into the exercise. Responders used the technologies to search for "disaster survivors" in simulated rubble piles and collapsed buildings.

"One of the great things about the collaboration we've done with DHS S&T is the ability to bring out new and emerging technologies to this exercise. Put those technologies in front of responders that are actually in a disaster simulated environment and try them out," said Brian Smith, program specialist with FEMA.

S&T planned the demonstration/integration model to expose the responders to the potential of the tools and inform the technology developers of needed design adjustments based on field use. "The benefit of DHS S&T being here has been that the future technology to do our job better was here. We could see it. We could test it. We could play with it," said Evan Schumann, Program Manager for Ohio Task Force 1 and one of the key players in the Shaken Fury exercise. "They can go back and make it better for us. And, hopefully, get it to us in the next few years."

One of S&T's transitioned, commercially-available technologies used at MUTC, X3 FINDER, allows responders to "see" through walls to locate trapped disaster survivors by detecting heartbeats and respiration. X3 FINDER was tested with US&R teams from the U.S. and Canada in both rubble piles and partially collapsed buildings. During a demo with the

Nebraska Task Force 1, FINDER was operating at the same time as rescue dogs were searching the building for survivors. In this evaluation, FINDER located each survivor and accomplished this faster than the dogs.

"The advantage to introducing something like this to Shaken Fury is to expose the US&R groups to new technology hands-on—not us telling them about it," said Michael Buckley, training director for SpecOps Group, developer of X3 FINDER. "We put it in their hands and teach them on the spot how to use it, then they see the results for themselves and then back up their findings with the data."

"The main thing is, X3 FINDER provides standoff first responder safety," Buckley said. "The first responder doesn't have to crawl through the building, voids and thresholds. We can set this thing up, we can scan and look for signs of life without risking the first responder."

The exercise also allowed a rare opportunity to test prototypes in a near real world environment. Two developers of unmanned aerial vehicles (UAV) platforms designed to operate indoors had the chance to do just that, alongside several Canadian US&R teams. With the ability to carry cameras and sensors enabling rescuers to conduct faster and safer searches inside compromised spaces, these tools are the next generation of life-saving robotics, extending the eyes, ears, and noses of people and search animals far past anything we can do today.

The industry partners developed the prototypes through S&T's Smart City Internet of Things Innovation Laboratory (SCITI Labs) effort.

"Interacting directly with the eventual end user community is critical—an opportunity that most developers never get," said David Ihrie, Chief Technology Officer at the Center for Innovative Technology, S&T's SCITI Labs partner.

"In a collapsed building resulting from an earthquake, the search for survivors is very important. In some cases, the responder teams may not know if the building is safe. There may be structural integrity questions about the building; the ability to send a UAV, a drone, in quickly, looking for signs of life, can help focus the search and get help to victims more quickly," Ihrie said.

The cutting-edge UAVs were demonstrated in "compromised" spaces like a smoke-filled subway airshaft and tunnel, a dark shipping container structure, and a collapsed building frame in high wind. Performance results and feedback from the first responders will inform further development of the technologies, which could be commercially available in 2020.

Alongside these technologies that were used in-play, S&T also set up a technology showcase tent where 10 industry vendors showed off new and emerging technologies. Approximately 400 participants could view the technologies and discuss requirements with the subject matter experts, which greatly contributes to the evolution of the technologies.

"The exercise was…tremendously rich in terms of offering the technology developers the opportunity to get feedback from the responders," said Murray. "We had a continuous stream of responders come in, get exposure to the new technologies, and offer feedback to the developers in terms of the potential that that technology has within an operational space. [Shaken Fury] was a very, very rewarding environment, and the feedback from the developers was very, very positive."

Successes, Lessons Learned, and what's next for Shaken Fury

A year-and-a-half ago, DHS S&T set on a path to bring cutting edge technology to one of the largest and most complex exercises. This summer, that was accomplished, and S&T demonstrated the value of technology to make operations more efficient, resource allocation more targeted, and ultimately help responders save more lives.

A second S&T Shaken Fury event—the Next Generation First Responder (NGFR) Birmingham Shaken Fury OpEx—occurred in August 2019. S&T's NGFR team worked with industry and local authorities to augment their public safety capabilities before the Alabama city hosts the World Games in July 2021. The OpEx used an earthquake scenario that caused a partial structural collapse and a HAZMAT leak.

"The work we're undertaking [through Shaken Fury] revolves around an earthquake scenario, but from the S&T standpoint, everything ,we deployed is applicable for all hazards," said Langhelm.

"…We're looking to carry this into the future. All the successes we demonstrated around this scenario, they can carry into the event that's going to happen tomorrow, two years, five, or ten years down the road."

An after-action report detailing lessons learned in Indiana, Kentucky, and Tennessee will be posted to S&T's website for agencies at every level to study and use when real-life disasters occur.

Incident Commander

Source: https://www.breakawaygames.com/incident-commander/

A small town faces a big problem, and the crisis will only get worse unless you step in. As Incident Commander, you deploy and coordinate responder teams from multiple organizations to deal with a sudden threat to the town's citizens and property.

Incident Commander uses a simplified approach to the Incident Command System. The focus is on operations. Players control police, fire, EMS, air operations, school, and public works units in real-time to deal with the emerging disaster.

The game supports one to five players. There is an Incident Command System framework for you to set up, but the framework does not force players into roles. Instead, players must learn to cooperate and divide the responsibilities for the most efficient operation. Player

communication and delegation are crucial for success. Otherwise, responder teams may receive conflicting orders from different players.
A tutorial and several scenarios provide many types of challenges, including fires, chemical spills, looting, electrical hazards, school shooting, and casualty collection. The town mayor will keep an eye on your progress and track Public Safety and Incident Budget. Are you up to the task, Commander?

Key Features

- Bird's-eye view of 3D world with animations and special effects such as damage from fires, toppled utility poles, chemical spills, and explosions
- Tutorial scenario explains how to assign tasks to units and call in nearby resources
- Cooperative multiplayer feature supports up to five players
- Events unfold in real-time play as you race to keep ahead of the situation
- Includes over 20 different types of teams and vehicles, from School Resource Officer to HAZMAT
- Use a helicopter to rescue citizens from danger or drop water on raging wildfires
- Neutralize threats by Assault, Negotiation, or Arrest and book them at the Police Station
- Use Wildland Engines to carry Wildland Firefighters off road to battle the fire from any side
- Employ Lockdown and Escort tactics to keep students safe during a school shooting
- Set up the Joint Information Center so Media Teams will not interfere with responders
- Repair utility hazards with Public Works squads, and use a Tow Truck to remove vehicles from danger

When natural disasters strike, men and women respond differently

Source: https://www.sciencedaily.com/releases/2019/09/190920095218.htm

Sep 20 – **Women are quicker to take cover or prepare to evacuate during an emergency, but often have trouble convincing the men in their life to do so**, suggests a new University of Colorado Boulder study of how gender influences natural disaster response.
The research also found that traditional gender roles tend to resurface in the aftermath of disasters, with women relegated to the important but isolating role of homemaker while men focus on finances and lead community efforts.
Even agencies charged with providing assistance still, at times, ask to speak to the "man of the house," the researchers found.

"We found that there are many barriers that disadvantage women in the event of a disaster, leaving them behind when it comes to decision-making and potentially slowing down their recovery," said lead author Melissa Villarreal, a PhD student in the Department of Sociology and research assistant at the Natural Hazards Center.

For the study, co-authored by Texas A&M University Assistant Professor Michelle Meyer and published in the journal *Disasters*, the researchers analyzed in-depth interviews with 33 women and 10 men across two Texas towns. Some were from Granbury, which in 2013 was hit by an EF-4 tornado that killed six and cut a mile-wide swath of destruction, damaging 600 homes. Others were from West, where an explosion at a fertilizer company that same year killed 15 and destroyed 100 homes.

Residents were asked about their experiences in the midst of and the year after the disaster. While the circumstances surrounding the events were very different, common gender-influenced patterns emerged.

"We often assume that men and women are going to respond the same way to these kinds of external stimuli but we are finding that's not really the case," said Meyer, director of the Hazard Reduction and Recovery Center at Texas A&M.

In one interview, a Granbury woman recounted hunkering down in the closet with her children, pleading with her husband -- who was looking out the window at the tornado -- to come in and join them. In another case, a woman resisted her husband's plan to get in the car and drive away from the storm, preferring to shelter in place. She ultimately deferred, and they ended up stuck in the car, the children in the back seat, being jostled by the wind as the tornado whipped through.

"Women seemed to have a different risk perception and desire for protective action than the men in their lives, but men often determined when and what type of action families took," Villareal wrote. "In some cases, this put women and their families in greater danger."

The findings are the latest in a series of studies that have found that women tend to have a higher perception of risk, but because they are framed as "worriers," they are sometimes not taken seriously.

Women in the new study also complained that recovery organizations tended to call the men of the household to find out where to direct aid, even when women had filled out the forms requesting it.

"Eliminating the male head-of-household model is crucial for speeding overall household recovery," the authors conclude.

During recovery, women were often charged with "private sphere" tasks like putting the house back together and caring for children while schools were closed, but they often felt excluded from leadership roles in community recovery projects.

"If your perspective is not taken into consideration and you feel isolated, that can impede your mental health recovery," said Villareal.

She recently embarked on a separate study, set in Houston, looking at the unique challenges Mexican immigrant populations are facing in the aftermath of Hurricane Harvey, which hit the region in 2017.

Ultimately, she would like to see government agencies consider gender differences when crafting disaster warnings and prioritize providing childcare post-disaster so that women can play a greater role in community efforts.

"If we can put racial and gender forms of bias aside and listen to all the people tell their stories about what is affecting them, that could go a long way in helping communities recover," said Villarreal.

Journal Reference: *Melissa Villarreal, Michelle A. Meyer.* ***Women's Experiences Across Disasters – A Study of Two Towns in Texas*** *.* Disasters, *2019; DOI: 10.1111/disa.12375*


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

The Greek Way to a Green Planet

By Evaggelos Vallianatos

Source: https://www.counterpunch.org/2019/08/28/the-greek-way-to-a-green-planet/

Aphrodite's Rock

Aug 28 – The dawn of the twenty-first century is giving us a whiff of another Dark Age. Christianity and Islam have been hovering over each other, fighting small-scale crusades. More than a billion Moslems hate America because America has been an ally of Israel and because America destroyed Iraq, eyeing the oil of the entire Middle East. Even Europeans resent America, its pretense of exceptionalism, superiority and military prowess.

Capitalism is fueling climate change

Second, and much more potent than religious conflicts, is the Western invention and globalization of nuclear weapons, and other weapons of mass destruction. In addition, the West prides itself of capitalism, which is at the core of a largely immoral private and state trade and business system that is daily impoverishing the Earth.

This is the Earth of the Greeks: their sacred Gaia or Ge.

Something is wrong: we, humans, and especially fossil fuel companies and governments, have lighted the fires of climate change. This anthropogenic initiative may turn out to be humanity's last.

It far surpasses the crime of Prometheus: stealing fire from the gods for the benefit of humans. This time insignificant humans, bloated with ignorance and hubris, acted like madmen. They dug up fossil fuels of millennial ages and, immediately, started burning them for their profit. They never thought if the burning of that primordial stuff was bad. They still refuse to admit, that their burning of very ancient petroleum, natural gas and coal triggers climate change or global warming. And certainly it did not cross their mind that climate change is fiddling with the Sun god Helios, the Earth, the cosmos, things of the gods.

Fossil fuel executives and the politicians they control deny climate change and the resulting overturning of the natural and human order.

Marginalizing the Greeks

Clearly this catastrophic climate change has nothing to do with the Greeks. In some fundamental ways, the crime of climate change documents how far we are from them.

According to Andrew F. Stewart, a scholar on the history of Greek art, "modernism has marginalized the Greeks." Americans, for instance, know much more about Elvis and Madonna than about Aphrodite, Alexander the Great and Achilles. Occasionally, Greek art makes a big splash in "blockbuster exhibitions" but, Stewart says, Greek art "has become culturally all but irrelevant: a curiosity for tourists to gawk at, merchants to profit from,

collectors to hoard, museums to display, postmodernists to pillage, and academics to argue about." (Art, Desire, and the Body in Ancient Greece, 1997, 3).
Our distance from the beauty and purpose of Greek art illustrates the schism between us and the Greeks. The Greek way of living and thinking about society and the cosmos has nothing to do with our modern maladies: crusades, nuclear bombs, the destruction of nature and climate change, undermining of our democracy.
The Greeks were not perfect. They fought with each other too many wars. They had slaves and did not give women the same rights they gave to men. So they did not live up to their ideals – and, in that failure, they mirror the tragic human condition.
Their poets, Pindar, Aeschylus and Sophocles, decried the ghost-like reality of human beings who, within moments, can go from the heights of heroism and splendor to destruction and extinction, all the edifice of men resembling a fogged glass, which, in times of trouble, one can use a wet sponge to wipe out.
The Greeks, however, recognized the extreme vulnerability of human beings. They tried to stay the course with maintaining their ancient traditions, piety for their gods, and celebration of their common culture. The Olympics and the Panhellenic games brought them closer to each other and their gods.

Republic of gods and men

The Greeks also understood the injustice of slavery. Alkidamas, a teacher of rhetoric born in the last quarter of the fifth century BCE, said gods gave all men freedom while "nature has made no man a slave." (The Works and Fragments, ed. and tr. J.V. Muir, 2001, Fragment no. 1, 32-33).
Greek tragic poets gave intelligent and heroic roles to women. Antigone defended the noblest virtues of Greek culture, the love of a sister for her brother, and the superiority of divine over arbitrary human conventions. It was from this understanding of the Greeks — that Greek and non-Greek and male and female, shared a common humanity — that convinced the West in the eighteenth century to end slavery and, a century or so later, close the gap in the inequalities between men and women.
The road to human rights starts with the Greeks, too. They, with all their shortcomings, and they had many, were the first people who lived the "examined life" of Socrates, their greatest moral philosopher. They also appreciated the culture of foreign people like the Egyptians and Ethiopians.
Herodotus, the fifth-century Greek historian, wrote some of the most exciting pages of Egyptian and Persian history. When he and the Greeks talked about barbarians they meant people who were living the lives of slaves.
The Greeks were, and continue to be, controversial. It is almost fashionable in American universities to dismiss and hate the Greeks for a variety of political reasons and careerist objectives. Such disparagement of the Greeks is as old as the Greeks.
A more balanced view of the Greeks is also ancient. Listen to the British scholar Gilbert Murray speaking about the Greeks almost a century ago, in 1921:
"It seems quite clear that the Greeks owed exceedingly little to foreign influence. Even in their decay they were a race … accustomed 'to take little and to give much'. They built up their civilization for themselves. We must listen with due attention to the critics who have pointed out all the remnants of savagery and superstition that they find in Greece: the slave-driver, the fetish-worshipper and the medicine-man, the trampler on women, the bloodthirsty hater of all outside his own town and party. But it is not those people that constitute Greece; those people can be found all over the historical world, commoner than blackberries. It is not anything fixed and stationary that constitutes Greece: what constitutes Greece is the movement which leads from all these to the Stoic or fifth-century 'sophist' who condemns and denies slavery, who has abolished all cruel superstitions and preaches some religion based on philosophy and humanity, who claims for women the same spiritual rights as for man, who looks on all human creatures as his brethren, and the world as 'one great City of gods and men'. It is that movement which you will not find elsewhere, any more than the statues of Pheidias or the dialogues of Plato or the poems of Aeschylus and Euripides." ("The Value of Greece to the Future of the World" in The Legacy of Greece, 15).
Clearly, we have a long way to go before we feel secure with the legacy of the Greeks. We need them to spark another rebirth of our Western culture, fortifying it, once again, with their verities and ethics, bringing about another Renaissance.

Another Renaissance

Writing in the late 1940s, a time after a savage world war and holocaust, a distinguished classicist, Gilbert Highet, said this:

"What the Renaissance [of the fifteenth and sixteenth centuries] did was to dig down through the silt [of Christianity] and find the lost beauties [of Greek and Roman culture], and imitate or emulate them." (The Classical Tradition: Greek and Roman Influences on Western Literature, 1966, 4.)

We have to do the same thing: Dig down through the silt of bad science and destructive economic development based on the burning of fossil fuels, deforestation, industrialized farming and the genetic engineering of crops, and overfishing. These activities are threatening the Earth with catastrophic climate upheavals. The side effects of this giant crisis manifest themselves in alarming religious tensions, violent technologies, and creeping undemocratic practices.

We need to rediscover the Greek texts and imitate or emulate the struggle of the Greeks for an ecological way of living and honest democratic life lived in freedom.

Climate change and CBRN defense

By Jozsef Padanyi, László Halász and László Földi

Source:https://www.academia.edu/21687057/CLIMATE_CHANGE_AND_CBRN_DEFENSE?email_work_card=view-paper

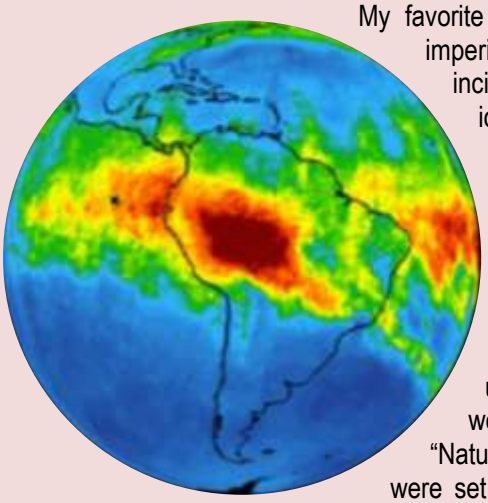
The fact of global climate change is undisputable nowadays. There are certain theories about the causes, and the authors of this paper do not want to argue with any of them. What they want is to start with the observable facts and highlight the most important consequences concerning the safety of the society, and with the threat increasing in the future to show the challenges concerning military forces and military activities. The paper describes the possible consequences of climate change concerning CBRN defense in details and the main problems of contamination avoidance, individual and collective CBRN protection, CBRN reconnaissance and decontamination, which need urgent solutions. Besides the presentation of challenges of climate change, the authors make some proposals to improve CBRN capabilities.

The Problem Isn't the "Lungs of the Earth." It's the "Brains of the Earth"

By Robert Tracinski

Source: https://thebulwark.com/the-problem-isnt-the-lungs-of-the-earth-its-the-brains-of-the-earth/

Sep 03 – A normal cycle of seasonal fires in the Amazon region touched off an international hysteria, with celebrities and politicians screaming that "the lungs of the Earth are in flames."



My favorite over-reaction is lefty writer Franklin Foer proposing a kind of eco-imperialism. Because Brazilian President Jair Bolsonaro has "presided over the incineration of the world's storehouse of oxygen," Foer argues that "inherited ideas about the sovereignty of states no longer hold in the face of climate change." So, we shouldn't have invaded Iraq, but we *should* invade Brazil: "The destruction of the Amazon is arguably far more dangerous than the weapons of mass destruction that have triggered a robust response."

All that this demonstrates is the enormous contempt for science among those who loudly proclaim themselves to be on the side of science.

First, the real story in Brazil is not some abnormal, uncontrolled forest fire. Rather, the fires are primarily on land already cleared for agricultural use, and they are part of normal field-clearing practices in that part of the world.

"Natural fires in the Amazon are rare, and the majority of these fires were set by farmers preparing Amazon-adjacent farmland for next year's crops and pasture," soberly explains The New York Times. 'Much of the land that is

burning was not old-growth rain forest, but land that had already been cleared of trees and set for agricultural use.'
It is routine for farmers and ranchers in tropical areas to burn their fields to control pests and weeds and to encourage new growth in pastures.

So, this is another case of "progressive" neo-imperialists in wealthy countries trying to dictate to the global poor how they should remain poor.
But the big lie behind this is the old myth about the Amazon being the "lungs of the Earth," the source of the bulk of our atmosphere's oxygen—a claim that has been repeatedly debunked.
Back in 2005, Amazon expert Daniel Nepstad told the *Los Angeles Times*, "It's not the lungs of the world. It's probably burning up more oxygen now than it's producing." The article concludes, "Left unmolested, the forest does generate enormous amounts of oxygen through photosynthesis, but it consumes most of it itself in the decomposition of organic matter." Another researcher sums it up: "For sure, the Amazon is not the lungs of the world. It never was."
It appears Nepstad has gotten even less patient in the years since, recently telling Michael Shellenberger at *Forbes* that the "lungs of the Earth" claim is "bullshit." "There's no science behind that. The Amazon produces a lot of oxygen but it uses the same amount of oxygen through respiration so it's a wash."
Probably the most thorough overview of the science on this is from Peter Brannen. In among a lot of pious throat clearing about global warming and fossil fuels—necessary to reassure the *Atlantic*'s readers that he's not a bad guy—he drops the news. "The Amazon is a vast, ineffable, vital, living wonder. It does not, however, supply the planet with 20 percent of its oxygen."
Brannen quotes geologist Shanan Peters on what would happen if not only the entire Amazon but everything else went up in flames tomorrow.
"What would happen if we combusted every living cell on Earth?" [Peters] asked. That is, Peters wanted to know what would happen to the atmosphere if you burned down not just the Amazon, but every forest on Earth, every blade of grass, every moss and lichen-spackled patch of rock, all the flowers and bees, all the orchids and hummingbirds, all the phytoplankton, zooplankton, whales, starfish, bacteria, giraffes, hyraxes, coatimundis, oarfish, albatrosses, mushrooms, placozoans—all of it, besides the humans.
Peters pulled up the next slide. After this unthinkable planetary immolation, the concentration of oxygen in the atmosphere dropped from 20.9 percent to 20.4 percent. CO2 rose from 400 parts per million to 900—less, even, than it does in the worst-case scenarios for fossil-fuel emissions by 2100.
By burning every living thing on Earth.

So where does our atmosphere's oxygen come from? Practically every living system on Earth uses up as much oxygen as it produces, but *not quite*, and over geologic time, that adds up.
The tiny remainder of photosynthetic stuff that isn't consumed and respired again by life—that 0.01 percent of plants and phytoplankton that manages to escape from this cycle of creation and destruction—is responsible for the existence of complex life on Earth…. On the time scale of tens of millions of years, such meager gifts can accumulate—apparently to 20.9 percent.
This, at least, is the best theory to date about the source of the world's oxygen. But it certainly puts the "lungs of the Earth" myth to rest. Brannen ends by trying to replace that hysteria with an overblown concern about current human consumption of fossil fuels, yet he has to admit that this, too, is overblown, at least when it comes to oxygen supplies.
Luckily, unlike carbon dioxide, we measure oxygen not in parts per million, but in parts per hundred. In other words, we have been gifted such an absurd surplus of oxygen by deep geological time, and by strange ancient life we'll never know, that it won't soon run out by our own hand, whether by deforestation or industry.
The "lungs of the Earth" myth has been repeatedly debunked for decades. But it lodged in everyone's brains some time back in the 1980s, when a bunch of celebrities and intellectuals first decided to pretend they really cared about the Amazon, and it has been endlessly repeated without question since.
That's the only real crisis we face here. The problem we have isn't with the lungs of the Earth, it's with the *brains of the earth*—the intellectuals whose job is to ask bold questions, but who too frequently end up repeating stale dogma instead.

Robert Tracinski *is editor of The Tracinski Letter and host of Salon of the Refused.*

Want to Avoid Climate-Related Disasters? Try Moving

By Peter Reuell
Source: http://www.homelandsecuritynewswire.com/dr20190904-want-to-avoid-climaterelated-disasters-try-moving

Sep 04 – For those who lived through the storms, their names — Katrina, Sandy, Harvey, Michael — are enough to trigger memories of homes, businesses, and loved ones lost in rising floodwaters. Other disasters elicited similar reactions, from the Midwest floods to the California wildfires, and droughts in the Great Plains.
The eventual response to catastrophes tended to be a defiant vow to rebuild, turn loss into lesson by making protective seawalls higher and stronger to hold back floods, or raising homes onto stilts to stay clear of the encroaching waves.
To this, A.R. Siders says, "Enough." The time has come to consider a different path: retreat. Abandon areas prone to repeated disaster in favor of those that are safer and do so in a deliberate, thoughtful way. Known as "**managed retreat**," Siders, an Environmental Fellow at the Harvard University Center for the Environment who recently joined the faculty of the University of Delaware, said the strategy has the potential to save not only lives, but possibly billions of dollars in direct and indirect costs to cities and towns. The idea is described in an Aug. 23 paper published in Science with co-authors Miyuki Hino and Katharine Mach.
"Traditionally speaking, there are three ways people respond to floods or hurricanes," Siders said. "There is protection — basically building a sea wall. There's accommodation, which often means homes that are elevated, or there's retreat.
"We see retreat listed as an option as early as 2001 by the [Intergovernmenal Panel on Climate Change], but retreat has been seen as largely theoretical — somewhere, sometime people might have to move. But what we're seeing more and more is that it might be here and that it might be now. It's no longer a theoretical last resort. It's something we should talk about now as a realistic option."
The purpose of the paper, Siders said, is to call attention to the need for a greater focus on the strategy as a way to avoid the fallout seen from earlier disasters.

"The point we're trying to make is: Retreat will happen; people will move. Not managing retreat doesn't stop people from moving," Siders said. "After Hurricane Katrina, people had their homes destroyed, and they moved with no help and no support. They just left."
For the neighborhoods they leave behind, the results can be corrosive.
"You have thousands of empty homes, and the city has to figure out who owns them," she said. "They have to sell or demolish them, and maintain the lots. So, it eats away at the community, because it's dotted with vacant homes, and it eats away at the city's resources.
"But if you do manage it and try to do this in a strategic way, then you have a better chance of avoiding those harms," she continued.
The notion of managed retreat, however, is about more than what happens to the homes people leave behind when they flee.
"It touches on so many aspects of a city," Siders said. "You have to think about things like where people are going — where they're choosing to go and where you want to provide incentives for them to go.
"What are the effects on the community they're moving to? Do they have enough services? Do they have enough hospitals and schools to take in the people they're receiving? For the people who stay behind, do they suddenly have no sense of community because of all these vacant lots, or do they have something like a new public park or feature to maintain a sense of community?"
Those questions only deepen, Siders said, when retreat crosses national and cultural borders.

***Peter Reuell** is a Harvard staff writer.*

IMPROVING THE CBRN DEFENCE OF COMBAT VEHICLES AS A RESPONSE TO THE CHALLENGES OF CLIMATE CHANGE

László HALÁSZ, József PADÁNYI and László FÖLDI

Abstract: CBRN defence continues to be an important component of the defence system of combat vehicles. On the effect of climate change the importance of examining the thermal characteristics of combat vehicles and the development of adequate air conditioners increased. After reviewing the different types of solutions the complex environment control system, containing self-regenerating filters, will be presented in details.

Source:https://www.academia.edu/21687293/IMPROVING_THE_CBRN_DEFENCE_OF_COMBAT_VEHICLES_AS_A_RESPONSE_TO_THE_CHALLENGES_OF_CLIMATE_CHANGE