7\20

HZS

C²BRNE DIARY

Dedicated to Global First Responders

July 2020

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

DIRTY R-NEWS

EMP Weapons: America's Next Pearl Harbor?

Source: https://www.thetrumpet.com/22553-emp-weapons-americas-next-pearl-harbor

June 24 – China has the ability to launch a crippling electromagnetic pulse (emp) attack on the United States at any time, warned a June 10 report by the emp Task Force on National and Homeland Security. Such an attack would come as a "surprise Pearl Harbor" that could cripple the military and permanently alter civilian life.

With the help of stolen and copied U.S. technology, China appears ready to make this situation a reality. Dr. Peter Vincent Pry, author of the report, warns that based on current information about Chinese tactics, Asia's primary superpower is not only well equipped, it is planning to strike first.

Any nuclear-capable nation can launch an emp strike. The attacker detonates a low-yield nuclear bomb at roughly 40 to 60 miles above ground; the higher the detonation, the larger the electromagnetic field. This overloads electronics within its range, damaging or even destroying them.

The U.S. military was the first to discover this effect after testing a nuclear bomb over the Pacific in 1962. The electromagnetic field from its detonation overloaded Honolulu's electrical grid, 870 miles away.

Today, such an attack would be calamitous for computer-reliant countries.

If one of these "super-emp" weapons exploded at about 18 miles above the central U.S., the effects would be felt in almost every major city. If just one bomb detonated over the Pacific, it could knock out electrical power to Taiwan, the Philippines and Guam all at once.

The exact effects of an emp blast are hard to predict because they change according to atmospheric conditions, weapon design and detonation height. What is certain is that they remain a critical threat to countries that rely on satellites and computers for the daily operation of their civil and military technology.

Total Information Warfare

"China's military doctrine closely associates cyberattacks with nuclear hemp [high-altitude electromagnetic pulse] attack, as part of a combined operation in what they call Total Information Warfare," states the report. These cyberattacks would seek to blind American satellites and sensors, and cause critical infrastructure like electrical grids to fail. This would be followed by the emp attack.

China could deliver its super-emp using hypersonic missiles, which are more difficult to shoot down than conventional missiles because they can accelerate past five times the speed of sound and turn rapidly. A satellite carrying a nuclear weapon is another possibility; it could approach over the South Pole, evading America's early-warning radar in the Arctic. Dr. Pry describes how China's militarized space program could place several of these weapons in orbit long before an attack, since the country already possesses "technical capability to clandestinely orbit a nuclear-armed satellite or satellites to be maintained in orbit for years."

The continental U.S. is not the only target these super-weapons would be aimed at. They are also effective against warships.

In March, according to the report, "a panel of China's military experts threatened to punish U.S. Navy ships for challenging China's illegal annexation of the South China Sea by making an emp attack—one of the options they considered least provocative, because the crew would be unharmed, but most effective, because the ship would be disabled."

emp attacks can destroy the circuitry aboard the aircraft carriers and destroyers that the U.S. relies on for dominance in the Pacific. Without radar, targeting or communication systems, a warship turns into floating target practice for enemies. The official newspaper of the Shanghai Communist Party noted in 2000 that a "high degree of electronization is like an Achilles' heel for an aircraft carrier fleet, which relies heavily on electronic equipment as its central nervous system."

He Who Strikes First Wins

What about those who believe that China's "no first use" policy precludes any nuclear weapons from being used in emp attacks? Dr. Pry answers:

"No First Use" for China does not withstand the test of common sense. No conservative military planner would adopt "No First Use" when China lacks bmews [ballistic missile early warning systems] and satellite early warning systems that would enable China to launch on tactical warning. "No First Use" would doom China's nuclear deterrent to certain destruction by a U.S. or Russian conventional or nuclear first strike, or to a nuclear first strike by India.

China's nuclear posture, especially the lack of early warning radars and satellites, is "use it or lose it," which logically should drive prc [People's Republic of China] military planners toward nuclear first use—indeed toward surprise first use early in a crisis or conflict, based on strategic warning. …

China's military doctrine—including numerous examples presented here of using hemp attack to win on the battlefield, defeat U.S. aircraft carriers, and achieve against the U.S. homeland a surprise "Pearl Harbor" writ large—is replete with technical and operational planning consistent with a nuclear first-strike.

Dr. Pry warns that trusting China's "no first use" policy is "naive," citing government officials who have testified before Congress and confirmed that this term is meaningless.
China's goal in a conflict would be to paralyze its adversary with cyberattacks and electrical overload before any response can take place. "The emp attack scenario presents the only attack option that meets the demand for making the first, paralyzing strike of a war," states a briefing from Taiwan's Military College of National Defense University.
Together, cyberattacks and nuclear emp super-weapons are a deadly combination—and China intends to use them. Should the West be concerned?
Trumpet editor in chief Gerald Flurry answered this question in his May 7 *Key of David* program titled "The China-America Clash Is Prophesied." He commented on China's increasing belligerence around the South China Sea, saying that it is a "colossal danger for the U.S. because China could literally stop all of that flow of commerce or eliminate anybody that they didn't want to go through there if they became aggressive militarily, which they are doing more and more all the time."
Bible prophecy predicted China's rise long before it was evident on the world scene. It also predicted that an aggressive China would contribute to the U.S. gradually losing control of the Pacific and being conquered by its enemies.
As proved in *The United States and Britain in Prophecy*, by Herbert W. Armstrong, the U.S. is descended from the Israel of the Bible. This makes the Bible's prophecies directly relevant for today.
Deuteronomy 28:52 says that Israel's enemies will soon "besiege" it in all its "gates." The U.S. will lose its strategic sea choke points throughout the Pacific as China expands its influence. This is leading to an economic siege, which the book of Ezekiel reveals will include an alliance between China and Europe, effectively shutting the U.S. out of global trade.
How will the world's number one military superpower arrive at this point?
The *Trumpet* has drawn attention to America's reliance on digital systems many times over the years, and for good reason. "America is the greatest superpower this world has ever known," Mr. Flurry wrote in 1999. "But we have a very vulnerable point in our military—our own Achilles' heel. It is so dangerous that I am amazed it hasn't received more publicity."
He wrote this after reading a publication by defense analyst Joseph de Courcy, who stated, "Computer dependence is the Western world's Achilles' heel," warning that "within a few years this weakness could be tested to the full."
Today, the relevance of this statement has increased immeasurably.
One Bible prophecy describes how this will affect the U.S. today: "They have blown the trumpet, even to make all ready; but none goeth to the battle: for my wrath is upon all the multitude thereof" (Ezekiel 7:14).
"It seems everybody is expecting our people to go into battle, but the greatest tragedy imaginable occurs!" Mr. Flurry wrote in 2005. "Nobody goes to battle—even though the trumpet is blown! Will it be because of computer terrorism?"
A militarized China was prophesied in your Bible thousands of years ago, and the threat it poses is now becoming clear to many analysts.
The warning is stark, but it also carries great hope. After all the devastation, Jesus Christ will intervene to put a stop to mankind's deadly obsession with war, forever. Request our free booklet *Russia and China in Prophecy*; it shows why we shouldn't take these prophecies lightly. Understanding these prophecies will give you hope for a world free from weapons of mass destruction.

Study: Single drop of blood could help rapidly detect radiation sickness

Ohio State University Wexner Medical Center
Source: https://www.sciencedaily.com/releases/2020/07/200715154246.htm

July 15 – A new proof-of-concept study reports evidence that a new testing method has the potential to rapidly identify radiation sickness based on biomarkers measured through a single drop of blood. Scientists at The Ohio State University Comprehensive Cancer Center - Arthur G. James Cancer Hospital and Richard J. Solove Research Institute (OSUCCC - James) say the test could help save lives through early and real-time identification of the condition to enable timely clinical interventions.
Radiation sickness, or acute radiation syndrome (ARS), is a condition caused by irradiation of major volume or the entire body by a high dose of penetrating radiation in a very short time period - usually a matter of minutes. Historically, this has been most relevant through accidental exposures or mass casualty radiologic events, like the ones witnessed in Hiroshima and Nagasaki during World War II or even a reactor accident such as the one at Chernobyl in 1986.
The condition can rapidly weaken a person through its side effects and lead to death without intervention. The current diagnostic test – a dicentric chromosome assay - requires three to four days to get results. ARS most often impacts the bone marrow and gastrointestinal systems early while the debilitating effects on pulmonary, cardiovascular and central nervous systems can be delayed. Death can occur in a matter of days for the most severe cases, but

most patients die within several months of exposure. Rapid identification of exposure levels is critical for responding and triaging patient treatments.

"This new test uses a single drop of blood - collected from a **simple finger prick** - and results are ready in a few hours. It is rapid, scalable and can serve as a point-of-care-type diagnostic tool for real-time evaluation to screen a large number of individuals in a short time," says Naduparambil K. Jacob, PhD, an associate professor and scientist in the OSUCCC - James Translational Research Program.

For this test, researchers compare the relative expression of two small molecules called microRNAs in the blood. The first is microRNA-150 – which Jacob's lab identified several years ago as a biomarker to measure the extent of bone marrow damage. This microRNA decreases as a function of radiation dose while the normalizer, called microRNA-23a, does not change. Comparing these two molecular measures allows scientists to quantify the actual radiation dose absorbed, and therefore the overall exposure risk.

"We measure ionizing radiation in grays. People who are exposed to two grays need to be identified and treated and it is predicted that if you are exposed to about four grays to the whole body, without timely treatment there is a 50 percent chance of survival," says Jacob.

He noted this tool would have critical relevance in responding to mass casualty disaster scenario like that Chernobyl, to identify at-risk military personnel and civilians who need immediate treatment. It also has relevance for cancer patients, especially bone marrow transplant patients and others who have intense radiation therapy, where overdosing as well as underdosing is of concern.

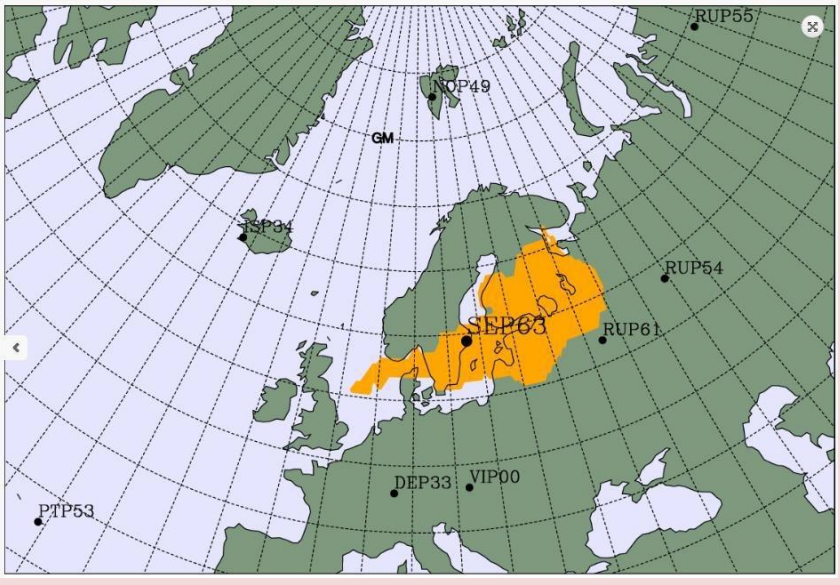
"Some patients develop major issues like thrombocytopenia and neutropenia as the result of radiation treatment. We can't look at a patient and determine how much radiation he or she has absorbed - but the impact can be cumulative. As a result, radiation sickness could occur weeks or months after the radiation therapy," explains Jacob. "With additional research, this new testing method could potentially help oncologists measure - in real time - absorbed radiation and intervene before radiation sickness occurs."

An Unexpected Radiation Spike Has Been Detected Over Europe

Source: https://www.sciencealert.com/unexpected-radiation-spike-detected-over-europe-authorities-say

June 29 – A mysterious increase in radiation levels over northern Europe was detected this month by authorities from several countries, although no nation has yet come forward to claim responsibility for the anomaly.

The subtle radiation spike – at levels that are considered harmless to humans, but significant enough to be picked up by radiation monitoring stations – began to make headlines last week, with European authorities announcing new readings of human-made radionuclide particles in the atmosphere.



"Very low levels of the radioactive substances cesium-134, cesium-137, cobalt-60 and ruthenium-103 were measured," the Swedish Radiation Safety Authority tweeted on Tuesday.

"The levels measured are so low that they pose no danger to people or the environment."

Similar observations were also made by radiation protection authorities in Norway and Finland.

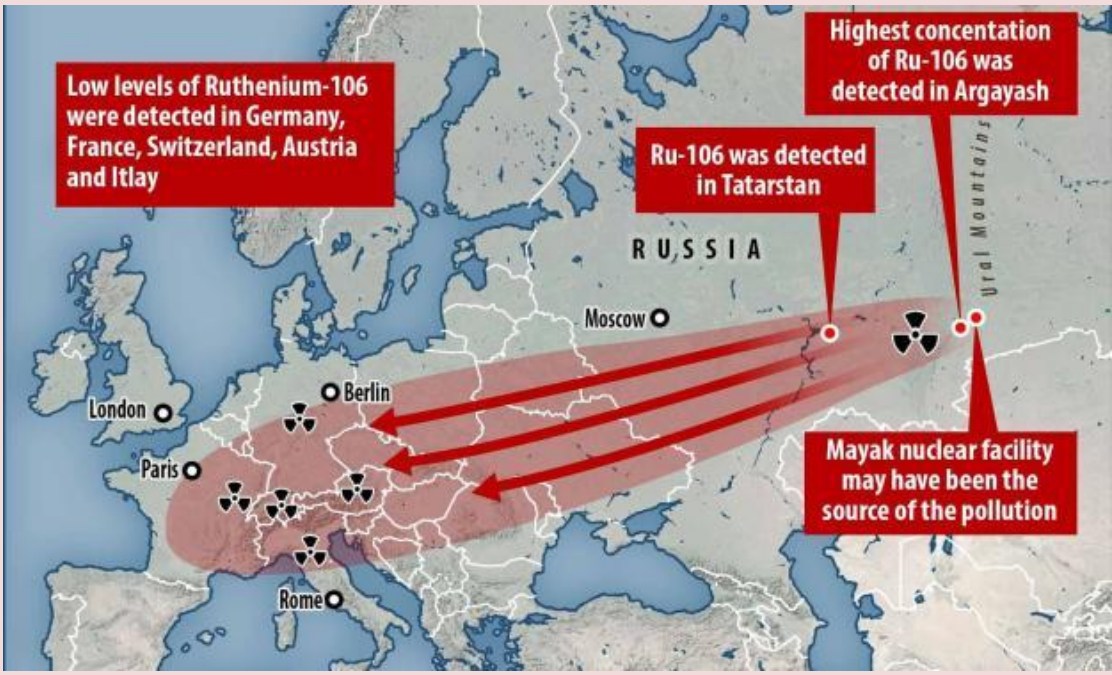
Later in the week, Lassina Zerbo, the Executive Secretary of the Comprehensive Nuclear-Test-Ban Treaty Organisation, tweeted a map outlining the possible source region of the anomaly, most of which was territory inside Russia, but also parts of Finland, Sweden, Denmark, and Norway.

"These isotopes are most likely from a civil source," Zerbo tweeted, suggesting a source related to nuclear power production, not nuclear weapons.

"We are able to indicate the likely region of the source, but it's outside the CTBTO's [Comprehensive Nuclear-Test-Ban Treaty Organization] mandate to identify the exact origin."

On Friday, the Dutch National Institute for Public Health and the Environment (RIVM) announced that, based on an analysis of the available data, the "combination of radionuclides may be explained by an anomaly in the fuel elements of a nuclear power plant".
On the available evidence, the organisation suggested that the radioactive particles detected had come from the direction of western Russia, but clarified that this did not mean they were definitively linked with Russian power plants.
"Some recent media reports claimed, possibly based on a mistranslation of our original report (in Dutch), that the radionuclides originated from western Russia," RIVM said in a statement.
"The claim RIVM makes is that the radionuclides travelled from the direction of western Russia to Scandinavia, but that no specific country of origin can be pointed out at this moment."

In response to online speculation that Russia was behind the radiation spike, a spokesperson for Rosenergoatom, part of Rosatom state nuclear energy corporation, said the nation's two nuclear power plants in the region were operating normally, with normal radiation levels being reported.



"Both stations are working in normal regime. There have been no complaints about the equipment's work," Rosenergoatom told Russian news agency TASS.
"Aggregated emissions of all specified isotopes in the above-mentioned period did not exceed the reference numbers. No incidents related to release of radionuclide outside containment structures have been reported."
As it stands, it's hard to say whether additional evidence will be able to confirm where this slight radiation surge originated, but the incident recalls **a similar situation that took place in 2017**, in which another radioactive cloud was detected over Europe.
During that episode – which was also detected at levels harmless to people – many suggested Russian power plants were responsible – a hypothesis that was later supported by scientific findings, although disputed by Rosatom

France Shuts Down Its Oldest Nuclear Plant

Source: http://www.homelandsecuritynewswire.com/dr20200702-france-shuts-down-its-oldest-nuclear-plant

July 02 – **France's state-owned power company EDF on Monday said that it had shut down the country's oldest nuclear plant located in Fessenheim in north-east France, 1.5 miles from the German border**.

The Fessenheim plant had two nuclear reactors on site. The first was shut down in February this year.
Le Figaro reports that the closing of one of France's 57 aging reactors was welcome news to critics of nuclear power, but the reaction to it demonstrated the division over nuclear power among green activists.
Critics of the anti-nuclear sentiment among some environmentalists said that phasing out nuclear energy is not the way forward.
Pro-nuclear energy protesters gathered in front of the Greenpeace headquarters in Paris to

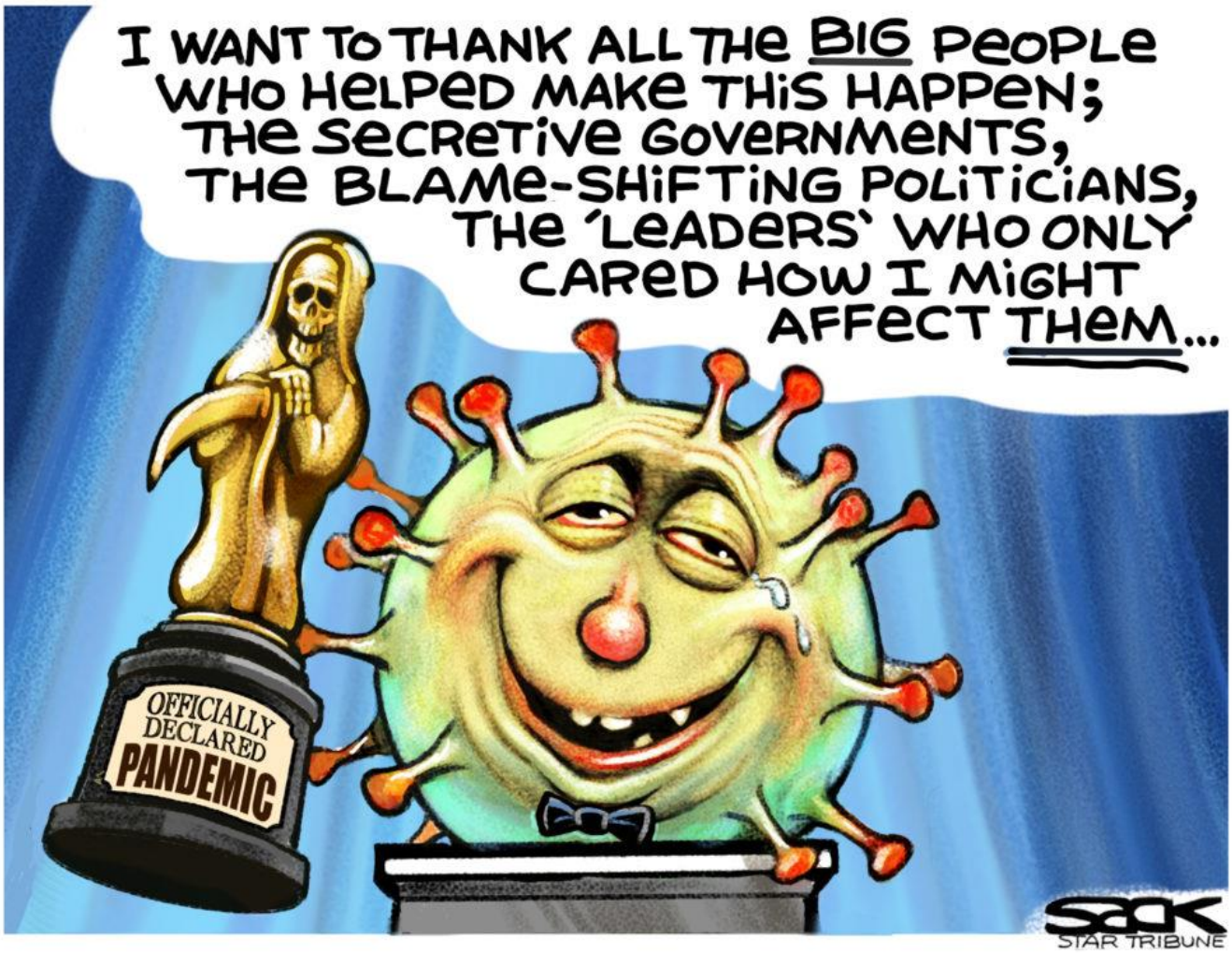
protest against Greenpeace's campaign to end the use of nuclear energy in France. "Less nuclear means more coal," chanted protesters.

France's strong trade union movement also criticized the closure, noting the loss of more than 1,000 jobs in the industrial Haut-Rhin region, which has witnessed a steady decline in manufacturing and industrial jobs over the last two decades.

Following the 2011 Fukushima nuclear disaster, France's then-President Francois Hollande committed to close Fessenheim, but the actual implementation had to wait the election of Emanuel Macron in 2017, who gave his final approval for the closure two years ago.

With the closure of Fessenheim, France now has 56 pressurized water nuclear reactors located in at 18 nuclear plants, generating about 70 percent of the country's electricity. Only the United States, with 98 reactors, has more (the United States had 104 reactors ten years ago, but following the Fukushima disaster, six where taken offline because they were built too close to seismic fault lines). France is leading other countries by a wide margin in the percentage of nuclear energy in its power consumption.

Macron has pledged to increase France's energy use of other renewables, and said 12 more nuclear reactors will be shut down by 2035.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

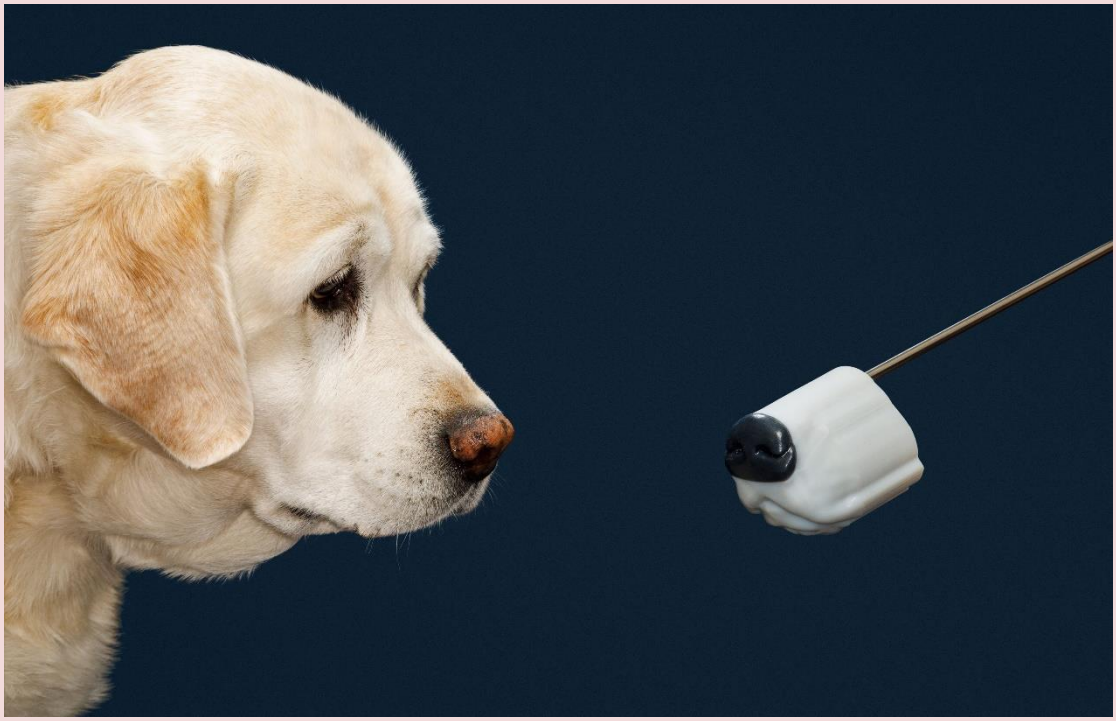
HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

Why explosives detectors still can't beat a dog's nose

Source: https://www.technologyreview.com/2019/10/24/132201/explosives-detectors-dogs-nose-sensors/



Oct 2019 – For nearly as long as armies have fought one another, they have enlisted animals to help. Horses, especially, were decisive for millennia. As historian Morris Rossabi has written of the Mongol conquest of Asia, "Mobility and surprise characterized the military expeditions led by Genghis Khan and his commanders, and the horse was crucial for such tactics and strategy. Horses could, without exaggeration, be referred to as the intercontinental ballistic missiles of the thirteenth century." Historian David Edgerton notes that as late as the First World War, "Britain's ability to exploit world horse markets was crucial to its military power."

Horses are still of occasional importance, as in the American invasion of Afghanistan in 2001, when Special Forces troops on horseback called in bomb strikes via satellite radios, using laser designators and GPS reference points to guide the bombs. But horses are only very rarely the tool that separates defeat from victory: in all but the most exceptional circumstances, they have been replaced by tanks, trucks, satellites, and airplanes.

Yet while horses are largely gone from modern armies, dogs are not. As of 2016, the US military counted over 1,740 military working dogs among its ranks. At Lackland Air Force Base in San Antonio, the military breeds its own sleek puppies—mainly German shepherds and Belgian Malinois—who are groomed for military service from their first whimper. Some will wash out; others will go on to four to seven months of basic obedience instruction before receiving more specialized training in how to guard bases, ambush enemy combatants, and sniff out explosive devices. From there the field narrows further. The US Army estimates that to produce 100 war-ready dogs, it must train 200.

Before entering buildings in Afghanistan, Thomas, a US army paratrooper who asked to be identified by a pseudonym, would often send his platoon's Belgian Malinois in first to ensure that no enemy soldiers or other surprises waited inside. During one day of particularly fierce fighting, Thomas was in a building, looking for somewhere to treat a wounded soldier, when he heard a noise from an adjacent room. As he rounded the corner to investigate, he remembers seeing "a shadow and a flash of light." It was a Taliban-hired Chechen fighter with an AK assault rifle aimed directly at his face.

"You want to be able to sample the environment in a smart way, and dogs have given us a lot of insight into what that looks like."

Just as the fighter squeezed the trigger of his weapon, the platoon's dog came blazing into the room from the hallway and latched onto his neck, jerking him backwards. His shot was diverted, sparing Thomas's life.

After that, Thomas brought the dog on every mission he could. "Sometimes people would say to me — 'Oh, you don't need a dog for that,'" he says. "And I'd say, 'Yeah, I need a dog. Are you on the ground? You're not on the ground. I'm bringing the dog.'"

The military also relies heavily on dogs to sniff out explosives. Dogs' sense of smell is estimated to be 10,000 to 100,000 times stronger than the average humans. Billions of dollars' worth of research on artificial detectors have yet to produce anything better. Unlike metal detectors, which are also used to locate roadside bombs and landmines, canines can be trained to pick up on non-metallic explosive devices concocted from fertilizer and other household items. This talent has proved

particularly useful in Afghanistan, where many buried explosives are improvised from common chemicals packed into plastic jugs.
Scientists have long tried—and failed—to create devices capable of outperforming a dog's snout. Starting in 1997, DARPA dedicated $25 million to an initiative called "Dog's Nose," which distributed grants to scientists to develop landmine detectors. At that point, an estimated 100 million mines were buried in approximately 60 countries. But according to the DARPA program's director, Regina Dugan, the technology to find them had not advanced much since the Second World War. "The only landmine detection equipment issued to US soldiers in the field were the metal detector and a sharp, pointy stick," she wrote in 2000. (The stick was to prod the ground for anomalies.)
The resulting machines, most of which featured polymer-coated tubes that reacted when exposed to explosives, seemed promising when used in sterile laboratories. But in more realistic environments things got messier. When one of the machines was pitted against landmine-detecting dogs at Auburn University in Alabama in 2001, the highest-performing canines were approximately 10 times more sensitive. In a 22-acre grassy facility in Missouri where DARPA invited participants to test their devices, some were too responsive, reacting to plants and soil in addition to explosives.
A decade later, in 2010, the commander of the Joint Improvised Explosive Device Defeat Organization (JIEDDO) admitted that despite a whopping $19 billion of government investment in spy drones, radio jammers, and aircraft-mounted sensors meant to combat improvised explosive devices (IEDs), dogs remained unparalleled as detectors of the dangerous devices. While sensors typically found half of the IEDs before they exploded, dog teams located 80% of them.

NIST

The newest artificial detectors can detect smaller traces of chemicals than a dog can. But those detectors are big, explains Matthew Staymates, a mechanical engineer and fluid dynamicist at the National Institute of Standards and Technology (NIST): "It's got to plug into a wall, you need an enormous amount of infrastructure, gases, and vacuum pumps—and you have to bring the sample to your machine."
Nonetheless, artificial detectors have a role to play in places like airports, where all passengers must pass through security checkpoints, and dogs have provided inspiration for improving them. Staymates used a 3D printer to replicate the nose of a female Labrador retriever named Bubbles. The result is a snout-shaped extension that goes on the front of commercially available explosives detectors. It sniffs air like a dog, inhaling and exhaling several times a second instead of continuously sucking air in as such machines normally do.
The researchers found that this method, counterintuitively, pulls in samples of air from farther away, drawing in more of the chemicals floating around. "Nine times out of 10, you don't know where the bad guy with a pipe bomb in his backpack is," Staymates explains. "So, you want to be able to sample the environment in a smart way, and dogs have given us a lot of insight into what that looks like."
Despite this progress, a dog is still much more effective than an electronic bomb-sniffer—not least because an animal, like a human but unlike a machine, can react to unpredictable situations. So some scientists have focused their efforts not on replacing working animals, but on improving their performance.
In 2017, a team at MIT's Lincoln Laboratory developed a new mass spectrometer, about the size of a large dresser, that could identify trace amounts of chemicals on a par with canine performance. Not only was it impressively sensitive, but it was fast, completing its assessments in about one second. The researchers were excited about the device's potential not to substitute for bomb-sniffing dogs, but rather to help train them.
The team had dogs locate explosives previously hidden in canisters, which were also analyzed with the spectrometer. The machine discovered that some of the perceived errors the dogs made—identifying explosives in supposedly empty vessels—weren't errors at all; the containers had been cross-contaminated. That allowed the trainers to better regulate when to praise and reward their canine students, reinforcing their detection abilities.
Though some labs wanted to adapt the machine to replace dogs, the MIT team disagreed. In a news release at the time, Roderick Kunz, who led the research, said: "Our feeling is that such a tool is better directed at improving the already best detectors in the world—canines."

Abandoned oil tanker off Yemen coast at risk of exploding

Source: https://www.nbcnews.com/science/environment/abandoned-oil-tanker-yemen-coast-risk-exploding-n1232254

June 26 — The United Nations said an abandoned oil tanker moored off the coast of Yemen loaded with more than 1 million barrels of crude oil is at risk of rupture or exploding, causing massive environmental damage to Red Sea marine life, desalination factories and international shipping routes.

Meanwhile, Houthi rebels who control the area where the ship is moored have denied U.N. inspectors access to the vessel. Internal documents obtained by The Associated Press shows that seawater has entered the engine compartment of the tanker, which hasn't been maintained for over five years, causing damage to the pipelines and increasing the risk of sinking. Rust has covered parts of the tanker and the inert gas that prevents the tanks from gathering inflammable gases, has leaked out. Experts say maintenance is no longer possible because the damage to the ship is irreversible.

Satellite image of the FSO Safer tanker moored off Ras Issa port, in Yemen, on June 17, 2020.Maxar Technologies / via AP file

For years, the U.N. has been trying to send inspectors to assess the damage aboard the vessel known as the FSO Safer and look for ways to secure the tanker by unloading the oil and pulling the ship to safety.

But one European diplomat, a Yemeni government official and the tanker's company owner said that Houthi rebels have resisted. The diplomat said the rebels are treating the vessel as a "deterrent like having a nuclear weapon." All three individuals spoke on condition of anonymity to discuss the subject with a reporter.

"They do say that openly to the U.N., 'We like to have this as something to hold against the international community if attacked,'" the diplomat said. "Houthis are definitely responsible for failure of the U.N. to look at the ship."

Money is also an issue, the diplomat said, adding that the Houthis initially were demanding millions of dollars in return for the oil stored in the tanker. The U.N. is trying to reach an arrangement where money could be used to pay workers and employees at Yemen's Red Sea ports, the diplomat added.

Some experts, however, criticize both the Houthis and the U.N. for failing to fully understand the magnitude of the crisis with the abandoned ship.

The external piping system of the FSO Safer and the hose failure that led to a spill, moored off Ras Issa port, Yemen.I.R. Consilium / via AP file

Ian Ralby, founder of I.R. Consilium, who specializes in maritime and resource security, told the AP that U.N.'s efforts to send a team to assess the ship is "futile." What the vessel needs is a salvage team, he said.

"It's real shame that they wasted so much money and time in this futile operation," said Ralby. "If you are taking these years to get a simple team to assess, we will not have a second chance to salvage," he added.

Ralby, who has written extensively about the tanker, told the AP that amid declining oil prices the cost spent on cleaning up the environmental damage from an explosion or leakage will be much more than the millions worth of oil on the ship.

But the Houthis have refused to back down from their demands.

Mohammed Ali al-Houthi, the rebel group's leader, blamed the U.S. and Saudis for not letting the rebels sell the oil, saying in a June 18 Twitter post that any "disastrous consequences ... God forbid," that could result from the collapse of the vessel will be the responsibility of these two countries.

The Iranian-backed Houthi rebels are in control of the western Red Sea ports, including Ras Issa, 6 kilometers (3.7 miles) from where the FSO Safer tanker has been moored since the 1980s. They are at war with the internationally recognized government, which is backed by a Saudi-led coalition and the United States. President Abed Rabbu Mansour Hadi is in exile in Saudi Arabia and his government in disarray.

The floating tanker is a Japanese-made vessel built in the 1970s and sold to the Yemeni government in 1980s to store for export up to 3 million barrels pumped from oil fields in Marib, a province in eastern Yemen. The ship is 360 meters (1,181 feet) long with 34 storage tanks.

A senior official at the state-owned oil company in charge of the tanker, said because of a shrinking operational budget, which used to be around 20 million dollars a year before the war, the company could no longer afford to purchase fuel needed to run the boilers on the ship. The boilers are needed to power generators that, among other things, keep an inert gas that prevents explosions flowing. The tanker needs 11,000 tons of the fuel, which cost about 8 million dollars each year.

"After the stoppage of the boilers the strong majority of the equipment and the machines of the tanker stopped because they all depend on steam power," the company official said. That includes the machines that power the ventilation system, which reduces humidity and prevents corrosion, he said.

The deck of the FSO Safer, indicating the lack of basic maintenance for several years, leading to incidental smaller spills, moored off Ras Issa port, Yemen.I.R. Consilium / via AP file

Since 2015, annual maintenance on the ship has come to a complete halt and most crew members, except for 10 people, were pulled off the vessel after the Saudi-led coalition imposed a land, sea, and air embargo before waging an extensive air campaign to dislodge the Houthi rebels from areas they seized including the capital, Sanaa.

The civil war in Yemen has caused massive destruction in most of the areas under Houthis control. Because of the proximity of the tanker to the contested Hodeida port, fears have grown that a stray shell or bullet could hit the tanker causing massive explosion or oil leak into the Red Sea.

Hodeida was at the center of Yemen's civil war in 2018 when coalition forces made major advances to take over the vital port, which is considered the life-line of most of northern Yemen, where most of Yemenis live and where the Houthis enjoy full control. A U.N.-brokered peace deal put an end to the offensive but failed to achieve peace or loosen Houthis' grip over the ports.

Over the past two years, the Yemeni government in exile, the U.N., and western diplomats have been sounding the alarm and putting pressure on Houthis to secure the tanker. The rebels initially agreed to let inspectors examine the tanker but later backtracked.

Top Houthi leaders often expressed cynicism toward the international community warnings.

"The life of the shrimps is more precious than the life of Yemeni citizen to the U.S. and its allies. Is this because they care about their naval ships or the Israeli presence in the Red Sea?" wrote Mohammed Ali al-Houthi in a May 25 Twitter post. "Why is Safer more dangerous than the siege and the assault of the American, British, Saudi, Emirati and their allies on the people?" he added in reference to the US-backed, Saudi-led coalition targeting the rebels in Yemen.

Yahia Sharaf Eddin, the deputy head of Yemen Red Sea Ports Corporation, defended the Houthis rebels and told the AP that the group had instructed port authorities to assist U.N. inspectors. He said it was the Saudi-led coalition that refused to give the U.N. a green light to board the decaying tanker.

The more delays in reaching a solution to the vessel, the more dangers it poses, Sharaf Eddin said.

A recent internal government memo obtained by the AP shows that earlier this month a diving team was dispatched by the state-run oil company that owns the tanker to seal holes in the ship that have allowed seawater to leak into the engine room.

The divers were able to make repairs, but it remain unclear if the work will hold, according to the July 13 report.

"We believe that the plugs/seals that were installed to prevent the entry of seawater into the engine room space will not withstand/hold long," the report read.

An earlier letter dated Oct. 2019 sent by the Yemeni minister of oil — who is affiliated with the Saudi-backed government — to the prime minister, and seen by the AP, found other problems with the tanker.

"Rust has covered some parts of the tanker along with equipment, fire distinguishing system stopped working, and what is more dangerous is that the gas which was covering the oil inside the tanks has leaked out. It was used to protect the tankers from exploding," the letter read.

The oil minister's letter recommended three different approaches to deal with the tanker: make repairs, pump the oil to another ship, or to pull the tanker away and safely unload it in another port.
The minister wrote that because of the "collapsing condition" of the vessel, the best solution is to pull it away to another port.
"We are notifying you about this dangerous situation to do your best and to get Yemen and the region out from such environmental dangers," he wrote.
The letter came months after the U.N.'s projects arm, known as UNOPS, put out a tender to hire an international agency to inspect the vessel after an initial agreement with Houthis.
The U.N. hired a team of experts and had them standing by in Djibouti. The AP obtained a copy of the tender letter and documents showing the experts' proposed inspection program and a list of equipment needed, including gas detector and oil sampling kits.
But the Houthis backed out of the agreement before the repair crew could be sent to Yemen.
Mark Lowcock, the U.N. humanitarian chief, told the U.N. Security Council last year that the U.N. assessment team was ready to be deployed but "the necessary permits remain pending with the Ansar Allah authorities" in reference to Houthis.
"I would just like to note that this is additionally frustrating when one recalls that the same authorities wrote to the United Nations early last year requesting assistance with the tanker and promising to facilitate our work," he added.
Sharaf Eddin, the Yemeni ports official, accused the U.N of siding with the Saudi-coalition and misleading the public by blaming Houthis for the delays.

"This is the same U.N. which is exploiting Yemen tragedy to collect donations then spend it on its own employees," he said, echoing Houthis' widely held anti-U.N. sentiment. He added that the coalition in 2017 refused to give access to a fuel vessel to head to the Safer tanker to run the power generators. "What is Houthis' interest in preventing a disaster? Any spark could cause massive explosion," he acknowledged.
He provided letters sent by Houthi-appointed government officials last summer, including one from the foreign minister, approving the visit by the U.N. But the European diplomat said the Houthis revoked their initial approval and put new conditions on U.N. activities.
The U.N. has repeatedly warned that delays in taking action to fix the FSO Safer could lead to a man-made environmental disaster in the Red Sea four times greater than the Exxon Valdez oil spill.
The Exxon Valdez disaster in 1989 was one of the largest oil spills in U.S. history. The tanker spewed nearly 300,000 barrels of thick, toxic crude oil into Alaska's pristine Prince William Sound. Scores of herring, sea otters and birds were soaked in oil, and hundreds of miles of shoreline polluted. The spill destroyed the livelihoods of hundreds of commercial fishermen in the area.
The senior official at the state-owned company in charge of the tanker issued an appeal for help to the international community saying that a similar oil spill off the coast of Yemen could accelerate Yemen's worsening humanitarian disaster.
"The disaster could happen at any second," he said, "Rescue Yemen from a terrible, imminent disaster that will add to Yemen's burdens for tens of years and deprive thousands from their source of living, and kill marine life in the Red Sea."

Yemen's Houthi rebels allow UN team to inspect 'time bomb' oil tanker

Source: https://www.criticalinfrastructureprotectionreview.com/news-july-2020/yemens-houthi-rebels-allow-un-team-to-inspect-time-bomb-oil-tanker/

July 12 – Yemen's Houthi rebels have given U.N. inspectors the green light to inspect a decaying oil tanker abandoned off the coast with 1.1 million barrels of crude onboard which experts say could rupture at any time.
A breach of the vessel would have disastrous results for Red Sea marine life and tens of thousands of impoverished people who depend on fishing for their livelihood.

The 45-year-old FSO Safer is anchored off the port of Hodeida under the control of the Iran-backed Houthi, who have previously blocked efforts to send inspectors to assess its condition.

Top Houthi leader Mohammed Ali al-Houthi said on Twitter last month that the rebels want guarantees the vessel will be repaired and that the value of the oil on board is used to pay salaries of their employees.

The market value of the oil is now estimated at $40 million, half what it was before crude prices crashed, although experts say poor quality could push it even lower.

Independent Yemen-based environmental group Holm Akhdar which means "Green Dream" in Arabic, warned an oil spill could stretch out from the Red Sea to the Gulf of Aden and into the Arabian Sea.

The region's ecology would need over 30 years to recover from an oil spillage of that size, it said in a recent report, adding that about 115 of Yemen's Red Sea islands would lose their biodiversity and natural habitats.

In a country where the majority of people already rely on aid to survive, an estimated 126,000 fishermen, including 68,000 in Hodeida, would lose their only source of income.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

CYBER NEWS

Chinese hackers attempted 40,000 cyber-attacks on Indian web, banking sector in 5 days

Source: https://www.indiatoday.in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24

June 24 – Hackers based in China attempted over 40,000 cyber-attacks on India's Information Technology infrastructure and banking sector in the last five days, a top police official in Maharashtra said on Tuesday.
The spurt in online attacks from across the border was noticed after tensions rose between the two countries in eastern Ladakh, said Yashasvi Yadav, Special Inspector General of Police of the Maharashtra Police's cyber wing.
'Maharashtra Cyber', the state police's cyber wing, collated information about these attempts and most of them were found to have originated in Chengdu area in China, he said.
"According to our information at least 40,300 cyber-attacks were attempted in the last four-five days on the resources in Indian cyberspace," he said. The attacks aimed at causing issues such as denial of service, hijacking of Internet Protocol and phishing, Yadav added.
Indian Internet users should pay attention to the threat of such attacks, create robust 'firewalls' and conduct cyber security audits, the IGP said.

California university pays $1 million ransom amid coronavirus research

Source: https://www.cyberscoop.com/ucsf-ransomware-payment-coronavirus/

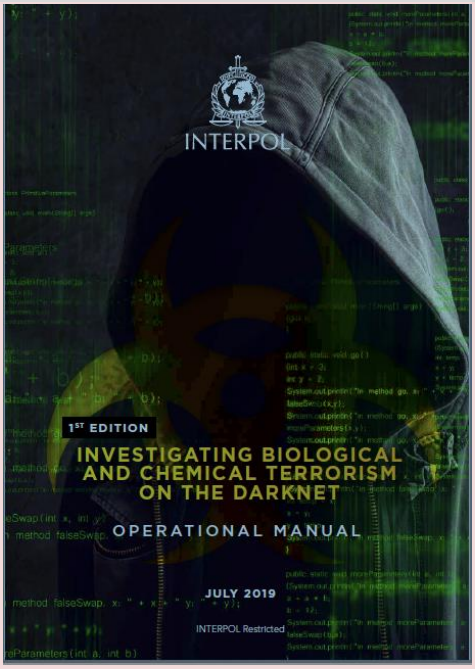
June 29 – A university in California previously reported to be conducting COVID-19 research has paid $1.14 million to digital scammers who locked the schools' systems and demanded an extortion fee.
The University of California, San Francisco said on Friday it paid the ransom after malicious software infected a "limited number of servers" in an attack detected on June 1 at the university's School of Medicine. While it remains unclear what, exactly, was affected, the school said the incident did not affect its patient care system, the campus network or the school's research on the coronavirus. Scientists at the university are conducting trials into whether anti-malarial drugs may help mitigate the COVID-19 pandemic, as Bloomberg first reported.
"Our investigation is ongoing but, at this time, we believe that the malware encrypted our servers opportunistically, with no particular area being targeted," university officials said in an announcement Friday. "The attackers obtained some data as proof of their action, to use in their demand for a ransom payment. We are continuing our investigation, but we do not currently believe patient medical records were exposed."
While U.S. law enforcement typically advises against paying ransomware demands, victimized organizations sometimes meet attackers' demands when decryption without hackers' help seems unlikely, or cost-prohibitive.
Attackers from the so-called Netwalker ransomware gang were behind this incident, BBC News reported, the latest in a series of ransomware hacks against universities and public health agencies. The scam also coincides with an evolution in ransomware techniques, as hackers increase the size of their demands and, in some cases, threaten to publicize stolen data when victims refuse to pay.

Leaked police docs reveal crypto's role in dark web bioweapons trade

Source: https://decrypt.co/35812/leaked-police-docs-reveal-cryptos-role-in-dark-web-bioweapons-trade

July 16 – A leaked INTERPOL manual covering the trade in chemical and biological weapons on the dark web includes advice for transacting in and seizing cryptocurrencies
The manual, titled 'Investigating Biological and Chemical Terrorism on the Darknet', coaches law enforcement on best practices for infiltrating the dark web's contrabandist subcultures. As well as advising investigators on how to transact in cryptocurrency, it also explains how to create an undercover identity, use the Tor browser and access dark web community forums such as Dread.

Seizing dirty Bitcoin
The document coaches law enforcement on how to seize cryptocurrency that is suspected to be tainted by crime. To protect the integrity of INTERPOL's investigative tradecraft, and to avoid a potential "Red Notice," *Decrypt* is declining to publish these findings.



In general, however, because cryptocurrencies are inherently not sovereign money, they are not beholden to any mutual legal assistance treaty (MLAT). If police have control of a suspect's wallet, they can transfer the money to a law-enforcement controlled account and no MLAT permission is required because no nation has dominion over it.

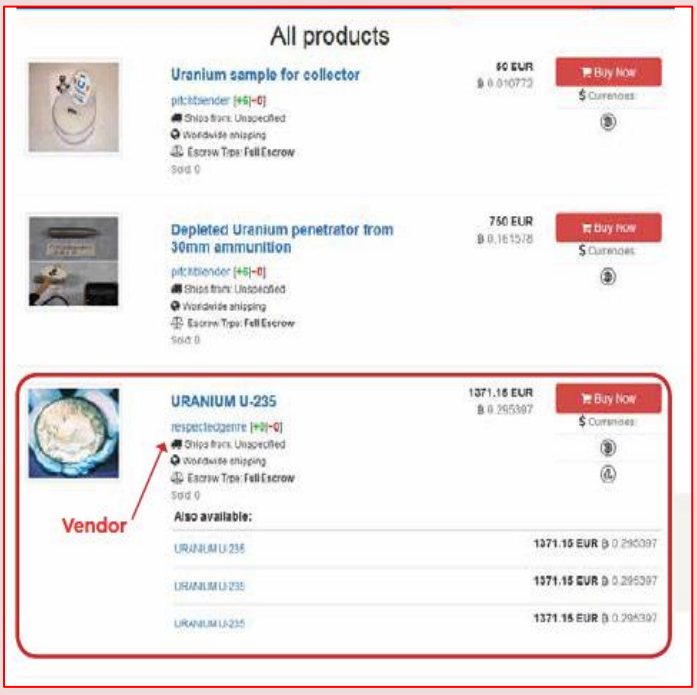
Still, the INTERPOL manual notes: "National legal frameworks and agency regulations related to Darknet access and investigations can differ from one country to another and must always be respected."

The manual also offers tutorials on how to operate virtual private networks (VPNs), work in virtual machine environments such as Whonix, and communicate covertly via messages ciphered with pretty-good-privacy (PGP) encryption.

Project Pandora and bioterrorism

The manual, published in 2019 and spanning 142 pages, was created in support of INTERPOL's Project Pandora, a 2018 initiative focused on "countering biological and chemical trade via the Darknet through the development of investigative and operational countermeasures."

The manual includes screencaps purporting to show Uranium and mustard gas that were scraped from the now-defunct darknet market, Berlusconi, which was seized by Italian authorities last November.



Growing international scrutiny of this dangerous trade comes at a time when law enforcement is increasingly encountering cases where people are discussing, or actually attempting to purchase, bacterial and chemical agents on the dark web—using cryptocurrency as a medium of exchange.

Uranium listings on the now-defunct Berlusconi dark web market (Source: INTERPOL)

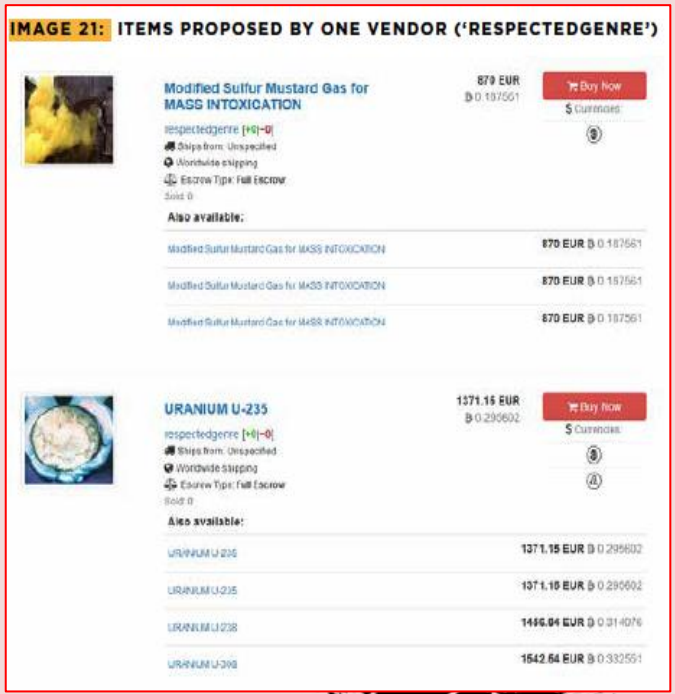
In July 2015, Liverpool, UK resident Mohammed Ali was convicted after attempting to buy 500mg of ricin from an undercover FBI agent, using Bitcoin

. The judge presiding over Ali's case said there was "no evidence that he was planning any sort of terrorist attack."

Modified Sulfur mustard gas and Uranium U-235 being sold on Berlusconi dark web market (Source: INTERPOL)

Last September, Oakland resident Samford "Bemi" Faison was sentenced to almost six years in jail for paying $95 in Bitcoin to an undercover FBI agent, in a bid to acquire a toxic chemical to kill his estranged wife. The former child actor authored a public post on a dark web forum openly soliciting chemicals; it was discovered by FBI agents, who then orchestrated a sting operation.

FBI undercover agents nabbed another would-be dark web chemical-weapon buyer last March, when they arrested 37-year-



old Sijie Liu of Winnipeg, Canada in Pembina, North Dakota. Liu was arrested after placing an order for 10 milliliters of toxin and protective equipment to handle it; the package was recovered at a commercial mail receiving facility. She was sentenced to six years in US prison at the end of last month.

Are biological and chemical weapons for sale on the dark web?

The above cases notwithstanding, experts who spoke to *Decrypt* are skeptical that there's a widespread market for biological and chemical weapons on the dark web. Madeleine Kennedy, a spokesperson for blockchain
investigation and compliance firm Chainalysis, told *Decrypt*, "We have not seen much on the dark web related to chemical and biological weapons and suspect most listings of that nature are scams."

Scott Stewart, vice president at protective intelligence firm TorchStone Global, and a former US Army intelligence officer and special agent for the State Department's Diplomatic Security Service, is similarly doubtful that a significant attack could be carried out using chemical or biological materials obtained from the dark web.

"A serious and sophisticated chemical or biological weapons program by an actor like the Al-Qaeda or ISIS would not be online at all. They know that is terrible OpSec (operational security) even on the dark web or using encrypted channels or devices," he told *Decrypt*.

More likely, he suggested, is that someone from a core group could communicate with a grassroots supporter using the dark web, ordering them to perform a terrorist attack. "But instead of telling them to use a knife, gun, or vehicle, they'd be instructing them to weaponize the chemical agent or disease," he added.

In the wake of the coronavirus pandemic, however, biological terrorism is increasingly on the authorities' radar. In April this year, UN Secretary-General António Guterres noted that COVID-19 could embolden threat groups to pursue pathogen-based attacks.

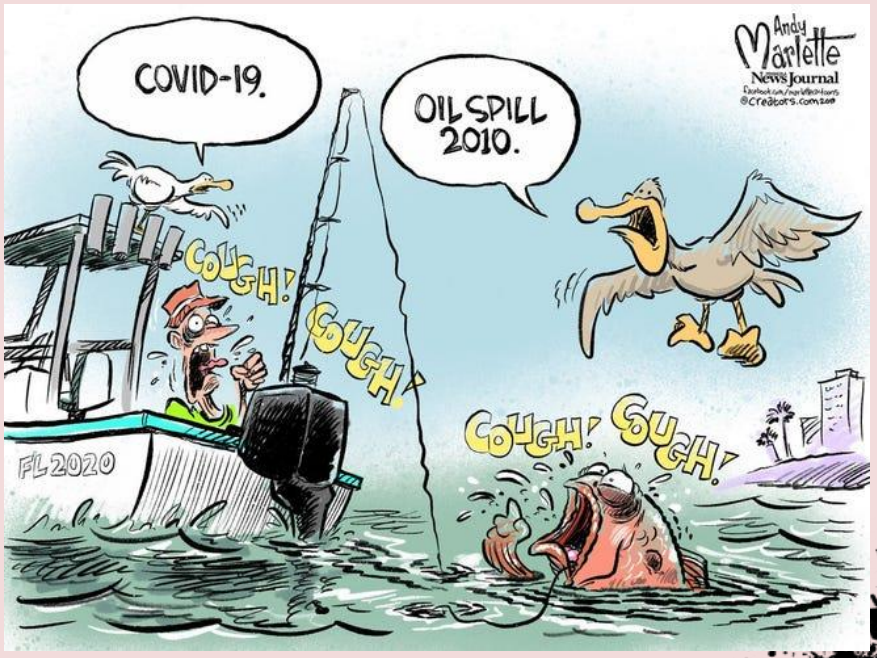
How did the INTERPOL manual leak?

An INTERPOL spokesperson told *Decrypt* that the agency "works with law enforcement and other global experts to develop manuals and handbooks on a wide variety of crime types."

"Such handbooks typically provide information on best practices, case studies, and the latest investigative tools and techniques," the spokesperson said. "These are made available to law enforcement investigators via the INTERPOL National Central Bureaus in each member country."

The INTERPOL manual was one of a cache of law enforcement documents, dubbed Blueleaks, which were acquired by hacktivist group Anonymous via a security breach at law enforcement web-hosting firm Netsential.

Originally posted online by "transparency collective" Distributed Denial of Secrets, the 270GB data dump reveals the inner workings of over 200 US police departments, including the techniques used by the FBI to track Bitcoin laundering on the dark web. German authorities seized DDoS' public data servers on July 2, but their website is still online.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Are Armed Drone Swarms A Weapon of Mass Destruction?

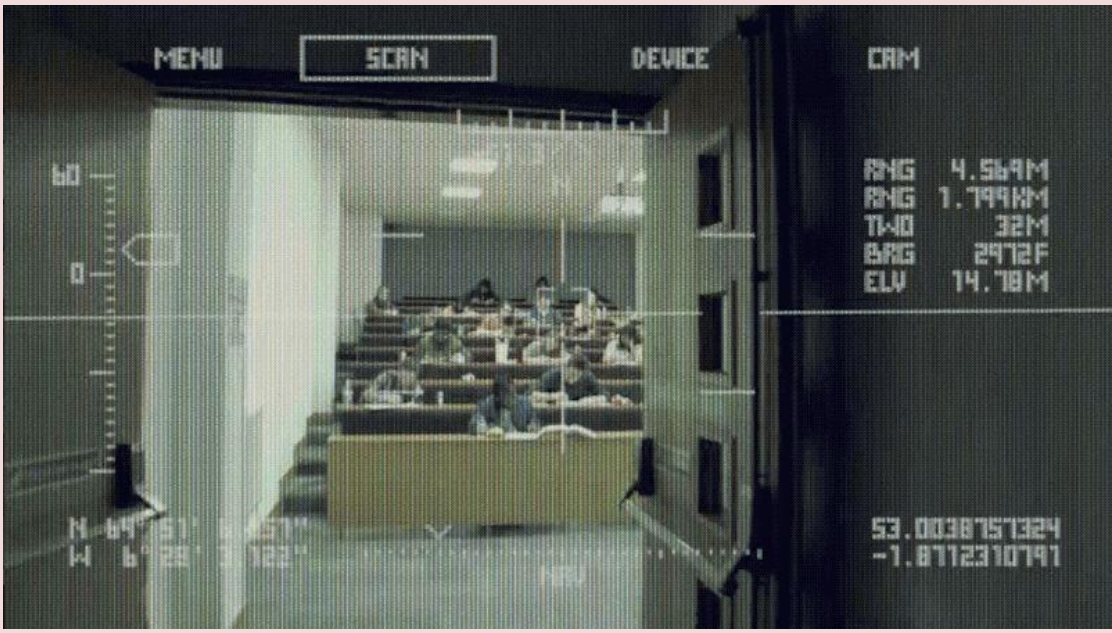
By Kelsey D. Atherton (defense technology journalist, Albuquerque, NM)
Source: https://www.forbes.com/sites/kelseyatherton/2020/06/29/are-armed-drone-swarms-a-weapon-of-mass-destruction/#4c339d3f52fb

June 29 – **How many armed flying robots does it take to equal a weapon of mass destruction?**
The question is both rhetorical and theoretical. While armed autonomous drone swarms do not yet exist, the spectre of masses of flying robots seeking and finding human targets was the subject of "Slaughtbots," an activist short film released in 2017. It's also an entirely possible end-goal from the conflux of a host of drone technologies, like cheap airframes, automated targeting, swarming, and explosive payloads, each separately in development.

So while the technology of Slaughterbots might not be ready for deployment any time soon, figuring out the possible implications of such a technology are worth doing before nations and militaries fully develop them.

"Armed, fully autonomous drone swarms should be classified as WMD because of their degree of potential harm and inherent inability to differentiate between military and civilian targets—both of which are characteristics of existing weapons categorized as WMD," writes Zachary Kallenborn, a Senior Consultant at ABS Group.

Kallenborn's argument is that these swarms present a technical challenge, limited military utility, and unacceptable risk, and should be regulated by norms and laws preemptively. Kallenborn makes this case in concise form by the Modern War Institute at West Point and in a longer monograph published by the U.S. Air Force Center for Strategic Deterrence Studies in May.



Video capture from Slaughterbots

Managing remotely piloted drones like the Reapers used today is a labor-intensive process, with pilots and sensor operators and analysts all tasked with guiding the robot and directing its lethal force. Even with that apparatus in place, drone strikes are capable of producing deadly errors that kill civilians incorrectly identified as combatants.

Introducing autonomy into the mix, which on scale alone a drone swarm must, means turning to code instead of human judgement for those decisions.

For example, the weapon needs to recognize whether a target is carrying a rifle or a rake. Accurate assessment depends heavily on image resolution and target visibility," writes Kallenborn. "Obscuring conditions such as rain, snow, or shadows may prevent civilian-military discriminators from being perceived accurately. [Armed Fully Autonomous Drone Swarms] must also identify and evaluate context. Even if a target is holding a rifle, the person may be a farmer, not a soldier. In addition, guerrilla or unconventional forces blur the line between farmer and soldier, because they lack clear indicators of military affiliation. Even if a target is a soldier, the person may be considered a noncombatant due to illness or injury."

The drone show in Seoul, which started with prevention messages, continued with messages of gratitude for medical workers in the front lines of the fight against the novel coronavirus

While Kallenborn holds out the possibility that sensors and software may someday be able to handle that problem of target discrimination, that day is nowhere close, and the risk is great.
It is this risk, in part, that has animated much of the international organizing against lethal autonomous weapon systems. Swarms cannot help but be fully autonomous if they are to work at all, so one possible solution in the near-term if swarms are developed is to prevent them from being armed, leaving humans in the loop and in control over any lethal decisions.
"Drone swarm technology, particularly self-targeting, self-mobile drone swarms, poses a significant risk to global security. Failing to develop international norms, supported by robust policies, to prevent and counter AFADS emergence risks a less secure United States and a far more dangerous world," Kallenborn concludes.

Dubai paves way for drone package deliveries with 'miniature airports' network

Source: https://www.thenational.ae/uae/transport/dubai-paves-way-for-drone-package-deliveries-with-miniature-airports-network-1.1044027

July 04: Dubai took the first steps to creating a commercial drone network on Saturday as it set out plans for miniature helipads and an air traffic control system.
The Dubai Sky Dome project would pave the way for the delivery of packages and even the transport of passengers, the government said.
Sheikh Ahmed bin Saeed, president of Dubai Civil Aviation Authority, said an initial framework has been drawn up that includes laws and regulations.

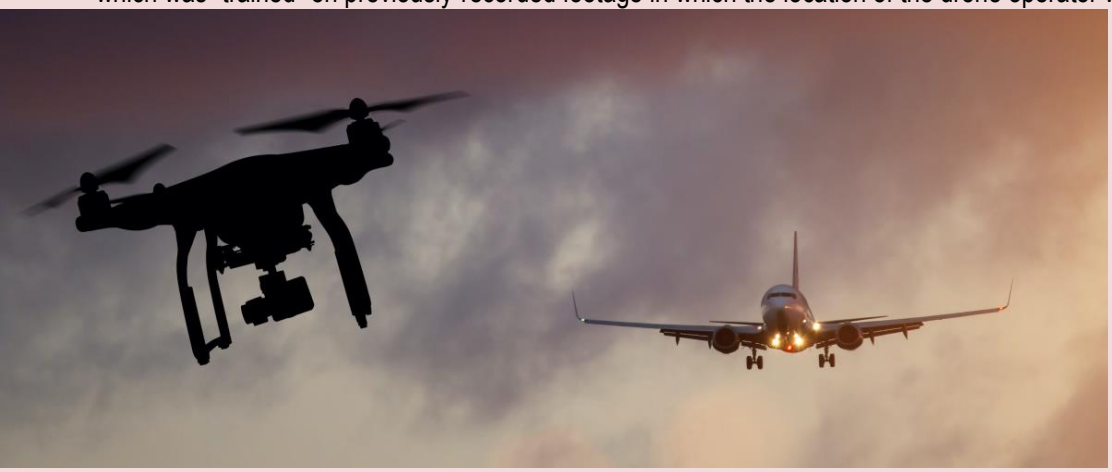
The **Dubai Sky Dome** will create an airspace infrastructure for unmanned aerial vehicles (UAVs) that could connect buildings through "runways and miniature airports across the city".
"Drone systems represent one of the most promising emerging technologies in the civil aviation and transport sector," said Sheikh Ahmed, also chief executive and founder of Emirates Airline.
An air traffic control system to manage the use of multiple UAVs would be named 'Dubai Shield'.
Officials said a series of measures would need to be in place to "address safety and security risks faced by the airspace due to drone activity".
Mohamed Abdullah Lengawi, head of the Dubai Sky Dome project team, said it "aims to tap into massive potential opportunities for drone systems".
"Global studies indicate that the drones transport systems market, which consists mainly of delivery of goods, transport of passengers and freight, surveying and imaging, holds considerable promise as an emerging sector."
Companies including Amazon, DHL and UPS have tested drones that can deliver packages in recent years as they look to cut down on traditional vehicle use.
Medical firms such as San Francisco-based Zipline has flown medicine delivery drones in Rwanda and Ghana for several years and in April asked US authorities for permission to operate domestic services as a result of the coronavirus pandemic.
The technology to collect a package and deliver it by air has existed for a number of years - but the lack of systems to manage multiple UAVs, especially over cities, has prevented the industry from picking up.
A surge in e-commerce and online shopping since the coronavirus outbreak has led to renewed interest in unmanned deliveries.
Dubai's government said a new law covers the use, circulation, registration, manufacturing, import, sale, and possession of drones. It also sets out rules governing the use of airspace, including around airports and other restricted and dangerous areas.

AI system could locate pilots of intrusive drones

Source: https://newatlas.com/drones/ai-system-drone-pilot-location/

July 08 – When an unauthorized drone is being flown in a restricted airspace, the authorities understandably want to locate its operator. A new AI-based system may allow them to do so, succeeding where other technologies fail.
First of all, it *is* possible to determine the approximate location of a drone's pilot, using multiple widely-spaced sensors to triangulate the originating point of its radio control signal. Those sensors do already have to be in place, however, plus they may not be able to pick up the radio signal if it's obstructed by other wireless signals (such as those from Wi-Fi or Bluetooth) that are present in the area.

Seeking a better alternative, researchers from Israel's Ben-Gurion University of the Negev have developed a system in which cameras optically track the drone's flight path in three-dimensional space. That video is analyzed utilizing a deep neural network, which was "trained" on previously-recorded footage in which the location of the drone operator was known.



Since pilots typically keep their drones within line of sight (or if nothing else, within radio range), analysis of flight patterns such as the aircraft's changing vertical and horizontal location, along with its tendency to move along a path that arcs around a central point that's off to one side, can be used to ascertain where the pilot is.

As a result, in computer simulations utilized so far, the system was able to locate a drone's operator with 78 percent accuracy. That figure should rise as the technology is developed further, which will include testing it on actual drones in the real world.

A paper on the research, which is being led by computer science student Eliyahu Mashhadi, was recently presented at the online Fourth International Symposium on Cyber Security, Cryptography and Machine Learning.

Drones of future – What the drones of future might do

By Debbie Fong

Source: https://www.digitalmarketnews.com/drones-of-future-what-the-drones-of-future-might-do/

July 11 – On Oct 11, 2019, the high precision surveillance along 50 km of the entire route traversed by Chinese President Xi Jinping's convoy in India by four drones created by Anna University made us wonder at the possibilities spurting from something like 3 cm resolution at an altitude of 100 m.

But on the other hand, the drone attack in Saudi Arabia in Sep 2019, which mopped away some five percent of the worldwide oil supply, and reverberated a difficult question. Will drones continue as the benefactors of humanity or they are going to become a weapon for mass destruction and terrorism in the future?

Three factors exist with drones. The requirement for good technology, huge investment, and fast adoption. All three levels can conspire in a scenario where the antithetical opportunities for prosperity and destruction might coexist susceptible to our **drones of the future.**

Introduction to Drones

A drone can be an unmanned aerial vehicle (UAV) that can be designed to fly autonomously by a dedicated remote unit. It has the power to perform certain operations in the air dictated by the computer program whereas flight mode controls are assisted by tracking devices such as GPS.

The origin of drones' attributes to the need realized by the government and military for intelligent warfare devices since the 1960s. During the Vietnam War, the US Army earnestly used drones for surveillance purposes accompanied by the later use by the Israeli military in 1982 throughout the Lebanon War.

However, with the advancement in technology, drones were later customized into different forms for a lot of commercial applications. To the great benefit of mankind have come assistance in accessing harrowing situations, finding missing people, creating 3D maps, surveying landscape, wildlife conservation, pipeline inspection, traffic monitoring, weather forecasting, and firefighting, agriculture, photography, video making, academic projects.

The cost of drones depends upon size and functionality. The mini version drones which fit in the palm could cost as less as $100 whereas the military-grade drones which easily fit into a backpack can cost tens of millions of dollars. One of the largest military drones is 47.6 feet long MQ-4 Global Hawk that is wider than a Boeing 737 airliner.

One of the most widely used drones in the market was the DJI Phantom 3 known for professional cinematography. The drone uses an advanced technology that is inherited by the latest drones such as the Mavic Air, Phantom 4 Pro, Inspire 2, Walkera Voyager 5, etc.

How Drones Work

A drone is made of light composite material to lessen weight and offer high altitude coverage. The motor operation is achieved by a tight high-torque multi-propeller system which makes this device highly independent and offers fail-safe features in a way that even though any motor inside this product stops working; it will continue flying because it gets support from propellers that are in a group. These propellers are operated by remote ground get a handle on systems (GSC) using radio waves, including Wi-Fi. Most of they contain removable batteries such that it can remain in the air for the long run. The flight time can increase with the use of powerful batteries in design.

The rates of rotation along with other parameters are relayed by the gyroscopes and sensors to computers that use algorithms to produce adjustments to the positioning of the drone. This keeps the drone balanced, hovering consistently and continue, backward, or vertically.

Computer algorithms assist the drone operator in controlling the drone's descent. While the drone pilot can control where and when the drone moves, it is the computer positioning algorithms that ensure a computerized stability level.

Navigational systems, such as for example GPS, are fixed in the nose of a drone which communicates the precise location of the drone. Optionally, an onboard altimeter can communicate the altitude vectors and keep the drone at a certain altitude, if commanded by the controller.

Evolving Technologies

The latest advanced drones of today are successfully outdoing previous versions in a variety of ways.

- **Collision avoidance systems** – Obstacle detection sensors are accustomed to scan the surroundings, while software algorithms produce the images in to 3D maps allowing the drone to sense and steer clear of obstacles. The most popular example is the latest DJI Mavic 2 Pro and Mavic 2 Zoom which have obstacle sensing on all 6 sides.
- **No Fly Zone Feature –** In order to boost flight safety and prevent accidents in restricted areas regulated and categorized by FAA (Federal Aviation Administration), the latest drones from DJI and other manufacturers include a "No Fly Zone" feature which provides a warning on entry into these zones.
- **FPV Live Video Transmission –** The FPV (First Person View) based technology consists of a video camera that is mounted on the drone and broadcasts the live video using the radio signal to the pilot on the ground. This gives real-time onboard experience to the ground pilot allowing the drone to fly greater and further than one can from looking at the aircraft from the ground.
- **Smart Interface –** Most of the drones today can be flown by a remote controller or from a smartphone app, which is often downloaded from Google Play or the Apple Store. Such a manufacturer-specific app allows for full control of the drone.

New Areas and Business Prospects

The drones useful for commercial applications are flourishing. This shall give different businesses a big scale chance to boost their revenue and help global economies grow in unimaginable ways.

- **Shipment services** – According to the recent reports, Google and Amazon are developing their own drones so that shipment can be delivered by air in a much shorter time. Facebook is about to develop giant drones to transport the signal to remote locations for internet access.
  In 2018, Boeing announced it had prototyped an unmanned electric VTOL cargo air vehicle (CAV) that can carry up to a 500-pound payload. As a part of WEF's "Medicine from the sky" initiative, Telangana Govt has adopted a framework to make use of drones for last-mile delivery of important medical supplies such as blood and medical samples in order to increase use of health care to communities across the state. Drones will also be in use by news reporters to gather information from inaccessible locations.
- **Collaboration with IoT** – An integral system of Drones with on-ground IoT sensor networks can help agricultural companies monitor land and crops, energy companies survey power lines and operational equipment and insurance companies monitor properties for claims and policies. In 2015, an experiment was conducted in Austin, Texas in which drones successfully spotted the IoT networks that have been present in residential and business areas of the city.
- **Measurement and estimation** – Drones can measure and record the height of crops, buildings, and mountains. This is completed by using remote sensing

technology called Lidar that illuminates the target with a laser and calculates distance and height by measuring what is reflected back.

- **Atmospheric studies** – Drones can fly to unsafe and inaccessible areas to measure air quality, search for the presence of specific micro-organisms or atmospheric elements, and even detect earthquakes.
- **Live recording** – Television sports networks use Drones in these times to capture sporting event footage that would otherwise be nearly impossible to find.

Given such sprawling grounds of new applications, below are a few recent business predictions on drone economy:

- PricewaterhouseCoopers has valued the drone-based companies service market at significantly more than $127 billion, with the top industries being infrastructure at $45.2 billion, agriculture at $32.5 billion, and transportation at $13.0 billion.
- The Association for Unmanned Vehicle Systems International (AUVSI) predicts the drone industry will create significantly more than 100,000 U.S. jobs and add $82 billion to the U.S. economy by 2025.
- Goldman Sachs predicts a $100 billion market for drones between 2016 and 2020, with the military creating the bulk of it with $70 billion spending. It is estimated that consumer drones will take a $17 billion share of that market, with commercial and civil government use making up $13 billion.
- The United Nations Institute for Disarmament Research quoted in its 2017 report that the global drone market might increase four times by 2022 from its 2015 value and surpass a net worth of $22 billion that features drones useful for both military and non-military purposes.

The above data clearly indicates that drones are here to stay, therefore is the threat they pose when they land in unsafe hands.

Threats due to Proliferation

No matter how impressive drones might appear, for the time being, they can become dangerous weapons in the future. The increasing popularity of drones and ease of usage is a reason behind a number of privacy, security, and safety concerns. Hence the importance of locating a way for them to safely coexist with manned aircraft is growing increasingly urgent.

- **Privacy threats** – These mischievous spies in the sky may take pictures of individuals inside their homes or other private locations. For example, a magazine like Splash News assembled about 200 photo sets of small episodes from the lives of the a-listers. Drones have also been within potentially unsafe areas such as for example urban locations and near airports.
- **Collisions** – The increasing drone traffic can lead to midair collisions and loss of drone control. The threat of drones flying too near commercial aircraft has prompted calls for regulation. For instance, in June 2019, Iran shot down a US military surveillance drone. The impact was the deterrence of major airline routes across the world in order to avoid attack in error on entering the country's airspace.
- **The possibility of civil attacks** – Drones are relatively cheaper when compared with conventional weapons and yet is capable of far more destructive results. It is this easy-to-procure, easy-to-operate, and foolproof technology that means it is an attractive weapon of mass destruction. In a 2017 study, the United Nations Institute for Disarmament Research (UNIDR) said that the same characteristics that produce drones appealing to militaries will make armed drones particularly prone to misuse. According to a written report in the Penn Political Review, many armed groups such as the Houthi rebels, Lebanese Hezbollah, Hamas, Libyan militias, Ukrainian separatists, Kurdish Peshmerga, Al Qaeda in Syria, Colombian FARC are known to possess and use drones. Besides, the recent case of the Saudi Aramco oil facility drone attack proves how the expensive anti-missile detector systems turn ineffective for drones because of their low altitudes and slow speed.
- **Hacking** – Drones in a few ways are like flying computers carrying an operating-system and pc software with programmable code that may be hacked. Drones have been developed to fly around seeking other drones, hacking to their wireless network, disconnecting the owner, and taking over the control.

Safety Regulations by the Government

Over time, regulators around the world have taken steps to prevent the possible misuse of drones.

- **China:** Any drone weighing more than 15 pounds or flying more than 400 feet requires a license from the Civil Aviation Administration of China (CAAC).
- **UK:** The Civil Aviation Authority (CAA) mandates the registration for drones weighing higher than a half-pound and prohibits flying above 500 feet.
- **U.S:** FAA specifically mandates certain regulations such as for example Remote Pilot Certificate for commercial drones and registration for increases to 100 mph, daylight-only operations with appropriate anti-collision lighting, and the prohibition of UAV operation over non-participants under a covered structure or inside a covered stationary vehicle.

- **Europe:** SESAR (Single European Sky ATM Research) is planning the roll-out of U-space foundation services, including e-registration, e-identification, and drone geofencing and full integration with manned aviation for the avoidance of interference and collision with commercial aircraft.

Conclusion

Drones are the spectacular presents of technology. Their expansion at large scale is inspiring almost all the countries to produce their drones for different applications. A drone of today is really a combination of all higher level technologies like microcontrollers, GPS, Wi-Fi, and sensor units. They need certainly to work in a synchronized fashion that is giving business to many organizations and start-ups. Besides, the profusion of drone kits, easy to learn programming languages, and course material on the internet makes it easy for newbies to build and code a drone.

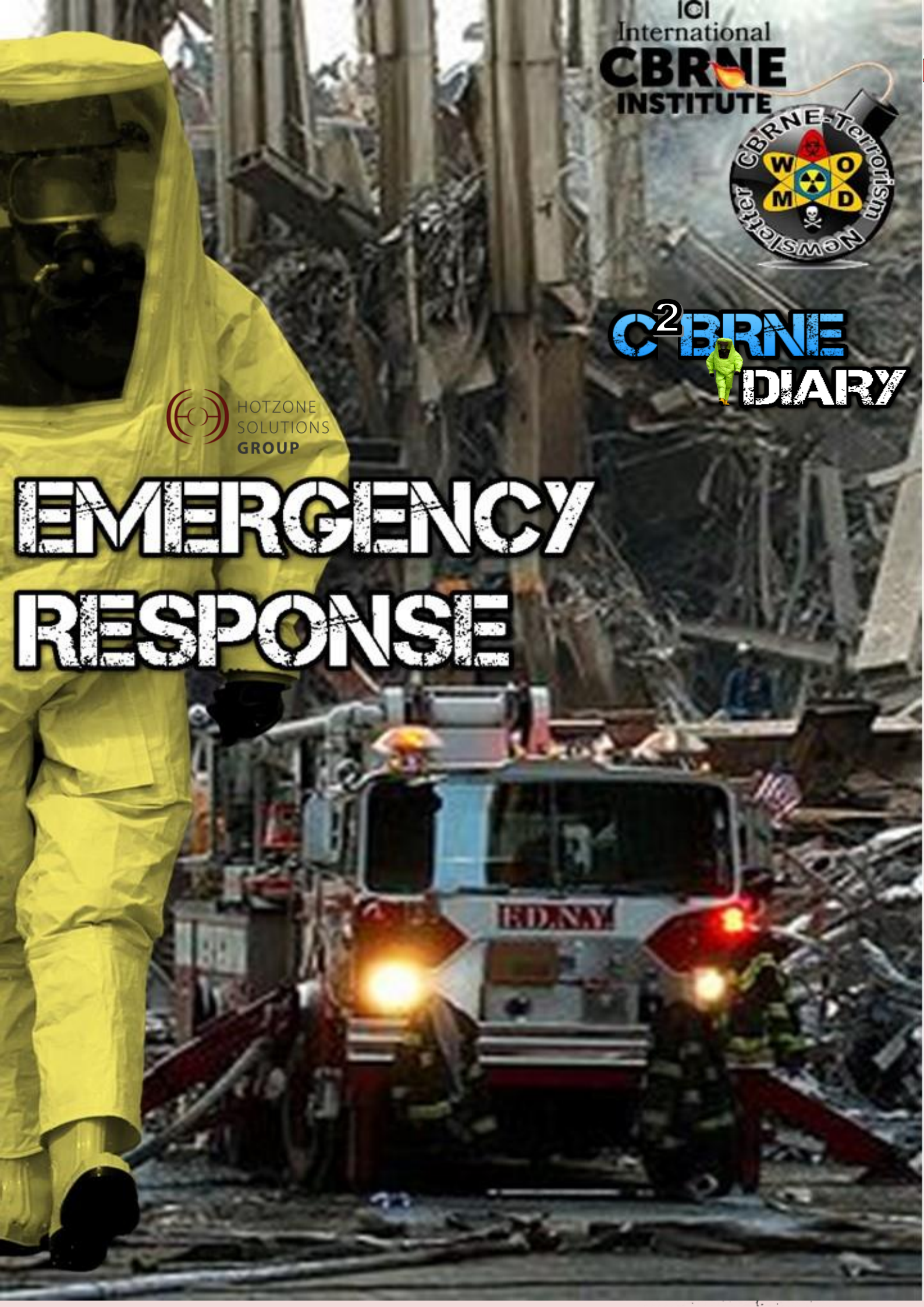
The role of the government is critical in such a scenario to enforce the development of low-cost detection systems. Such systems should be higher level enough to identify malevolent drones and to build strong regulations. Lest the trespassers will misuse this precious technology.

Bharti Jain *is an Electronics and Communication Engineer, graduated from Amity School of Engineering and Technology, GGSIPU, Delhi in 2011. She started her career as a Digital Signal Processing Firmware Engineer in Azcom Info solutions Pvt. Ltd, Delhi-NCR. She spent some time working on Physical Layer of LTE in MATLAB and C for over 2 yrs., delivering the TI emulators to French army for LTE-based communication. Presently, she's a PMP and ISO 9001:2015 Certified Project manager in RITES Ltd, Ministry of Railways. With an immense experience of management of Signaling and telecommunication projects for Indian Railways and energy sectors across the country. She has received training in a few technical courses such as 'Train Protection and Warning Systems, Automatic Fare Collection System in Metro train, Basic Signaling Courses, and Project Management Professional Course as a part of the global Project Management Institute, USA. She has also received various accolades from the company on her behalf innovative efforts and technical publications.*

Drones: A Report on the Use of Drones by Public Safety Agencies--and a Wake-Up Call about the Threat of Malicious Drone Attacks

Source: https://www.hsdl.org/?view&did=838632

This report is about two opposite but related issues: (1) the use of drones by police agencies to protect public safety and (2) the use of drones by malicious actors to commit various crimes such as acts of terrorism. [...] This report should be seen as two separate reports. The bulk of the document, chapters 1 and 2, provides guidance to police and sheriffs' departments about how to identify the ways in which drones could facilitate their work and how to create a drone program to accomplish those goals. The remainder of the document, chapter 3, is about the malicious use of drones.


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

Opinion: There are no natural disasters

By Sebastian Miscenich

Source: https://www.statepress.com/article/2020/07/spopinion-there-are-no-natural-disasters

July 02 – Even discounting indisputably human catastrophes, 2020 has been relentless. This year has given us wildfires from California to Australia, a global pandemic and the earliest third-named tropical storm on record. Arizona hasn't been spared either, with a brush fire forcing evacuations and keeping part of a state highway closed.

The toll of these disasters is immense. The new coronavirus has infected over 10 million people, killing over 500,000 worldwide. Tropical Storm Cristobal caused immense damage to Mexico and the U.S. The Arizona brush fires have burned over 150,000 acres. But, while disease, storms and fire are all considered natural phenomena, it takes human mismanagement to create a disaster.

Take Arizona's response to the COVID-19 pandemic, for example. In January, Arizona was one of the first states to have a COVID-19 case. While the state government declared a public health emergency on March 12, Gov. Doug Ducey didn't limit public gatherings, as other states had done, until March 19. A stay-at-home order wasn't issued until the end of March, at which point victims had begun dying.

And now, after a hasty reopening, Arizona has a record number of hospitalizations and cases of the virus. While the disease is natural, the disastrous situation is completely unnatural.

To prove it, I'll compare our predicament to how things went down in Wuhan, the Chinese city where COVID-19 was first discovered. On January 23, the central government of China put Wuhan under quarantine. Masks were made mandatory in public, and public health officials still are taking the temperature of travelers leaving the city. Fully functional hospitals were rapidly constructed to accommodate the surge of cases. By April, the lockdown was eased, with citywide testing conducted as late as May.

Wuhan reported 0 new cases by June. Keeping masks on as a precaution, life in the city has slowly returned to normal.

China wasn't alone in addressing the hazard of COVID-19 head-on. Vietnam was accused of overreaction in its aggressive response to the virus, but through early efforts was able to keep infections low, without a single death reported.

Cuba sent doctors to Italy when the European country was at the height of its infection rate — an offer that the U.S. refused 15 years ago when New Orleans was recovering from the unnatural disaster caused by the aftermath of Hurricane Katrina due to the U.S.'s ongoing economic blockade of Cuba.

Madison West graduated from ASU in 2019 with an M.S. in Justice Studies and an M.A. in Sustainability. She says that the "natural" in the term "natural disasters" takes responsibility away from human actions.

If disasters were unavoidable acts of God, then Wuhan should be far more greatly afflicted by COVID-19 than Arizona. Governments of action in China, Vietnam and Cuba fought for the people, declared war on the virus and emerged victorious.

Arizona's impatient and short-sighted rulers reflected the American government's way of confronting crisis: unable to sacrifice immediate economic interests, no matter the cost.

"When we're looking at 'natural disasters' like climate change, the brush fires or the coronavirus, they're natural in the sense that they might have happened, but they wouldn't have been this bad." West said. "The 'natural' part of it takes away responsibility from human actions, specifically around capitalism."

West says that capitalist authorities are already forced to acknowledge some degree of personal responsibility for disasters, but that this responsibility is highly individualized when the causes are systemic.

"If you have a forest, and you dry it out, and companies dump flammable fluid all over it, and some kid accidentally drops a lit cigarette and lights the whole forest on fire, then is it really that kids fault?" West said. "Companies create these situations to begin with."

Stemming from the White House, there have been calls in the United States to blame China for the COVID-19 pandemic, despite its efforts to fight the virus and its international solidarity with countries affected by the disease. West says that this push of blame is an enlarged version of the move to assign individual responsibility for systemic, human causes.

"We can't prove where (the new coronavirus) came from, but we're just going to blame China because 'China is evil'," West said. "Better approaches to justice look at what harm was caused; how can we address the harm caused and how can we make sure that it doesn't happen again."

West also said that we should rethink negative assumptions of China's sustainability.

"China is kind of a boogeyman in sustainability circles," West said, "but they're the only country that hit their Paris Climate Accord commitment."

West said that to prevent future natural hazards from developing into disasters, the principles of sustainability should be adopted.

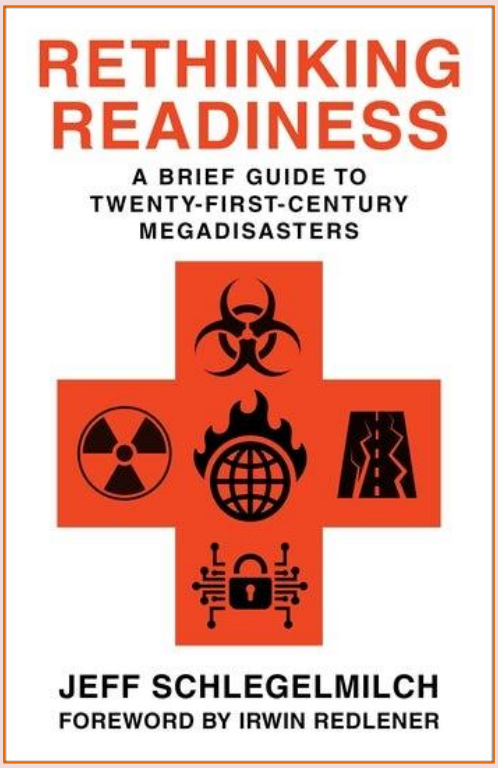
"You can't take more than you need, you can't take more without being able to replenish natural resources. That's the whole idea behind a balanced, planned economy," West said.

Instead of resigning to the perceived inevitability of disaster, we should fight for a system that can confront crises and serve the people first.
China's COVID-19 response has been called the country's Sputnik moment, harkening to the sublime accomplishment in space travel by the Soviet Union that left the capitalist West in the dust.
This achievement is further proof that a rationally planned economy and a strong, centralized state can handle crises and confront disaster.

Coming Soon? A Brief Guide to Twenty-First-Century Megadisasters

By Kevin Krajick
Source: http://www.homelandsecuritynewswire.com/dr20200720-coming-soon-a-brief-guide-to-twentyfirstcentury-megadisasters

July 20 – When it comes to calamities, Jeffrey Schlegelmilch thinks big. In his upcoming book, *Rethinking Readiness: A Brief Guide to Twenty-First-Century Megadisasters*, he explores menaces that potentially could change not just lives or communities, but entire societies. He groups these into five categories: climate change; cyber threats; nuclear war; failures of critical infrastructure such as electric grids; and biological perils including pandemics.



Schlegelmilch, director of Columbia University's National Center for Disaster Preparedness, has devoted his career to thinking about catastrophe. Trained in business and public health, he worked previously, among other things, as an epidemiologist and emergency planner. Schlegelmilch wrote the book before the coronavirus emerged. Columbia University Earth Institute's *State of the Planet* spoke with him in light of what has since happened.

Kevin Krajick: Will the disasters of the 21st century be different from those of the past?

***Jeffrey Schlegelmilch*:** The disasters we are seeing are already different than in the past. We can see this through more and more billion-dollar weather events, more spending on disaster response and recovery, more lives disrupted. This is because human activity is contributing to both the underlying threats, and our vulnerability to them. Climate change is one example. We are pumping pollutants into the atmosphere at unprecedented rates, leading to more extreme weather events. At the same time, we are building in flood zones and other hazard-prone areas. This dynamic is not unique to climate change. Other disasters, like pandemics, have components where societal development is increasing both the threat and our vulnerability.

Krajick: What distinguishes a megadisaster from a plain old catastrophe?

Schlegelmilch: This is one of those terms with fuzzy edges that is used a lot in disaster management. In broad strokes, I think of megadisasters as those that are so large, they disrupt the very systems that are designed to respond to disasters. The book amplifies this concept a little further, defining them as disasters with society-altering potential. This can be along the lines of the Black Death in Europe, the Great Potato Famine in Ireland. These disasters do more than impact society for a while; they permanently alter the course of history.

Krajick: When all is said and done, do you think the coronavirus will qualify as a megadisaster?

***Schlegelmilch*:** As COVID-19 was starting to circle the globe, I was reviewing the proofs for the book. It was eerie reading the section on pandemics, because the research and the quotes from experts I interviewed could easily have been part of a postmortem for why COVID-19 got so out of control so quickly. But while COVID-19 will certainly have a major impact on our society and the global community, in some ways it could be much worse. The Black Death in the 14th century and the 1918 influenza killed greater numbers. This is a horrible pandemic to be sure, and it will leave scars on our society for generations. But we still have it within our power to mitigate the impacts, and build more resilient systems for future pandemics. The scale of disaster that COVID-19 becomes in the history books is still being determined by the choices we make today. So, I am reluctant to put it in the same category as these others. We still time to reduce the impacts, if we are holistic in our perspective, and collaborative in our approaches.

Krajick: Many people would probably argue that climate change is the overarching megadisaster of coming decades, casting its shadow on all others. Would you agree?

***Schlegelmilch*:** I'll answer this in a roundabout way. Scenario-based planning is very popular among the public and elected officials—that is, the kind of planning where you game out a scenario, like an earthquake, a hurricane, or Godzilla coming out of the river to destroy the town. This helps create a story that can be built out at different angles with different requirements. However, most emergency planners prefer to start instead with a functional approach: to establish the building blocks that you would use in any scenario, such as communications, logistics or public information. Then you start to run scenarios to test these overarching issues under different stressors.

My book takes the functional approach in reverse: It lays out five broad megadisaster scenarios in order to frame the overarching issues. I sincerely believe that potential megadisasters are all products of an unsustainable development trajectory, where growth is prioritized over resilience, and where we demand simplicity in an increasingly complex and interdependent world. You won't solve any of these scenarios by focusing on just one. And none of these scenarios occur in isolation from the others. We need to foster capabilities that apply to multiple scenarios, and that can respond to the uncertainty ahead of us.

Krajick: Nuclear war has been out of vogue for a while as a big worry. Why bring it up now?

***Schlegelmilch*:** It is precisely because it is out of vogue that it is so important to talk about. There is this belief that the threat of nuclear annihilation went away with the collapse of the Soviet Union. But the threat just changed form. In fact, it created new rivalries among China, Russia and the U.S. The economic turmoil of Russia after the Cold War, and the emergence of additional nuclear powers, including rogue nations like North Korea, has increased the potential for smaller-scale nuclear conflict, and nuclear terrorism. The use of nuclear weapons may be more likely than ever before, but it is also much more survivable than in the height of the Cold War. Rather than the vast global killing arsenals of past superpowers, the threats today are more nuanced. It is not a lost cause to think about life after a nuclear conflict, with the right kind of preparedness.

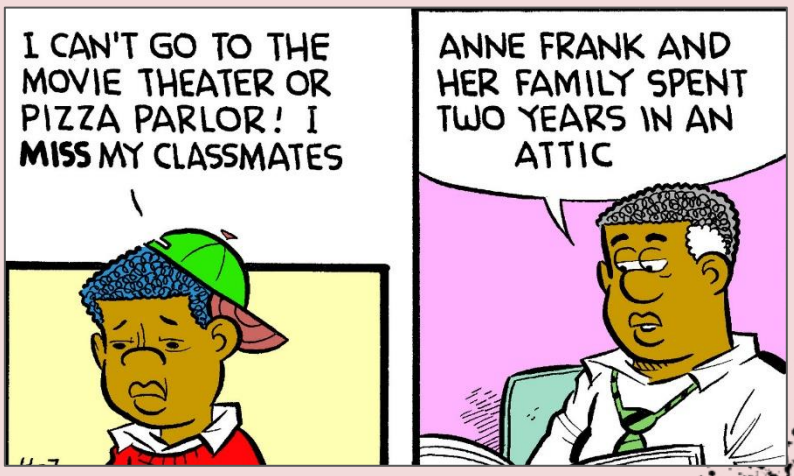
Krajick: One disaster can magnify the effects of others, if they happen around the same time or same place. Can this kind of synergy be predicted, or are we dealing with wild cards?

***Schlegelmilch*:** The risk can be predicted, and there are patterns to be sure. But there is also a certain degree of randomness. The COVID-19 pandemic is illustrative. A pandemic was predicted by experts—just not this pandemic at this moment. Now, we are also staring down the barrel of hurricane season, which is forecast to be more active than normal, plus fire seasons in the western U.S. All in the context of many millions of people working from home, relying on our cyber infrastructure. I can't tell you what will happen when, but there is clearly an outsize risk of COVID-19 transmission in shelters from storms and fires. And our cyber-dependence and vulnerability is greater than ever. However, we can still be ready. For instance, emergency managers around the county are reviewing and updating their sheltering plans, and companies are upgrading security for meeting software. Establishing the boundaries of uncertainty, then creating options for managing that uncertainty is vital.

Krajick: Do you have a favorite disaster that you fantasize about, and how you and your loved ones would survive it?

***Schlegelmilch*:** I don't have a particular disaster that I focus on, but am fortunate to be surrounded by family and friends, as well as colleagues who are creative and compassionate. Some people tell me my job must be depressing, because I have to think up so many horrible scenarios. But it does not take an overactive imagination to predict megadisasters. In fact, the scenarios I imagine are really just reflections on history, and on warning signs from smaller disasters. Imagination is an important asset for this work, to be sure. But an overactive imagination will pull you away from the tell-tale signs we already have before us.

Kevin Krajick *is the Earth Institute's senior editor for science news.*




HOTZONE
SOLUTIONS
GROUP
✓ Consultation
✓ CBRN Training
✓ CBRN Products
www.hotzonesolutions.org