# CBRNE DIARY

Dedicated to Global First Responders

October 2019

www.cbrne-terrorism-newsletter.com

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

# DIRTY R-NEWS

# Predicting the civilian reaction to a nuclear WMD event

**By Steven Pike**

Source: https://www.argonelectronics.com/blog/predicting-the-civilian-reaction-to-a-nuclear-wmd-event

Sep 22 – Being able to predict how civilian individuals will react within the first minutes, hours and days of a major nuclear attack could well provide a life-saving resource for government agencies and emergency first responders.

And it this specific goal that has served as the impetus for an innovative Homeland Defence and Security Information Analysis Centre (HDIAC) research project titled 'A Framework for Modelling Society Following a Nuclear WMD Event'.

In a recent HDIAC webinar for CBRN professionals, Dr William Kennedy from George Mason University provided an overview of the project's methodology, its challenges and its achievements over the past three years.

As Dr Kennedy explained, the project has sought to model the effects of a "no-notice" detonation of a small nuclear weapon of mass destruction (WMD) at 10am on a weekday morning in New York City.

In particular the aim has been to characterise the initial reactive behaviours of the individuals - both of those fleeing the area, and of those travelling towards ground zero (ie first responders and other rescue personnel making their way to the scene).

As Kennedy outlined: "To collect information, and make sense of it, we need to build a model of the individuals themselves...quantifying how many people do what...and taking into account the variations in their reactions."

But as he also stressed, modelling people is no easy task - or to quote one of the 20th century's leading particle physicists, Dr Murray Gell-Mann: "Imagine how much harder physics would be if electrons could think?"

## Synthesising a mega-city

Over the past three years, Dr Kennedy and his team have been building and refining a 1:1 agent-based model (ABM) of a civilian population residing within a mega-city - in this case recreating the geography and inhabitants of New York City and the surrounding region, covering an area of 160 miles by 145 miles.

The research team began by 'capturing' and synthesising the physical environment, its topography and infrastructure - first connecting the roads in order to create a 'skeleton' - then adding waterways, subways etc.

Using US 2010 census information, they were then able to create the individual agents (individuals), to establish the social ecology (the relationships and networks) of those agents, and to populate them within physical living spaces such as homes, workplaces, schools etc.

The project has also modelled the routine behaviours of each individual in order to establish where they would typically be at any given point throughout the day (whether commuting to or from work, at home, at work, at school etc.)

To date, the project has succeeded in demonstrating, benchmarking and verifying a synthesised population of 23 million agents, the commuting patterns of a population of 260,000 and the initial agent reactions of a population of 23,000.

## Future research goals

The initial three-year project has received funding for a further two years - with future efforts to be focused on:

- Refining the fidelity of the agent modelling (including additional health effects, communication and shift schedules)
- Further exploring the characterisation of agent reactions

- Extending the infrastructure modelling to account for damaged road networks and communications and additional modes of transportation
- Adding parameter-driven Electromagnetic Pulse (EMP) effects (ie the damage or destruction caused to electronic equipment, buildings and structures)

**Dr William Kennedy Ph. D**

Dr Kennedy has been an associate professor at George Mason University since 2008 where he specialises in computational cognitive modelling and computational social science.

Prior to this appointment he completed a 30-year career with the US Navy, as well as ten years with the federal government Nuclear Regulatory Commission and fifteen years service with the Department of Energy.

In 2003 Kennedy was awarded a Ph. D in Information Technology - specialising in Artificial Intelligence.

It was while further continuing his studies at the Naval Research Laboratory, that his interests shifted to cognitive science - and in particular the modelling of human behaviour in agent-based models of groups and societies.

Alternative Energy
Medical
Weapons of Mass Destruction
Biometrics
CBRN Defense
Critical Infrastructure Protection
Homeland Defense and Security
Cultural Studies
HDIAC
Homeland Defense & Security Information Analysis Center

**About HDIAC**

The Homeland Defence and Security Information Analysis Centre (HDIAC) is one of three Department of Defence (DoD) Information Analysis Centres in the US.

It is responsible for the collection, analysis, synthesis and distribution of relevant technical and scientific information across eight focus areas - including CBRN Defence, Weapons of Mass Destruction, Critical Infrastructure Protection and Homeland Defence and Security.

The HDIAC describes its mission as follows: "To be the go-to science and technology (S&T) and research, development, testing, and evaluation (RDT&E) leader within the homeland defence and security (HDS) community."

The organisation has also developed a Subject Matter Expert (SME) network of qualified individuals whose experience, education, expertise and professional practice falls within the HDIAC's core focus areas.

## ISIS Had 'Perfect' Ingredient to Build Huge Dirty Bomb in Mosul

**By Mordechai Sones**

Source: http://www.israelnationalnews.com/News/News.aspx/232922

July 2017 – ISIS terrorists nearly stumbled on the main ingredient for a "dirty bomb" when they overran Mosul in 2014, reports the Mail Online.

Two caches of cobalt, a metallic substance with lethally high levels of radiation, were found inside two radiotherapy machines at the University of Mosul.

Iraqi forces found the cobalt-60 machines had not been touched when they liberated the city this month. A Health Ministry official said of ISIS: "They are not that smart."

Western intelligence agencies were supposedly aware of the cobalt and monitored for three

years for any signs ISIS might try to use it. Cobalt is used to kill cancer cells when it is contained within the heavy shielding of a radiotherapy machine.

However, in terrorist hands, cobalt could have been used to create a "dirty bomb."

Fears were intensified in late 2014 when ISIS claimed it had obtained radioactive material and then again last year when they seized laboratories at the same Mosul college campus with the apparent goal of building new weapons.

A November 2015 draft report found that the radioactive cores of the material, when new, "contained about nine grams of pure cobalt-60 with a potency of more than 10,000 curies — a standard measure of radioactivity." A person standing three feet from the unshielded core would receive a fatal dose of radiation in less than three minutes, the Washington Post reported.

US officials have requested their current location not be disclosed.

It is unclear why ISIS failed to take advantage of the cobalt stored at the Mosul college campus. Nuclear experts suggest they may have been concerned about how to remove the machines' thick shielding without exposing themselves to deadly radiation.

A "dirty bomb" made from cobalt could have resulted in "panic and an expensive disruptive cleanup", David Albright, a nuclear weapons expert and former UN weapons inspector told the Washington Post.

He added: "There would likely not have been that many deaths, but the panic could have been profound, leading to the emptying of parts of the city as residents fled, fearful of the effects of radiation."

ISIS insurgents seized control of Mosul in the summer of 2014.

The east side of the city was recaptured by Iraqi fighters in January this year, though the west side of the city took far longer.

An aerial bombardment on the west, which includes the Old City, started in February and lasted until early July.

ISIS fighters had turned the city into a fortress, holding tens of thousands of civilians as human shields.

Iraqi forces often turned to artillery and US-led coalition airstrikes. The Old City was the last battlefield.

## IAEA: Iran Expands Enrichment in New Breach of Nuclear Deal

Source: http://www.homelandsecuritynewswire.com/dr20190926-iaea-iran-expands-enrichment-in-new-breach-of-nuclear-deal

Sep 26 – Iran has started using advanced centrifuges to enrich uranium, the UN’s nuclear watchdog says, in a further breach of its 2015 nuclear deal with world powers.

Advanced centrifuges “were accumulating, or had been prepared to accumulate, enriched uranium,” the Vienna-based International Atomic Energy Agency (IAEA) said in the report to member states cited by Western news agencies on September 26.

In addition, IAEA inspectors have verified that Iran has pushed ahead with preparations to install more advanced centrifuges that can refine uranium more efficiently.

Under the 2015 nuclear agreement that puts curbs on Iran’s nuclear program in exchange for an easing of sanctions, Tehran is only meant to enrich uranium using less efficient centrifuges.

The accord has been in jeopardy since May last year when the United States withdrew from it and reimposed sanctions on Iran, targeting its oil exports and crippling its economy.

In response, Tehran has reduced some of its commitments under the nuclear accord over the past few months.

The deal’s European signatories — Britain, China, France — have tried to salvage the accord, but Iran has repeatedly accused them of not doing enough to protect it from the effects of U.S. sanctions.

U.S. President Donald Trump wants to force Iran to renegotiate the 2015 nuclear accord, arguing that the terms were not tough enough to prevent the country from developing nuclear weapons, and agree curbs to its ballistic-missile program.

Iran has refused, insisting its nuclear program was strictly for civilian energy purposes and that its missile capabilities were not negotiable.

Speaking on September 26 on the sidelines of the UN General Assembly in New York, Iranian President Hassan Rohani said Iran’s steps to scale back its nuclear commitments are reversible if the European parties to the nuclear agreement carried out their promises to salvage the pact.

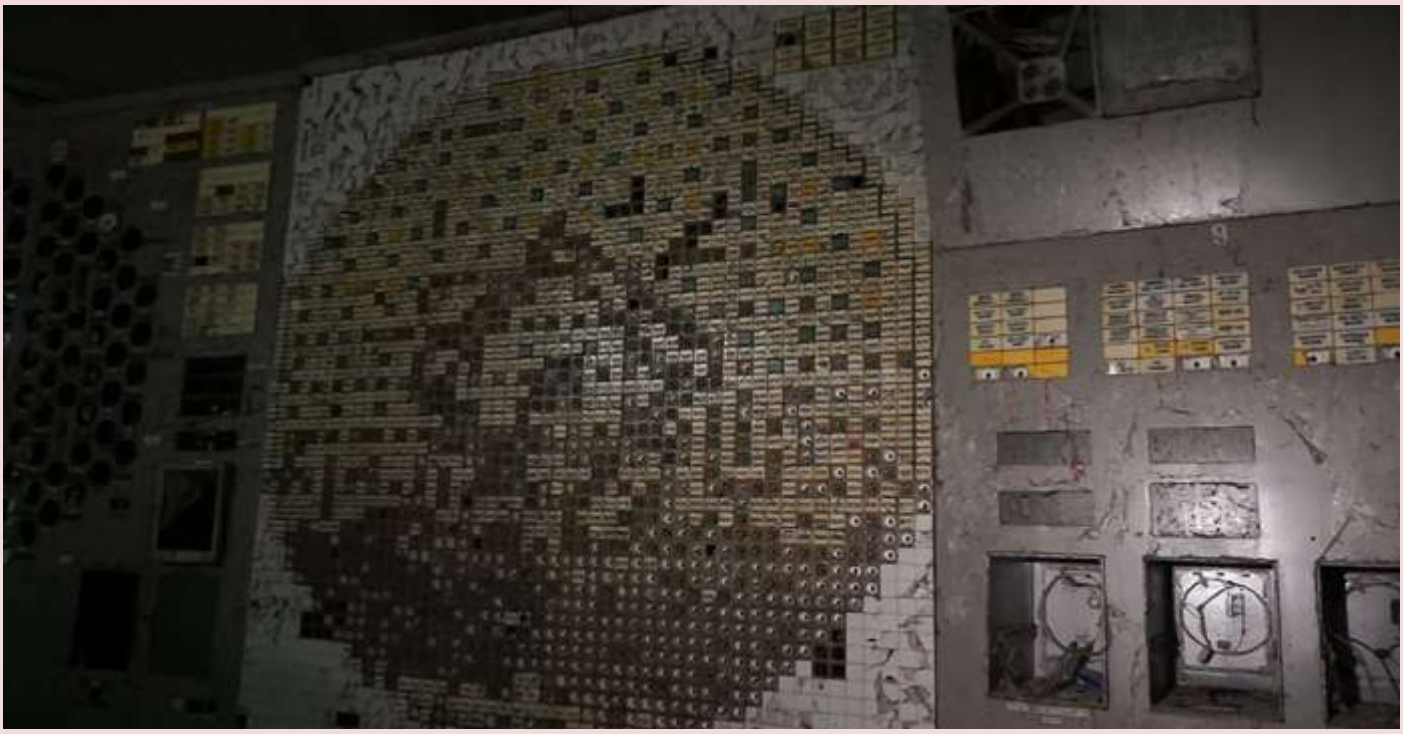
He also urged Washington to "cease this policy of maximum pressure" in favor of "dialogue, logic, and reason," a day after the U.S. administration stepped up pressure on Tehran, authorizing the State Department to bar senior Iranian officials and family members from entering the United States as immigrants or nonimmigrants.

Rohani said the move had no impact as "Iranian officials have no desire to travel to America."

"We only come here for the UN events," he added.

## Journalists peek inside the Chernobyl's infamous reactor no. 4

Source (video): https://www.youtube.com/watch?time_continue=4&v=PJHKfMo-MiA



A group of 15 journalists gained access to Chernobyl Nuclear Power Plant's fourth reactor control room on Wednesday (Sep 19, 2019) as part a presentation of a new guide book on the Chernobyl Exclusion Zone.

## India-Pakistan Nuclear War Could Kill Millions, Lead to Global Starvation

Source: http://www.homelandsecuritynewswire.com/dr20191002-indiapakistan-nuclear-war-could-kill-millions-lead-to-global-starvation

Oct 02 – **A nuclear war between India and Pakistan could, over the span of less than a week, kill 50-125 million people—more than the death toll during all six years of World War II**, according to new research.

A new study conducted by researchers from the University of Colorado Boulder and Rutgers University examines how such a hypothetical future conflict would have consequences that could ripple across the globe. Today, India and Pakistan each have about 150 nuclear warheads at their disposal, and that number is expected to climb to more than 200 by 2025.

The picture is grim. That level of warfare wouldn't just kill millions of people locally, said CU Boulder's Brian Toon, who led the research published today in the journal *Science Advances*. It might also plunge the entire planet into a severe cold spell, possibly with temperatures not seen since the last Ice Age.

His team's findings come as tensions are again simmering between India and Pakistan. In August, India made a change to its constitution that stripped rights from people living in the long-contested region of Kashmir. Soon after, the nation sent troops to Kashmir, moves that Pakistan criticized sharply.

"An India-Pakistan war could double the normal death rate in the world," said Toon, a professor in the Laboratory of Atmospheric and Space Physics (LASP). "This is a war that would have no precedent in human experience."

**Death Toll**

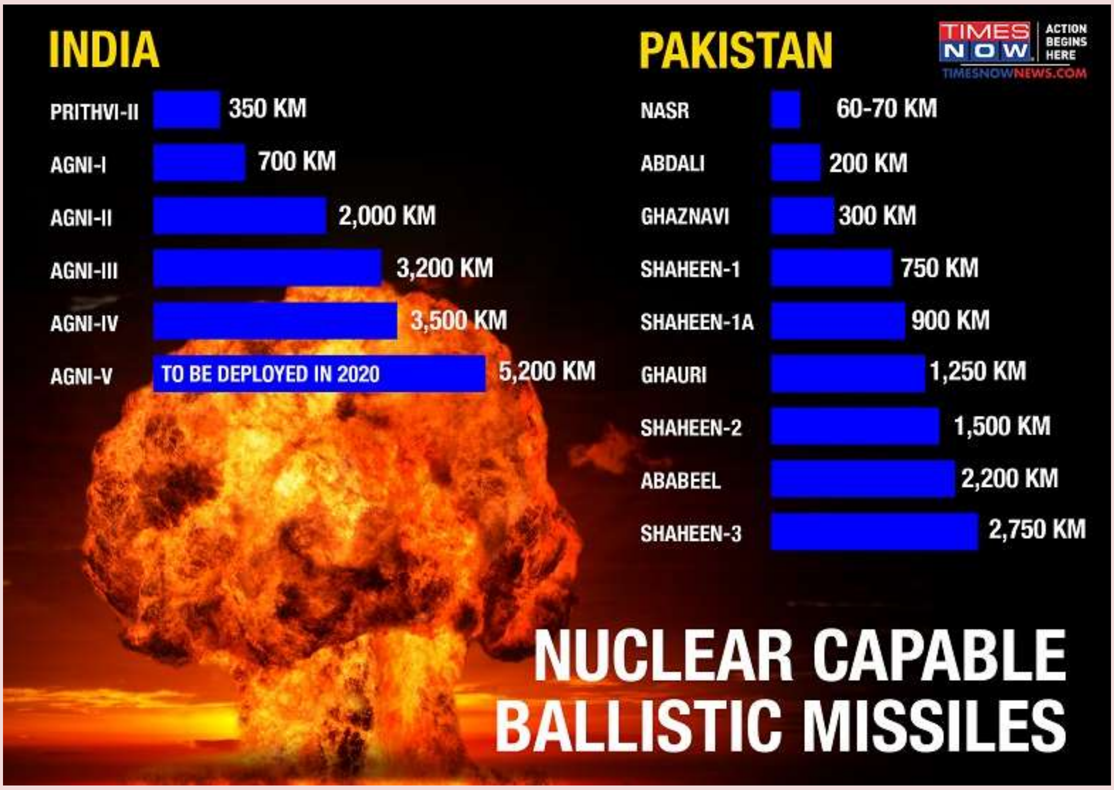
Colorado says that it's a subject that Toon, also of the Department of Atmospheric and Oceanic Sciences, has had on his mind for decades.

He came of age during the height of the Cold War when schoolchildren still practiced ducking-and-covering under their desks. As a young atmospheric scientist in the early 1980s, he was part of a group of researchers who first coined the term "nuclear winter"—a period of extreme cold that would likely follow a large-scale nuclear barrage between the U.S. and Russia.

And despite the collapse of the Soviet Union, Toon believes that such weapons are still very much a threat—one that's underscored by current hostilities between India and Pakistan.

"They're rapidly building up their arsenals," Toon said. "They have huge populations, so lots of people are threatened by these arsenals, and then there's the unresolved conflict over Kashmir."

In his latest study, he and his colleagues wanted to find out just how bad such a conflict could get. To do that, the team drew on a wide range of evidence, from computer simulations of Earth's atmosphere to accounts of the bombings of Hiroshima and Nagasaki in Japan in 1945.



Based on their analysis, the devastation would come in several stages. In the first week of the conflict, the group reports that India and Pakistan combined could successfully detonate about 250 nuclear warheads over each other's cities.

There's no way to know how powerful these weapons would be—neither nation has conducted nuclear tests in decades—but the researchers estimated that each one could kill as many as 700,000 people.

**Food Shortages**

Most of those people wouldn't die from the blasts themselves, however, but from the out-of-control fires that would follow.

"If you look at Hiroshima after the bomb fell, you can see a huge field of rubble about a mile wide," Toon said. "It wasn't the result of the bomb. It was the result of the fire."

For the rest of the globe, the fires would just be the beginning.

The researchers calculated that an India-Pakistan war could inject as much as 80 billion pounds of thick, black smoke into Earth's atmosphere. That smoke would block sunlight from reaching the ground, driving temperatures around the world down by an average of between 3.5-9 degrees Fahrenheit for several years. Worldwide food shortages would likely come soon after.

"Our experiment, conducted with a state-of-the-art Earth system model, reveals large-scale reductions in the productivity of plants on land and of algae in the ocean, with dangerous consequences for organisms higher on the food chain, including humans," said study coauthor Nicole Lovenduski, an associate professor of atmospheric and oceanic sciences and a fellow of the Institute of Arctic and Alpine Research (INSTAAR).

Toon recognizes that the scope of such a war may be hard for people to wrap their heads around. But he hopes that the study will show people around the world that the end of the Cold War didn't eliminate the risk of global nuclear war.

"Hopefully, Pakistan and India will take note of this paper," he said. "But mostly, I'm concerned that Americans aren't informed about the consequences of nuclear war."

PAKISTAN
INDIA
THE GOVERNMENT CAN'T AFFORD TO GIVE YOU AN EDUCATION BECAUSE WE'VE GOT TO TEACH OUR ENEMIES A LESSON.
Nicholson

# How to Dismantle a Nuclear Bomb: Team Successfully Tests New Method for Verification of Weapons Reduction

**By Peter Dizikes**

Source: http://www.homelandsecuritynewswire.com/dr20191002-how-to-dismantle-a-nuclear-bomb-team-successfully-tests-new-method-for-verification-of-weapons-reduction

Oct 02 – How do weapons inspectors verify that a nuclear bomb has been dismantled? An unsettling answer is: They don't, for the most part. When countries sign arms reduction pacts, they do not typically grant inspectors complete access to their nuclear technologies, for fear of giving away military secrets.

Instead, past U.S.-Russia arms reduction treaties have called for the destruction of the delivery systems for nuclear warheads, such as missiles and planes, but not the warheads themselves. To comply with the START treaty, for example, the U.S. cut the wings off B-52 bombers and left them in the Arizona desert, where Russia could visually confirm the airplanes' dismemberment.

It's a logical approach but not a perfect one. Stored nuclear warheads might not be deliverable in a war, but they could still be stolen, sold, or accidentally detonated, with disastrous consequences for human society.

"There's a real need to preempt these kinds of dangerous scenarios and go after these stockpiles," says Areg Danagoulian, an MIT nuclear scientist. "And that really means a verified dismantlement of the weapons themselves."

**Now MIT researchers led by Danagoulian have successfully tested a new high-tech method that could help inspectors verify the destruction of nuclear weapons. The method uses neutron beams to establish certain facts about the warheads in question — and, crucially, uses an isotopic filter that physically encrypts the information in the measured data.**

A paper detailing the experiments, "A physically cryptographic warhead verification system using neutron induced nuclear resonances," is being published today in *Nature Communications*. The authors are Danagoulian, who is an assistant professor of nuclear science and engineering at MIT, and graduate student Ezra Engel. Danagoulian is the corresponding author.

### High-Stakes Testing

The experiment builds on previous theoretical work, by Danagoulian and other members of his research group, who last year published two papers detailing computer simulations of the system. The testing took place at the Gaerttner Linear Accelerator (LINAC) Facility on the campus of Rensselaer Polytechnic Institute, using a 15-meter long section of the facility's neutron-beam line.

Nuclear warheads have a couple of characteristics that are central to the experiment. They tend to use particular isotopes of plutonium — varieties of the element that have different numbers of neutrons. And nuclear warheads have a distinctive spatial arrangement of materials.

The experiments consisted of sending a horizontal neutron beam first through a proxy of the warhead, then through a an encrypting filter scrambling the information. The beam's signal was then sent to a lithium glass detector, where a signature of the data, representing some of its key properties, was recorded. The MIT tests were performed using molybdenum and tungsten, two metals that share significant properties with plutonium and served as viable proxies for it.

The test works, first of all, because the neutron beam can identify the isotope in question.

"At the low energy range, the neutrons' interactions are extremely isotope-specific," Danagoulian says. "So you do a measurement where you have an isotopic tag, a signal which itself embeds information about the isotopes and the geometry. But you do an additional step which physically encrypts it."

That physical encryption of the neutron beam information alters some of the exact details, but still allows scientists to record a distinct signature of the object and then use it to perform object-to-object comparisons. This alteration means a country can submit to the test without divulging all the details about how its weapons are engineered.

"This encrypting filter basically covers up the intrinsic properties of the actual classified object itself," Danagoulian explains.

It would also be possible just to send the neutron beam through the warhead, record that information, and then encrypt it on a computer system. But the process of physical encryption is more secure, Danagoulian notes: "You could, in principle, do it with computers, but computers are unreliable. They can be hacked, while the laws of physics are immutable."

The MIT tests also included checks to make sure that inspectors could not reverse-engineer the process and thus deduce the weapons information countries want to keep secret.

To conduct a weapons inspection, then, a host country would present a warhead to weapons inspectors, who could run the neutron-beam test on the materials. If it passes muster, they could run the test on every other warhead intended for destruction as well, and make sure that the data signatures from those additional bombs match the signature of the original warhead.

For this reason, a country could not, say, present one real nuclear warhead to be dismantled, but bamboozle inspectors with a series of identical-looking fake weapons. And while many additional protocols would have to be arranged to make the whole process function reliably, the new method plausibly balances both disclosure and secrecy for the parties involved.

### The Human Element

Danagoulian believes putting the new method through the testing stage has been a significant step forward for his research team.

"Simulations capture the physics, but they don't capture system instabilities," Danagoulian says. "Experiments capture the whole world."

In the future, he would like to build a smaller-scale version of the testing apparatus, one that would be just 5 meters long and could be mobile, for use at all weapons sites.

"The purpose of our work is to create these concepts, validate them, prove that they work through simulations and experiments, and then have the National Laboratories to use them in their set of verification techniques," Danagoulian says, referring to U.S. Department of Energy scientists.

Karl van Bibber, a professor in the Department of Nuclear Engineering at the University of California at Berkeley, who has read the group's papers, says "the work is promising and has taken a large step forward," but adds that "there is yet a ways to go" for the project. More specifically, van Bibber notes, in the recent tests it was easier to detect fake weapons based on the isotopic characteristics of the materials rather than their spatial arrangements. He believes testing at the relevant U.S. National Laboratories — Los Alamos or Livermore — would help further assess the verification techniques on sophisticated missile designs.

Overall, van Bibber adds, speaking of the researchers, "their persistence is paying off, and the treaty verification community has got to be paying attention."

Danagoulian also emphasizes the seriousness of nuclear weapons disarmament. A small cluster of several modern nuclear warheads, he notes, equals the destructive force of every armament fired in World War II, including the atomic bombs dropped on Hiroshima and Nagasaki. The U.S. and Russia possess about 13,000 nuclear weapons between them.

"The concept of nuclear war is so big that it doesn't [normally] fit in the human brain," Danagoulian says. "It's so terrifying, so horrible, that people shut it down."

In Danagoulian's case, he also emphasizes that, in his case, becoming a parent greatly increased his sense that action is needed on this issue, and helped spur the current research project.

"It put an urgency in my head," Danagoulian says. "Can I use my knowledge and my skill and my training in physics to do something for society and for my children? This is the human aspect of the work."

The research was supported, in part, by a U.S. Department of Energy National Nuclear Security Administration Award.

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

## John Wayne, Susan Hayward, and 90 other people developed cancer after filming "The Conqueror" near a nuclear testing site

Source: https://www.thevintagenews.com/2018/02/19/the-conqueror-film/

**February 2018** – Nowadays, no one in their right mind would choose to shoot a feature film near a functioning nuclear testing site. In 1927, American geneticist Herman Joseph Muller discovered that prolonged exposure to radiation can have crippling effects on human health, and by the early 1950s it was known that nuclear blasts produce massive amounts of fallout that is highly radioactive and potentially lethal. Still, the producers of the film ***The Conqueror***, which was released in 1956, decided to shoot the film near the remote town of St. George in the Utah desert, merely a hundred miles away from the infamous **Nevada Test Site**.

"I am Temujin...Barbarian...
I fight!
I love!
I conquer
...like a
Barbarian!"
HOWARD HUGHES presents
JOHN WAYNE · SUSAN HAYWARD
THE CONQUEROR
CinemaScope
TECHNICOLOR
2 YEARS IN THE MAKING . . . AT A COST OF $6,000,000!
PEDRO ARMENDARIZ · AGNES MOOREHEAD · THOMAS GOMEZ · JOHN HOYT · WILLIAM CONRAD · TED de CORSIA
A DICK POWELL Production · Written by OSCAR MILLARD · Produced and Directed by DICK POWELL

**Approximately 100 nuclear bombs of various yields were detonated at the Nevada Test Site throughout the 1950s. In 1953, 11 atmospheric nuclear tests were carried out in the area as a part of Operation Upshot-Knothole:** The mushroom clouds were tens of thousands of feet high, and strong winds carried radioactive particles all the way to the Utah desert**. In 1954, when the filming of *The Conqueror* began, the barren hills around St. George were likely covered with a layer of deadly nuclear dust.**

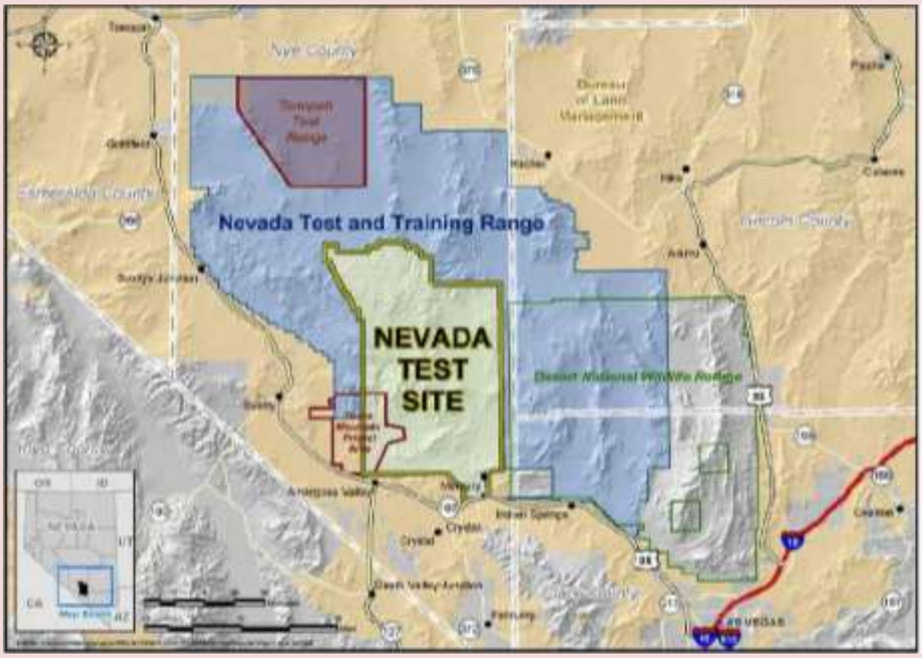
*The Conqueror*, a film that depicts a turbulent love affair between a Mongol warrior chief named Temujin and the beautiful daughter of his worst enemy, features a stellar cast of John Wayne, Susan Hayward, and Pedro Armendáriz. However, despite its high-profile cast and moderate box office success, the film was an absolute critical flop. Due to Wayne's catastrophically bad portrayal of a barbarian warlord and Hayward's underwhelming portrayal of his lover, the film was even listed as one of the 50 worst films of all time in 1978.

Wayne and Hayward weren't too dismayed by the harsh comments of the critics of the time. They were both filthy rich and immensely popular, so they simply continued making films. Unfortunately, the fact that the film was shot in the vicinity of a nuclear test site is thought to have affected their lives in a lasting way.

**Namely, out of 220 people who worked on the production of *The Conqueror*, 92 died of cancer, including Wayne, Hayward, and Armendáriz.** At the time when the filming took

place, the authorities labeled the filming site as safe from harmful effects of radioactive fallout even though abnormal levels of radiation were detected when the area was examined.

Still, modern research has shown that the soil in some areas around the town of St. George likely remained dangerously contaminated until 2007. Therefore, the fact that almost half of the cast and crew died of cancer likely wasn't a coincidence but a result of prolonged exposure to radiation.


Nye County
Tonopah Test Range
Bureau of Land Management
Nevada Test and Training Range
NEVADA TEST SITE
Desert National Wildlife Range
Las Vegas

**Wayne** first suffered from lung cancer and then died of stomach cancer in June of 1979. Although many of his friends tried to convince him that his condition was a result of exposure to radiation on the set of *The Conqueror*, he claimed that the illness was caused by his deadly habit of smoking six packs of cigarettes per day. However, Wayne's sons Patrick and Michael, who visited the set in 1954 and played with Geiger counters around contaminated rocks, both developed benign tumors that had to be surgically removed.

**Susan Hayward** won her first and only Academy Award in 1958, two years after *The Conqueror* was released, for her role as a death row inmate named Barbara Graham in the influential film *I Want to Live!*. Fifteen years later, her career abruptly ended when she was diagnosed with brain cancer, which also likely resulted from exposure to high levels of radiation. She died 1975, at the age of 57.

*The Conqueror* was produced by none other than the famous producer and business magnate Howard Hughes. In the early 1970s, Hughes realized that the people involved in the production of the film were dying. Since he was the person who approved the filming at the site near the town of St. George, and since he knew that the site was potentially dangerous, he felt so guilty that he paid $12 million to buy all existing copies of the film.

Although it cannot be definitively proven that the cancers that killed half of the cast and crew of *The Conqueror* were linked to the shooting location, experts argue that so many cases of the deadly illness among people who worked on the set cannot be dismissed as mere coincidence.

## AI Risks to Nuclear Deterrence Are Real

**By Zachary Kallenborn**

Source: https://warontherocks.com/2019/10/ai-risks-to-nuclear-deterrence-are-real/

Oct 10 – Why does the United States have so many nukes? Over 1,750 warheads are currently deployed on submarines, aircraft, and in missile silos. It's less than the total at the peak of the Cold War — the U.S. stockpile exceeded 31,000 warheads in 1967 — but it's still a lot.

There are a few reasons for this, but the most important is that nuclear deterrence relies, in part, on the ability of nuclear forces to survive a first strike. A nuclear threat is not as effective if an adversary can eliminate all U.S. nuclear forces in a single strike. The survivability of that deterrent is a core component of overall U.S. national security. As new technologies like artificial intelligence (AI) emerge and grow, an obvious question to ask is: What does this mean for nuclear deterrence?

In "Will Artificial Intelligence Imperil Nuclear Deterrence?" Rafael Loss and Joseph Johnson argue that technical limitations prevent AI from threatening the deterrent value of today's nuclear forces. In theory, AI-based image recognition systems could identify second-strike capabilities. But Loss and Johnson highlight two key challenges: bad data and an inability to make up for bad data. Few images of mobile nuclear missile launchers are available to compare with he images of commercial trucks from which the AI system would have to distinguish. Available data is also insufficient because a machine cannot infer the difference between a regular truck and a nuclear launcher. Even the best AI technologies cannot make up for these limitations. To reduce Loss and Johnson's argument to a cliché: garbage in, garbage out.

I believe that AI could help create windows of opportunity in which a successful decapitation strike is possible. AI enables the development of novel platforms to collect intelligence and attack nuclear systems. Although AI has limitations, other, non-AI capabilities mitigate AI's limitations regarding information processing. This means the potential for AI-based systems to aid second-strike platform identification should not be ignored.

While Loss and Johnson persuasively highlight real technical challenges with AI, their arguments do not support overall confidence in the survivability of U.S. and allied nuclear forces. AI-based systems only exist as part of a broader military apparatus that counteracts some of AI's limitations. AI also enables the creation and improvement of novel platforms to collect sensor data and strike nuclear platforms.

This state of vulnerability is not inevitable. The United States and allied countries can reduce the risks AI creates by exploring new means of operating stealthily and developing new decoys.

### AI Enables Platform Development

AI enables the development of novel autonomous platforms with significant relevance to nuclear deterrence. Developments in machine learning enable significant improvements in autonomous vehicle operation. Vehicles can better recognize and avoid obstacles, including hostile projectiles. Likewise, autonomous vehicles can better make decisions for themselves and plan their own tasks. And virtually every major military power has or is developing unmanned systems with varying levels of autonomy.

AI also enables the use of drones en masse and true drone swarms. Human cognition limits how many drones an operator can control at once. However, greater autonomy reduces the cognitive load. Cheap, autonomous drones enable wide area coverage and swarming enables them to coordinate their searches. Swarms also allow more complex searches: Drones can be equipped with different sensor packages to collect different types of information and reduce false positives.

Autonomous platforms also enhance risks to nuclear forces and second-strike platforms. Aerial, surface, and undersea autonomous platforms may search the ocean for adversary submarines. They may distribute sensors in proximity to submarine ports, strategic chokepoints, and the broader ocean. AI-based systems can also help analyze the collected data and optimize the overall sensor network. Autonomous systems can also carry out strikes against command-and-control nodes, early warning systems, and nuclear weapon-delivery systems. Provided platform costs stay low, autonomous systems also enable the use of mass, overwhelming adversary defenses. Although AI has limitations, the broader defense apparatus mitigates them.

### AI Does Not Work Alone

AI-enabled technologies pose a threat to the survivability of nuclear forces. The threat is not only from AI operating alone. Every military technology exists only as part of the overall defense ecosystem. The broader military bureaucracy, existing capabilities, and other emerging technologies raise the likelihood of AI's success in second-strike platform identification.

AI may help intelligence analysts sort through the huge masses of collected information. States deploy a wide variety of assets to collect and assess data on adversary nuclear forces. Human intelligence assets may collect information on classified military plans and technical characteristics of nuclear systems and their stealth capabilities, satellite and aircraft flights may identify nuclear weapons-related activity, while a broad range of anti-submarine capabilities search the ocean for adversary submarines. AI-based systems may identify information of interest with a higher probability of pointing to a second-strike platform's location.

Collection assets also collect data that can help train AI detection systems. For example, news reports have noted numerous drone sightings over Bangor Kitsap naval base where eight Trident submarines are stationed. Although open-source reports do not identify who controlled the drones, an adversary could certainly use drones to collect extensive imagery, video, and other sensor data related to nuclear submarines. The same drones could also collect information on

broader base activity, such as when a submarine enters or leaves.

Whether that training data is enough for robust AI is a difficult question for the public to assess. The capabilities of those assets, their deployment, and the data itself are likely to be highly classified. If states knew the what, where, and how of information collection, they would change their behavior. States with better intelligence networks and assets will also have more and better training data for their AI systems. And even imperfect AI detection can be significant.

Humans make up for some limitations of AI. The Department of Defense emphasizes the concept of human-machine teaming: Humans and machines work together symbiotically. Humans provide higher-order decision-making and ensure ethical and appropriate operation of autonomous systems. For example, a "loyal wingman" drone flies alongside manned aircraft, offering a range of capabilities from radar jamming to weaponry usable at the pilot's discretion. Human-machine teaming is relevant to the nuclear domain too.

In a world in which AI-based systems help locate mobile nuclear forces, humans can verify the results. Analysts can consult available satellite or aircraft imagery of the area. Human and unmanned assets can be deployed to collect additional data and track any identified mobile nuclear system. Humans can also help narrow searches based on assessments of military doctrine, behavior, and platform locations at known times. For example, if a submarine is spotted leaving Bangor Kitsap, the area of ocean to search shrinks drastically. Of course, verification takes time beyond any AI-based system processing. But AI also enables the creation of novel platforms that can help carry out these and other tasks.

AI creates risks for nuclear deterrence, and other emerging technologies worsen those risks by mitigating some of AI's challenges. As Loss and Johnson note, the time to train AI algorithms limits AI's usefulness in platform identification. However, improvements to quantum computer reliability and usability and supercomputing writ large improve computing power to more quickly process large volumes of data. In fact, Google reportedly achieved quantum supremacy, meaning it created a quantum computer more powerful than the world's most powerful supercomputers. (Although Google's quantum computer is only capable of a single, highly sophisticated calculation, it demonstrates the real potential of quantum computing.) New computer chips and other hardware optimized to support AI applications will speed the process too. Overall, this means faster, more effective AI. These developments in combination pose real risks to nuclear deterrence.

### A Window of Opportunity Is Enough to Threaten Nuclear Stability

AI only needs to help create a window of opportunity in which a strike is possible to pose a serious risk. Since a successful decapitation strike is essentially a game-ender and the risks of failure are huge, any thoughtful adversary would wait until they are confident in their knowledge of second-strike platform positions before launching a strike. Even if AI-based detection is not perfect, AI only needs to be good enough to allow that to happen, perhaps with some luck involved. Even a peephole is a window.

Even the potential for a window to open is destabilizing. Adversary knowledge of U.S. nuclear force positions is a closely guarded secret and vice versa. In a crisis, policymakers on both sides would not know if the window was wide open or shut tight. They might take actions to enhance survivability that are interpreted as a desire to exploit a decapitation opportunity. For example, a Russian policymaker might think: "Did the United States deploy its strategic bombers because it fears a strike or because it is preparing to carry one out?"

However, AI is unlikely to pose a day-to-day risk to second-strike forces. As Loss and Johnson highlight, AI-based systems may fail to recognize a missile launcher. Processing the large volume of data may also take a long time, and especially when including more voluminous sensor data.

For a true window of opportunity to open, actors must also be confident they have sufficient military assets in close enough range. Adversaries must have sufficient nuclear and conventional capabilities to eliminate mobile and immobile nuclear launch platforms. AI makes that easier too, because of the way autonomous platforms augment nuclear and conventional strike capabilities.

Of course, one should not assume a state would take the opportunity. The window may not open during a time of crisis when tensions are high and war appears close. If the window opens during peacetime, states will decide what to do based on state policy and military doctrine. One state may consider the possibility, while others find the notion abhorrent. Nonetheless, states can take action to reduce the risk.

### Mitigating the Threat

Current trends suggest AI will have a significant, but not apocalyptic impact on nuclear deterrence. A small window that allows a decapitation strike is still a window worth worry. Of course, the likelihood of a window opening depends on a host of unanswered questions, such as whether fundamental AI research continues to progress, how effective AI counter-measures are, and how robust AI needs to be in the roles described above. As Loss and Johnson rightly highlight, the brittleness of AI also limits the overall impact. Smart investments can mitigate emerging AI risks to nuclear deterrence without turning a tornado into a hurricane.

The United States should explore ways to hide from AI-based detection systems. The brittleness of AI

systems can be exploited for defensive gain. The United States could consider cyber means of manipulating adversary AI. For example, changing the labels on adversary training data for machine-vision systems could poison all systems that use the trained algorithm. Besides releasing manipulated images, the United States could spread other forms of bad data, such as acoustic emitters to mimic submarine signatures. The United States could also explore means to disable sensors via electronic, cyber, or space-based attacks. Additional decoy platforms would help, too.

The likelihood of a successful decapitation strike decreases if an adversary must target more second-strike platforms. Each additional platform must be identified and attacked. The United States and allied nations could build additional decoy platforms, using advancements in AI, machine learning, and robotics. For example, unmanned undersea vehicles could be designed to emulate the signatures of nuclear submarines. Russia is reportedly doing exactly that. Such "sub-sinks" could also be equipped with weapons and sensors to help identify and defend nuclear undersea platforms against conventional threats.

The technical limitations of AI mean the sky is not falling; however, AI does create real risks. Action now can reduce the likelihood of a window opening in which an adversary could eliminate the United States' second-strike capabilities. Such action is necessary to preserve the security of the United States.

***Zachary Kallenborn*** is a freelance researcher and analyst, specializing in chemical, biological, radiological, and nuclear (CBRN) weapons, CBRN terrorism, drone swarms, and emerging technologies writ large. His research has appeared in the *Nonproliferation Review, Studies in Conflict and Terrorism, Defense One, the Modern War Institute at West Point,* and other outlets. His most recent study, "*Swarming Destruction: Drone Swarms and CBRN Weapons,*" examines the threats and opportunities of drone swarms for the full scope of CBRN weapons.

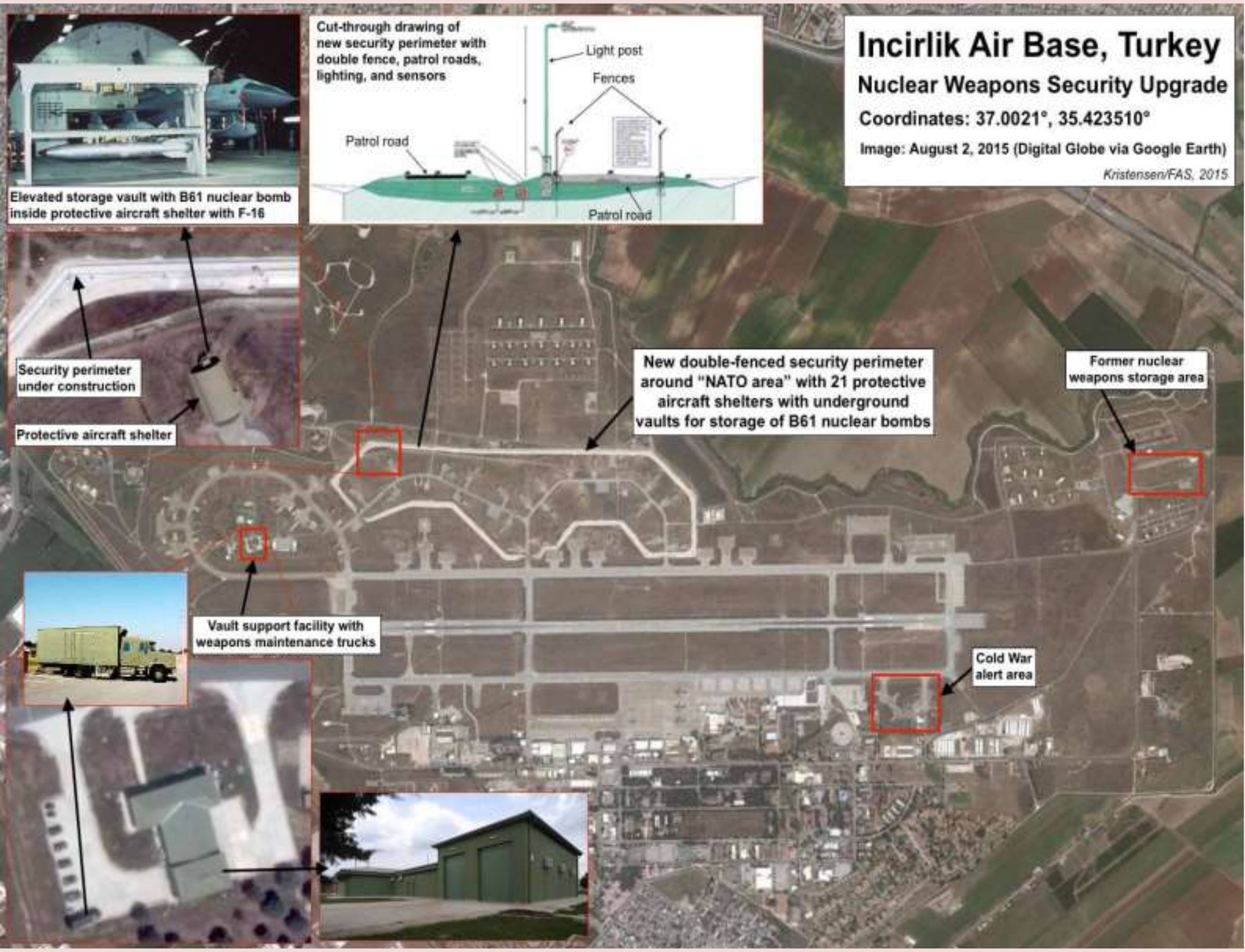
## U.S. Nuclear Weapons at Incirlik Air Base, in effect, "Erdogan's hostages": U.S. Official

Source: http://www.homelandsecuritynewswire.com/dr20191016-u-s-nuclear-weapons-at-incirlik-air-base-in-effect-erdogan-s-hostages-u-s-official

Oct 16 – Analysts say that the growing tensions between the United States and Turkey – tensions which are likely to intensify if Turkey expands its incursion into Syria, and if the United States imposed more meaningful economic sanctions in Turkey than those announced on Tuesday – may lead to a situation in which the U.S. nuclear weapons stored at the Incirlik air base in south-central Turkey would become, in effect, "hostages" of Turkey.

Trump announced his decision to withdraw U.S. troops from northern Syria in a series of Tweets on Sunday, despite months of warnings from the Pentagon, the NSC, the U.S. intelligence community, and the Department of State. As a result, no plans were made to deal with the **fifty or so nuclear bombs kept at Incirlik**.

The *New York Times* reports that the president's hasty decision left administration officials scrambling to find a plan to secure the nuclear weapons stored under American control at Incirlik Air Base, which is shared by the United States and Turkey.


Incirlik Air Base, Turkey
Nuclear Weapons Security Upgrade
Coordinates: 37.0021°, 35.423510°
Image: August 2, 2015 (Digital Globe via Google Earth)
Kristensen/FAS, 2015
Elevated storage vault with B61 nuclear bomb inside protective aircraft shelter with F-16
Cut-through drawing of new security perimeter with double fence, patrol roads, lighting, and sensors
Light post
Fences
Patrol road
Patrol road
Security perimeter under construction
Protective aircraft shelter
New double-fenced security perimeter around "NATO area" with 21 protective aircraft shelters with underground vaults for storage of B61 nuclear bombs
Former nuclear weapons storage area
Vault support facility with weapons maintenance trucks
Cold War alert area

The *Times* notes that officials from the State Department and Energy Department, which in charge of U.S. nuclear materials, met over the weekend to evaluate different plans to retrieve the estimated fifty tactical nuclear weapons kept at the site.

One official told the *Times* that the nuclear bombs at the base were now effectively Erdogan's hostages. **There are worries that removing the weapons may be interpreted as bringing to an end the relations between the two NATO allies, while leaving them at the air base could lead to a situation in which the weapons may be seized by Turkey.**

The *Independent* reports that only last month, Erdogan expressed his frustration with the restrictions on acquiring nuclear weapons which the 1980 Nuclear Nonproliferation Treaty imposed on Turkey – restrictions that Erdogan called "unacceptable."

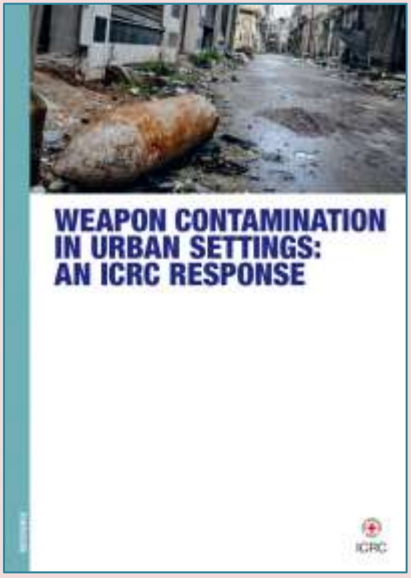
International CBRNE Institute
CBRNE-Terrorism Newsletter
2BRNE DIARY

# EXPLOSIVE NEWS

# Weapon Contamination in Urban Settings: An ICRC Response

Download PDF (1.68 MB)

Unexploded and abandoned ordnance constitutes a clear and serious danger to civilians and humanitarian operations wherever it is found. But its presence in urban settings raises particular concerns and challenges.


WEAPON CONTAMINATION IN URBAN SETTINGS: AN ICRC RESPONSE

This document outlines the risks and consequences that these weapons have in such settings for civilian communities, critical civilian infrastructure and humanitarian operations, including those of the ICRC.

The document also highlights the assistance that the ICRC's Weapon Contamination Unit can provide to ICRC units and programmes, as well as to the broader International Red Cross and Red Crescent Movement. This assistance aims to help the Movement assess and mitigate the dangers of weapon contamination (WeC) so as to protect staff and civilians and allow humanitarian services to be delivered unimpeded.

The document draws on two existing ICRC studies, Urban Services in Protracted Armed Conflict (2016) and Explosive Weapons in Populated Areas (2015), which emphasize the impact and challenges associated with the use of explosive ordnance in urban areas. It also includes a series of examples from the field, or operational vignettes, which illustrate the impact of weapon contamination and the actions taken by the WeC Unit in support of the work of ICRC delegations and National Red Cross and Red Crescent Societies.

In November 2017, a round-table discussion was held in Geneva to explore the growing interconnection between WeC activities and the work of other ICRC units. This discussion helped to identify a "spectrum of WeC response activities" that could be offered to ICRC and National Society programmes in a variety of situations. As reflected in the table below and elsewhere in this document, the services range from technical advice and guidance to actual explosive ordnance clearance and disposal.

# Lebanese Clear Civil War-Era Mines from Famed Cedar Forests

Source: http://www.naharnet.com/stories/en/265029-lebanese-clear-civil-war-era-mines-from-famed-cedar-forests

Sep 28 – Three decades after the civil war ended, deminers are still working to clear this mountainous northern region, famous for its centuries-old cedar trees, which are Lebanon's national emblem.

Humanity and Inclusion, an international demining organization, says it has removed hundreds of mines and other explosives since 2011.

"I feel very happy every time I discover a mine," Humayed said after he safely removed the anti-personnel mine. "I just feel that I helped save the life of a human being or an animal."

Lebanon's lush cedar forests are a source of pride for this small Mediterranean country. The ancient tree, often dubbed "Cedars of God," is emblazoned on the national flag, and forests across the north are prime tourist attractions.

**Hadath El-Jebbeh, a village in the northern Becharre region, is home to one of the largest cedar forests in the country.** But it sees few visitors because of mines left over from the 1975-1990 civil war, when the area was on the front lines between the Syrian army and the Lebanese Forces, a Christian militia.

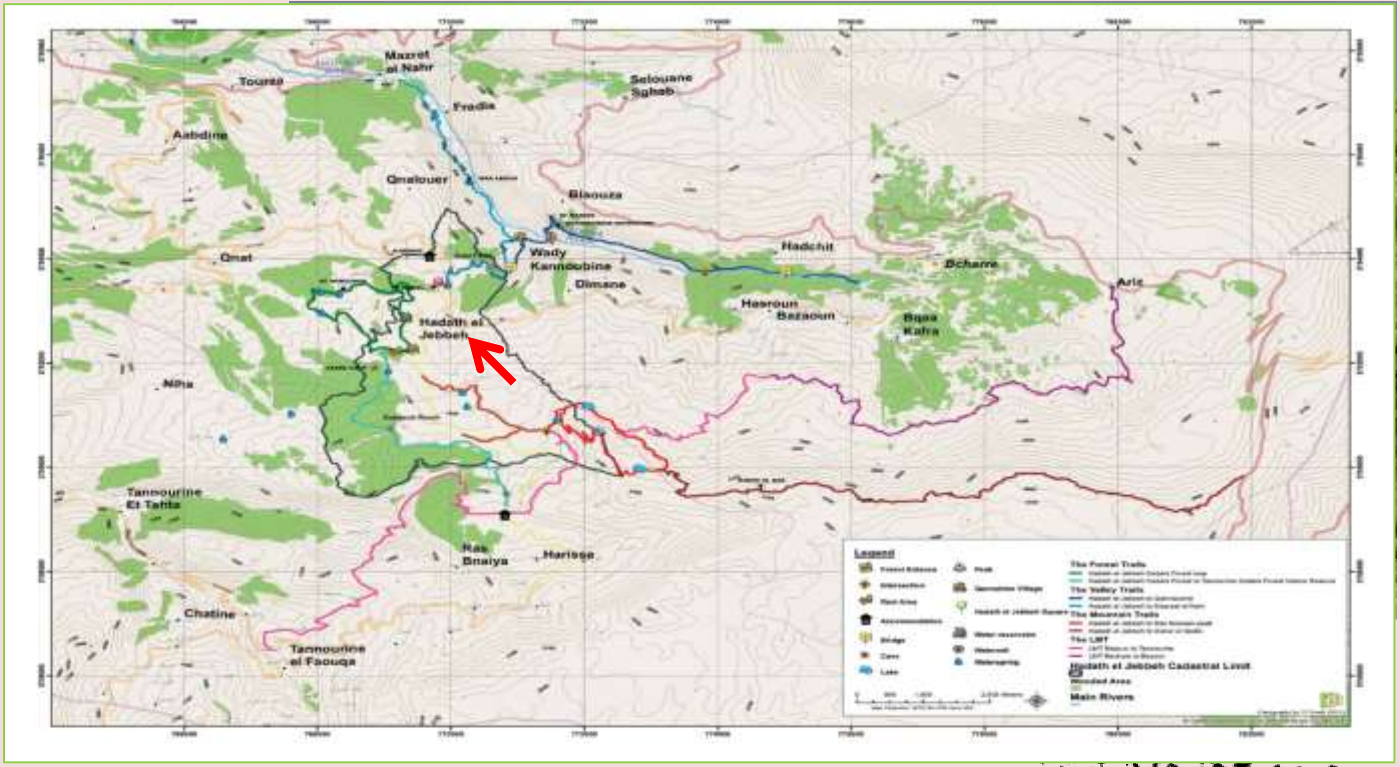
As the deminers took a break under the cedar trees, a shepherd shouted from a distance that he saw something suspicious. The deminers told him to stay away from it, saying they would check it out in the coming days.

Despite the dangers, local shepherds still bring flocks of sheep and goats to graze nearby. Hikers have also wandered into the area, not knowing about the hidden mines. It might be sheer luck that there have been no reports of fatalities in the area in recent years.

Kneeling beneath Lebanon's ancient cedars, Waheeb Humayed peers through a protective visor and waves a metal detector until he hears the tell-tale beep. He clips the grass, pushes a small prodder into the ground and gently sweeps the dirt away with a garden trowel, revealing another deadly mine.

Lebanon is littered with mines left over from decades of conflict. Israel left thousands of mines behind when it withdrew from southern Lebanon in 2000 after an 18-year occupation. **Israeli forces dropped cluster bombs, many of which failed to detonate, during the 2006 war with Hezbollah. Islamic militants used mines and explosives in northeastern Lebanon, near the Syrian border, in 2017.**

Brig. Gen. Jihad Al Bechelany said deminers have cleared about 70% of the more than 54 square kilometers (20 square miles) of minefields, removing 12,520 mines last year alone.



"Most of the minefields here are unorganized and we don't have maps that give us the exact numbers of mines," said Al Bechelany, who heads the Lebanon Mine Action Center, part of the Lebanese army. Some **100,000 mines were left behind from the civil war, with another 360,000 deposited along the border with Israel,** he said.

**Mines have killed 918 people and wounded 2,886 in Lebanon since 1975**, according to Al Bechelany. He said Lebanon had hoped to clear all the mines by 2020 but now expects the work to continue for another decade because of a lack of funding. It could take even longer if the country, which is grappling with an economic crisis, does not get an expected influx of $340 million for demining efforts.

Funding comes mostly from the United States, the European Union, Japan and local Lebanese institutions, according to David Ligneau, mine action program manager at Humanity and Inclusion. He called on everyone to step up funding and for all states, including Lebanon, to join treaties banning the use of mines.

On a single day, Associated Press reporters watched a team dispose of 10 mines in the forests of Hadath el-Jebbeh.

Explosive experts wired small detonators to each mine and called out that they would blow them up within five minutes. The countdown ended with a huge explosion, sending a mushroom cloud of dust into the air.

Lebanon still has a long way to go, particularly in the south, where mines and cluster bombs still kill and maim. Last month, cluster bombs left over from the 2006 war killed a man and a boy. The presence of mines prevents local communities from making use of large swaths of land, affecting everything from farming to tourism.

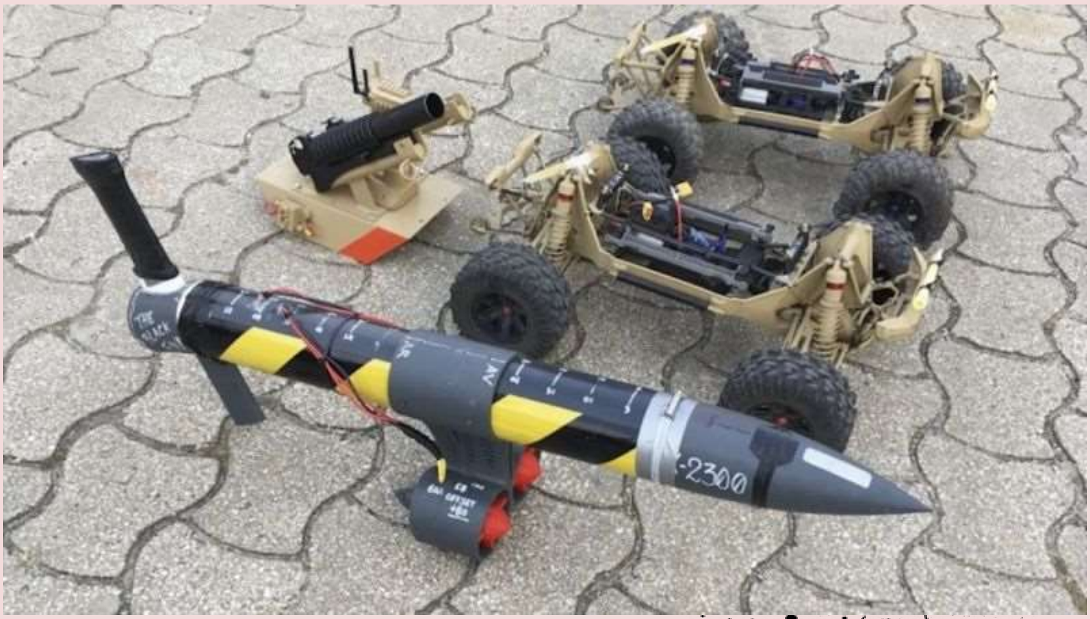
Standing beneath the giant cedars, Ligneau said he hoped his group's efforts would grant the Lebanese people "free access to this beautiful forest."

## Portugal's navy reveals "tech guerrilla" unit creating tech toys that kill

**By Sean Gallagher**

Source: https://arstechnica.com/information-technology/2019/10/portugals-navy-reveals-tech-guerrilla-unit-creating-tech-toys-that-kill/

Oct 02 – You don't need a huge budget like the US Department of Defense's to harness emerging technology for mayhem. During NATO's Recognized Environmental Picture Maritime Unmanned Systems (REPMUS) event last month—an uncrewed systems exercise held on the coast of Portugal—the Portuguese navy revealed its own in-house robot and drone capabilities, including some developed by the navy's Unmanned Vehicle Experimentation Cell (Célula Experimentação Operacional de Veículos Não Tripulados, or CEOV). This unit—made up of a handful of sailors with extensive technical training and talents in hardware hacking and engineering—has built prototype weapons using off-the-shelf hardware.



A "Black Fin" uncrewed submersible vehicle and two weaponized radio-controlled cars, produced from off-the-shelf hardware by the Portuguese navy's Unmanned Vehicle Experimentation Cell.

Modified radio-controlled cars configured with cameras and grenade launchers were among the devices shown off for journalists—one of whom was James Rands of Jane's Defence

Weekly. The deadly RC racers are part of CEOV's effort to "fight asymmetric threats with asymmetric thinking," according to Portuguese Navy Fleet Commander Vice Admiral Gouveia e Melo. Commanded by Lieutenant Tiago Mendes, CEOV reports directly to the fleet commander.

Citing "Martec's Law"—a proposal by tech executive Scott Brinker that technologies change exponentially while organizational change is a lot harder and slower (and at best logarithmic)—Lt. Mendes told journalists that the Portuguese navy's procurement process was too slow to bring in cutting-edge technology. As a result, he said, sailors' cell phones had more computing power than the ships they sailed on. Smaller organizations, such as terrorist cells, could exploit new technologies much faster—as was seen when ISIS turned off-the-shelf quadcopter drones into grenade-dropping bombers.

The things developed by CEOV aren't necessarily intended to be used by the Portuguese navy against enemies. Instead, they are intended as a way to explore what an asymmetric, innovative enemy could do so that the military can develop countermeasures. "We're like the flu vaccine," Mendes said. "We don't do the change—we start the process."

## If you can turn a vacuum into an improvised weapon, DARPA may want your help

**By Sean Gallagher**

Source: https://arstechnica.com/information-technology/2016/03/darpa-to-host-killer-improv-performances-with-hacked-hardware/

**November 2016** – In an effort to understand the kinds of improvised weapons, devices, and systems that could be used against US forces in the field today, the Defense Research Projects Agency's Defense Science Office is preparing for an alternative sort of "improv" performance. DARPA is inviting researchers, developers, and hardware-hacking hobbyists to join in, and the goal of the planned jam session is to discover ways that off-the-shelf commercial technology could be modified to be used against the military by its adversaries.

The US military has dealt with a wide range of improvised weapons and tools in the hands of adversaries over the past decade, including cell phone activated improvised explosives, off-the-shelf software used to intercept drone video feeds, and USB drives laden with malware that ran rampant on computer networks in Afghanistan. Today there's growing concern about how commercial and consumer drone and robotics technology, Internet-of-Things devices, and other burgeoning technology could be used to spy on, harass, impede, or even kill members of the military.

IEDs made from artillery shells captured in Baghdad are the last generation of improvised threats. DARPA wants to know what the next is. US Army

So today, DARPA officially unveiled **Improv**—a program that will fund "innovative research proposals for prototype products and systems that have the potential to threaten current military operations, equipment, or personnel and are assembled primarily from commercially available technology," according to the announcement.

The rules are pretty straightforward. "Proposers are free to reconfigure, repurpose, program, reprogram, modify, combine, or recombine commercially available technology in any way within the bounds of local, state, and federal laws and regulations," the announcement noted. "Use of components, products, and systems from non-military technical specialties (e.g., transportation, construction, maritime, and communications) is of particular interest."

Part of this broad-based hacker "red-teaming" of potential improvised threats is focused on what can be done within a tight budget and a tight deadline. Selected "performers" will compete against each other for a chance to build their prototype during a short DARPA-funded feasibility study phase (with up to $40,000 funding per individual awards). The performing teams will have only two weeks to construct a prototype once they've been chosen, with up to $70,000 additional funding and up to $20,000 for provisioning for the evaluation test.

Winning performances may be selected by DARPA for a follow-up study on how to develop countermeasures to the improvised technologies. So, here's your chance to build that killer Roomba hack you've always dreamed of, or maybe an actual *Fallout 4* Tactical Junk Jet—and get a foot in the door with DARPA. The program is open to all, including foreign nationals (with a bit of extra paperwork), since there's nothing particularly secret about off-the-shelf hardware and software.

***Sean Gallagher** is the IT editor and national security editor at Ars Technica. A University of Wisconsin grad, he wrote his first program in high school on a DEC PDP-10, and his first database app on a dual-floppy Apple II. Sean's first paid writing gig was producing "supplemental content" for Microprose's Gunship 2000 and F-117 Stealth Fighter 2.0 game manuals. A former naval officer, Sean served aboard the USS Iowa (BB-61) and at a river patrol boat squadron—where discovery of his computer skills landed him the assignments of network administrator and computer security officer. Aside from a few dark years as a systems integrator and a stint as Ziff Davis Enterprise's director of IT strategy, Sean has been either in the review lab or on a tech beat for most of the last two decades.*

## Chemical used for terrorism seized

Source: https://www.dawn.com/news/1509496/chemical-used-for-terrorism-seized

Oct 07 – A huge quantity of a chemical being used in making explosive devices and producing drugs has been seized in a raid in the Gatbrot area of Chagai district.

Speaking at a press conference in Dalbandin on Sunday, Chagai's Deputy Commissioner Fateh Khan Khajjak said that Levies and Quick Reaction Force jointly conducted the raid and intercepted three pickups loaded with cans filled with the chemical.

"Smugglers were carrying **4,800 litres of chemical in 240 cans**," he said, adding that the consignment was being smuggled to Iran via Pakistan.

Mr Khajjak said the seized chemical was very dangerous and it was used in **terrorist activities and manufacturing drugs**.

Article continues after ad

"Six suspects have been arrested and Levies confiscated the pickups," he said.

Six Kabuli vehicles, he said, had also been seized near the Yak Mach area of Chagai district in another raid and Levies arrested three suspects.

## The Bomb in College Classrooms

**By Sarah Bidgood**

Source: https://www.insidehighered.com/views/2019/10/14/colleges-arent-adequately-teaching-students-about-weapons-mass-destruction-opinion

Oct 14 – Millions of high school graduates recently packed their bags and headed off to their first year on college campuses across the country. To mark the occasion, everyone, from *The New York Times* to world-weary upperclassmen, offered tips for making the most out of the next four years. Their suggestions revealed less for their insights than for what they tell us about each person's own undergraduate experience. It's clear that, for many, college was the place where they found their passion and that this discovery enabled them to make a difference in the world once they left.

As someone who works as a nonproliferation researcher, I have some specific hopes for how this might play out for the Class of 2023. I spend my days looking for ways to prevent the spread of weapons of mass destruction and devising recommendations for how we can do this more effectively. It's certainly one of the most difficult moments for this work in recent memory. Between the crisis in U.S.-Russia relations, the unraveling of arms control and the growing potential for nuclear conflict around the world, most of us have been working overtime to keep up. And there's no end in sight.

In fact, so much work must be done, and the stakes for failure are so high, that it simply won't be possible to do it all alone. We need more creative ideas, more questioning minds and more outspoken voices to help prevent a global catastrophe. Instead, my field is facing a personnel crisis that is making us less effective at grappling with these and other international security challenges.

By 2023, for example, nearly 40 percent of the employees at the National Nuclear Security Administration will be eligible to retire. In 2029, the same will be true for 80 percent of the U.S. State Department's senior civil servants. The number of people taking the foreign service exam is at its lowest point in years.

Against this backdrop, we should be concerned that most current college students will graduate without any formal introduction to weapons of mass destruction and their means of control.

That was the central takeaway from a recent study I authored on how nonproliferation and disarmament of weapons of mass destruction are taught to undergraduates in the United States. To understand this landscape, I combed through hundreds of course catalogs and surveyed faculty members from 75 of the top-ranked public, private and military institutions in the country. I looked for classes that were offered sometime between 2016 and 2018 and that touched upon nuclear, chemical or biological weapons. After countless hours of searching, I found only 524 courses that met these criteria.

That number may sound like a lot to some people. What it means, however, is that each of those 75 institutions offered an average of just seven such courses during the two-year period in question. For comparison, the nation's three leading public, private and liberal arts institutions each offered as many as 19 to 30 courses that covered climate change during just the 2017-18 academic year alone. Given that climate change and weapons of mass destruction both threaten humanity's survivability, why are they taught at such discrepant levels to the generation whose responsibility they will become?

Much more can be done to empower students to address the challenges posed by weapons of mass destruction, and a first step should be ensuring that they have access to courses that focus on these topics -- regardless of institution they attend. Colleges and universities have significant room for improvement, considering that public universities offered fewer WMD-related courses than private ones during the period of my study. Because first-generation college students and students of color disproportionately attend public institutions, they had even fewer opportunities to discover these topics than their counterparts at private institutions.

This disparity is problematic, considering that our field already has very little diversity. What's more, since we know that homogeneous groups generate worse outcomes than those with more diverse members, this imbalance also makes us less effective in our jobs. From this vantage, ensuring that a broader population of students has the chance to pursue careers in the field is not only fair but also, quite literally, a matter of international security.

Fortunately, American colleges and universities are well positioned to be agents of change in this process. With buy-in from both faculty members and administrators, institutions could take a number of steps to substantially improve the situation. Those include offering interdisciplinary first-year seminars that encourage incoming students to explore issues related to weapons of mass destruction from different perspectives. They could also entail inviting nonproliferation experts to address faculty members and students at campuses that convene regular common hours or convocations. Another option would be to develop cross-disciplinary nonproliferation-focused courses that bring in expertise from the hard sciences, humanities and social science. Such efforts, while certainly not without cost, would go a long way toward helping all students engage substantively with these critical issues in ways that they can't today.

Individual faculty members can also take small steps that could have an immediate impact without requiring broader institutional support. The most obvious would be to introduce units on weapons of mass destruction into undergraduate classes that already exist. In a course on Stalinist history, that might mean a week on the Soviet atomic bomb program. In an introductory biology class, it could mean a debate over the possible proliferation implications of gene-editing technologies. For students who are learning skills that fall under the digital humanities, this may entail looking at satellite imagery for evidence of a failed missile launch. These small encounters won't be enough to enact major change, but they may be the only chance such students have to engage with such issues during their four-year college career.

Think tanks, research institutions and nongovernmental organizations can do more to support these efforts, too. Compiling a database of diverse experts who are available to guest lecture in undergraduate classrooms could be especially useful in this endeavor. Another would be offering development workshops for faculty members who want to introduce specific nonproliferation topics into their courses. A third could be providing reading lists, class materials and handouts for faculty members to use in developing a nonproliferation-related syllabus. Those activities would help to ensure that any college or university can introduce their students to these topics, even if they don't have the in-house expertise to do it all themselves.

These recommendations on their own won't be enough to create greater sustainability in my field or to solve the big problems that are keeping me and my colleagues up at night. They will, however, lead to more discussions about these issues within higher education -- and that could pave the way for more substantial and far-reaching efforts to get students thinking about careers in this domain.

I hope at least some of the members of the Class of 2023 discover that WMD nonproliferation, disarmament and arms control are their passions. These are areas where we're still going to need a lot of their help four years from now.

***Sarah Bidgood*** *is the director of the Eurasia Nonproliferation Program at the James Martin Center for Nonproliferation Studies in Monterey, Calif. She also directs the center's Young Women in Nonproliferation Initiative.*

## New x-ray system helps law enforcement better deal with suspicious package situations

Source: https://www.kgun9.com/news/local-news/new-x-ray-system-helps-law-enforcement-better-deal-with-suspicious-package-situations

Oct 15 – A new x-ray system is helping the Tucson Police Department's bomb squad better deal with suspicious package callouts. The Tucson Police Department was able to get the new system after applying for a Department of Homeland Security grant. The Southern Arizona Law Enforcement Foundation also helped TPD purchase the system.

The new x-ray system helps bomb squad members get a quick and clear look into what is inside of a potential suspicious package. Sergeant Dain Salisbury with the Tucson Police Department told KGUN9 the new x-ray system will help officials a whole lot more than the old system.

The old system required officers to scanned the item and take it back to a vehicle to develop the photo of the inside.

"When we had the old film it'd take about 30 minutes to x-ray a package to see what was inside. This new x-ray system that we have takes approximately two to five minutes which means we can tell what's inside of a package fairly quickly so that way the community can get back to enjoying the event that they are at," said Salisbury.

The new system is primarily being used during University of Arizona home football games and home basketball games.

During a UA home game up to 50,000 people can be in attendance, which means law enforcement officials also have to show up in big numbers.

Officers with Marana Police , Oro Valley Police , Tucson Police, UAPD , the TPD Bomb Squad, and SWAT all have law enforcement officials patrolling during games.

The hope is the new x-ray system along with law enforcement officials will be able to take care of suspicious package callouts a lot faster.

I'M E.O.D. WE BLOW STUFF UP. WHAT DO YOU DO?
I'M A SEABEE. WE BUILD STUFF.
...WELL THIS IS AWKWARD.
BROADSIDE.NET
©2013

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CBRNE DIARY

# CYBER NEWS

## Ransomware attack affects 1,500 health system computers, disrupts services

Source: https://www.mcknightsseniorliving.com/home/news/ransomware-attack-affects-1500-health-system-computers-disrupts-services/

Sep 25 – A ransomware attack at a Wyoming health system that includes a long-term care facility has affected all 1,500 computers, disrupted service provision and forced the use of paper charts instead of electronic health records. And one official says such incidents are increasing across the country.

The attack at Gillette, WY-based Campbell County Health — which includes The Legacy Living and Rehabilitation Center, with a secure memory care wing, as well as a hospital, medical group with almost 20 clinics, and a surgery center — occurred around 3:30 a.m. Friday, according to system officials.

"Ransomware attacks have doubled in 2019 … so it's a problem that is bigger than Wyoming," Tim Walsh, a supervisor in the state Department of Enterprise Technology, said at a Monday press conference.

Ransomware, according to the Department of Homeland Security, "is a type of malicious software, or malware, designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website."

Campbell County Health first reported "serious computer issues resulting in service disruptions throughout the organization" at 10:30 a.m. Friday. Officials continued to provide updates on the system's website.

By Saturday morning, system officials said in an online post that long-term care residents and home health and hospice patients continued to be cared for. "We are working with regional facilities to transfer patients who need a higher level of care," they said.

By Tuesday, some system services were being provided "on a case-by-case basis" and others still were not being offered. Radiology services are being affected the most, Chief Operating Officer Colleen Heeter had said at the previous day's press conference.

Campbell County Health is not disclosing the number of people affected by the ransomware attack, she said.

The health system is working with local, state and federal authorities. There is no time estimate for resolution of the cybersecurity issue, Matt Sabus, the system's IT director, said at the press conference. No indication currently exists that any resident or patient medical data were affected, he added.

County commissioners issued a disaster declaration on Friday as a precaution, to try to prevent the potential imposition of Medicare penalties for the system using outside services that might be deemed a lower level of care, said David King, Campbell County Emergency Agency management coordinator. Use of some electronic equipment has been problematic, he noted.

## What Data Hackers Can Get about You from Hospitals?

Source: http://www.homelandsecuritynewswire.com/dr20190925-what-data-hackers-can-get-about-you-from-hospitals

Sep 25 – When hospitals are hacked, the public hears about the number of victims – but not what information the cybercriminals stole. New research from Michigan State University and Johns Hopkins University is the first to uncover the specific data leaked through hospital breaches, sounding alarm bells for nearly 170 million people.

"The major story we heard from victims was how compromised, sensitive information caused financial or reputation loss," said John (Xuefeng) Jiang, lead author and MSU professor of accounting and information systems. "A criminal might file a fraudulent tax return or apply for a credit card using the social security number and birth dates leaked from a hospital data breach."

MSU notes that until now, researchers have not been able to classify the kind or amount of public health information leaked through breaches; thus, never getting an accurate picture of breadth or consequences.

The findings, published in Annals of Internal Medicine, encompass 1,461 breaches that happened between Oct. 2009 and July 2019. Jiang and co-author Ge Bai, associate professor of accounting at Johns Hopkins Carey Business School and Bloomberg School of Public Health, discovered that 169 million people have had some form of information exposed because of hackers.

To uncover what specific information was exposed, the researchers classified data into three categories: demographic, such as names, email addresses and other personal identifiers; service or financial information, which included service date, billing amount, payment information; and medical information, such as diagnoses or treatment.

"We further classified social security and driver's license numbers and birth dates as sensitive demographic information, and payment cards and banking accounts as sensitive financial information. Both types can be exploited for identity theft or financial fraud," Jiang said. "Within medical information, we classified information related to substance abuse, HIV, sexually transmitted diseases, mental health and cancer as sensitive medical information because of their substantial implications for privacy."

Over 70 percent of the breaches compromised sensitive demographic or financial data that could lead to identity theft or financial fraud. More than 20 breaches compromised sensitive health information, which affected 2 million people.

“Without understanding what the enemy wants, we cannot win the battle,” Bai said. “By knowing the specific information hackers are after, we can ramp up efforts to protect patient information.”

With a newfound understanding of what explicit data was leaked – and how many over the last decade were affected – the researchers offer hospitals and health providers suggestions on how to better protect patients’ sensitive information.

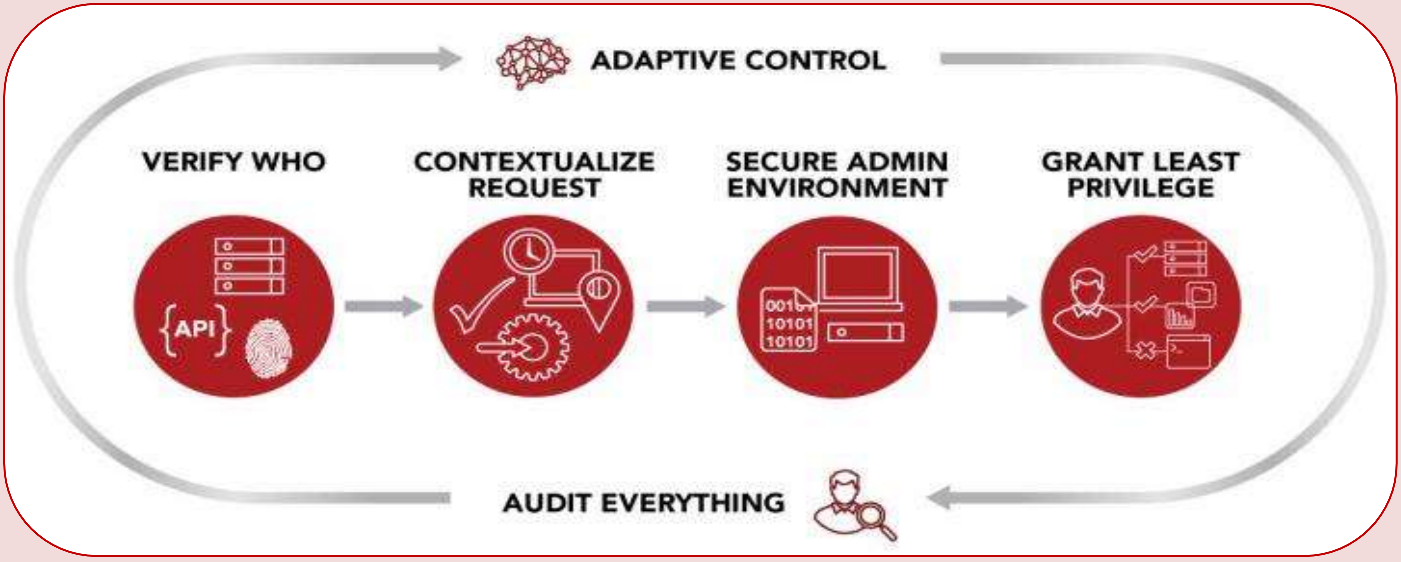
The researchers suggest that the Department of Health and other regulators formally collect the types of information compromised in a data breach to help the public assess the potential damages. Hospitals and other healthcare providers, Jiang said, could effectively reduce data breach risks by focusing on securing information if they have limited resources. For example, implementing separate systems to store and communicate sensitive demographic and financial information.

Jiang noted that the Department of Health and Human Services and Congress recently proposed rules that encourage more data-sharing, which increases the risks for breaches. He said that he and Bai plan to work with lawmakers and industries by providing practical guidance and advice using their academic findings.

## Zero Trust – The new default for Information Security

Source: http://www.worldsecurity-index.com/pressdetails.php

Sep 27 – Since the dawn of information security, trust has been a critical element. Over time, as information technology has become more distributed, the notion of trust has evolved around who logically needs to be able to access a service. For example, if you are seeking to get onto your corporate network then you will need to have a unique username and password to view the corporate information sources and private documents. In addition, firewalls are used to prevent outsiders and other potential threats from entering these zones.



Nevertheless, only using usernames and passwords to be able to access this kind of corporate information poses problems for those people who need to be permitted to access specific company resources through the internet, such as field engineers. As a result, VPNs have been created to provide trusted communication tunnels that can securely grant access to specific ports of enterprise data, controlled by IT departments.

For a while, this combination of usernames, VPNs, and firewalls was enough to create a high level of security within an organization’s network of employees and external actors. However, this has changed dramatically over the past decade with the explosion of mobile computing. The shift from working on a monitor to a personal laptop and to our devices, like phones and tablets, has proven to be a significant challenge for IT departments. No longer can they call the shots by only allowing corporate data to be accessed through company issued computers.

What’s more, this huge proliferation of personal devices has also been accompanied by the adoption of cloud computing and cloud applications, such as Salesforce, Office 365 and DropBox. This means the ways in which sensitive data can be shared has also increased exponentially. In working on projects with other companies it has become commonplace to share files, even for sensitive initiatives like new marketing releases. IT departments have therefore often resorted to blocking any unsanctioned applications or traffic from unmanaged devices. However, the cost of this is excessive and can inhibit innovation within the workforce, forcing employees to use potentially outdated programs and devices that prevent remote working. It is for these reasons that trust-based systems for protecting enterprise information are becoming obsolete.

While hacking corporate network systems from the outside requires a certain degree of skill to break through the firewalls and VPNs, an easier way to gain access to sensitive corporate data is to go via an employee who has access to such data. One such way to do this is via phishing attacks – pretending to be a trusted system to trick an employee into giving over their username and password. Once inside, the hacker can enter the trusted zone and acquire sensitive data or trigger other malicious attacks. It is this realization of internal threats that coined the term 'Zero Trust'. This mindset is simple – any user or device trying to access confidential data cannot and should not be trusted by default, even if they work for the company.

When discussing how to implement a Zero Trust framework it must be noted that one size does not fit all in terms of what degree of security needs to be put in place and how segregated access needs to be. However, there are two key enablers that are helpful to take into consideration when adopting Zero Trust posture; Identity and Access Management (IAM) and Network Micro-segmentation.

IAM essentially lets system administrators manage the identities of different users and entities; and regulate access to systems or networks based on the roles of individual users within the enterprise. Roles are defined according to job competency, authority and responsibility within the enterprise. A good example of this is the special permissions that more senior figures in the organization may have access to compared to their juniors. In practical terms this may mean that only a Practice Head would have access to the Purchasing System to approve a purchase request. One of the key advantages of Access Management systems is that they can enable or revoke access regardless of a user's location or device type. This gives system administrators a lot of flexibility in organizations that have a lot of remote or nomad workers; while giving employees the freedom to work from any location. Their value as key resource in cybersecurity is highlighted by the fact that 75% of organizations rely on access management to secure their external users' logins to online corporate resources.

Network Micro-segmentation works by slicing a network into different segments that can only be accessed by a known number of users. For example, if you worked in HR for your company you could not access the section of documents meant for the Finance team and vice versa. It also means that if a worker's credentials are used by a hacker, they could not compromise more data than that individual had access to – each application or resource is isolated with its own firewall to secure it. However, although this reduces the lateral movement of threats, a company will still have to use an identity and access management system to identify users, devices and other resources in the first place.

While both these approaches are different, they are complementary in a variety of ways and in the long term most companies will likely need to balance both to significantly reduce the insider threat and create a version of a Zero Trust framework that works for them. As the threat landscape continues to advance and evolve it is important that companies do not forget that sometimes the worst threats come from those you might normally trust the most – the insiders! **Never trust, always verify!**

## Are cyber-operations a U.S. retaliatory option for the Saudi oil field strikes? Would such action deter Iran?

**By Jacquelyn Schneider**

Source: https://www.washingtonpost.com/politics/2019/10/01/are-cyber-operations-us-retaliatory-option-september-oilfield-strikes-would-this-deter-iran/

Oct 01 – The mounting evidence that Iran was behind the September cruise missile and drone strikes on two Saudi oil facilities has left Saudi Arabia, the European Union and the United States looking for options to "deter Iran" without igniting an all-out war in the region. This week, Crown Prince Mohammed bin Salman made it clear that Saudi Arabia wants to avoid a military confrontation with Iran.

What do we know about cyber-operations, one of the options on the table? Reports of National Security Council meetings shortly after the drone and missile strike suggest that President Trump has mentioned the possibility of using cyberattacks on Iranian targets. The United States and Iran have already clashed in the cyber-sphere. A report a few months back suggested that the Trump administration conducted a cyberattack to retaliate when Iran downed a U.S. drone. Iranian-sponsored hackers reportedly have launched cyberattacks on U.S. government sites.

But retaliatory cyberattacks may have complicated consequences. Successful retaliatory strikes need to do two things. First, they send a credible signal to the target that attacks of

this kind will not be tolerated. Second, they need to limit the risk of escalation through spiraling retaliation and counter-retaliations. Can cyber-operations do this? Research suggests that this is difficult, but maybe not for the reasons you'd expect.

**The Trump administration is thinking more aggressively about cyberattacks**

The Trump White House has advocated for a more assertive and preemptive use of cyber-operations. The Obama administration generally was more cautious in how it used cyberattacks, fearing they would lead to escalation.

The Trump administration, in contrast, sees cyber-operations as a way to "defend forward" and "persistently engage" — terms that describe the Defense Department's new strategy of preemptive cyber-operations to degrade adversary nations' ability to conduct cyberattacks. The White House has delegated authorities for action (or permission to conduct cyber-operations) to the Defense Department to make it easier to respond quickly, and has approved cyber-operations against the Islamic State and Russia.

So it's not surprising that the Trump administration is actively considering cyberattacks. However, the idea is getting pushback from national security reporters including David Sanger and Julian Barnes, who suggest that cyberattacks are ineffective and likely to lead to escalation.

**There's evidence to suggest cyberattacks aren't escalatory**

Recent work by myself and Sarah Kreps finds that the American public is less likely to support retaliation against cyberattacks than against an airstrike, even when they create similar effects. U.S. government security decision-makers seem to feel the same way. Research by Brandon Valeriano and Benjamin Jensen, as well as evaluation of strategic war games, finds that players are less likely to respond to a crisis by escalating when they are given cyber-tools — and less likely to respond with violent escalation when the adversary conducts a cyberattack.

These researchers looked at responses from people in the United States for the most part. However, statistical analysis of international cyber-incidents reaches mostly similar conclusions, as does research on battlefield operations in Ukraine. The emerging consensus among researchers is that cyberattacks aren't unusually escalatory. If anything, the opposite is true.

**Less escalatory may mean less effective**

However, cyberattacks are less likely to deter adversaries for the same reasons they are less likely to lead to escalation. Deterrence is all about sending signals to other countries that there will be consequences if they behave badly.

As other scholars have noted, the best deterrence signals are ones that are costly, visible and credible. Here's why cyber-operations often fail this test: They may be hard to detect, hard to attribute to their source and hard to turn into a credible threat, because they may rely on vulnerabilities that are easy to plug if the target knows about them. This all makes cyber-operations less escalatory, but also harder to use to send clear signals.

Moreover, as Sanger and Barnes note, the United States is in a particularly vulnerable position when it uses cyberattacks, because the U.S. way of life is more dependent on digitally dependent technologies than Iranian society. So if Iran retaliates to a cyberattack with another cyberattack, the United States may come off worse. Furthermore, the United States depends more on the global communications infrastructure than Iran does, generating further vulnerabilities that might deter America from using cyberattacks.

### Cyberattacks have trade-offs

These are the kinds of trade-offs that the Trump administration will think about when deciding whether to use cyber-retaliation to deter attacks from Iran. But it's important to note that cyber-operations aren't just used for deterrence.

The Defense Department is also engaged in "defending forward," which focuses on undermining the enemy's ability to conduct cyberattacks through cyber-operations and special partnerships with critical infrastructure and the Department of Homeland Security. These operations are not specifically about deterring future attacks as much as they are actively degrading capabilities to conduct attacks today. Related, the United States could use cyber-operations to decrease Iranian military capabilities, especially in conjunction with conventional military strikes. The United States may very well be contemplating the benefits and disadvantages of such actions, especially if relations with Iran deteriorate further.

***Jacquelyn Schneider** is a Hoover Fellow with the Hoover Institution at Stanford University and a nonresident fellow at the Naval War College's Cyber and Innovation Policy Institute.*

## Cybercrime: AI's Growing Threat

**By Marc Wilczek**

Source: https://www.darkreading.com/risk/cybercrime-ais-growing-threat-/a/d-id/1335924

April 2019 – These days, the use of artificial intelligence (AI) is becoming increasingly commonplace. Companies and governments use facial recognition technology to verify our identities; virtually every smartphone on the market has mapping and translation apps; and machine learning is an indispensable tool in diverse fields including conservation, healthcare, and agriculture.

As the power, influence, and reach of AI spreads, many international observers are scrutinizing the dual nature of AI technology. They're considering not only AI's positive transformative effects on human society and development — think of medical AI applications that help diagnose cancer early — but also its downsides, particularly in terms of the global security threats to which it can expose us all.

### AI as a Weapon

As AI gets better and more sophisticated, it also enables cybercriminals to use deep learning and AI to breach security systems (just as cybersecurity experts use the same technology tools to detect suspicious online behavior). Deepfakes — using AI to superimpose one person's face or voice over another in a video, for example — and other advanced AI-based methods will probably play a larger role in social media cybercrime and social engineering. It sounds scary, and it's not science fiction.

In one noteworthy recent example of a deepfake that generated headlines in The Wall Street Journal, criminals employed AI-based software to replicate a CEO's voice to command a cash transfer of €220,000 (approximately $243,000). Cybercrime experts called it a rare case of hacking that leveraged artificial intelligence.

In that scam, the head of a UK-based energy company thought he was on the phone with his boss, the chief executive of the firm's German parent firm, who directed him to send the money to a Hungarian supplier. The German "caller" claimed the request was urgent and ordered the unwitting UK executive to initiate the transfer within the hour.

### The IoT is a Bonanza for Cybercriminals

That's just one instance of how AI has huge potential to transform how crime, and cybercrime in particular, is conducted. Using AI, bad actors will be able to refine their ability to launch attacks and discover new targets, such as by altering the signaling system in driverless cars. The growing ubiquity of the Internet of Things (IoT) is a particular gold mine for cybercriminals. There's also increasing convergence of operational IT and corporate IT; which means that the production lines, warehouses, conveyor belts, and cooling systems of tomorrow will be even more exposed to an unprecedented volume of cyber threats. Even pumps at gas stations could be controlled or taken offline from afar by hackers.

Like any connected device that's improperly secured (or not secured at all), it's possible that Internet-connected gas pumps and other smart devices could be co-opted into botnets for use in distributed denial-of-service attacks, with bad guys recruiting them in their efforts to overload online services.

But it's not only companies that are vulnerable. Cyberattacks on critical infrastructure can lead to widespread blackouts that can cripple a major city, an entire region, or a country for days or weeks, which makes such attacks a massively destructive weapon for malicious nation-states. North Korea is infamous for cyber warfare capabilities including sabotage, exploitation, and data theft. According to the United Nations, the country has racked up roughly $2 billion via "widespread and increasingly sophisticated" cyberattacks to bankroll its weapons of mass destruction programs.

Qualys's Chairman and CEO, Philippe Courtot talks about changes in the security landscape he's witnessed during the company's 20-year lifespan, as well as what motivated the vendor to give away its Global IT Asset Discovery and Inventory app for free.

**Damages to Exceed $5 Trillion by 2024**

Because of the general trend toward corporate digitization and the growing volume of everyday activities that require online services, society is becoming ever more vulnerable to cyberattacks. Juniper Research recently reported that the price tag of security breaches will rise from $3 trillion each year to over $5 trillion in 2024, an average annual growth of 11%. As government regulation gets stricter, this growth will be driven mainly by increasingly higher fines for data breaches as well as business losses incurred by enterprises that rely on digital services.

According to Jupiter's report, the cost per breach will steadily rise in the future. The levels of data disclosed certainly will make headlines, but they won't directly impact breach costs, as most fines and lost business are not directly related to breach sizes.

**AI-Based Attacks Require AI-Based Defenses**

As cyberattacks become more increasingly devious and hard to detect, companies need to give their defense strategies some serious second or third thoughts. AI can constantly improve itself and change parameters and signatures automatically in response to any defense it's up against. Given the global shortage of IT and cybersecurity talent, merely putting more brilliant and ingenious noses to the grindstone won't solve the problem. The only way to battle a machine is with another machine.

On the plus side, AI has the potential to expand the reach for spotting and defending against cyberattacks, some of which have had worldwide impact. When it comes to detecting anomalies in traffic patterns or modeling user behavior, AI really shines. It can eliminate human error and dramatically reduce complexity. For example, Google stopped 99% of incoming spam using its machine learning technology. Some observers say AI may become a useful tool to link attacks to their perpetrators — whether it's a criminal act by a lone actor or a security breach by a rogue state.

In the cybersecurity world, the bad guys are picking up the pace. As a result, the corporate sector must pay attention to AI's potential as a first line of defense. Doing so is the only way to understand the threats and respond to the consequences of cybercrime.

***Marc Wilczek** is a columnist and recognized thought leader, geared toward helping organizations drive their digital agenda and achieve higher levels of innovation and productivity through technology. Over the past 20 years, he has held various senior leadership roles across the ICT industry. Before serving as chief operating officer at Link11, he was member of the management board of T-Systems' Computing Services & Solutions (CSS) division. Prior to that, he served as senior vice president, Asia Pacific/Latin America/Middle East & Africa at CompuGroup Medical, and as managing director, Asia Pacific, for Sophos. He is an Alfred P. Sloan Fellow and holds master's degrees from FOM Graduate School for Economics and Management in Frankfurt and London Business School.*

# Disinformation and Terrorism

Source: http://www.homelandsecuritynewswire.com/dr20191015-disinformation-and-terrorism

Oct 15 – Most of the discussions that take place around the concept of disinformation–false information spread deliberately to deceive–typically focus on the role of nation-states like Russia and China. But violent non-state actors, including terrorist groups, rely on disinformation as well, and some groups have developed fairly sophisticated disinformation capabilities.

The *Cipher Brief* writes that the objectives of these non-state actors can vary but are almost always some combination of spreading fear and terror, recruiting new followers to the cause, radicalizing individuals, and confusing and distracting public safety officials in order to sap finite resources. In Pakistan, there have been terrorist disinformation campaigns against polio vaccinations. There is an added danger that terrorist disinformation may contain malicious code, intended to infect the hard drives and networks of entities that access the material online.

The Cipher Brief continues:

> *As has been documented in the aftermath of deadly terrorist attacks, including the 2017 Manchester attack, 'sock puppets,' or online identities used for deception, were highly active in attempting to spread messages with an anti-Islam agenda. While in some cases the objective was to cause confusion, in others it was merely to exacerbate tensions in society, to the supposed benefit of those responsible for the disinformation. Disinformation can take many forms, including the use of manipulated images and videos, and digital engineering attacks, including 'spoofing,' 'truthing,' and 'social proofing.' Western countries have been slow to respond to the advent of disinformation, and when they have reacted, the measures put in place to inoculate against the corrosive effects of disinformation have mostly been ineffective and in some cases counterproductive. So-called counternarratives to push back against terrorist disinformation have been widely panned, with few successful examples of note.*
>
> *The so-called Islamic State has relied significantly on photoshopped images intended to sow fear and confusion; images of terrorists transposed against backdrops of major Western cities, intended to suggest that an operation could be imminent, or merely to inspire lone actors to launch an attack. The Statue of Liberty and the Eiffel Tower have been used in IS images and propaganda in the past. Back in 2014, IS in Libya used social media to amplify disinformation that it had taken full control of Derna, a port city of 100,000 on the Mediterranean. While IS did indeed capture some government buildings, it was far from full control of the city as a whole as the group boasted, a claim that was picked up and repeated by mainstream media outlets including CNN.*
>
> *In 2017, the Islamic State claimed involvement in the horrific shooting in Las Vegas, NV, the single deadliest incident of mass murder on American soil, although the Federal Bureau of Investigation has since dismissed any involvement by the group. Analysts still debate why IS would make false assertions that Stephen Paddock, the assailant responsible for the Las Vegas attack, was a 'soldier of the caliphate,' particularly when the group had not been known to issue deliberately erroneous claims of responsibility. Some speculated that the group was merely seeking to keep its name in the news cycle, especially as it suffered battlefield losses in the Levant. But it does make sense when viewed through the lens of disinformation, which deliberately attempts to confuse an adversary and divert precious resources and manpower to dealing with threats. In the case of Las Vegas, IS also spread fear and sought to have a devastating psychological impact on its target audience, an objective that has been greatly enhanced through the use of disinformation-related capabilities.*

*Biohacking DIY frog*

# DRONE NEWS

# Terrorist Groups, Artificial Intelligence, and Killer Drones

**By Jacob Ware**

Source: https://warontherocks.com/2019/09/terrorist-groups-artificial-intelligence-and-killer-drones/

Sep 24 – In 2016, the Islamic State of Iraq and the Levant (ISIL) carried out its first successful drone attack in combat, killing two Peshmerga warriors in northern Iraq. The attack continued the group's record of employing increasingly sophisticated technologies against its enemies, a trend mimicked by other nonstate armed groups around the world. The following year, the group announced the formation of the "Unmanned Aircraft of the Mujahedeen," a division dedicated to the development and use of drones, and a more formal step toward the long-term weaponization of drone technology.

Terrorist groups are increasingly using 21st-century technologies, including drones and elementary artificial intelligence (AI), in attacks. As it continues to be weaponized, AI could prove a formidable threat, allowing adversaries — including nonstate actors — to automate killing on a massive scale. The combination of drone expertise and more sophisticated AI could allow terrorist groups to acquire or develop lethal autonomous weapons, or "killer robots," which would dramatically increase their capacity to create incidents of mass destruction in Western cities. As it expands its artificial intelligence capabilities, the U.S. government should also strengthen its anti-AI capacity, paying particular attention to nonstate actors and the enduring threats they pose. For the purposes of this article, I define artificial intelligence as technology capable of "mimicking human brain patterns," including by learning and making decisions.

## AI Could Turn Drones into Killer Robots

The aforementioned ISIL attack was not the first case of nonstate actors employing drones in combat. In January 2018, an unidentified Syrian rebel group deployed a swarm of 13 homemade drones carrying small submunitions to attack Russian bases at Khmeimim and Tartus, while an August 2018 assassination attempt against Venezuela's Nicolas Maduro used exploding drones. Iran and its militia proxies have deployed drone-carried explosives several times, most notably in the September 2019 attack on Saudi oil facilities near the country's eastern coast.

Pundits fear that the drone's debut as a terrorist tool against the West is not far off, and that "the long-term implications for civilian populations are sobering," as James Phillips and Nathaniel DeBevoise note in a Heritage Foundation commentary. In September 2017, FBI Director Christopher Wray told the Senate that drones constituted an "imminent" terrorist threat to American cities, while the Department of Homeland Security warned of terrorist groups applying "battlefield experiences to pursue new technologies and tactics, such as unmanned aerial systems." Meanwhile, ISIL's success in deploying drones has been met with great excitement in jihadist circles. The group's *al-Naba* newsletter celebrated a 2017 attack by declaring "a new source of horror for the apostates!"

The use of drones in combat indicates an intent and capability to innovate and use increasingly savvy technologies for terrorist purposes, a process sure to continue with more advanced forms of AI. Modern drones possess fairly elementary forms of artificial intelligence, but the technology is advancing: Self-piloted drones are in development, and the European Union is funding projects to develop autonomous swarms to patrol its borders.

AI will enable terrorist groups to threaten physical security in new ways, making the current terrorism challenge even more difficult to address. According to a February 2018 report, terrorists could benefit from commercially available AI systems in several ways. The report predicts that autonomous vehicles will be used to deliver explosives; low-skill terrorists will be endowed with widely available high-tech products; attacks will cause far more damage; terrorists will create swarms of weapons to "execute rapid, coordinated attacks"; and, finally, attackers will be farther removed from their targets in both time and location. As AI technology continues to develop and begins to proliferate, "AI [will] expand the set of actors who are capable of carrying out the attack, the rate at which these actors can carry it out, and the set of plausible targets."

For many military experts and commentators, lethal autonomous weapon systems, or "killer robots," are the most feared application of artificial intelligence in military technology. In the words of the *American Conservative* magazine, the difference between killer robots and current AI-drone technology is that, with killer robots, "the software running the drone will decide who lives and who dies." Thus, killer robots, combining drone technology with more advanced AI, will possess the means and power to autonomously and independently engage humans. The lethal autonomous weapon has been called the "third revolution in warfare," following gunpowder and nuclear weapons, and is expected to reinvent conflict, not least terrorist tactics.

Although completely autonomous weapons have not yet reached the world's battlefields, current weapons are on the cusp. South Korea, for instance, has developed and deployed the Samsung SGR-A1 sentry gun to its border with North Korea. The gun supposedly can track movement and fire without human intervention. Robots train alongside marines in the California desert. Israel's flying Harpy munition can loiter for hours before detecting and engaging targets, while the United States and Russia are developing tanks capable of operating autonomously. And the drones involved in the aforementioned rebel attack on Russian bases in Syria were equipped with altitude and leveling sensors, as well as preprogrammed GPS to guide them to a predetermined target.

Of particular concern is the possibility of swarming attacks, composed of thousands or millions of tiny killer robots, each capable of engaging its own target. The potentially devastating terrorist application of swarming autonomous drones is best summarized by Max Tegmark, who has said that "if a million such killer drones can be dispatched from the back of a single truck, then one has a horrifying weapon of mass destruction of a whole new kind: one that can selectively kill only a prescribed category of people, leaving everybody and everything else unscathed." Precisely that hypothetical scenario was illustrated in a recent viral YouTube video, "Slaughterbots," which depicted the release of thousands of small munitions into British university lecture halls. The drones then pursued and attacked individuals who had shared certain political social media posts. The video also depicts an attack targeting sitting U.S. policymakers on Capitol Hill. The video has been viewed over three million times, and was met with increasing concern about potential terrorist applications of inevitable autonomous weapons technology. So far, nonstate actors have only deployed "swarmed" drones sparingly, but it points to a worrying innovation: Swarming, weaponized killer robots aimed at civilian crowds would be nearly impossible to defend against, and, if effective, cause massive casualties.

## Terrorists Will Be Interested in Acquiring Lethal Autonomous Weapons

Terrorist groups will be interested in artificial intelligence and lethal autonomous weapons for three reasons — cost, traceability, and effectiveness.

Firstly, killer robots are likely to be extremely cheap, while still maintaining lethality. Experts agree that lethal autonomous weapons, once fully developed, will provide a cost-effective alternative to terrorist groups looking to maximize damage, with Tegmark arguing that "small AI-powered killer drones are likely to cost little more than a smartphone." Additionally, killer robots will minimize the human investment required for terrorist attacks, with scholars arguing that "greater degrees of autonomy enable a greater amount of damage to be done by a single person." Artificial intelligence could make terrorist activity cheaper financially and in terms of human capital, lowering the organizational costs required to commit attacks.

Secondly, using autonomous weapons will reduce the trace left by terrorists. A large number of munitions could be launched — and a large amount of damage done — by a small number of people operating at considerable distance from the target, reducing the signature left behind. In Tegmark's words, for "a terrorist wanting to assassinate a politician … all they need to do is upload their target's photo and address into the killer robot: it can then fly to the destination, identify and eliminate the person, and self-destruct to ensure nobody knows who was responsible." With autonomous weapons technology, terrorist groups will be able to launch increasingly complex attacks,

and, when they want to, escape without detection.

Finally, killer robots could reduce, if not eliminate, the physical costs and dangers of terrorism, rendering the operative "essentially invulnerable." Raising the possibility of "fly and forget" missions, lethal autonomous weapons might simply be deployed toward a target, and engage that target without further human intervention. As P. W. Singer noted in 2012, "one [will] not have to be suicidal to carry out attacks that previously might have required one to be so. This allows new players into the game, making al-Qaeda 2.0 and the next-generation version of the Unabomber or Timothy McVeigh far more lethal." Additionally, lethal autonomous weapons could potentially reduce human aversion to killing, making terrorism even more palatable as a tactic for political groups. According to the aforementioned February 2018 report, "AI systems can allow the actors who would otherwise be performing the tasks to retain their anonymity and experience a greater degree of psychological distance from the people they impact"; this would not only improve a terrorist's chances of escape, as mentioned, but reduce or even eliminate the moral or psychological barriers to murder.

### Terrorist Acquisition of Lethal Autonomous Weapons Is Realistic

The proliferation of artificial intelligence and killer robot technology to terrorist organizations is realistic and likely to occur through three avenues — internal development, sales, and leaks.

Firstly, modern terrorist organizations have advanced scientific and engineering departments, and actively seek out skilled scientists for recruitment. ISIL, for example, has appealed for scientists to trek to the caliphate to work on drone and AI technology. The individual technologies behind swarming killer robots — including unmanned aerial vehicles, facial recognition, and machine-to-machine communication — already exist, and have been adapted by terrorist organizations for other means. According to a French defense industry executive, "the technological challenge of scaling it up to swarms and things like that doesn't need any inventive step. It's just a question of time and scale and I think that's an absolute certainty that we should worry about."

Secondly, autonomous weapons technology will likely proliferate through sales. Because AI research is led by private firms, advanced AI technology will be publicly sold on the open market. As Michael Horowitz argues, "militant groups and less-capable states may already have what they need to produce some simple autonomous weapon systems, and that capability is likely to spread even further for purely commercial reasons." The current framework controlling high-tech weapons proliferation — the Wassenaar Arrangement and Missile Technology Control Regime — is voluntary, and is constantly tested by great-power weapons development. Given interest in developing AI-guided weapons, this seems unlikely to change. Ultimately, as AI expert Toby Walsh notes, the world's weapons companies can, and will, "make a killing (pun very much intended) selling autonomous weapons to all sides of every conflict."

Finally, autonomous weapons technology is likely to leak. Innovation in the AI field is led by the private sector, not the military, because of the myriad commercial applications of the technology. This will make it more difficult to contain the technology, and prevent it from proliferating to nonstate actors. Perhaps the starkest warning has been issued by Paul Scharre, a former U.S. defense official: "We are entering a world where the technology to build lethal autonomous weapons is available not only to nation-states but to individuals as well. That world is not in the distant future. It's already here."

### Counter-Terrorism Options

Drones and AI provide a particularly daunting counter-terrorism challenge, simply because effective counter-drone or anti-AI expertise does not yet exist. That said, as Daveed Gartenstein-Ross has noted, "in recent years, we have seen multiple failures in imagination as analysts tried to discern what terrorists will do with emerging technologies. A failure in imagination as artificial intelligence becomes cheaper and more widely available could be even costlier." Action is urgently needed, and for now, counter-terrorism policies are likely to fit into two categories, each with flaws: defenses and bans.

Firstly, and most likely, Western states could strengthen their defenses against drones and weaponized AI. This might involve strengthening current counter-drone and anti-AI capabilities, improving training for local law enforcement, and establishing plans for mitigating drone or autonomous weapons incidents. AI technology and systems will surely play an important role in this space, including in the development of anti-AI tools. However, anti-AI defenses will be costly, and will need to be implemented across countless cities throughout the entire Western world, something Michael Horton calls "a daunting challenge that will require spending billions of dollars on electronic and kinetic countermeasures." Swarms, Scharre notes, will prove "devilishly hard to target," given the number of munitions and their ability to spread over a wide area. In addition, defenses will likely take a long time to erect effectively and will leave citizens exposed in the meantime. Beyond defenses, AI will also be used in counter-terrorism intelligence and online content moderation, although this will surely spark civil liberties challenges.

Secondly, the international community could look to ban AI use in the military through an international treaty sanctioned by the United Nations. This has been the strategy pursued by activist groups such as the Campaign to Stop Killer Robots, while leading artificial intelligence

researchers and scientific commentators have published open letters warning of the risk of weaponized AI. That said, great powers are not likely to refrain from AI weapons development, and a ban might outlaw positive uses of militarized AI. The international community could also look to stigmatize, or delegitimize, weaponized AI and lethal autonomous weapons sufficiently to deter terrorist use. Although modern terrorist groups have proven extremely willing to improvise and innovate, and effective at doing so, there is an extensive list of weapons — chemical weapons, biological weapons, cluster munitions, barrel bombs, and more — accessible to terrorist organizations, but rarely used. This is partly down to the international stigma associated with those munitions — if a norm is strong enough, terrorists might avoid using a weapon. However, norms take a long time to develop, and are fragile and untrustworthy solutions. Evidently, good counter-terrorism options are limited.

The U.S. government and its intelligence agencies should continue to treat AI and lethal autonomous weapons as priorities, and identify new possible counter-terrorism measures. Fortunately, some progress has been made: Nicholas Rasmussen, former director of the National Counterterrorism Center, admitted at a Senate Homeland Security and Governmental Affairs Committee hearing in September 2017 that "there is a community of experts that has emerged inside the federal government that is focused on this pretty much full time. Two years ago this was not a concern … We are trying to up our game."

Nonstate actors are already deploying drones to attack their enemies. Lethal autonomous weapon systems are likely to proliferate to terrorist groups, with potentially devastating consequences. The United States and its allies should urgently address the rising threat by preparing stronger defenses against possible drone and swarm attacks, engaging with the defense industry and AI experts warning of the threat, and supporting realistic international efforts to ban or stigmatize military applications of artificial intelligence. Although the likelihood of such an event is low, a killer robot attack could cause massive casualties, strike a devastating blow to the U.S. homeland, and cause widespread panic. The threat is imminent, and the time has come to act.

***Jacob Ware** holds a master's in security studies from Georgetown University and an MA (Hons) in international relations and modern history from the University of St Andrews. His research has previously appeared with the International Centre for Counter-Terrorism – The Hague*.

## As Attack Drones Multiply, Israeli Firms Develop Defenses

Source: https://www.voanews.com/middle-east/attack-drones-multiply-israeli-firms-develop-defenses

Sep 26 – Israel, one of the pioneers of drone warfare, is now on the front lines of an arms race to protect against attacks by the unmanned aircraft.

A host of Israeli companies have developed defense systems they say can detect or destroy incoming drones. But obstacles remain, particularly when operating in crowded urban airspaces.

"Fighting these systems is really hard ... not just because you need to detect them, but you also need to detect them everywhere and all the time," said Ulrike Franke, a policy fellow at the European Council of Foreign Relations.

Ariel Gomez, a system engineer works on the Popstar system that can track and identify flying objects day or night without being detected, at Israel Aerospace Industries, in the town of Yehud near Tel Aviv, Sept. 9, 2019.

Drones present unique challenges that set them apart from traditional airborne threats, such as missiles or warplanes.

They can fly below standard military radar systems and use GPS technology to execute pinpoint attacks on sensitive targets for a fraction of the price of a fighter jet. They can also be deployed in "swarms," which can trick or elude conventional defense systems. Even small off-the-shelf drones can be turned into weapons by rigging them with explosives or simply crashing them in crowded areas.

A series of drone strikes across the Middle East, including an attack on a Saudi oil field and processing plant that jolted international markets earlier this month, have underscored the devastating effectiveness of small unmanned attack aircraft.

The drone attack on Saudi energy infrastructure knocked out about half of the kingdom's oil supplies.

Yemen's Iran-aligned Houthi rebels claimed the attack, but the U.S. has blamed Iran itself, which is a leading developer of drone technology and is locked in a bitter rivalry with both Saudi Arabia and Israel.

Similar drone attacks on Saudi Arabia's oil industry by the Houthis a month earlier caused a "limited fire."

Elsewhere in the region, Israeli warplanes last month struck what Israel said was an Iranian-trained Hezbollah squad that was preparing to launch a group of drones toward Israel from Syria. A day later, Hezbollah said two Israeli drones crashed outside the group's offices in Beirut. Israeli media said the drone strike had destroyed valuable equipment used to make guided missiles.

Earlier this month, the Israeli military said an unmanned aircraft crossed into Israel from the Gaza Strip and dropped explosives on a military vehicle, causing minimal damage and no casualties. It was the second such attack from Gaza in the past year.

These threats are not confined to the battlefield. London's Gatwick Airport shut for parts of three days, stranding over 100,000 travelers ahead of Christmas last year, after drone sightings.

Israel has long been a dominant player in the military drone export business, developing small attack aircraft as well as long-range spy planes. Now, Israeli firms are at the forefront of a global industry developing means to protect against the drone threat.

"There is a lot of knowledge that was adapted from the area of unmanned aerial vehicles, which is something that the military had to deal with for a long, long time," said Ben Nassi, a researcher at Israel's Ben Gurion University specializing in drone threats.

In a laboratory near Israel's main international airport, Israel Aerospace Industries offered a glance at its new optical detection system: a black cube resembling a souped-up subwoofer that it says can spot a standard commercial drone from several miles (kilometers) away.

The state-owned company says the **Popstar system** can track and identify flying objects day or night without being detected. Developers say the system, which has already been field tested by the Israeli military, can differentiate threats from standard civilian aircraft with an advanced algorithm.

"On a daily basis we see these small-scale threats, such as drones, that can tie up a whole airport and shut down the entire air traffic," said Ariel Gomez, a systems' engineer at IAI who worked on the new drone detection platform.

"Our system can discern from several kilometers away any threat that approaches," he said.

Popstar focuses on protecting fixed, high-value targets like airports or energy infrastructure. Experts say it is much more difficult to use the technology in crowded urban environments, where heavy air traffic and high-rise buildings can create confusion and obstacles.

"Most of the industry is actually targeting the threats in a no-fly area," said Nassi. "When it comes to populated areas, law enforcement has much more difficulties to understand whether a drone is being used maliciously or not."

Israeli company Vorpal says it has found a partial solution to these challenges by developing a system that can detect and track virtually all commercial UAVs in urban airspaces.

Avner Turniansky, Vorpal's vice president of strategy, said the company has compiled a database of signals — what it calls the "signature" — emitted by 95% of drones on the market.

With these signatures, it says it can identify a drone — and locate its operator — within two seconds. Customers can track these aircraft and determine whether they pose a threat.

He said the system has a range of several kilometers, but still has some limitations. If an operator is flying a commercial drone whose signal hasn't been previously collected, it won't be identified. The system would also struggle to identify sophisticated drones built by hostile governments, since those signatures are likely unknown.

Still, he said the system can track "the vast majority" of popular drones on the market.

He said the firm has conducted several successful tests with the New York Police Department and counts Israel's national police force and the Defense Ministry as customers. During this year's Eurovision song contest in Tel Aviv, he said police caught more than 20 operators who were flying drones in no-fly zones.

According to Israel's Economy Ministry, UAV exports topped $4.6 billion between 2005 and 2013, around 10% of the country's defense exports.

Over a dozen Israeli firms presented cutting-edge anti-drone technologies at London's DSEI exhibition this month, from defense heavyweights Elbit Systems, Raphael and Israel Aerospace Industries, to smaller start-ups like Vorpal. They are part of a booming global industry with competitors from the U.S., Europe, Singapore, and China.

Anti-drone defenses fall into several categories. Detection systems usually rely on either radio or optical technology to spot incoming drones.

Other systems can stop the aircraft with jammers that down aircraft by scrambling communications, kinetic systems that try to knock the craft out of the sky or systems that allow authorities to seize control of an aircraft.

But for now, none of these systems can provide full protection.

**"It's a nasty target. It's a problem," said Turniansky. "It's going to be cat and mouse for a while."**

## Kamikaze Drones Join Turkish Fleet

Source: https://i-hls.com/archives/94948

Sep 24 – Turkey is enhancing its unmanned aerial vehicle fleet with kamikaze drones. 30 upgraded KARGU (Autonomous Tactical Multi-Rotor Attack UAV) kamikaze drones will join the Turkish Armed Forces' inventory as of 2020 to take part in critical operations in the country's east and along the Syrian border.

As a rotary-wing drone, the KARGU can carry various types of explosives, playing an efficient role in asymmetric warfare and the fight against terrorists.

The drones were developed by Turkish Defense Technologies Engineering and Trade. The **KARGU battle drone**, designed to support the tactical and field needs of Turkish security forces, eliminates targets more efficiently with new features such as enhanced ammo capacity and improved accuracy, according to dailysabah.com.

The 30 drones will also have the capacity to destroy an entire brigade and warship.

STM General Director Murat Ikinci said the newest upgrade would take the Turkish military to the next level. Ikinci noted that while each drone within the squadron has a specific mission, "if one of them is attacked or malfunctions during the operation, the other KARGUs will be able to replace it and perform the preset mission."

Stating that all the drones within the squadron have artificial intelligence (AI) and facial recognition systems, Ikinci elaborated on the drones' properties: "The drones are less than 70 kilograms each. They can also carry explosives and various equipment. They have a range of 15 kilometers. They can stay in the air for 30 minutes with explosives."

STM works on naval and air platforms, cyber-security, big data, autonomous systems, and artificial intelligence.

## Terrorist Groups, Artificial Intelligence, and Killer Drones

Source: http://www.homelandsecuritynewswire.com/dr20190924-terrorist-groups-artificial-intelligence-and-killer-drones

Sep 24 – In 2016, the Islamic State of Iraq and the Levant (ISIL) carried out its first successful drone attack in combat, killing two Peshmerga warriors in northern Iraq. The attack continued the group's record of employing increasingly sophisticated technologies against its enemies, a trend mimicked by other nonstate armed groups around the world. The following year, the group announced the formation of the "Unmanned Aircraft of the Mujahedeen," a division dedicated to the development and use of drones, and a more formal step toward the long-term weaponization of drone technology.

Jacob Ware writes in *War on the Rocks* that terrorist groups are increasingly using 21st-century technologies, including drones and elementary artificial intelligence (AI), in attacks. As it continues to be weaponized, AI could prove a formidable threat, allowing adversaries — including nonstate actors — to automate killing on a massive scale. "The combination of drone expertise and more sophisticated AI could allow terrorist groups to acquire or develop lethal autonomous weapons, or "killer robots," which would dramatically increase their capacity to create incidents of mass destruction in Western cities," Ware writes. "As it expands its artificial intelligence capabilities, the U.S. government should also strengthen its anti-AI capacity, paying particular attention to nonstate actors and the enduring threats they pose."

Ware writes:

> *The U.S. government and its intelligence agencies should continue to treat AI and lethal autonomous weapons as priorities, and identify new possible counter-terrorism measures. Fortunately, some progress has been made: Nicholas Rasmussen, former director of the National Counterterrorism Center, admitted at a Senate Homeland Security and Governmental Affairs Committee hearing in September 2017 that "there is a community of experts that has emerged inside the federal government that is focused on this pretty much full time. Two years ago, this was not a concern … We are trying to up our game."*
>
> *Nonstate actors are already deploying drones to attack their enemies. Lethal autonomous weapon systems are likely to proliferate to terrorist groups, with potentially devastating consequences. The United States and its allies should urgently address the rising threat  by preparing stronger defenses against possible drone and swarm attacks, engaging with the defense industry and AI experts warning of the threat, and supporting realistic international efforts to ban or stigmatize military applications of artificial intelligence. Although the likelihood of such an event is low, a killer robot attack could cause massive casualties, strike a devastating blow to the U.S. homeland, and cause widespread panic. The threat is imminent, and the time has come to act.*

## Are Air Defense Systems Ready to Confront Drone Swarms?

**By Seth Frantzman**

Source: https://www.meforum.org/59453/can-air-defense-systems-stop-drone-swarms

Sep 26 — The attack on Saudi Arabia's Abqaiq and Khurais oil facilities on Sept. 14 served as a reality check for countries struggling to define the level of the threat posed by drone swarms and low-altitude cruise missiles.

Now, in a region where that threat is particularly acute, countries are left to reexamine existing air defense technology.

According to the Saudi Defense Ministry, 18 drones and seven cruise missiles were fired at the kingdom in the early hours the day in mid-September.

The drones struck Abqaiq, a facility that the Center for Strategic and International Studies think tank had warned the month before was a potential critical infrastructure target. Several cruise missiles fell short and did not hit the facility. Four cruise missiles struck Khurais. Saudi and U.S. officials put blame on Iran, but the government there denies involvement.

What is clear is the failure of existing air defense systems to stop the attack.

The Abqaiq facility's air defenses reportedly included the American-made Patriot system, Oerlikon GDF 35mm cannons equipped with the Skyguard radar and a version of France's Crotale called Shahine. Satellite images posted by Michael Duitsman, a research associate at the James Martin Center for Nonproliferation Studies, shows the setup: Impeded by radar ranges and the facility itself, as well as the speed and angle of the drones and missiles, Saudi air defense apparently did not engage the drones.

"If U.S.-supplied air defenses were not oriented to defend against an attack from Iran, that's incomprehensible. If they were, but they were not engaged, that's incompetent. If they simply weren't up to the task of preventing such precision attacks, that's concerning," said Daniel Shapiro, a former U.S. ambassador to Israel and a visiting fellow at the Institute for National Security Studies. "And it would seem to validate Israeli concerns that even effective air and missile defense systems, as Israel has, could be overwhelmed by a sufficient quantity of precision-guidance missiles."

There is a debate about the level of this threat. Brig. Gen. Pini Yungman, a former air defense commander with the Israeli Air Force and current head of Rafael's air defense systems division, contrasts the drone swarm with a cruise missile with a range of 1,000 kilometers and equipped with a large warhead. "Drones, even drone swarms, are not a strategic threat, even if you take dozens to attack. They carry a very low weight of bomb or ammunition," Yungman said.

Uzi Rubin, former director of the state-run Israel Missile Defense Organization, doesn't think what happened in Saudi Arabia could happen in Israel. "We have a smaller area, and that has an advantage in many respects because it is an advantage in controlling our airspace."

He said the primary challenge in stopping an attack like that in Saudi Arabia is not the ability to shoot down the threats, but rather to detect the low-flying threats. "When it comes to missiles, missile defense sensors will aim above the horizon because the missile is above it and you don't want clutter. So when it comes to guarding, the issue is things that can sneak in near the ground," he explained. The key, then, is to close the gap that potentially exists near the ground.

"It's not too difficult to close the gap; the Saudis can do it with local defenses," he asserted. But he acknowledged that the larger the land area, the more difficult it can be to maintain control.

Rubin said shooting down drone swarms can be accomplished with anti-aircraft guns, noting that Iraq downed several Tomahawk cruise missiles in 1991 after discovering their flight path.

"You don't need anything fancy," he said — the Russian SA-22 or Pantsir system, with 30mm cannons, missiles and infrared direction finders would do.

"I think once the surprise of the [Sept. 14] attack wears off, then one should sit back and see it is not a very devastating attack." Like Yungman, he said a long-range precision missile aimed at a strategic facility like a nuclear reactor in a European country would be a more serious threat.

However, Thomas Karako, a senior fellow at the CSIS think tank, told *Defense News* that the attack suggests a dramatic escalation. "More broadly speaking, it is what I've been talking about: The specter of complex, integrated air and missile attack is not theoretical — it has arrived."

He argues that the Abqaiq attack draws a "bright red line under the problem set" and that "we need a mix of active and passive measures, kinetic and non-kinetic to counter."

"It's not a technological problem, it's an engineering problem," he said. "You need to look beyond the horizon and look in every direction." That would include 360 coverage by radar and elevated sensors.

### Israel, the Test Bed

Yungman considers the Middle East, particularly Israel, to be a proving ground. Since the 1940s, a number of different weapons systems, many made in Western countries or the Soviet Union, were used in regional combat.

"In this region, the asymmetric threat became bigger. So, in the north there are almost 200,000 short-range rockets and missiles and accurate missiles as a threat" from Hezbollah, he said. "And in Syria we can see accurate, maneuvering ballistic missiles and cruise missiles. So air defense and air missile defense became, from the asymmetric aspect, bigger and bigger, and the air defense system became an issue we need to invest in and develop as fast as we can."

With the support of the United States, Israel built and tested the Arrow system in the 1990s, becoming one layer of the country's multilayered system that eventually included Arrow-2, Iron Dome and David's Sling.

Short of using preemptive airstrikes against drone manufacturers and launch teams, Israel is upgrading its air defense on a "daily basis," Yungman noted.

"The main threat is not face-to-face [combat] threats — it is rockets, drones, cruise missiles, maneuvering [theater ballistic missiles] and [short-range ballistic missiles] with big and small warheads. When we are talking about thousands or tens of thousands or more, it is very complicated, but it can be defeated," he said.

One way to confront drone swarms involves soft-kill measures. Because drones are operated by GPS and radio control, jamming or taking control of the drone is one route.

But Rubin said what stands out about the Abqaiq incident is that the homing by the drones appeared to be optical, not GPS-guided.

Also noteworthy, evidence indicates that some of the UAVs weren't carrying warheads, as they didn't all explode.

Alternatively, a hard-kill approach might involve using a 5- to 10-kilowatt laser. Lasers can destroy drones up to 2.5 kilometers away, according to Yungman.

The U.S. has looked at lasers for its Stryker armored vehicles, and Germany, Russia and Turkey are among the nation-states developing the technology. Israel's Rafael has been working on laser interceptors for years, including the Drone Dome laser-based intercept system.

"I can say that from 2 kilometers I could hit a drone the size of a penny," Yungman claimed.

Another option could be drone-on-drone combat, though that capability is still under development.

While systems like the Iron Dome are combat-proven, questions remain about their ability to confront a drone swarm.

In theory, when using radar and electro-optics, an air defense system should be able to cover the bands necessary to track the drones using several systems and 360-degree phased-array coverage.

"In our research and technology, we have the radar and electro-optical and jamming, GPS-denying [capabilities]," Yungman said. "And we have the ability to kill it."

Rubin described the attack on Saudi Arabia as a kind of "Pearl Harbor," and it reminded him to an Aug. 17 attack on the Shaybah oil field in Saudi Arabia by Houthi rebels involving 10 drones.

"The surprise was not in the attack, but the audacity," Rubin recalled, adding that a precision attack by drones doesn't make the aircraft less vulnerable to air defense systems.

The Stunner interceptor missile of David's Sling, for instance, has the capability to intercept drones, missiles and other ordnance, including low-flying cruise missiles. But for that to work, there can't be a gap in the radar coverage, Rubin noted.

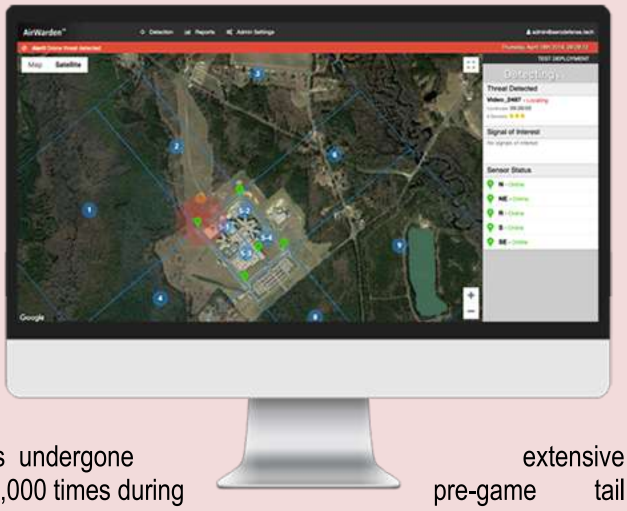
Certainly, the recent attack in Saudi Arabia will impact industry and spur development from the key players in this area of defense, according to Karako of CSIS.

"I think you'll see global demand signal for a variety of means to counter these threats," he said. "It will spark a lot of solutions."

***Seth Frantzman,*** *a writing fellow at the Middle East Forum, is the author of After ISIS: America, Iran and the Struggle for the Middle East (2019), op-ed editor of The Jerusalem Post, and founder of the Middle East Center for Reporting and Analysis.*

## AirWarden™ Drone Detection System

Source: https://aerodefense.tech/airwarden-drone-detection-system



AirWarden™ is an advanced drone detection system that identifies and classifies Radio Frequency (RF) drone and controller signatures and uses these signals to locate both devices.

### *Urban Environment Performance*

Many drone detection systems were developed, in remote areas, like the desert. This gave developers wide open areas to fly drones and test their system. The challenge is they've had limited experience in urban areas where buildings, cars, and other RF signals in the environment have a huge impact on the ability to detect drones and controllers.

AirWarden™ was developed in urban New Jersey. Moreover, it has undergone extensive testing at an NFL Stadium where ambient RF signals can increase by 50,000 times during pre-game tail gaiting. As a result, the system provides reliable detection and a low false positive rate, even in the toughest, busiest urban environments.

### *Sends Alerts*

When the system detects a drone or controller near your facility, it can alert security personnel via:

- **Command Console** – A web-based user interface that can run in a command center or be accessed remotely.
- **Email and Text** – Security personnel can be sent alerts via email and text. Alerts can also be sent to local law enforcement for a coordinated response.

### *Detects Both Known and Unidentified Drones*

**AirWarden™ can detect any drone that emits an RF signal. This includes popular, ready-to-fly consumer drones, commercial drones, custom "kit" or Do It Yourself (DIY)**

**drones and even a swarm of tiny micro-drones.** Because the system uses the physical signature of a signal to identify drones, it can detect both known and unidentified drones. This means that it will detect new drones on the market even if the system's 'drone library' has not been updated.

### *Fully Legal System*

If an RF detection solution "decodes" or "demodulates" the signal to extract the drone type, GPS coordinates or the "Return to Launch" GPS coordinates, it violates U.S. Federal Wiretapping laws. The AirWarden™ system is a passive system that uses physical characteristics of the signal to detect and locate. This means it is fully legal, and will not be affected when drone manufacturers start to encrypt the signal between their drones and controllers. In addition, decoding and demodulating signals takes more time than physical signal analysis. This means systems using this method take longer to detect and locate a device.

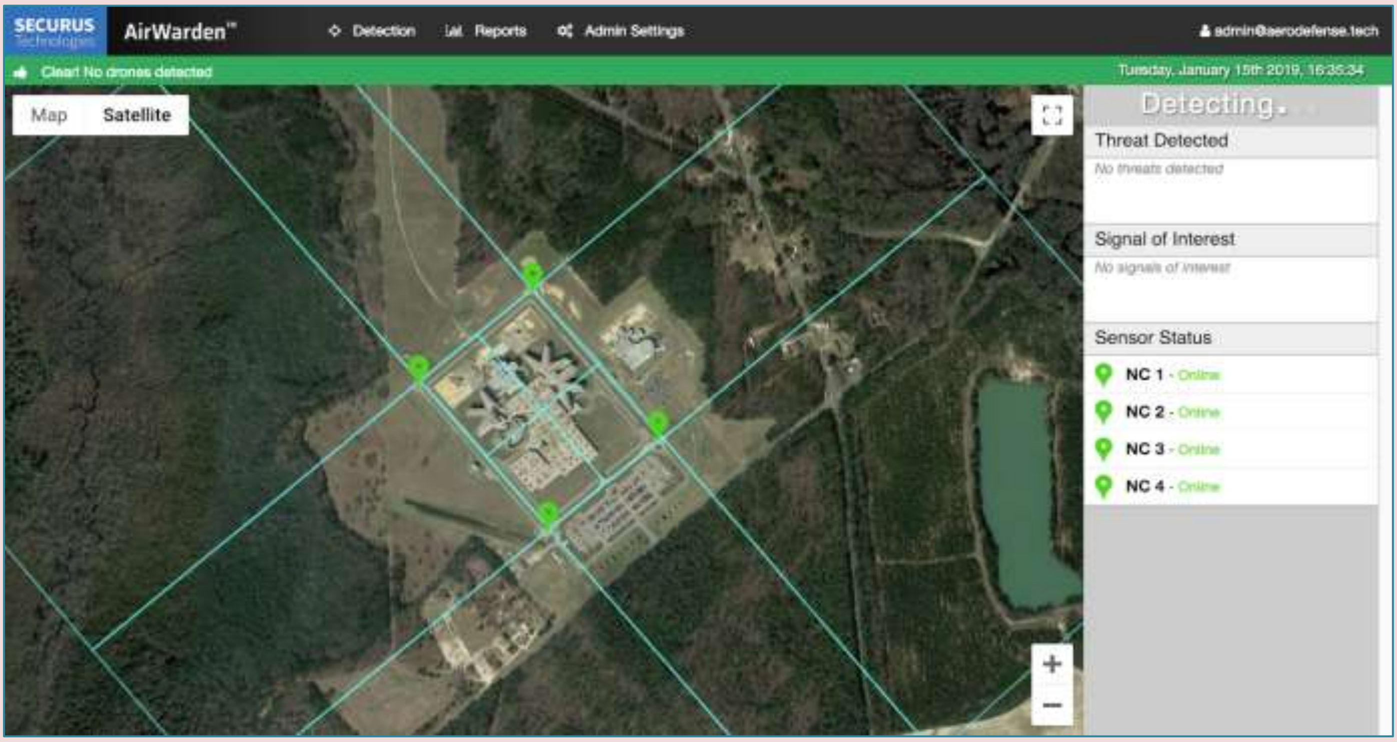
### *Detects in all Weather Conditions*

Because AirWarden™ uses the physical signals from drones to detect and locate, it can operate in all weather conditions. **It is unaffected by lighting, sound, rain, clouds, fog, background clutter (like leaves or trash being blown about by the wind), or line of site** making it suitable for air, ground, and marine UAV detection.

### *Detection Range*

**The system's detection range is equal to the connection range between a drone and a controller.** This means that if a drone and controller can connect up to 1 km apart, AirWarden™ can detect at 1 km or slightly more. If a drone and controller can connect at 5 km, AirWarden™ can detect at 5 km or slightly more.

However, it's important to note that the connection range of a drone and controller can vary greatly. A drone and controller that can connect at 5 km in a desert environment may only be able to connect at, say, 1km in an urban environment. This is because RF signals behave very differently in built up environments. It also means the drone can't fly as far away from the controller in urban areas.



Clear! No drones detected

Tuesday, January 15th 2019, 16:35:34

Detecting...

Threat Detected

No threats detected

Signal of Interest

No signals of interest

Sensor Status

NC 1 - Online

NC 2 - Online

NC 3 - Online

NC 4 - Online

### *System Integration*

The AirWarden™ open architecture allows communication to/from other systems such as your organization's existing alarm monitoring or reporting system.

### *Single Sensor Type*

The AirWarden™ system uses only one type of sensor. This means it has:

- Lower maintenance

- Fewer sensors required
- Less points of failure
- More system redundancy

This results in a lower total cost of ownership.

***Mobile Sensor Options***

While the typical installation consists of four or more fixed sensors, AirWarden™ offers several mobile options:

- **Single Sensor Trailer** – This can be used to detect and evaluate drone threats at a facility before installing a full system
- **Multi-Trailer Network** – Several trailer-based sensors can be networked to provide both detection and location
- **Marine Vessel Sensor** – This can act as a standalone sensor or join a network of fixed or mobile sensors on land.
- **Mobile Vehicle Sensor** – This can act as a standalone sensor or join a network of fixed or mobile sensors, either land or marine based.

T

## The UAV Engine of the Future

Source (+video): https://i-hls.com/archives/95352

Oct 05 – A company pioneering in microturbine technology has recently announced the first flight of its first-of-a-kind **microturbine propulsion system**. Developed by UAV Turbines Inc, the **Monarch 5 engine** showed off its capabilities at Griffiss International Airport. The engine is designed to deliver a reliable and efficient propulsion system medium-sized commercial and military UAVs.

The Monarch 5 engine is planned to replace older and unreliable engines currently used by many UAVs. It offers UAV operators ease of use, remote start, quiet operation, and relatively little maintenance work.

The FAA expects that by the year 2023, the commercial UAV market will triple in size. UAVs will be in high demand for medical, cargo, search and rescue, and transportation needs. In order to effectively support these UAV applications, unmanned aircraft of the future will need to offer much more safety and reliability than current engines. The Monarch engine offers a propulsion system that provides a solution to this problem.

Uasvision.com reports that the Monarch family of engines are also ideal for applications such as ground and auxiliary power, as they can be configured as turbogenerators.

## Drone as Crowd-Management Solution

Source: https://i-hls.com/archives/80869

**January 2018** – India will use drones for both crowd management and infrastructure inspection. As one of the most populous countries in the world, India is interested in crowd-management solutions in public places. The state-owned Indian Railways recently completed a trial in which camera-drones were deployed in three prioritized railroad areas across the country.

A government statement makes it clear the government is eager to test the potential efficacy of standardizing the implementation of unmanned aerial vehicles across the country's railroad stations, particularly during festival seasons.

The project is designed "to enhance safety and efficiency in train operations," and that "it will help in various activities especially project monitoring and maintenance of tracks and other railway infrastructure." In other words, the government has noticed how aerial monitoring via drone could boost the amount of functional data streamed to railroad-monitoring hubs, which would in turn help assess how one could do better at managing and regulating not only crowds, but the infrastructure itself.

According to thedrive.com, the country's festival seasons are a definite motivating factor in implementing these drones. Every year, millions of citizens migrate throughout the country using railroad infrastructure, and amassing useful data as to how to optimize this activity is certainly a rational and affordable response when considering drones as the tool to do so.

The statement mentions plans to expand drone use to more lines and division, as well as "Important Bridge inspections and Monsoon [sic] preparedness."

## Russia Develops Radar to Detect Miniature Drones

Source: https://www.defenseworld.net/news/25645/Russia_Develops_Radar_to_Detect_Miniature_Drones#.XaHqGH9S_IU

Radar developed to detect tiny drones (image: Ruselectronics)

Oct 11 – Russia's Ruselectronics Group has developed a radar station that can detect miniature drones measuring one square foot at a distance of up to 7.5 km, Defence holding company, Rostec said.

Called the target illuminating radar, it can detect and track small-size targets with a radar cross-section of 30 and more square centimeters (one square foot), flying at a wide range of speeds at low and ultra-low altitudes.

"The traditional methods of radar-based detection fail to reliably detect unmanned aerial vehicles with a small reflection surface. The device developed by our Ruselectronics Group successfully accomplishes this task," said Oleg Yevtushenko, Rostec Executive Director.

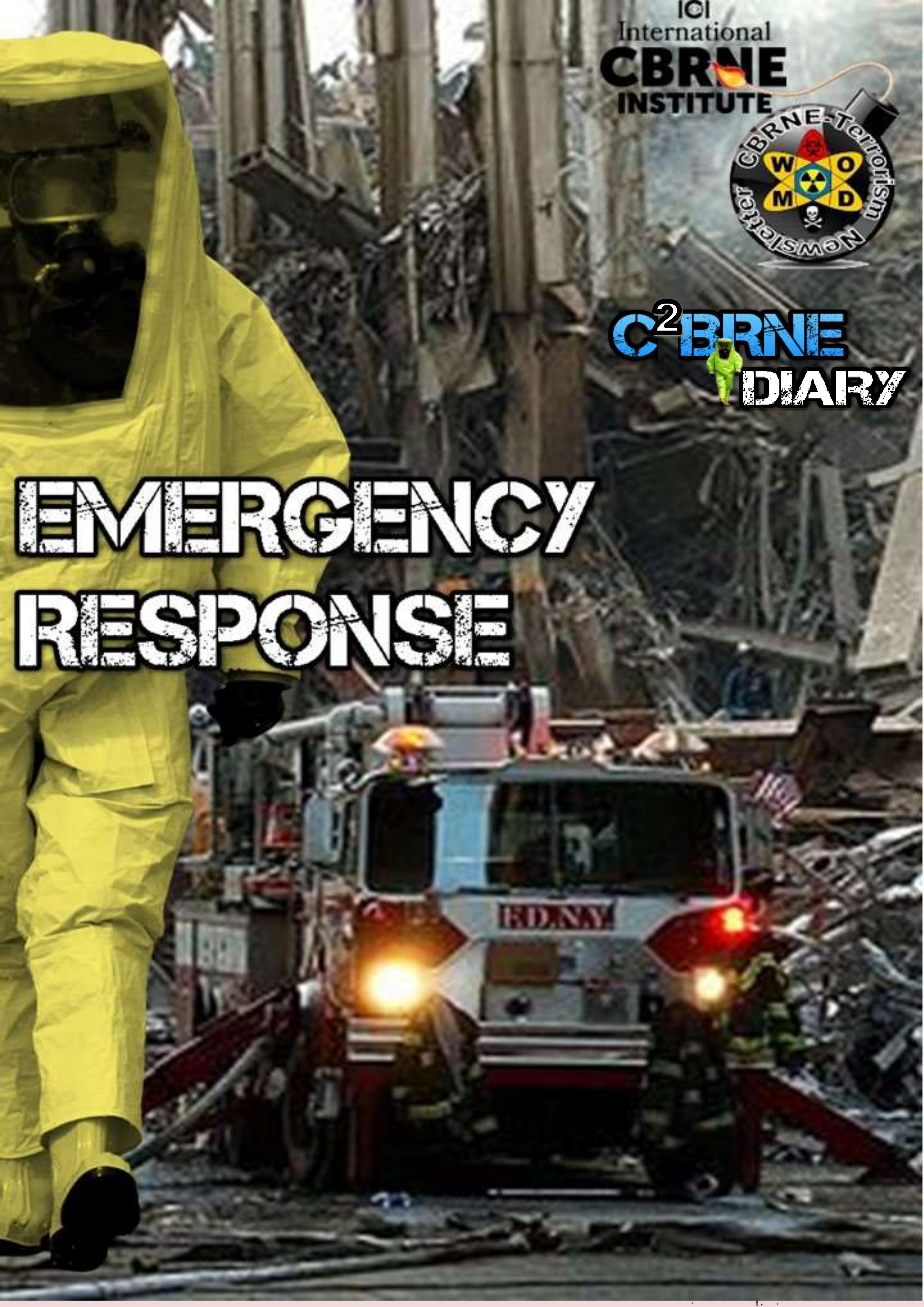
The radar station has been jointly developed by the Salyut Research and Production Association (part of Ruselectronics Group) and the Fakel Design Bureau of Machine-Building. The radar was made using solely Russian components. The first models of the new radar have already undergone field trials, Rostec said.

The station consists of a compact Ka-band multi-channel radar, a rotating device to provide for a panoramic view and a control notebook. The radar can be operated manually and in the automated mode. Upon detecting a target, the station transmits data to an operator's post or a control center.

The Russian air base at Hmeimim in Syria has come under repeated attacks with small drones. In one incident during early 2018, a swarm of tiny drones numbering over a hundred were launched at the base with more than three fourths of them falling prey to Russian Air Defences.

Since then, the base has come under repeated drone attacks which the Russian MoD claims it has successfully repelled in all cases. It is quite likely that the new drone-detecting radar was developed in response to the Russian Army's field experience in Syria and may have been tested there too.

Small-size drones may pose a serious danger as they are capable of conducting surveillance, reconnaissance, carrying explosives or other armament and serving as an attack weapon. They can operate on their own or as part of a whole swarm of drones, Yevtushenko said.



# EMERGENCY RESPONSE

# The Early Years: Shaping a National Stockpile for Preparedness

**By Greg Burel**

Source: https://www.domesticpreparedness.com/healthcare/the-early-years-shaping-a-national-stockpile-for-preparedness/

Oct 09 – In today's emergency response landscape, public health jurisdictions across the United States rely on the Strategic National Stockpile (SNS) when incidents prove large enough or severe enough to deplete medicines and supplies needed to protect communities. In just 20 years, the SNS – now managed by the U.S. Department of Health and Human Services' (HHS) Assistant Secretary for Preparedness and Response (ASPR) – has grown to a $7 billion enterprise poised to respond to a variety of public health threats. These threats include anthrax, botulism, smallpox, plague, tularemia and viral hemorrhagic fevers, as well as emerging infectious diseases, pandemic influenza, natural disasters, and other chemical, biological, radiological, and nuclear incidents. Although predicting the future of any program is challenging, the SNS has evolved from humble beginnings to a formidable component of national security.

Early discussions about establishing a federal stockpile of medical products centered around planning for the year 2000 – commonly called Y2K – amid fears of terrorist attacks significant enough to cause healthcare facilities to run short on supplies. In January 1999, Congress charged HHS and the Centers for Disease Control and Prevention (CDC) with creating a repository of medical countermeasures (MCMs) for use in the event of a chemical or biological terrorist attack on U.S. civilian populations. This repository was initially named the National Pharmaceutical Stockpile.

Cargo containers specially designed for SNS products in the stockpile's early years are still in use today. The shape allows for better configuration for air cargo transport. (*Source:* Strategic National Stockpile, date unknown)

### *Building the Stockpile Piece by Piece*

With a $51 million appropriation and a handful of public health professionals quietly housed in CDC's National Center for Environmental Health, the program expanded systematically to meet Congress' intent to protect the American people. Within one month, the stockpile was augmenting the National Medical Response Team's inventory by providing funds to HHS to procure and forward-position treatments and antidotes for up to 10,000 individuals if a nerve agent release occurred. This effort ultimately became today's CHEMPACK program, a far-forward-placed stock of medicines to respond to chemical nerve agent attacks or incidents involving organophosphorus pesticides.

Using the 1999 HHS Anti-Bioterrorism Operating Initiative as a starting point for which threat agents to address, stockpile personnel developed concepts for the 12-hour Push Package – a broad spectrum of medicines and supplies for an unidentified threat – and vendor-managed inventory. They began meeting with external subject matter experts to review potential threats and recommended treatments. At the same time, CDC hosted a similar meeting with its Bioterrorism Preparedness and Response Program concerning biological threat agents. From these meetings, stockpile personnel initiated the development of the early formulary and the medical materiel requirements deemed necessary to protect the United States from a growing list of threats. By September 1999, the stockpile finalized its first total requirements list. Then, on 27 December 1999, the stockpile readied its first 12-hour Push Package to respond to a potential Y2K terrorist incident.

The one-year mark proved a busy time for the budding stockpile. The program established transportation contracts to move stockpiled assets, if needed, and created its Program Planning, Response and Training Team to work with HHS emergency coordinators in the field to ensure planning efforts were well-coordinated and integrated with activity at the state and local levels. Personnel were writing and establishing initial development contracts for new smallpox and anthrax vaccine and new botulism antitoxin to include in the stockpile, and they served as project officers for the development of these pharmaceuticals.

Over time, stockpile staff continued to adjust the formulary and build and configure the 12-hour Push Packages. They worked with warehouse vendors and transportation partners to establish some early processes and procedures that have been tested and refined for use by the SNS today. In September 2000, the Food and Drug Administration (FDA) granted approval for the stockpile to participate in the FDA/Department of Defense (DoD) Shelf-Life Extension Program (SLEP). Originally, SLEP was viewed simply as a method to save money. Today SNS continues to use SLEP to maximize returns on investment by holding MCMs for as long as possible while ensuring stability and potency. SLEP also allows the SNS program to build up stock over time to reach the full quantities needed to protect Americans. This benefit is especially important because some stockpiled products are produced in such low quantities and have such short shelf life that otherwise would prevent the program from meeting its overall preparedness goals.

### *Testing Stockpile Response Capabilities*

One of the stockpile's first collaborative efforts with emergency response planning was working with the New York City Department of Emergency Operations and the Federal Aviation Administration. On 11 September 2001, one month after the three organizations staged their first full-scale exercise, an early morning attack on the World Trade Center and the Pentagon confirmed the country's worst fears. The stockpile was called into action as part of the government's immediate response to the deadliest terrorist attack on U.S. soil. Within seven hours of the order to deploy to New York City, the stockpile delivered by both ground and air cargo a 12-hour Push Package of medicines and supplies as well as ventilators, ancillary supplies, and burn-and-blast supplies. The delivery was met by a response team of stockpile experts called a Technical Advisory Response Unit, which was able to deploy to New York via chartered aircraft. On that day, the only other non-military flight in U.S. airspace was Air Force One.

On the heels of 9/11, the stockpile was called upon again to respond to a series of anthrax attacks and subsequent inhalation anthrax cases in the United States. Using its vendor-managed inventory capability, the stockpile responded to 65 separate drug requests for post-exposure prophylaxis, all of which were filled within an average of five hours from initial contact to delivery.

The events of 2001 shed light on the need to strengthen national public health preparedness and response efforts. Immediately following these two responses, the stockpile rapidly expanded with both inventory and appropriations. The HHS secretary directed the stockpile to increase its capacity to provide full post-exposure prophylaxis for anthrax for up to 12 million people. The number of 12-hour Push Packages grew from eight to 12. Congress appropriated $643 million for the stockpile in FY 2002 to fund these initiatives as well as to run a state preparedness grant program, to establish packages of chemical nerve agent antidotes and antibiotics, and to grow the program to a team of 79 personnel.

### *Expanding the Stockpile for an All Hazards Approach*

During the next two years, the stockpile developed and solidified partnerships across the federal interagency community as well as with private warehouse and transportation organizations. The program was granted responsibility for the transport of existing and future supplies of botulism antitoxin and anthrax vaccine as well as for storing and transporting the nation's current and future supplies of smallpox vaccine. Stockpile experts were looking to improve speed and efficiency and worked with private sector partners to design the first specialized cargo containers for the 12-hour Push Package. In this timeframe, the stockpile also created a pilot program called CHEMPACK, which placed federally owned and managed nerve agent antidotes in forward locations selected by local authorities to integrate with their hazardous material response plans. Fast forward 20 years and the SNS remains ready today to respond to chemical nerve agent incidents through CHEMPACK, which has forward placed more than

1,900 containers of antidotes at more than 1,300 locations across the United States and its territories.

While the stockpile was expanding its mission and role in storing and transporting critical products for national health security, staff was developing a comprehensive training and exercise program to ensure state and local health jurisdictions were ready to receive, distribute, and dispense these products in an emergency. Internally, the program was implementing a professional inventory and financial tracking system to provide a real-time capability to manage SNS assets and mission readiness. With continual updates, this system is still used by the SNS to integrate financial and inventory information and to ensure inventory accountability, reconciliation, and financial reporting.

On 1 March 2003, the Homeland Security Act of 2002 took effect, and the stockpile was transferred from HHS to the Department of Homeland Security (DHS). At the same time, the National Pharmaceutical Stockpile was renamed the SNS to reflect its evolving formulary to store more than just pharmaceuticals, but also medical supplies and devices earmarked for public health emergencies. Additionally, formulary governance in the early years was established by the stockpile via the creation of the Intragovernmental Committee, chaired by CDC's associate director for science and made up of members from various federal organizations including HHS, CDC, FDA, DoD, and DHS.

Specialized cargo containers were designed for the 12-hour Push Package to improve delivery speed and efficiency. (*Source:* Strategic National Stockpile, date unknown)

By the close of 2003, the stockpile program had increased staffing to 120 employees and contractors. The staff grew with specialists in public health, emergency response, and, importantly, now professional medical logisticians. The annual appropriation hovered around $300 million, there were a dozen 12-hour Push Packages in 10 sites across the nation, and the stockpile was positioned to provide up to 12 million people with a full 60 days of post-exposure prophylaxis if faced with a large-scale anthrax response. Also, the stockpile added 400,000 doses of antiviral drugs to its formulary in preparation for a pandemic influenza. This was the first procurement for the formulary beyond the original mission focused on terrorist incidents and represented an entirely new and different scope.

When Project BioShield – a program to expedite late-stage development and procurement of next generation vaccines and other MCMs against a range of potential terrorist weapons – became law on 21 July 2004, the SNS returned to HHS. Under this new legislation, the SNS was designated as the procurement and storage partner for Project BioShield and would manage the delivery of products in a bioterrorist attack or other emergency. The SNS remains with HHS today, although the program transferred from CDC to its current place in ASPR in October 2018.

In the program's first five years, the SNS grew from a small organization with a modest budget and a handful of staff to a robust and critical piece of federal preparedness and response. Real-world incidents tested the stockpile's capabilities, and state and local jurisdictions worked in concert with stockpile experts on major planning initiatives. These early achievements set the course for the next 15 years as the SNS evolved to broaden its focus to serve as the nation's resource for protecting the public's health.

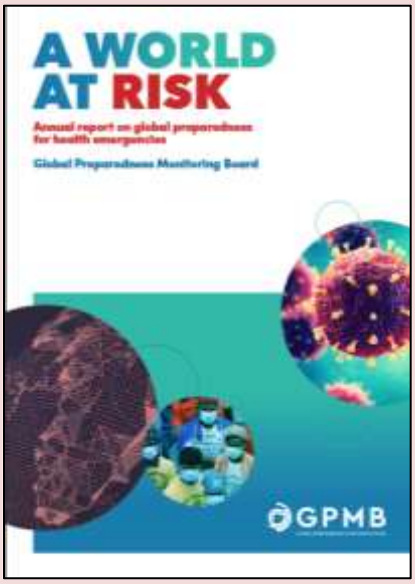
***Greg Burel*** *is director of the Strategic National Stockpile, managed by the Department of Health and Human Services' Assistant Secretary for Preparedness and Response. As head of the nation's largest stockpile of medicines and supplies available for emergency use, he is a leading expert on medical supply chain management in the United States. With more than 35 years of civil service, he has risen through the ranks of the federal government, beginning his career at the Internal Revenue Service and serving in leadership roles in both the General Services Administration and the Federal Emergency Management Agency. In 2006, he assumed the helm of Strategic National Stockpile operations. He was awarded the Samuel J. Heyman Service to America Medal for Management Excellence and selected as a National Academy of Public Administration fellow in 2016.*

**Significant contributions to this article were made by:**

***Steve Adams*** *is the SNS deputy director. He joined SNS at its inception in January 1999 and has played an integral role in the assisting state and local jurisdictions in planning for and implementing responses to large-scale public health emergencies. Prior to joining SNS, he held roles at CDC providing direct assistance to the states for STD/HIV prevention and control efforts and managing environmental research projects to quantify the health impact on humans during the Cold War nuclear weapons production era. He holds a bachelor's degree in economics/political science from The Ohio State University and a Master of Public Health from the University of North Carolina at Chapel Hill.*

***Susan E. Gorman*** *is a licensed pharmacist and board-certified clinical toxicologist who serves as associate director for science and chief of the SNS Science Branch. An original staff member of the SNS, she oversees the formulary and provides technical and scientific advice on all SNS pharmacological and toxicological issues. She earned a Bachelor of Science in pharmacy from Duquesne University, a Doctor of Pharmacy from the University of Maryland, and completed a postdoctoral residency in emergency medicine and toxicology at the University of Illinois at Chicago. She also earned a Master of Science in biosecurity and disaster preparedness from the St. Louis University School of Public Health. Prior to joining the SNS, she was assistant director for the Georgia Poison Center where she continues to serve as a toxicologist. She is actively involved in the American Board of Applied Toxicology and is a fellow of the American Academy of Clinical Toxicology.*

***Stephanie M. Bialek*** *is the SNS Stockpile Communication Services Section chief. She has 20 years of public relations and communications experience in government, academia, and health sciences and joined the federal government in 2010 to provide communications expertise and strategy for the SNS. She holds both a bachelor's and master's degree in journalism and mass communications from the University of Georgia.*



A WORLD AT RISK

Annual report on global preparedness for health emergencies

Global Preparedness Monitoring Board

GPMB

## A World at Risk: Annual Report on Global Preparedness for Health Emergencies

Source: https://apps.who.int/gpmb/assets/annual_report/GPMB_annualreport_2019.pdf

Oct 07 – The Global Preparedness Monitoring Board explores and identifies the most urgent needs and actions required to accelerate preparedness for health emergencies, focusing in particular on biological risks manifesting as epidemics and pandemics. The Board identified seven actions for implementation to prepare for pressing threats.

# Protecting critical infrastructure

Source: http://www.homelandsecuritynewswire.com/dr20191015-protecting-critical-infrastructure

Oct 15 – Energy, water, food, fuel, information, transportation – ensuring a supply of these essential services and commodities is vital for a properly functioning society and economy. So essential, in fact, that we only realize their importance when suddenly they are no longer there. The infrastructure and systems that supply us with these assets are increasingly connected and, for this reason, highly vulnerable to natural disasters, accidents and criminal or terrorist attacks.

Fraunhofer says that in response, the Fraunhofer research institute is devising solutions and strategies to safeguard our critical infrastructure.

### Critical Infrastructure Energy Supply

Electricity is the power that drives modern technological society. Earlier this year, inhabitants of the Köpenick neighborhood of Berlin were confronted with what it means when the supply suddenly fails. On 19 February shortly after 2:00 p.m., a major outage plunged the district into darkness. Streetcars ground to a halt. Stores, restaurants, schools and kindergartens were forced to lower the shutters. Stoplights went out, and the police had to direct traffic in order to tame the chaos on the roads. There was no district heating or hot water, because cogeneration plants were forced to shut down. One hospital, despite having an emergency power supply, had to transfer its ICU patients to another clinic. The phone lines went dead – as did all cell networks, since the radio masts require electricity to function. All in all, it took 30 hours to remedy the problem, caused by cable damage, during which time 30,000 households were without power. The synchronous grid of Continental Europe is one of the world's most reliable electricity networks. Outages of this duration are a rarity, but there is no absolute safeguard, and power failures can happen any time and any place.

Energy infrastructure is part of what is known as critical infrastructure. If any such infrastructure is compromised or destroyed, this has serious implications for the functioning of society. The rapid pace of digitalization means that more and more systems – some completely heterogeneous – are connected to one another. This makes them more vulnerable to disruption. Within this complex nexus of interdependencies, the failure of a single element or system can quickly snowball and trigger an outage in a related supply network. Critical infrastructure therefore requires special protection and must be safeguarded against all kinds of danger: natural disasters, accidents, technical or human error, criminal activity.

### Cyber attacks on Critical Infrastructure Operators

The WannaCry ransomware attack first manifested itself on 12 May 2017. It also impacted private individuals, but those principally affected in Germany were large organizations and facilities such as railroad operator Deutsche Bahn and hospitals. WannaCry infected computers with a so-called ransomware cryptoworm, which encrypted data and only decrypted them following payment of a ransom in Bitcoin. What made WannaCry especially treacherous was that it spread from one computer to another without any action on the part of users. Germany's Federal Office for Information Security was still receiving reports of attacks more than six months later. All in all, over 200,000 computers in 150 countries were infected.

Industroyer, also known as CrashOverride, was a malware that caused a major power outage in the Ukraine capital, Kiev, in 2016. It enabled hackers to hijack the process control systems of Ukraine's power grid. Although it principally targets power utilities, this sophisticated and highly dangerous malware is designed to attack industrial control systems in any sector whatsoever. Investigators therefore concluded that the hackers evidently had substantial funds and resources at their disposal and that their long-term goal was to sabotage industrial companies and critical infrastructure.

### Research and Development for Enhanced Cybersecurity

The importance of IT security continues to grow, not least in the realm of critical infrastructure. In the past, such systems were largely operated as stand-alone facilities and, as such, well monitored and easy to control. Today, digitalization has interconnected them, with the result that they are no longer isolated and insulated against attack. Naturally, this also means they can now be remotely accessed, and their data retrieved for analysis. And this connectivity creates a host of openings for new research and development. For example, technology is required to ensure efficient monitoring and reliable operation of critical infrastructure as well as a rapid response in the event of problems. But it also generates risks: key facilities and processes can be manipulated, and critical infrastructure can be made to crash with devastating consequences for civil security and the supply of essential services.

### Analytic Tools for Evaluating Security in Critical Infrastructure for Specific Sectors

Fraunhofer says thatfor many years now, the Fraunhofer Institute for Applied and Integrated Security AISEChas been carrying out research and development projects with and on behalf of operators of critical infrastructure

on the regional, national and European level. Such projects focus on the development and systematic implementation of security concepts specially tailored to the specific requirements of critical infrastructure. Many operators of critical infrastructure simply lack the expertise and the human resources to properly assess the IT security risks they face and to determine the appropriate measures on the basis of a cost-benefit analysis. This is where a lot of Fraunhofer AISEC projects begin.

Within the EU-funded SPARKS (Smart Grid Protection Against Cyber Attacks) project, for example, Fraunhofer researchers have teamed up with a number of municipal utilities in order to develop an easy-to-implement, IT-supported methodology for use with, in particular, smart grids. This enables power grid operators to practice systematic risk management, including threat identification and impact assessment.

The ECOSSIAN (European Control System Security Incident Analysis Network) project – itself part of the European Program for Critical Infrastructure Protection (EPCIP) – focused on the development of key technology and reference architecture for delivering secure critical infrastructure. This was designed to enable preventive services such as early warning and anomaly detection across multiple locations, and to improve emergency and disaster management. Processes developed in the course of this project include AI-driven anomaly detection methods and multi-party protocols for the secure transfer of sensitive data between infrastructure operators, thereby enabling them to share general situational awareness information without having to reveal confidential infrastructure details. In addition, researchers devised and implemented hardware-based procedures for authentication and data-protection compliance in conjunction with smart meters and smart meter gateways. This system has been tested in various scenarios involving critical infrastructure in the financial, transportation and energy sectors. Fraunhofer AISEC was also involved in drawing up recommendations for future security standards for smart grids and for an early-warning system that enables information-sharing on current threat levels without the requirement to reveal sensitive data from the jeopardized facilities.

In the course of such projects, Fraunhofer AISEC has acquired a wealth of expertise in critical infrastructure. This is now to be made available to small and medium-sized operators of critical infrastructure, who often face major organizational hurdles in terms of ensuring IT security. This problem was also the focus of the MoSaIK project, which investigated model-based security assessments of ICT-reliant critical infrastructure. Funded by the Federal Ministry of Education and Research (BMBF), the project spawned a number of innovative approaches that enable operators without specialized IT security know-how to analyze the IT security of their systems.

### National Research Center for Applied Cybersecurity CRISP

Recent advances in areas such as artificial intelligence and quantum technology are generating exciting new opportunities. Yet they also entail risks, which in turn pose major challenges for cybersecurity research. At Germany's National Research Center for Applied Cybersecurity CRISP in Darmstadt, some 450 scientists are now investigating how best to safeguard critical infrastructure and provide long-term protection for IT systems. CRISP is a research facility established by the Fraunhofer-Gesellschaft for its two Darmstadt institutes, the Fraunhofer Institute for Secure Information Technology SIT and the Fraunhofer Institute for Computer Graphics Research IGD. It also involves the participation of TU Darmstadt and Darmstadt University of Applied Sciences. CRISP is funded by the Federal Ministry of Education and Research (BMBF) and the State of Hesse.

# What the Swedes learned from the terrorist attack in Stockholm

**By Ingrid P. Nuse** (*based on an article by Bård Amundsen*)

Source: https://sciencenordic.com/forskningno-society-society--culture/what-the-swedes-learned-from-the-terrorist-attack-in-stockholm/1554596

June 2019 – The incident was terrible. **Five people were killed and ten injured when a terrorist drove a truck into the crowd in central Stockholm on 7 April 2017.** Yet, it could have turned out much worse when terrorist Rakhmat Akilov hijacked a brewery truck and drove about 500 meters at high speed down the popular pedestrian street of Drottninggatan – through a human sea – on a Friday afternoon.

## Police were prepared

As the truck tore along the pedestrian street, it crashed into several obstacles and made lots of noise. This enabled many people to dash to safety.

Fortunately, the terrorist was not particularly competent. A suicide bomb he brought with him failed to detonate, and instead he lit himself and the truck on fire.

Bildetekst: The truck hijacked by the terrorist began to burn when he failed to detonate a suicide bomb. (Photo: Maja Suslin / Sweden Out / NTB scanpix)

The Swedish police also had luck on their side.
Just a little before 3 pm on Friday afternoon, Sweden's police officers were wrapping up a week-long anti-terrorist conference at the Police Academy in Stockholm. There was no lack of leadership present.
On top of that, the police shift change took place at 3 pm in central Stockholm, doubling the number of available law enforcement officers.
And, the whole police force had recently been trained to deal with terrorist attacks.

## Downtown full of people

Per Engström is chief superintendent and a specialist in terrorist attacks at the Swedish Police in Stockholm. During the recent national emergency preparedness conference at Elverum, he told Norwegian emergency response leaders what Swedish police and other authorities had learned from the Stockholm terrorist attack two years ago. The conference was hosted by INN University, the Norwegian Police University College and the Norwegian Defence University College.
In contrast to the chaos that reigned when Norway was hit by a well-planned terrorist attack against Oslo and Utøya on 22 July 2011, Sweden’s newly implemented counterterrorism measures turned out to function well during the Stockholm attack.
The city centre is full of people on this fine-weather afternoon. As with the attack in Oslo, information from the public starts pouring into the police station in Stockholm.

## Everyone on the scene in 15 minutes

The first reports are that a major traffic accident has occurred. Then, reports of shooting come in from several different locations. The situation is chaotic.
Standing orders for Swedish police are that if any suspicion of a terrorist act is present, that is what they prepare for.
Police with heavy weapons immediately move out. The national Swedish emergency force are on the scene in Stockholm’s city centre within ten minutes. Police in other cities are notified to secure areas where large numbers of people are gathered.
Everything and everyone can be in place in as little as 15 minutes.
The Swedish police also experienced how, with the help of camera surveillance in downtown Stockholm, they could quickly identify the fugitive terrorist and initiate an intensive hunt for Akilov. He was caught at 8 pm that night.

## One decision maker

Until four years ago, 21 different public authorities in Sweden dealt with terror security.
Now just a single authority, with a single leader, decides – the Chief of Police.
"This gives us completely different options for dealing with terror," said Engström.
The Swedes also removed other bureaucratic barriers. Previously, a Swedish police officer needed to gain approval to act from as many as 12 higher level officials. Today, Swedish police work within a much simpler structure that is the same for all police officers across the country. The Swedish Armed Forces follow a similar format.
On 7 April 2017, the Swedes saw the value of having cleaned up their bureaucracy and cumbersome decision-making process.

## Wrong to clear out people from city centre

In retrospect, Swedish police recognize that clearing Stockholm's city centre of people during the attack might have been a poor decision.
With buses and trains no longer running after the terrorist attack, several hundred thousand people started walking home.
**“When city people need to find their way home on their own, they’re often not very good at it. They get onto the tracks that they normally ride and follow them until they reach the station where they usually get off the train or metro,”** Engström says.
This wasn’t safe. **Now Swedish police are more aware that they themselves can trigger dangerous situations in a terrorist attack.**

### First officer on the scene in charge

Swedish police patrols are required to uphold a guideline stating that the first police officer on the scene takes command of the operation.

“On Drottninggatan the first patrol on the square took charge initially since it had the best overview of the situation. When other leaders arrived, they took over once they were briefed by those who came first,” says Engström.

“If we don’t run things this way, we risk creating passivity throughout the system,” he says. “Initiative and trust are key when time is of the essence.”

The Swedish terrorist specialist also believes the police have to allow themselves to make the occasional mistake. In critical situations, it may be **more important for an officer to act quickly than to do everything right.**

### Danger of radicalization

**Society shouldn’t overreact to terror.** If we do, we risk having more individuals becoming radicalized. This is just what terrorists want.

“This isn’t simple for law enforcement – or politicians – to deal with. It’s easy for politicians to think that we have to be tougher or impose stricter penalties,” Engström says.

“But,” he reminded the officers at the Elverum conference, **“terrorists, whether they’re on the right or left of the political spectrum, grow stronger when they face opposition.”**

**EDITOR’S COMMENT:** One good point from this article: “An officer should act quicly than choose to do everything right”. And one question: what is the meaning of the last sentence of this article? Until now, I thought that when terrorists face opposition, they change targets’ level or move to another region or country with less security. And how the Swedish expert defines “over-reaction to terrorism”?

Okay, well, you may want to re-evaluate your company's disaster program.
IN CASE OF EMERGENCY BREAK GLASS

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

$^2$BRNE DIARY

# ASYMMETRIC THREATS

# What will the world look like in 2050?

**By Katharine Gammon** (University of Southern California)

Source: https://phys.org/news/2019-10-world.html

It's 2050, and another balmy day in Los Angeles. A young woman steps outside and puts on her air filtration mask. The air is thick with smog, which aggravates her asthma. As she hurries to get into an air-conditioned, self-driving car, she wonders if the temperature will finally dip below 90 degrees today—for the first time this November.

One hundred miles northwest, a third-generation vineyard owner finishes packing up his family and saying goodbye to the land. It has become too hot to produce his Pinot Noir grapes anymore—all the nearby vineyards now grow wheat to fit the hotter weather. He is heading to Oregon's cooler climes to start again.

Meanwhile, on the coast, a boy and his grandfather walk along the beach, careful not to touch the water. A telltale bright red stain in the waves warns them of a toxic algal bloom. The water level has risen a little bit over the years, and the grandfather wonders how much land will still be above water when his grandson reaches his age.

By 2050, climate change and its reality will no longer be up for debate. The subtle signs we're starting to see around us will be more pronounced, scientists say, and their impact will be easy to spot in everyday life. The warming trend can feel overwhelming to understand, much less confront—especially with so many factors believed to affect how the planet is changing. But there's good news: Humanity has tools to shape our future, USC researchers say, and some are already working in places across the globe.

**Weather in 2050: Hot, Hotter, Hottest**

"The global climate is like an aircraft carrier; turning it around is slow," says Julien Emile-Geay, an associate professor of Earth sciences at the USC Dornsife College of Letters, Arts and Sciences. "If we don't start now, we'll be stuck in a very tough place in 2050." As an expert in climate dynamics, Emile-Geay has devoted his career to understanding what's coming for the planet.

The 20th century was Earth's warmest period in nearly 2,000 years, he says. Data he examined from a wide variety of sources, including ice cores, tree rings and coral reefs, show that the warming trend began after the industrial revolution—the 1850s. For most of the globe, the warmest temperatures have come within the past 100 years. He agrees with the broad scientific consensus that if the trend continues—and physics says it will—sea level rise and droughts could render areas of the planet unsafe or even uninhabitable. Refugees leaving their homes for livable climates could lead to geopolitical instability. The World Bank predicts as many as 140 million people could be displaced by 2050.

In the Southern California of 2050, Angelenos could spend a quarter of the year sweating it out in temperatures of 90 degrees or more. That's 95 days of dangerously hot weather a year, significantly higher than the 67 days we see in 2019. Air conditioning will raise energy bills, but researchers anticipate costs to health as well. When temperatures spike, deaths rise too, says USC Dornsife environmental economist Paulina Oliva. Research suggests that uncomfortable heat stresses the body, increasing risk of heart problems and stroke, especially in the elderly. High temperatures have also been linked to an increase in pre-term births and infant mortality. Studies on students and stockbrokers and other workers have shown that temperatures above 80 degrees slow down thinking processes, making it harder to focus and make decisions. These problems disproportionately harm people with the fewest resources to deal with the discomfort and health risks.

Several researchers raise the alarm that any climate plan has to address our society's systemic inequalities. "The pregnant mother who doesn't have a car is going to have to walk to public transportation and expose her baby to these high temperatures in utero," Oliva says. "Even though we do have means to adapt, wealthier people are going to be better able to adapt than poor people."

The climate is likely to become extreme in several ways, including an increase in both fires and floods, rainy days and droughts, cold snaps and temperature spikes. In California, unpredictable fluctuations could devastate the agricultural sector, which accounts for an eighth of the country's agricultural production. It's likely that some crops, like grapes and apples, could only be grown farther north. Farmers who opt to stay in California might switch products—say, from corn to wheat—to better match the new climate reality.

**Environment in 2050: Something in the Air**

We don't need to time travel to 2050 to imagine the impact of climate change on the air. In spring 2018, Los Angeles' air quality exceeded federal safety levels for 87 days, says Antonio Bento, director of the USC Center for Sustainability Solutions and professor at the USC Price School of Public Policy and the Department of Economics.

When temperatures rise, so does "bad" ozone. Don't confuse this ozone with the ozone layer in the upper atmosphere, which shields Earth from the sun's radiation. Bad ozone forms at ground level when pollutants from cars and other industrial sources react to sunlight. "Ozone is dependent on temperature, sunlight and heat waves," Bento says. "That means that higher heat brings on worse air quality."

In Los Angeles, it's one of the biggest reasons climate change endangers human health: More days above 90 degrees means more ozone, more asthma, more lung damage and more deaths. By 2050, if climate mitigation strategies and air pollution regulation don't halt rising temperatures, the skies of Los Angeles could revert to the soupy smog of the 1970s, Bento says.

That was a time before the Clean Air Act, when more than half the days in the city had unsafe levels of pollution. Angelenos couldn't see the mountains through the thick smog. "In part due to climate change, many of the benefits that we have achieved are quickly being undone," says Bento, who recently published research showing how a rollback of vehicle emissions standards would be dangerous. "We have arrived at a point where for us to prevent major damage, we would have to rely on adaptation."

For a long time, Bento was sure that leaders would take up the urgent issue of climate change based on a global consensus, so he focused his policy recommendations on broad, far-reaching solutions. But recently, he shifted his thinking. He's increasingly examining how local policy changes could benefit countries and states.

Reducing greenhouse gas emissions would not only reduce health problems related to air pollution impacts, but it also could bring along other benefits, like spurring technological innovation, improving the reliability of the power supply by diversifying energy sources, reducing fuel costs and boosting employment.

"If we account for these co-benefits of climate action, it's in the best interest of countries to act independently of what others are doing," he says. "And it's in the best interest of California to implement climate policies, because even if others don't act, we will get these additional benefits."

Bento has worked with the city of Los Angeles and other local governments in the U.S. and abroad to craft climate-mitigation strategies. By 2050, 68% of the world population will live in cities, up from 55% today, so the actions of municipal and regional governments are critical. "If cities become the unit at which we do climate policy, we end up with comprehensive climate legislation even without national leadership," he explains. "That's the future of our cities and the environment. It really depends on how we communicate the climate crisis to the public."

Bento is also researching ways to create optimal carbon pricing, which shifts responsibility back to the producers of greenhouse gas emissions. Carbon pricing works by estimating the external cost of a company's greenhouse gas emissions and issuing a tax. This puts the financial burden on businesses instead of on local and vulnerable communities, while also financially incentivizing companies to opt for cleaner technology.

"It's frustrating, because we have known how to do these things for decades, but we're not yet doing them," he says. "As we move toward 2050, we have to adapt in ways that don't put more burdens on communities that are vulnerable already."

**Oceans and Water in 2050: Beneath the Surface**

More than 90% of the warming created by humans since the 1970s has been absorbed by the oceans. And just as on land, there is a shift underway in the sea that will affect the global oceans of 2050, says David Hutchins, a USC Dornsife professor of marine and environmental biology. "The ocean is warming, acidifying, losing oxygen and being overfished and choked with pollutants ranging from nutrients to plastic," he says. "Nearly the entire marine environment is in flux right now."

Numbers of large predator fish have plunged, and about half of the world's coral reefs have been lost to bleaching caused by warming temperatures, Hutchins says. By 2050, most reefs may have vanished, according to a National Oceanic and Atmospheric Administration report.

Some governments, like Australia's, are taking action, trying to protect reefs by reducing other threats to coral such as dredging and runoff from land. And scientists are identifying and growing types of resistant coral that may be better able to cope with warm water.

In Southern California, people will have to deal with rising sea levels as polar ice continues to melt. Some of California's most valuable coastal real estate may go underwater later this century, Hutchins says. Another aquatic impact: unwelcome bursts of harmful algal blooms that thrive in warmer waters and poison human and marine life.

"The climate emergency is happening now, today, not sometime in the far-off future," Hutchins says. "I'd like people to think about the kind of world we want to leave for our children and grandchildren, and to make our choices—from the way we live to the leaders we vote for—with that in mind. There is literally no time to lose."

Water distribution across the planet is a challenge, too: By 2050, more parts of the world will go through droughts, while others will be deluged with floods. It's hard to believe that a place like Phuket, Thailand, could suffer from a water shortage when about 100 inches of rain falls there per year, says Amy Childress, the Gabilan Distinguished Professor in Science and Engineering at the USC Viterbi School of Engineering. But right before the monsoon season begins, the reservoirs can get very low as reserves from the last monsoon season dwindle.

Areas like Phuket can't wait until 2050 to figure out a sustainable plan for their water supply; they need to plan now. That goes for California, too.

"In Southern California, we are simultaneously preparing for the drought scenario—alternative water supplies, expansion of the water supply portfolio—and the flood scenario, which includes dam maintenance and flood risk management," Childress says. Then there's the water we need to drink.

In the future, more people will depend on drinking water that's been recycled. The idea of drinking water that's "secondhand" from wastewater or other human uses is off-putting to many, maybe because the public prefers to think it should come from a pristine mountain stream, Childress says. That's not realistic, even today. "Typically, our drinking water comes from a source that was used upstream by others and is being reused by us," she says. "We have regulations in place to ensure that this practice is safe."

In addition to recycled water, Californians of 2050 will rely more on desalinated seawater, she predicts. Desalinating seawater is usually the last choice for a region's water supply because the process is so energy intensive, but it is a reliable supply that will become more useful in the years to come. Right now, 12 desalination plants operate in California, but ocean filtration systems operate in more than 120 countries and are especially critical in countries in the Middle East and the Mediterranean.

**Lifestyle in 2050: Changes at Home**

For a long time, Bento says, academics were so concerned with getting their climate change models right—and assessing broad existential threats—they failed to communicate how changes are already affecting daily life. That's no longer the case.

Commuting, travel, shopping, eating, housing—they all may be transformed by 2050 as people come to understand their effect on the planet. Bento, for one, already drives an electric car, but he questions whether he needs one at all. "It was just such an unquestioned expectation for me, that I would get a car as a teenager," he explains. "And when electric vehicles arrived, I thought I was doing something for the environment. But now we are moving into new models. "If we could move to a system that is more efficient, and that integrates density of development with public transit and car-sharing, perhaps we could have much better outcomes."

Earth scientist Emile-Geay has cut travel to most academic conferences. Instead of flying several times a year to meet other scientists—trips that leave a big carbon footprint—he chooses just one conference to attend. "I started to ask myself: What am I getting out of these conferences and what do others get from my presence?" he says. "And so I prioritize small, more intimate gatherings where there's a real exchange of ideas."

Similarly, when people travel for pleasure in the future, more could opt to use low-carbon transportation to explore their own regions instead of taking trips to faraway countries. Besides changing his travel habits, Emile-Geay also has stopped eating meat, and tries to choose foods grown as locally as possible.

"Some like to pit a healthy planet against a healthy economy," he says. "That's a false dichotomy. It's in our power to build an economy centered on ecological and humanistic values instead. The laws of physics won't change, but our laws can."

A possible low-carbon future, he says, could include less driving and more local focus, leaving more time with family and friends, which creates safer communities with stronger social bonds.

Oliva sees promise for slowing climate change, as more governments around the world seek immediate action. "And also, we're not sitting and waiting around here," she says of California. "There's quite a bit of progress being made at the state and local level." She believes the state is a model for how sustainability and business can work together. "We're showing that these climate policies really are not going to be as costly as they're being portrayed," Oliva says. "California was an early adopter of stricter greenhouse gas policies and businesses didn't all flee the state. So that gives me hope."

Emile-Geay sees an opportunity for a more civic-oriented and equitable future. Supply chains could be more efficient. Instead of shoppers ordering a product from across the Pacific, a neighborhood 3-D printer could fabricate the items people need and a bicycle courier could ferry it to their homes. He even imagines climate change spurring people to rethink the way they live.

"It's like somebody being given a diagnosis of a terminal illness. It's a wake-up call. Suddenly it makes you ask: "What am I doing with the rest of my time on Earth?"" he says. "That could be the kick we need to re-engineer our social networks and get more local, more focused on community, which is what many psychologists and social scientists say is good for us anyway."