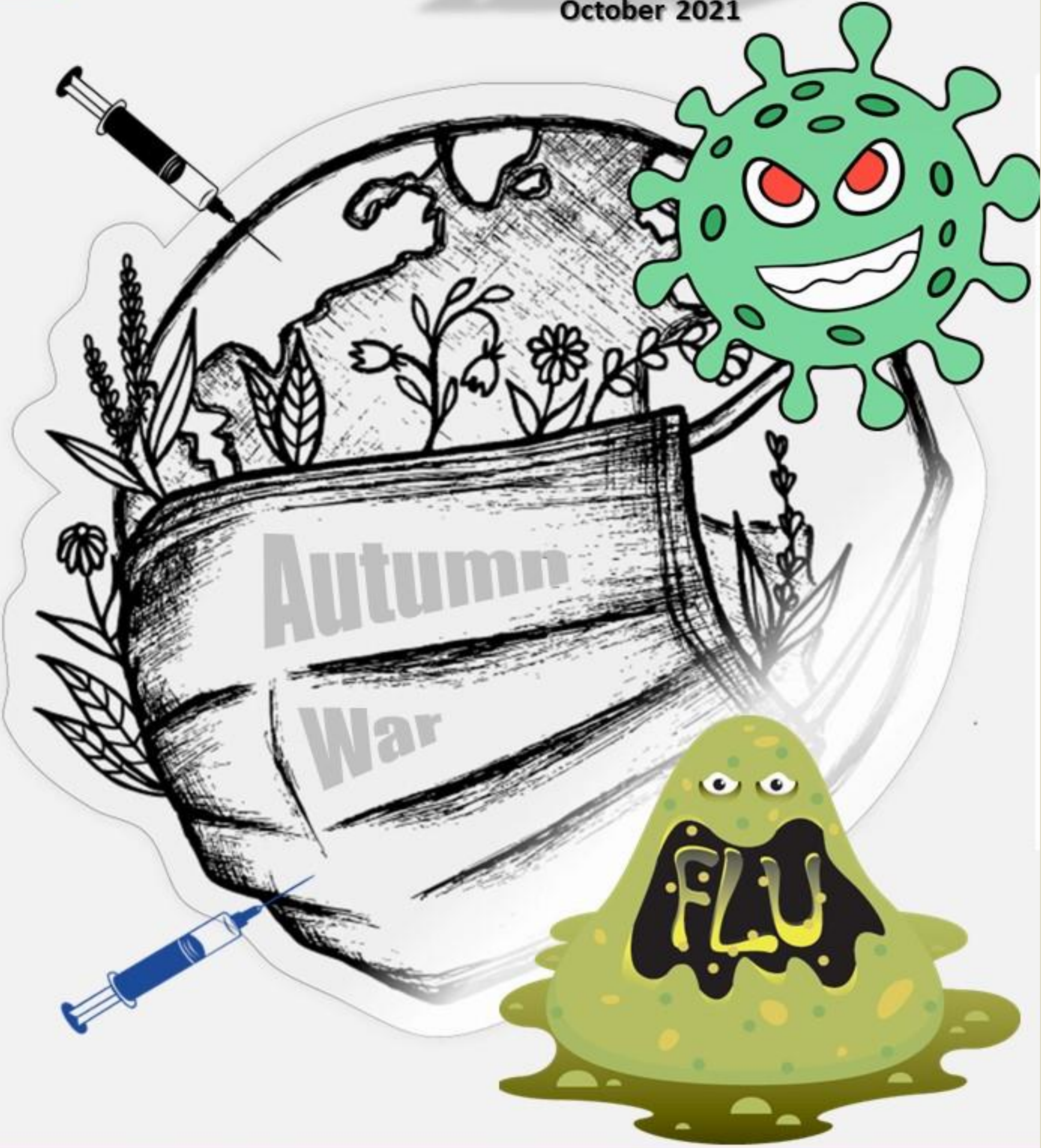
10\21

HZS C²BRNE DIARY

Dedicated to Global First Responders

October 2021



A HOTZONE SOLUTIONS GROUP PUBLICATION

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

DIRTY R-NEWS

With Naming of New Atomic Chief, Is a Nuclear Taliban Possible?

By Tom O'Connor

Source: https://www.newsweek.com/naming-new-atomic-chief-nuclear-taliban-possible-1633694

Sept 29 – The new Taliban-led administration in Afghanistan has inherited an entire nation to run, and with it a wide range of responsibilities, one of them being a fledgling peaceful nuclear agency established a decade ago under the previous government.

With the naming of a new atomic chief, the Taliban appears poised to press forward in this field. That has raised questions as to whether the Islamic Emirate could seek to militarize nuclear energy to develop a weapon of mass destruction, though experts remain deeply skeptical of such an endeavor at this juncture.

Officially, no policy to this end appears to have been adopted, nor has the Taliban yet ruled out such an outcome.

"There has been no decision so far on the development of nuclear weapons," one Taliban official told *Newsweek* on the condition of anonymity.

But a number of observers took notice last week when a list of official postings for the Taliban's interim government decreed by Taliban Supreme Leader Hibatullah Akhundzada and shared by the group's spokespersons identified "Engineer Najeebullah" as "Head of Atomic Energy."

Out of the 17 names on this list and dozens of others announced since the formation of the acting Taliban government earlier this month, Najeebullah has the distinction of only being mentioned by surname, casting intrigue on his identity and why the new administration sought to obscure it.

Reached for comment, the International Atomic Energy Agency said it was following the situation.

"We are aware of the media reports you are referring to," IAEA head of media and spokesperson Fredrik Dahl told *Newsweek*.

But as a matter of protocol, he declined to weigh in on how this might affect the U.N. nuclear watchdog's relationship with Afghanistan. "In line with standard practice related to Member State decisions and appointments," he added, "we have no comment."

Fighters of the Taliban's newly established Islamic Emirate pose in this image posted September 8 by the group's Al Hurat media outlet. Al Hurat

Afghanistan was among the founding members of the IAEA in 1957, and cooperated with the international organization for more than two decades. That relationship was interrupted in the late 1970s by civil unrest and an intervention by the Soviet Union against mujahideen rebels backed by the United States and Pakistan. The conflict stretched throughout most of the following decade, ultimately ending with a Soviet withdrawal and an eventual Taliban takeover in the 1990s.

IAEA cooperation would not restart until after the first iteration of the Taliban's Islamic Emirate was dismantled by a 2001 U.S.-led invasion that followed the 9/11 attacks conducted by Al-Qaeda, a Taliban ally at the time. In 2011, the Afghanistan Atomic Energy High Commission was established to explore nuclear technology for civil society.

As the Taliban began to resurge nationwide, however, the Afghanistan Nuclear Energy Agency began to voice concerns that instability could endanger its work.

In an address to the IAEA given in February of last year, then-Afghan ambassador to Austria Khojesta Fana Ebrahimkhel warned that "the current security situation in Afghanistan is such that some areas of the country are controlled by insurgent groups and national and international terrorist groups are active across the country," and "as a result, we have a serious concern about the illegal transportation of nuclear materials through Afghanistan by these groups.

"In light of this, we believe that such illegal activities will make the current situation more complex and may put the lives of thousands of people in danger," he said at the time. "Thus we sincerely request IAEA members to pay careful attention to this matter."

Unrest in Afghanistan only worsened, however, and two weeks later, the Trump administration reached a deal with the Taliban that paved the way for a U.S. military withdrawal from the country. The Biden administration completed the exit last month.

But the leadup to the pull-out was accompanied by rapid Taliban gains nationwide, and by the time the last U.S. military plane left Afghanistan, the group had established full control of Kabul with little resistance. For the second time in a quarter of a century, the Islamic Emirate of Afghanistan was officially declared.

Though the new Taliban-led government remains unrecognized by any nation, it has pledged cooperation with the international community. This includes pledges to curb the spread of transnational militant groups, combat climate change and foster trade.

But in addition to worries about how the developments in Afghanistan could affect human rights issues, especially as they relate to vulnerable groups such as women and non-Pashtun minorities, some officials and commentators have raised the alarm over how any turmoil might undermine the security of neighboring Pakistan's nuclear arsenal.

In a testimony that contradicted White House claims that the Pentagon backed a timely U.S. withdrawal by the August 31 deadline that had been set, Joint Chiefs of Staff Chair General Mark Milley told lawmakers Tuesday he and his team "estimated an accelerated withdrawal would increase risks of regional instability, the security of Pakistan and its nuclear arsenals, a global rise in violent extremist organizations, our global credibility with allies and partners would suffer, and a narrative of abandoning the Afghans would become widespread."

Adding to these concerns, Pakistan has a history of extraterritorial nuclear proliferation. Nuclear physicist A.Q. Khan, commonly referred to as "the godfather" of Pakistan's nuclear weapons program, has long been at the center of international accusations that he provided classified information, including centrifuge designs, to Libya, Iran and North Korea.

د افغانستان د هستوي انرژۍ اداره
اداره انرژی هستوی افغانستان
Atom for peace & development
Afghanistan Nuclear Energy Agency

Libya shuttered its nascent nuclear program as part of a deal reached in 2003 with the United States, which earlier that year had invaded Iraq over what proved to be false allegations of weapons of mass destruction. The U.S. would also go on to intervene in Libya and help overthrow its government in 2011.

The logo for the Afghanistan Nuclear Energy Agency is seen as present on the agency's website and social media channels, which have gone inactive since the Taliban took Kabul in mid-August. Among the stated goals of the agency included innovations in the fields of security, economic growth, nutrition, medicine, water management, the regulation of radioactive activities, mining and nuclear electricity. Afghanistan Nuclear Energy Agency

Iran maintains a robust nuclear program, despite international accusations and assassinations of its scientists. Tehran has consistently denied any military aspirations for its program and has blamed the assassinations on Israel, which is also widely believed to have nuclear weapons.

North Korea possesses a full-fledged nuclear weapons program, complete with far-reaching missiles it credits with staving off foreign interference.

Pakistan, for its part, set out to attain nuclear weapons in response to rival India's first test in 1974. That test came a decade after China, also locked in a violent territorial dispute with India, conducted its first nuclear weapons test.

The Taliban finds itself in the midst of these geographic and geopolitical feuds, which persist to the present day, as it seeks to govern Afghanistan once again.

And while Pakistan has maintained close ties to the Taliban throughout its rise, fall and resurgence, there remain concerns even in Islamabad that certain separatist and fundamentalist groups could take advantage of the situation to threaten the region.

Former Trump national security adviser and veteran Washington war hawk John Bolton has amplified this anxiety to the point of suggesting that the Taliban's return to ruling Afghanistan creates an imminent threat to Pakistan and the security of its nuclear weapons.

"The Taliban in control of Afghanistan threatens the possibility of terrorists taking control in Pakistan too, and there are already a lot of radicals in the Pakistani military," Bolton told the WABC 770 radio show on Sunday. "But if the whole country gets taken over by terrorists, that means maybe 150 nuclear weapons in the hands of terrorists, which is a real threat to us and our friends."

Pakistani permanent representative to the United Nations Munir Akram responded to this take by Bolton, whom the senior diplomat argued had sought to disarm Islamabad's nuclear stockpile to no avail.

"Well, I believe that Mr. Bolton tried very hard to get his hands on Pakistan's nuclear weapons, and he failed miserably," Akram told *Newsweek*. "If Mr. Bolton couldn't get his hands on our weapons. I do not believe that somebody like the Taliban are capable of doing so."

Daryl Kimball, who has served for two decades as the executive director of the Washington, D.C.-based Arms Control Association nonprofit membership group, shared skepticism toward the notion that Pakistan's nuclear arsenal faced any heightened threat in the wake of the Taliban's victory in Afghanistan.

"I just don't think that there's an added risk today versus a year ago vis-à-vis Pakistan, even though John Bolton is out there making some wacko claims," Kimball told *Newsweek*. "Is Pakistan's nuclear infrastructure more vulnerable today than it was a year ago? I don't think that anybody can say it is."

He argued that when it comes to the Taliban itself, acquiring or developing nuclear weapons was far from being in their interest, both as a result of technological shortcomings and their proven strategy of beating superpowers through conventional methods.

"I think the motives for the Taliban...to acquire nuclear weapons is extremely low or it should be, because their strategy of guerrilla resistance for the last two decades against the United States and the U.S.-supported government in Kabul has ultimately succeeded," Kimball said. "So their lesson from their history is that they can resist and they can do that without resorting to the most destructive of all weapons, nuclear weapons, which are outside of their reach."

But he did raise the prospect of another threat that has existed for some time: a more rudimentary "dirty bomb" in the hands of militants less invested in Afghanistan's stability and more focused on wreaking havoc in the region. He recalled how evidence emerged in past years that Al-Qaeda had explored plans to obtain such a device.

Kimball said that even in the limited amount nuclear materials used for medicinal purposes in hospitals, "you've got radioactive sources that could be stolen or could be sold and used as a dirty bomb." He explained that this kind of product may yield enough material to create "an IED," or improvised explosive device, "with radioactive material," a weapon that could inflict serious damage, but far from the scores of casualties associated with nuclear warheads.

Pakistani military helicopters fly past a vehicle carrying a long-range ballistic Shaheen III missile as they take part in a military parade to mark Pakistan's National Day in Islamabad on March 25. Pakistan is one of the world's nine suspected nuclear powers, alongside Russia, the United States, China, France, the United Kingdom, Israel and North Korea. AAMIR QURESHI/AFP/Getty Images

Such a scenario, however, would almost certainly prove as devastating for the Taliban as it would the intended target. The new Afghan administration already finds itself in conflict with the Islamic State militant group's national Khorasan affiliate (ISIS-K), and has attempted to portray the Islamic Emirate as the answer to Afghanistan's decades-long security issues.

Toby Dalton, co-director and a senior fellow of the Carnegie Endowment's Nuclear Policy Program, found a more compelling argument for the Taliban to continue the previous administration's relationship with the IAEA, and saw the appointment of an atomic chief as likely evidence of this.

"Presumably the new Taliban government in Afghanistan would wish to continue cooperation with the IAEA for the good of the Afghan people, so the appointment of a new minister to oversee these issues makes sense," Dalton, who formerly served as acting director for the U.S. Department of Energy's Office of Nuclear Safeguards and Security and senior policy adviser to the Office of Nonproliferation and International Security, told *Newsweek*. "Most countries have ministries for such applications, so Afghanistan is not unusual in this respect."

And, like Kimball, he emphasized how far away Afghanistan was from establishing even the most basic foundation for a nuclear weapons program. Such an effort would require "substantial outside assistance, whatever the political or military rationale it might have for seeking such weapons."

He also said the group's hesitation on taking a nuclear weapons stance might be strategic. By seeking to ensure continued cooperation with the IAEA, they could open yet another door to the international community.

"I'm not especially concerned that the government has not reiterated its commitment as a signatory to the Nuclear Non-Proliferation Treaty to not seek nuclear weapons," Dalton said. "If the Taliban government formally renounced its commitment to abjure nuclear weapons, that would be pretty noteworthy and unusual – only North Korea has done that before. It would also, practically, end Afghanistan's ability to cooperate with the IAEA on peaceful uses of nuclear technology."

***Tom O'Connor** is an award-winning senior writer of foreign policy at Newsweek, where he specializes in the Middle East, North Korea and other areas of international affairs and conflict. He has previously written for International Business Times, the New York Post, the Daily Star (Lebanon) and Staten Island Advance.*

Irradiating the Mail: The Anthrax Attacks of 2001

By Allison Marsh

Source: https://spectrum.ieee.org/irradiating-the-mail-the-anthrax-attacks-of-2001

This October marks the 20th anniversary of the anthrax terror attacks in the United States. The attacks targeted major media outlets and members of Congress and were delivered through letters containing highly refined anthrax spores. Five people died, 18 others became seriously ill, and dozens more tested positive for anthrax exposure in Florida, New Jersey, New York, and the Washington, D.C., area. The victims included staffers at the targeted destinations and postal workers who handled the mail. Coming on the heels of 9/11, the attacks alarmed Americans as the threat of bioterrorism became real. While the FBI investigated the anthrax attacks, the U.S. Postal Service turned to technology to sanitize the mail and decontaminate their processing facilities.

E-beams and X-rays stopped the spread of anthrax spores

Anthrax is caused by the bacterium *Bacillus anthracis,* the spores of which can remain inactive for decades until they find a favorable environment to germinate, such as blood or tissue. Infection can occur through inhalation, ingestion, and contact with the skin. Anthrax can be treated with antibiotics, but an inhalation infection is almost always deadly if not identified and treated early.

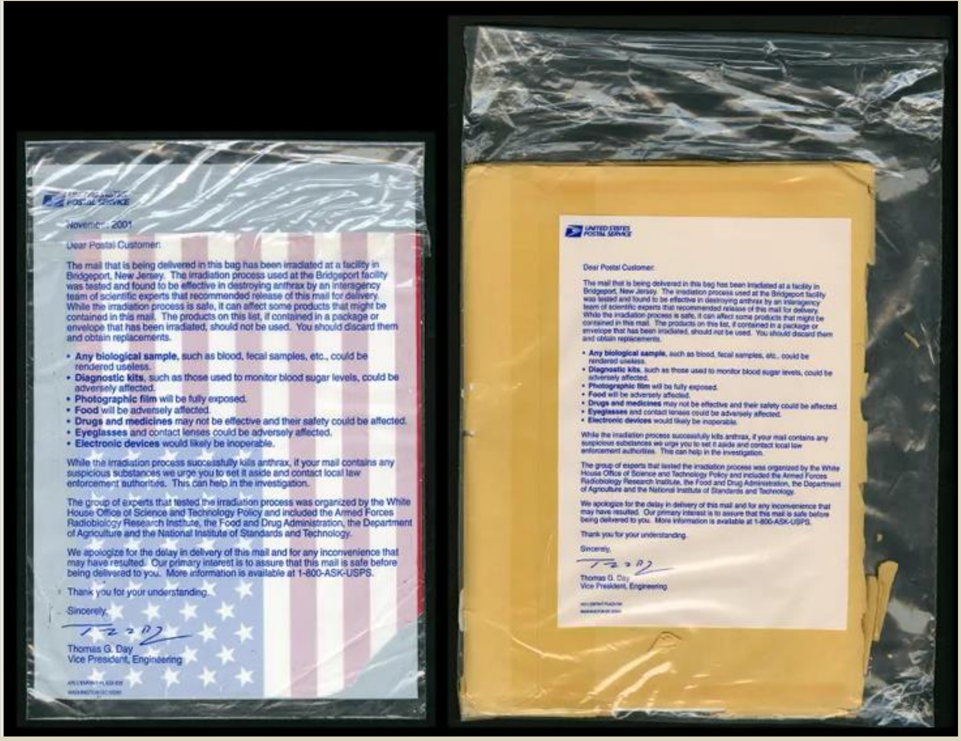
As it happens, the Armed Forces Radiobiology Research Institute (AFRRI) was already studying how to render anthrax spores harmless through irradiation prior to the mail attacks of 2001. The work grew out of concerns that at least seven countries hostile to the United States were developing anthrax for biological warfare. AFRRI's testing confirmed that two forms of ionizing radiation could be used to sanitize the mail: electron beams and X-rays.

Irradiation had been used for decades to sterilize medical equipment, prepare food for human consumption, and artificially alter the color of gemstones. While both methods kill anthrax, neither was a clear winner when it came to irradiating the mail. With an e-beam, a heated filament generates electrons that accelerate through a vacuum tube. The beam then passes through an electromagnetic lens, which focuses the beam on the target. E-beams could process a high volume of mail efficiently but had limited penetration, so they could be used only on letters and flat envelopes.

X-rays have a deeper penetration, which allows them to treat parcels and boxes, but the X-ray machines of 2001 could process only one-tenth as much mail as the e-beam machines could. Plus, X-rays required safety shielding and monitoring to protect workers.

But the Postal Service needed to process approximately 1.8 million pieces of contaminated mail, and so they quickly contracted with two companies, Ion Beam Applications (IBA) and Titan Corp. (now part of L3Harris Technologies), to irradiate the lot, along with all letters, large envelopes, newsletters, and magazines destined for congressional and government offices in the Washington, D.C., ZIP codes 20200 to 20599.

Scaling up e-beam and X-ray machines to process all that mail proved a huge logistical challenge. IBA had a facility in Bridgeport, N.J., with a Rhodotron, a continuous-wave accelerator capable of generating both e-beams and X-rays. The machine was designed to irradiate polymers with e-beams and frozen hamburgers with X-rays. To irradiate the mail, it functioned in e-beam mode at about 170 kilowatts at 10 mega-electronvolts. Mail was packaged flat, double bagged, boxed, and sealed. Each box was about the size of the trays now used at airport security. The box was irradiated once, manually flipped over, and then irradiated a second time. The facility could handle about 2,040 kilograms of mail per hour.


UNITED STATES POSTAL SERVICE

November , 2001

Dear Postal Customer:

The mail that is being delivered in this bag has been irradiated at a facility in Bridgeport, New Jersey. The irradiation process used at the Bridgeport facility was tested and found to be effective in destroying anthrax by an interagency team of scientific experts that recommended release of this mail for delivery. While the irradiation process is safe, it can affect some products that might be contained in this mail. The products on this list, if contained in a package or envelope that has been irradiated, should not be used. You should discard them and obtain replacements.

- **Any biological sample**, such as blood, fecal samples, etc., could be rendered useless.
- **Diagnostic kits**, such as those used to monitor blood sugar levels, could be adversely affected.
- **Photographic film** will be fully exposed.
- **Food** will be adversely affected.
- **Drugs and medicines** may not be effective and their safety could be affected.
- **Eyeglasses** and contact lenses could be adversely affected.
- **Electronic devices** would likely be inoperable.

While the irradiation process successfully kills anthrax, if your mail contains any suspicious substances we urge you to set it aside and contact local law enforcement authorities. This can help in the investigation.

The group of experts that tested the irradiation process was organized by the White House Office of Science and Technology Policy and included the Armed Forces Radiobiology Research Institute, the Food and Drug Administration, the Department of Agriculture and the National Institute of Standards and Technology.

We apologize for the delay in delivery of this mail and for any inconvenience that may have resulted. Our primary interest is to assure that this mail is safe before being delivered to you. More information is available at 1-800-ASK-USPS.

Thank you for your understanding.

Sincerely,

Thomas G. Day
Vice President, Engineering

UNITED STATES POSTAL SERVICE

Dear Postal Customer:

The mail that is being delivered in this bag has been irradiated at a facility in Bridgeport, New Jersey. The irradiation process used at the Bridgeport facility was tested and found to be effective in destroying anthrax by an interagency team of scientific experts that recommended release of this mail for delivery. While the irradiation process is safe, it can affect some products that might be contained in this mail. The products on this list, if contained in a package or envelope that has been irradiated, should not be used. You should discard them and obtain replacements.

- **Any biological sample**, such as blood, fecal samples, etc., could be rendered useless.
- **Diagnostic kits**, such as those used to monitor blood sugar levels, could be adversely affected.
- **Photographic film** will be fully exposed.
- **Food** will be adversely affected.
- **Drugs and medicines** may not be effective and their safety could be affected.
- **Eyeglasses** and contact lenses could be adversely affected.
- **Electronic devices** would likely be inoperable.

While the irradiation process successfully kills anthrax, if your mail contains any suspicious substances we urge you to set it aside and contact local law enforcement authorities. This can help in the investigation.

The group of experts that tested the irradiation process was organized by the White House Office of Science and Technology Policy and included the Armed Forces Radiobiology Research Institute, the Food and Drug Administration, the Department of Agriculture and the National Institute of Standards and Technology.

We apologize for the delay in delivery of this mail and for any inconvenience that may have resulted. Our primary interest is to assure that this mail is safe before being delivered to you. More information is available at 1-800-ASK-USPS.

Thank you for your understanding.

Sincerely,

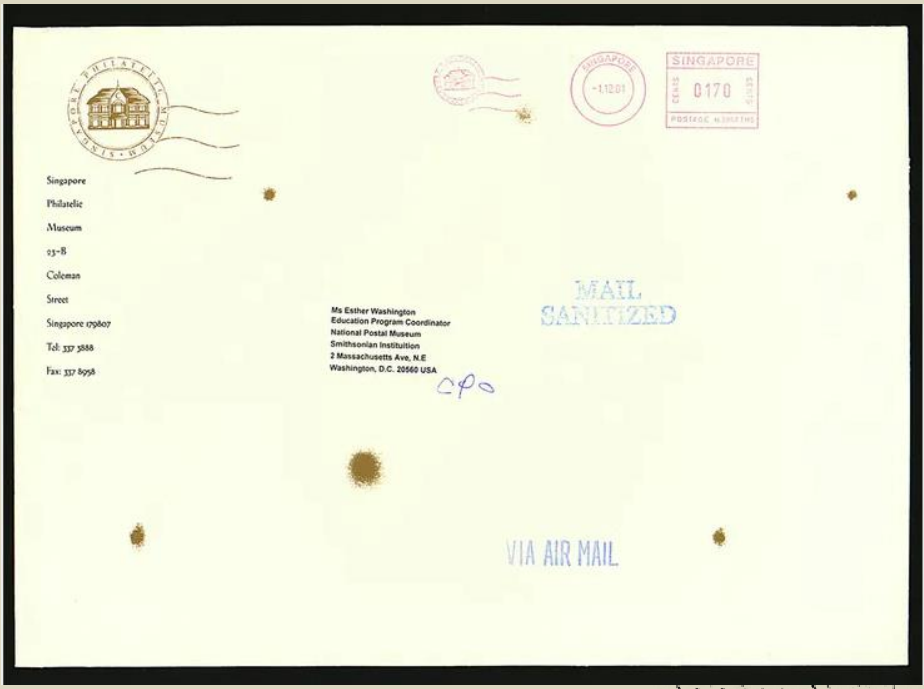
Thomas G. Day
Vice President, Engineering

Irradiated mail was placed in plastic "body bags" imprinted with an explanation of the adverse effects of X-ray and e-beam exposure. National Postal Museum/Smithsonian Institution

Titan had a facility in Lima, Ohio, with a single accelerator operating at 18 kW at 10 MeV. It was designed to sterilize medical products. Mail arrived packaged vertically in trays. Similar to the IBA's operation, the trays were double bagged, boxed, and sealed. At Titan, each box of mail was irradiated four times, with the conveyor automatically rotating the boxes for each pass. The facility could handle approximately 454 kg of mail per hour. It took several weeks for the contractors to process the backlog, although it took up to three months for some agencies to receive their waylaid mail. For new mail heading to government offices, the process added approximately five days to delivery times. Initially, neither vendor had suitable X-ray equipment for irradiating large boxes, but eventually they found they could place the boxes in large stainless-steel totes that were suitable for X-raying. Later, the delay times were reduced to two days for letters and three days for packages.

Collectors coveted letters damaged by irradiation

Although irradiation killed the anthrax, one downside was that it made paper brittle and discolored, as evidenced by the letter pictured below, which was sent to the National Postal Museum dated 1 December 2001. Irradiation also warped plastics, exposed film, fogged glass products, weakened the potency of pharmaceuticals, and destroyed biological samples from doctors' offices and scientific labs. Many companies and government offices, including philatelic societies and the Smithsonian Institution, began using alternative shipping services to avoid having their materials irradiated.


SINGAPORE PHILATELIC MUSEUM

SINGAPORE
-1.12.01

SINGAPORE
CENTS 0170 CENTS
POSTAGE

Singapore
Philatelic
Museum
03-B
Coleman
Street
Singapore 179807
Tel: 337 3888
Fax: 337 8958

Ms Esther Washington
Education Program Coordinator
National Postal Museum
Smithsonian Institution
2 Massachusetts Ave, N.E
Washington, D.C. 20560 USA

cpo

MAIL
SANITIZED

VIA AIR MAIL

A letter that was irradiated to kill any traces of anthrax spores shows scorch marks and discoloration. National Postal Museum/Smithsonian Institution

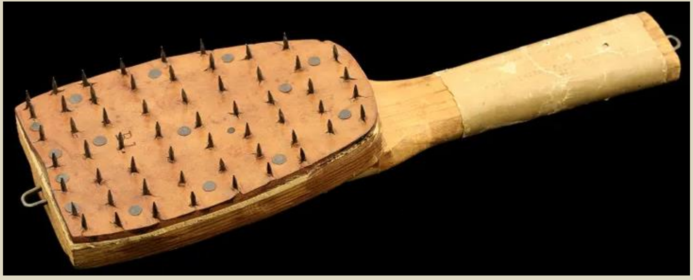
Of course, this process also inadvertently opened up a new path for collectors. Some philatelists began to specialize in collecting irradiated mail, just as some people collect mail from disasters such as the *Hindenburg* and the *Titanic*.

Once the backlog of contaminated mail was processed, the U.S. Postal Service had to determine what safety steps to implement permanently. The General Accounting Office, which examines the use of public funds and provides guidance to help Congress make informed decisions, then worked with the USPS, the AFRRI, and industry experts to look for long-term solutions based on cost, effectiveness, efficiency, and safety.

The GAO report, "Diffuse Security Threats: Technologies for Mail Sanitization Exist, but Challenges Remain," published in April 2002, estimated that the cost for irradiating mail nationwide could be up to US $4.2 billion over a 10-year period. That was too big a price tag, but the Postal Service continues to irradiate mail bound for certain government addresses. Additionally, the agency installed biohazard-detection equipment at each of its 272 processing and distribution centers nationwide to identify anthrax in the U.S. mailstream. (In this May 2019 profile of MEMS pioneer Kurt Petersen, he describes how his startup Cepheid's automated polymerase-chain-reaction (PCR) machines were selected to screen the mail for anthrax.)

When "postage stamp tongue" was a new disease

Although the 2001 anthrax attacks were the most high-profile examples of a deliberate attempt to make people sick through the mail, it was not the first time the post was tied to illness. A century earlier, many people still believed in the miasma theory of disease—the idea that sickness was caused by bad smells and poisonous vapors. The Post Office Department attempted to control outbreaks of yellow fever, smallpox, plague, typhus, cholera, diphtheria, measles, leprosy, scarlet fever, tuberculosis, influenza, and mumps by fumigating the mail. Without effective contact tracing, it was easy to suspect that letters or newspapers circulated disease from infected areas to healthy ones.



During an outbreak of yellow fever in 1899, this nail-studded paddle was used into perforate mail, in preparation for fumigation with sulfur. National Postal Museum/Smithsonian Institution

In 1899 the Montgomery, Ala., Board of Health used a wooden paddle with a nail-studded leather face to perforate the mail. Postal workers would then fumigate the letters with sulfur. It may have done little to stop the spread of disease, but the hygiene theater calmed worried customers.

Meanwhile, though, the germ theory was gaining ground, and other postal practices started coming under attack. A *Washington Post* article from 22 November 1896, for example, questioned the practice of licking a stamp to activate its glue. It warned that "Postage Stamp Tongue was a new disease" and suggested that stamps were threatening the nation's public health as a harbor for virulent germs. Joseph Schermack introduced this "sanitary" stamp-vending machine to address public concerns that disease could spread by handling postage stamps.National Postal Museum/Smithsonian Institution

Joseph Schermack, who is generally credited with producing the first practical stamp-vending machine, formed the Sanitary Postage Service Corp. in 1926. His machines dispensed stamps in sanitary folders to a clientele that feared germs. This fear largely receded as the public became more informed about disease transmission and self-sticking stamps became common, leaving the sanitary stamp packaging as a curious reminder of society's evolving relationship with illness and risk.

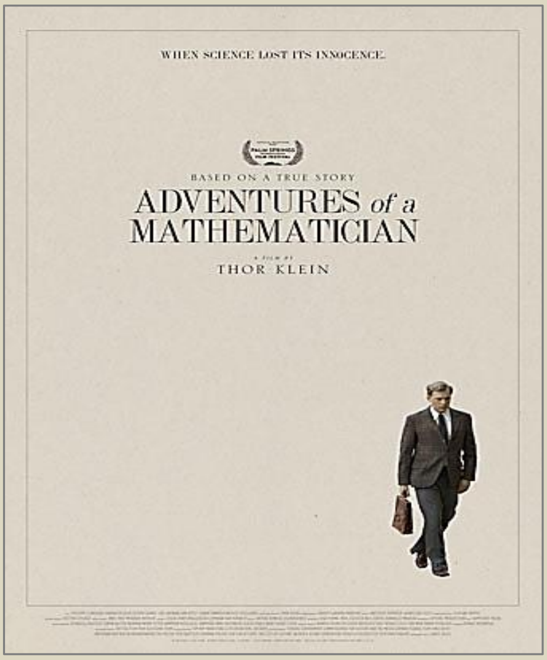
Fears of biological contamination through the mail resurfaced last year in the early months of the global pandemic, when scientists were unsure of how COVID-19 spread. Should we wipe down letters and packages? Should we wear gloves to handle the mail? Should we let everything sit for 24 hours before opening? The Centers for Disease Control and Prevention published guidelines for mail and parcel delivery drivers, which the USPS followed. After new science showed little likelihood from contracting COVID from the mail, the CDC archived its guidelines. Opening the mail today remains a low-risk activity.

***Allison Marsh** is a professor at the University of South Carolina and codirector of the university's Ann Johnson Institute for Science, Technology & Society. She combines her interests in engineering, history, and museum objects to write the Past Forward column, which tells the story of technology through historical artifacts.*

Adventures of a Mathematician

Source: https://filmthreat.com/reviews/adventures-of-a-mathematician/

Oct 01 – ***Adventures of a Mathematician*** follows a group of young scientists at the dawn of the nuclear age. Based on the memoirs of Polish mathematician Stanis "Stan" Ulam (Philippe Tlokinski), the film chronicles the moral ambiguity of creating the atomic bomb during the height of World War II. Despite his ethical objections to creating such a destructive force, Stan must come to terms with the cost of ending the war and creating history's most infamous weapon.


WHEN SCIENCE LOST ITS INNOCENCE
BASED ON A TRUE STORY
ADVENTURES of a MATHEMATICIAN
A FILM BY
THOR KLEIN

At the start, Stan is living a relatively comfortable life teaching at Harvard. But, regardless of his considerate demeanor, he struggles with living in the U.S. while his family is under the threat of Nazi rule in his home country. As World War II calls him to action, Stan's friend Johnny (Fabian Kociecki) offers him the chance to fight Hitler, not with bullets but with mathematics. Moving himself and his new wife Franciose (Esther Garrel) to New Mexico, Stan soon finds himself at a crux of history working on the Manhattan Project.

Writer and director Thor Klein raises many philosophical questions throughout ***Adventures of a Mathematician***. He highlights the analytical side to creating a weapon of mass destruction and looks into the brilliant minds who consciously built it. Tlokinski plays Stan as a cold, calculated man conflicted by his ability to create such destruction. In contrast to Tlokinski's approach, Garrel plays Franciose with empathy towards her husband's trials with the bomb. The contrasting approaches fit the character's motivations brilliantly and expand on the central themes of nuclear apocalypse and the probability of impending Cold War.

While watching the movie***,*** the phrase "hurt in the edit" continued to pop into my mind. The story explores profound philosophical questions about the ethics of nuclear weapons, the humanity of creating and using such a weapon. Yet, scenes often cut just as the conversations get interesting. Stan and Johnny frequently discuss the impacts such a weapon would have on the world. There is even a tearful moment when a scientist breaks down after the dropping of the first atomic bomb. However, the film often flashes to the next point in Stan's life rather than explore these emotions further. The screenplay does an excellent job of raising these questions about warfare and humanity yet rarely delivers.

I enjoyed the performances of ***Adventures of a Mathematician*** and, I more than appreciate the premise. The idea of holding a mirror to the world at the cusp of nuclear creation is a fascinating subject and, exploring the minds of a man who made nuclear war possible is engaging. However, the movie often feels like a timeline of Stan Ulam's life in general rather than a focused narrative on the complex emotions of creating "death the destroyer of worlds." Regardless of these hang-ups, the film still crafts a compelling story for those interested in WWII or slow-burning historical dramas. If you like titles like ***The Good Traitor*** or want a movie to accompany the memories of Stannis Ulam, this is worth a watch.

Nuclear Armed Iran More Dangerous Than North Korea

By Majid Rafizadeh

Source: https://www.gatestoneinstitute.org/17825/nuclear-armed-iran

Oct 02 – The Iranian regime is nearing an atomic milestone in acquiring nuclear weapons. In the meantime, the Biden administration does not seem to have a clear agenda to prevent the mullahs from going nuclear. Even the *New York Times* reported that the Islamic Republic is "within roughly a month of having enough material to fuel a single nuclear weapon".

Ever since the Biden administration assumed office, the Iranian regime has been accelerating its enrichment of uranium to "near weapons grade". As the International Atomic Energy Agency pointed out:

"Since 23 February 2021 the Agency's verification and monitoring activities have been seriously undermined as a result of Iran's decision to stop the implementation of its nuclear-related commitments".

The threats of a nuclear-armed Iran must not be underestimated. First, the regime has frequently threatened to wipe a whole country -- Israel -- off the map. One of the core pillars of the Islamic Republic has been destroying the Jewish state. It is also one of the religious prophecies of the founder of the Islamic Republic of Iran, Ayatollah Ruhollah Khomeini, as well as his successor, the current Supreme Leader Ayatollah Ali Khamenei, that Israel will be eventually erased from the face of the earth.

General Hossein Salami, the chief of Islamic Revolutionary Guard Corps (IRGC) has made the Iranian regime's plans vehemently clear: "Our strategy is to erase Israel from the global political map," he stated on Iran's state-controlled Channel 2 TV in 2019. Khamenei has also published a 416-page guidebook, titled "Palestine," about destroying Israel.

Second, the theocratic establishment of the mullahs is anchored in prioritizing the pursuit of its revolutionary ideals, which include exporting its Islamist system of governance to other countries around the world. The mullahs, in fact, incorporated this critical mission into its constitution. The preamble stipulates: "The mission of the constitution is to create conditions conducive to the development of man in accordance with the noble and universal values of (Shiite) Islam." The regime's constitution goes on to say that it "provides the necessary basis for ensuring the continuation of the revolution at home and abroad."

Since 1979, by deploying its IRGC and its elite branch, the Quds Force, Iran's leaders have managed to expand Tehran's influence throughout the Middle East from Yemen to Lebanon, Syria, and the Gaza Strip through its proxy groups, including the Houthi militia, Hezbollah, Hamas and the Popular Mobilization Forces (PMF), a conglomerate of more than 40 militia groups in Iraq.

Third, there is the dangerous likelihood of nuclear weapons falling into the hands of Iran's proxy and militia groups, or that the Iranian regime will share its nuclear technology with its proxies and allies such as the Syrian regime or the Taliban in Afghanistan.

The Iranian regime has already been setting up weapons factories abroad, and manufacturing advanced ballistic missiles and weapons in foreign countries, including in Syria. These include precision-guided missiles with advanced technology to strike specific targets.

As Iran's regime is already supplying advanced weapons to its proxies, what would stop it from sharing its nuclear technology to empower its proxies and militia groups, to undermine its perceived adversaries' national security interests and to expand its reach? The latest UN annual report revealed this year that the Houthis have been receiving significant amount of weapons from the Iranian regime: "An increasing body of evidence suggests that individuals or entities in the Islamic Republic of Iran supply significant volumes of weapons and components to the Houthis."

Iran has for years been designated by the US Department of State as a "State Sponsor of Terrorism". One of Iran's diplomats, Assadollah Assadi, is on trial in Europe for a failed terror bombing plot in Paris, France, where a "Free Iran" rally was held. Iran continues to use undercover agents or dispatch troops. Several countries, including Kuwait, have detained more than a few Iranians trying to infiltrate their country. Tehran has been found using its embassies and diplomats in foreign countries for such purposes.

Just as telling, Iran does not treat its own citizens particularly well. In Iran, as recent reports document:

"Security forces used unlawful force to crush protests. The authorities continued to arbitrarily detain hundreds of protesters, dissidents and human rights defenders, and sentenced many to imprisonment and flogging. Women, as well as ethnic and religious minorities, faced entrenched discrimination as well as violence. Enforced disappearances, torture and other ill-treatment were committed with impunity on a widespread and systematic basis. Judicial corporal punishments amounting to torture, including floggings and amputations, were imposed. Fair trial rights were systematically violated. The death penalty was used as a weapon of political r epression. Executions were carried out, one in public and some others in secret. Those executed included people aged under 18 at the time of the crime. The authorities continued to commit crimes against humanity by systematically concealing the fate and whereabouts of several thousand political dissidents forcibly disappeared and extrajudicially executed in secret in 1988. Mass graves believed to contain their remains were subject to ongoing destruction."

If this is how Iran's leadership treats its own citizens, what makes anyone think they would treat their perceived adversaries any better? As others have asked: If Hitler had acquired a nuclear weapon, do you think he would have hesitated to use it?

If the predatory regime of Iran's mullahs obtains nuclear weapons, one can only imagine how much more hostile and emboldened it will become. Once such leaders have weapons of mass destruction, it is far more costly in life and treasure to try and stop them. Iran might not even need to use its nuclear weapons; the threat should be more than enough.

***Dr. Majid Rafizadeh** is a business strategist and advisor, Harvard-educated scholar, political scientist, board member of Harvard International Review, and president of the International American Council on the Middle East. He has authored several books on Islam and US foreign policy.*

Fukushima operator to dig tunnel for dumping water from crippled plant

Source: https://sputniknews.com/asia/202108241083703338-fukushima-operator-todig-tunnel-for-dumping-water-from-crippled-plant-reports-say/

Aug 24 – Japanese utility TEPCO, the operator of the crippled Fukushima Daiichi nuclear plant, plans to dig an offshore tunnel to dump treated radioactive water farther into the ocean. TEPCO needs the approval of the national nuclear regular before the work begins. It hopes to start preparations this year and dig the tunnel in 2022, before the planned water release begins in spring 2023.

Only Russians allowed in core of nuclear power plant in southern Turkey, says engineer

Source: https://www.duvarenglish.com/only-russians-allowed-in-core-of-russian-built-akkyuku-nuclear-power-plant-in-turkey-says-engineer-news-59043

Akkuyu
SYRIA
Construction of Turkey's first nuclear reactor by Russian group Rosatom

Oct 01 – Hardly any Turkish engineers working in the Russian-built Akkuyu Nuclear Power Plant in southern Turkey are allowed to enter the core of the plant, wrote journalist Can Ataklı in his column in daily Korkusuz on Oct. 1.

Ahead of the meeting between Turkish President Recep Tayyip Erdogan and Russian President Vladimir Putin in Sochi on Sept. 29, ruling Justice and Development Party (AKP) officials claimed Turkish employees had been trained in Russia to operate the plant.

An anonymous engineer of the plant however told journalist Ataklı that was untrue. He said that only Turkish engineers had been trained in Russia, not all employees, and regardless of their training none of those engineers were allowed in the core of the plant.

Over the course of AKP tenure in Turkey, Russia and Turkey have had a tumultuous relationship. The two countries were on opposing sides in the Syrian civil war, and have at times opposed each other in the conflict in Libya.

In 2015, a Turkish F-16 fighter jet shot down a Russian Sukhoi S-24M attack aircraft near the Turkish border, leading to diplomatic disaster. However, since the Turkish coup attempt of July 2016 and the subsequent souring of relations between Turkey and the West, a tentative alliance has formed between the two countries. One of the flagship projects of this renewed alliance was the Russian-built Akkuyu Nuclear Power Plant. At the meeting between Putin and Erdoğan, the two leaders discussed further collaboration, especially in security and defense.

Before the AKP delegation went to Sochi to meet with Putin, Erdoğan said in a statement that 13,000 people were working in the plant, set to start operating in 2022 (full operation is expected by 2023). Some 10,000 of those were Turkish, he said, and they had all been sent to Russia for training.

The engineer interviewed by journalist Ataklı, however, countered this claim. According to him, only Turkish engineers, not all 10,000 employees, were sent to Russia for training. Further, despite that training, most Turkish engineers are not allowed in the core of the plant, where the reactor is -- in other words, they are not allowed in the most critical part of the plant. Only Russian engineers, with a few Turkish exceptions, are.

“The vast majority of the engineering staff is Russian,” he said. “Up to 2,000 Russian engineers will work in the core section of the power plant and we will not be able to go there.”

The plant engineer further emphasized that this contradicts AKP’s “Yerli, Milli” slogan - meaning “local, national” - which encourages goods and services to be produced domestically. With the setup at Akkuyu, the most critical part of the plant will be run by foreign nationals, not Turkish citizens.

"When the power plant opens, there will only be Russians in the most critical part of the plant, with one or two of our compatriots," the engineer said. "This means that Russians will have complete control of the plant. They always talk about 'local and national,' this power plant will never be local or national."

How to reduce the risk of a catastrophic spent nuclear fuel fire near the Persian Gulf

By Tara Burchmore, Tom Spence, and Ali Ahmad

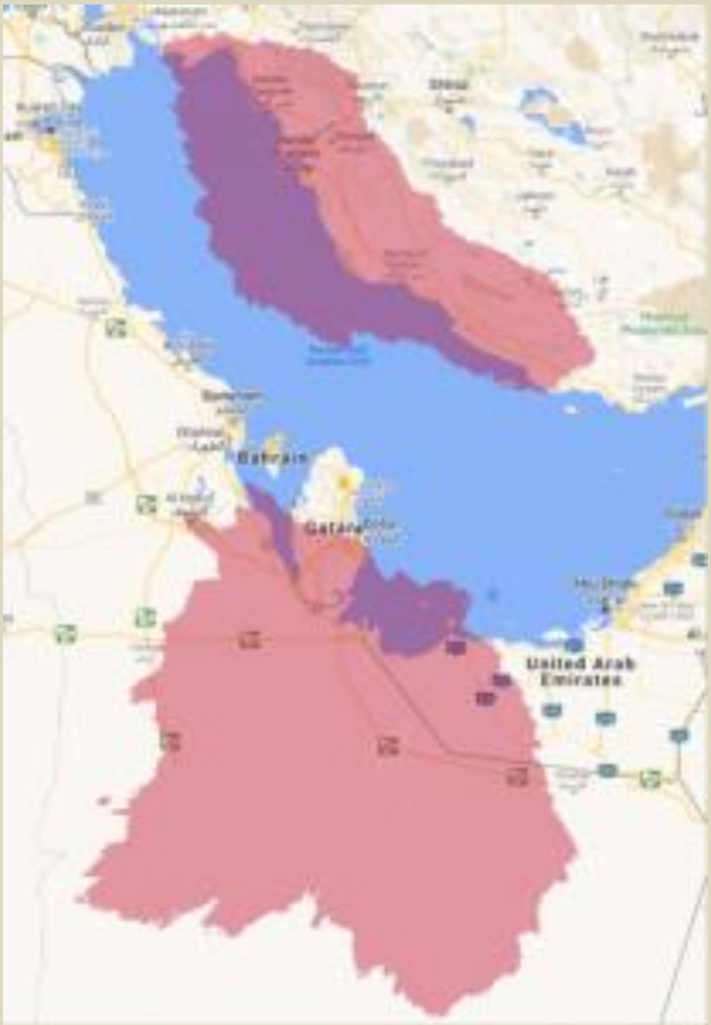
Source: https://thebulletin.org/2021/10/how-to-reduce-the-risk-of-a-catastrophic-spent-nuclear-fuel-fire-near-the-persian-gulf/

Oct 06 – The 2021 operational launch of two reactors at the Barakah power plant in Abu Dhabi, United Arab Emirates (UAE) demonstrates the growth of nuclear energy in the Middle East. Over the next two years, there will be five reactors operating in the Persian Gulf—four reactors at Barakah and Iran's Bushehr reactor, which has been running since 2013. If Iran and Saudi Arabia fulfill their proposed plans to build new nuclear reactors, the number will rise to at least eight reactors in the gulf by 2030.

There are many reasons for concern about the safety of nuclear facilities in the gulf. Particularly in the region where Bushehr is located, Iran is prone to seismic activity. The UAE has limited experience in operating nuclear facilities. And terrorist groups have identified energy infrastructure as a key target—and even attacked nuclear installations.

It is in this context we raise an alarm about the possibility of a severe nuclear accident in the gulf, driven by a fire in one of the spent nuclear fuel pools of the Bushehr or Barakah power plants. As we explain in detail in our recent paper in *Science and Global Security*, the local and possibly global economic implications of such an accident are huge.

Since the Fukushima Daiichi disaster more than a decade ago and the "near miss" catastrophe of a fire at the unit 4 spent fuel pool, higher attention has been given to the long-overlooked risks of such densely packed pools, which typically have less fortified containment than a reactor core but may contain much larger amounts of radioactivity. Frank von Hippel and his colleagues have since produced important analyses revising the risks of spent nuclear fuel fires and highlighting their human and economic costs.



Map showing areas in the Persian Gulf with higher than 10 percent probability of receiving above 1.5 megabecquerels per square meter of contamination following a radiation release from a spent nuclear fuel fire in Barakah and Bushehr.

Cities at risk

In our paper, we modelled what might happen if a spent nuclear fuel fire was to start at either the Barakah or Bushehr nuclear power plants, using an atmospheric modeling program to simulate how the plume of radioactive smoke from the fire would spread over the gulf region based on probable weather patterns. Based on thousands of dispersion simulations using real historical weather data, the results show that several major cities in the gulf region could be contaminated by cesium 137 fallout if a spent fuel fire occurred at Barakah or Bushehr. The cities at the highest risk from fires at Barakah are those centered around the Gulf of Bahrain: Doha, Manama, Dammam, and al-Hofuf. For each of these cities, there is a greater than five percent chance of being contaminated with more than 1.5 megabecquerels per square meter of cesium 137 (the likely threshold over which the population would need to be evacuated). Of these, Doha presents the biggest risk—in over 10 percent of simulations, evacuation of the city would be required. The cities around Bushehr are at lower risk because that plant would contain less spent fuel than Barakah. The city at the highest risk from spent fuel fires at Bushehr is Ahvaz, which was contaminated with more than 1.5 megabecquerels per square meter of cesium 137 in two percent of the simulations.

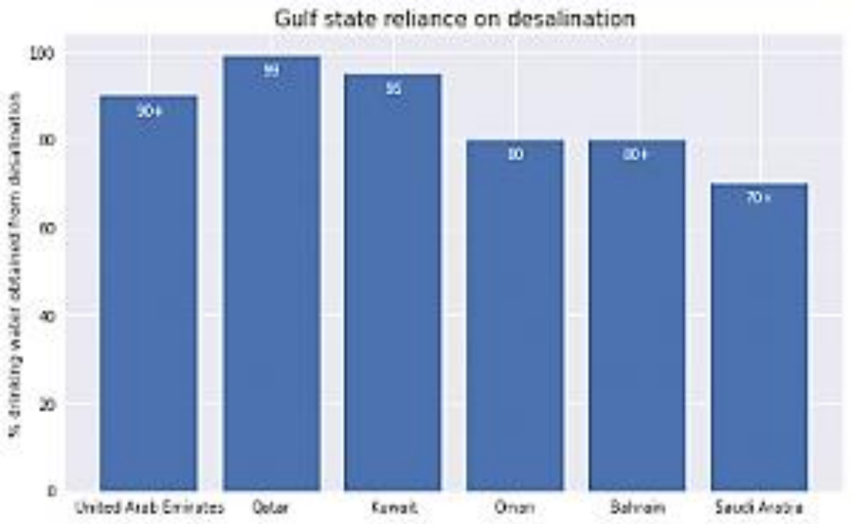
Map showing areas in the Persian Gulf with higher than 10 percent probability of receiving above 1.5 megabecquerels per square meter of contamination following a radiation release from a spent nuclear fuel fire in Barakah and Bushehr.

Both cyberattacks and physical attacks on nuclear power plants in the gulf region are real risks. While the Geneva Conventions and International Atomic Energy Agency resolutions have strengthened protections on nuclear sites, the Middle East has seen a number of attacks on such facilities. The 2010 Stuxnet attack on Iran's nuclear program damaged critical systems, while airstrikes have targeted nuclear installations in Iran, Iraq, and Syria. Another major risk in the gulf region specifically is the presence of violent non-state actors. In 2017, Houthi militants claimed to have launched a cruise missile at the Barakah site while the reactors were under construction. The Nuclear Facilities Attack Database (NuFAD) also shows that Hamas targeted Israel's Negev Nuclear Research Facility near Dimona in 2014 with a rocket attack that was intercepted by missile defenses.[3]

Magnified vulnerabilities

A nuclear accident in any location is likely to trigger some major public health and economic problems. In the Persian Gulf region, however, these problems will be magnified by three major factors: First, population and economic activity is highly concentrated in cities that are located on the coast and stretch only a few kilometers deep inland, which would complicate relocation efforts. Qatar and Bahrain particularly have limited land to house evacuees—their geography would likely require evacuees from a spent fuel fire to cross international borders.

Second, gulf cities are very dependent on desalinated water. This poses a serious water security threat not only to countries that host nuclear power plants, but to the entire gulf population. The scale of the problem is compounded by the fact that the gulf is a semi-closed, shallow body of water with water circulation estimated to take between two and five years. Some desalination plants can remove cesium from seawater alongside sodium, either through coagulation and sedimentation or reverse osmosis, but in the event of direct fallout, plant operations would be interrupted as workers were evacuated.[4] Gulf cities that rely heavily on water desalination (Doha, Abu Dhabi, Dubai, Manama, Sharjah) only have a few days of storage capacity, so even a temporary shutdown in water production could have severe impacts for them.



Source: "An Integrated System-Oriented Model for the Interoperability of Multiple Emergency Response Agencies in Large-Scale Disasters: Implications for the Persian Gulf" by Najmedin Meshkati and Maryam Tabibzadeh, International Journal of Disaster Risk Science, 7(2016), 227-244

Third, gulf countries have a high concentration of economic activities that are either located on the coast or dependent on transport through the gulf. Primary among these activities are oil and gas production and transport. The Persian Gulf's Strait of Hormuz is the only sea passage from the gulf to the open ocean, making it a major shipping corridor that is potentially vulnerable to contamination from a spent nuclear fuel fire.

Following the 2011 Fukushima disaster, the German government recommended that ships avoid passing within 100 kilometers of the stricken Fukushima reactors, while Japanese authorities advised a 30 kilometer distance and the United States recommended 80 kilometers.[5] As the Strait of Hormuz is 55 kilometers wide at its narrowest point[6] and the gulf is about 340 kilometers at its widest, a recommended avoidance distance of 100 kilometers could be detrimental to shipping, particularly if an accident was to occur at Bushehr. Previous attacks on oil tankers in the region exemplify the vulnerabilities and risks associated with an industry so reliant on a singular narrow sea passage for all export activity and demonstrate how destructive to the global supply chain a nuclear disaster could be.[14]

A nuclear accident restricting passage through the Strait of Hormuz will likely to result in a global economic shock; a third of world oil is produced in Persian Gulf countries,[7] and 30 percent of all seaborne-traded crude oil passes through the Strait of Hormuz during the export process.[8] If exports are unable to pass through the strait, the oil-dependent world will suffer, particularly Asia, which receives 80 percent of the gulf's crude exports.[9]

Without the strait, Persian Gulf exports may be unable to be transported, halting most of the economic activity in the region. While some countries, including Saudi Arabia, the UAE, and Iraq, can devise alternate routes for shipping exports, Kuwait, Qatar, and Bahrain are entirely dependent on shipping through the strait.[10] Given their high dependency on oil revenues, an economic shock in the gulf that is driven by a nuclear accident will likely result in an unprecedented level of socioeconomic pressure.

Recommendations

The safest way to mitigate the risk of spent nuclear fuel fires in the Persian Gulf region would be to end the deployment of nuclear energy in the Middle East and rely instead on the region's natural gas and renewable energy resources. This, of course, will not happen.

However, risks can be reduced by not adding new nuclear capacity beyond what is currently built. Additionally, governments could reduce risks by timely transfer of spent fuel into dry cask storage and ultimately into geological storage, limiting the dense packing of spent fuel pools. Iran has agreed to transfer Bushehr's spent nuclear fuel to Russia and could seek to do so as soon as it has cooled sufficiently. States also should work to prevent attacks on nuclear facilities. One model could be a multilateral arrangement similar to the bilateral one reached between India and Pakistan. Finally, gulf states should bolster their emergency preparedness and management plans for nuclear accidents and incidents involving potential radiation release in the region.

Notes

[1] Alvarez et al., "Reducing the Hazards from Stored Spent Power-Reactor Fuel in the United States," 3; "Lessons Learned from the Fukushima Nuclear Accident", 36; J. Sam Armijo to Allison M. Macfarlane, "Staff Evaluation and Recommendation for Japan Lessons-Learned Tier 3 Issue on Expedited Transfer of Spent Fuel," December 18, 2013.

[2] MacLean, Trevor, Robert Borrelli, and Michael Haney. "Cyber Security Modeling of Non-Critical Nuclear Power Plant Digital Instrumentation." In *Critical Infrastructure Protection XIII*, edited by Jason Staggs and Sujeet Shenoi, 87–100. Cham: Springer International Publishing, 2019.

[3] Reuters, "UAE denies Yemen's Houthis have fired missile toward UAE," Reuters, December 3, 2017, https://es.reuters.com/article/us-yemen-security-emirates-denial-idUSKBN1DX0DD; START, Nuclear Facilities Attack Database (NuFAD), 2020, https://www.start.umd.edu/nuclear-facilities-attack- database-nufad.

[4] Sasaki, Takao, Jun Okabe, Masahiro Henmi, Hiromasa Hayashi, and Yutaka Iida. "Cesium (Cs) and Strontium (Sr) Removal as Model Materials in Radioactive Water by Advanced Reverse Osmosis Membrane." Desalination and Water Treatment 51, no. 7–9 (February 1, 2013): 1672–77. https://doi.org/10.1080/19443994.2012.704696.
Kitada, S., T. Oikawa, S. Watanabe, K. Nagai, Y. Kobayashi, M. Matsuki, K. Tsuchiya, et al. "Removal of Radioactive Iodine and Cesium in Water Purification." Desalination and Water Treatment 54, no. 13 (June 26, 2015): 3494–3501. https://doi.org/10.1080/19443994.2014.923205.

[5] Kelly, Marie. "Fukushima – Some Implications for the Shipping Industry – International Law – Australia." *Mondaq Norton Rose Fulbright Australia*, April 12, 2011. https://www.mondaq.com/australia/international-trade-investment/129262/fukushima–some-implications-for-the-shipping-industry.

[6] "World Oil Transit Chokepoints." U.S. Energy Information Administration, July 25, 2017. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints.

[7] Meredith, Sam. "Here's Why the Strait of Hormuz Is the World's Most Important Oil Chokepoint." CNBC, July 11, 2019. https://www.cnbc.com/2019/07/11/oil-heres-why-the-strait-of-hormuz-is-so-critical-to-energy-markets.html.

[8] "World Oil Transit Chokepoints." U.S. Energy Information Administration, July 25, 2017. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints.

[9] "World Oil Transit Chokepoints." U.S. Energy Information Administration, July 25, 2017. https://www.eia.gov/international/analysis/special-topics/World_Oil_Transit_Chokepoints.

[10] Ratcliffe, Verity, Julian Lee, and Javier Blas. "Why the Strait of Hormuz Is a Global Oil Flashpoint." *Bloomberg.Com*, January 10, 2021. https://www.bloomberg.com/news/articles/2021-01-10/why-the-strait-of-hormuz-is-a-global-oil-flashpoint-quicktake.

Tara Burchmore *is a research assistant at the Belfer Center's Managing the Atom Project and a Master in Public Policy degree candidate at the Harvard Kennedy School with a concentration in Democracy, Politics and Institutions. Prior to the Kennedy School, Tara worked at D.C. lobbying and communications firm the Glover Park Group and spent time doing philanthropic community development work in rural Idaho. Tara studied Government and Public Policy at Dartmouth College.*

Tom Spence *is a data analyst at Aleph Insights and a graduate of the Public Policy and International Affairs graduate programme at the American University of Beirut. Prior to this, Tom acquired an MSc in Natural Sciences from the University of Cambridge and worked in the energy industry across a range of operational and analytical roles.*

Ali Ahmad *is a Research Fellow studying energy policy at Harvard Kennedy School's Project on Managing the Atom and International Security Program. His research interests include energy security and resilience and the political economy of nuclear energy in newcomer markets, with focus on the Middle East.*

U.S. Has a Stockpile of 3,750 Nuclear Warheads

Source: https://www.homelandsecuritynewswire.com/dr20211007-u-s-has-a-stockpile-of-3-750-nuclear-warheads

Oct 07 – The United States on Tuesday (5 October) revealed the number of warheads in the country's nuclear arsenal for the first time in four years, ending a Trump-era blackout on the figure.
The number of nuclear weapons — both active and inactive — in the U.S. military's stockpile stood at **3,750 as of 30 September 2020**, according to the data released Tuesday.

Cold War Peak

The figure is down from 3,785 in 2018. As recently as 2003, the United States' nuclear weapon stockpile was just above 10,000.
In 1967, at the height of the cold war with Russia, the country's nuclear reserve peaked with a total of 31,255 warheads.

"Transparency" the Key to "Disarmament"

"Increasing the transparency of states' nuclear stockpiles is important to nonproliferation and disarmament efforts," the State Department said in a statement.
The Trump administration had kept updated figures a secret after 2018 and had also turned down a request by the Federation of American Scientists to declassify them.
"Back to transparency," Hans Kristensen, director of the Nuclear Information Project at the Federation of American Scientists, said.

Arms Control

The figures were released on the heels of a bid by President Joe Biden's office to restart arms control dialogue with Russia after stalling under Trump.
President Biden's administration is also conducting a nuclear weapons posture and policy review that is expected to be completed early in 2022.
In February this year, Secretary of State Antony Blinken told the Conference on Disarmament that "President Biden has made it clear: the US has a national security imperative and a moral responsibility to reduce and eventually eliminate the threat posed by weapons of mass destruction."

EDITOR'S (naive) COMMENT: This means that the US has 3,750 targets in a single country? Or are they going to attack other countries simultaneously? Do they think that the planet can withstand 3,750 nuclear explosions? Plus the retaliation nuclear explosions from the other side of the conflict? Do they think that the opponent will not be able to launch at least one nuclear missile against their country? Do they think that other non-nuclear countries are "afraid" of nuclear weapons – openly at least? (e.g., Turkey vs. USA or Turkey vs. France).

Nuclear scientist Dr Abdul Qadeer Khan passes away

Source: https://www.geo.tv/latest/374982-nuclear-scientist-dr-abdul-qadeer-khan-passes-away

Oct 10 – Pakistan's renowned nuclear scientist Dr. Abdul Qadeer Khan, 85, passed away Sunday after his health deteriorated.
Dr. AQ Khan is considered the father of Pakistan's nuclear program and is revered at home as a hero for building the Muslim world's first atomic bomb.

Dr. Abdul Qadeer Khan's health started deteriorating Saturday night, after which he was brought to the KRL hospital Sunday morning in an ambulance, at 6:00 am.
Sources said the nuclear scientist experienced discomfort in breathing after which he was brought to the hospital. However, his health took a turn for the worse when his lungs started bleeding.
Doctors tried their best to save the renowned scientist's life but were unable to do so, resulting in his death at 7:04 am. Doctors have said Dr. Abdul Qadeer Khan passed away as his lungs collapsed (Covid-19). The hospital administration is trying to make arrangements to shift Dr. Abdul Qadeer Khan's body to his E-7 residence. His funeral prayers will be offered at the Faisal Mosque in Islamabad at 3:30 pm, said his family.

Speaking to Geo News, Interior Minister Sheikh Rasheed showered praise on the scientist, adding that all necessary arrangements were made to save Dr. Qadeer's life.

Rasheed confirmed that the government will accord a state funeral to the scientist in recognition of his services for Pakistan.

The interior minister said Dr. Abdul Qadeer Khan had helped him a lot in educational activities, adding that he had remained a visionary leader in times when Pakistan was going through a sensitive time.

"He is indeed the *Mohsin-e-Pakistan,*" said Rasheed.

Dr. Abdul Qadeer Khan became a national hero overnight, not only in Pakistan but in the Islamic world as well, when in May 1998 Pakistan gave a befitting response to India by conducting its nuclear tests.

Following the tests, Pakistan became the sole nuclear power in the Muslim world and the seventh country to possess nuclear weapons. Pakistan's nuclear weapons have kept Indian aggression in check.

Dr. AQ Khan's life in a snapshot

Dr. Abdul Qadeer Khan, born on April 1, 1936, in Bhopal, India, was a renowned Pakistani metallurgist and nuclear scientist.

He was among those who migrated to Pakistan in 1947 with their families.

Khan is widely regarded as the "Father of Islamic Nuclear Bomb" or founder of gas-centrifuge enrichment technology for Pakistan's nuclear deterrent program as he developed the Muslim world's first atomic bomb.

He acquired his engineering degree from a university in the Netherlands in 1967 and later went on to secure a doctorate in metallurgical engineering from Belgium.

Dr. Khan was the first Pakistani to be awarded three presidential awards. He has been awarded the Nishan-e-Imtiaz (Order of Excellence) twice and the Hilal-e-Imtiaz (Crescent of Excellence) once.

AQ Khan: The most dangerous man in the world?

Source: https://www.bbc.com/news/world-asia-58857827

Oct 10 – On December 11 2003, a group of CIA and MI6 officers were about to board an unmarked plane in Libya when they were handed a stack of half a dozen brown envelopes.

The team was at the end of a clandestine mission involving tense negotiations with Libyan officials. When they opened the envelopes on board the plane, they found they had been given the final piece of evidence they needed: inside were designs for a nuclear weapon.

Those designs - as well as many of the components for an off-the-shelf nuclear programme - had been supplied by AQ Khan, who has just died aged 85.

Khan was one of the most significant figures in global security in the last half-century, his story at the heart of the battle over the world's most dangerous technology, fought between those who have it and those who want it.

Former CIA Director George Tenet described Khan as "at least as dangerous as Osama bin Laden", quite a comparison when bin Laden had been behind the September 11th attacks.

The fact AQ Khan could be described as one of the most dangerous men in the world by Western spies but also lauded as a hero in his homeland tells you much about not just the complexity of the man himself but also how the world views nuclear weapons.

AQ Khan did not come to Europe as a nuclear spy, but he would become one. He was working in the Netherlands in the 1970s just as his country began a renewed drive to build a bomb in the wake of its defeat in a 1971 war, and fearful of India's nuclear advances.

Khan was working at a European company involved in building centrifuges to enrich uranium. Enriched uranium can be used for nuclear power or, if enriched enough, for a bomb. Khan was able to simply copy the most advanced centrifuge designs and then return home. He went on to build a clandestine network, largely of European businessmen, who would supply the crucial components.

Often described as the "father" of Pakistan's nuclear bomb, in reality he was one of a number of key figures. But he carefully cultivated his own mythology which made him a national hero, seen as having secured Pakistan's safety against the threat of India.

What made Khan so significant is what else he did. He turned his network outwards from import to export, becoming a globe-trotting figure and doing deals with a range of countries, many of which the West considered "rogue states".

Iran's centrifuge programme at Natanz, the source of intense global diplomacy in recent years, was built in significant part on designs and material first supplied by AQ Khan. At one meeting Khan's representatives basically offered a menu with a price-list attached from which the Iranians could order.

Khan also made more than a dozen visits to North Korea where nuclear technology was believed to have been exchanged for expertise on missile technology.

With these deals, one of the key mysteries has always been the extent to which Khan was acting alone or under the orders of his government. Particularly with the North Korean deal, all the signs are the leadership were not just aware but closely involved.
Sometimes it was suggested that Khan was simply after money. It was not so simple. As well as working closely with his country's leadership, he wanted to break the Western monopoly on nuclear weapons. Why should some countries be allowed to keep the weapons for their security and not others, he questioned, criticising what he saw as Western hypocrisy. "I am not a madman or a nut," he once said. "They dislike me and accuse me of all kinds of unsubstantiated and fabricated lies because I disturbed all their strategic plans."

Image caption, Soldiers hold Khan's flag-draped coffin during his funeral (Image source, AFP via Getty Images)

Others in his network, some of whom I met when writing a book about Khan, seemed more in it for the cash. The Libyan deal, brokered in the 1990s, offered rewards but also hastened their downfall.
Britain's MI6 and America's CIA had begun tracking Khan. They watched his travels, intercepted his phone calls, and penetrated his network, offering vast amounts of money (at least a million dollars in some cases) to get members to become their agents and betray secrets. "We were inside his residence, inside his facilities, inside his rooms," a CIA official would say. After the September 11th, 2001 attacks, fears that terrorists could get hold of weapons of mass destruction intensified, and so did the complexity of dealing with Pakistan and persuading it to act against Khan.
In March 2003, just as the US and UK were invading Iraq over weapons of mass destruction which turned out not to exist, Libyan leader Colonel Gaddafi decided he needed to get rid of his program. That would lead to the secret visit from the CIA and MI6 team, and soon after a public announcement of a deal. That would provide the crucial leverage for Washington to push Pakistan to take action against Khan.
Khan was placed under house arrest and even forced to make a televised confession. He would live out his remaining years in a strange nether-world, neither free nor really confined. Still lauded as a hero by the Pakistani public for bringing them the bomb, but stopped from traveling or talking to the outside world. And so the full story of what he did - and why - may never be known.

Preventing an accidental nuclear crisis in Iran and beyond

By Samuel M. Hickey

Source: https://thebulletin.org/2021/10/preventing-an-accidental-nuclear-crisis-in-iran-and-beyond

Oct 11 – There has been no sign as to when nuclear talks with Iran may recommence. But after weeks of consultations, Iran and the International Atomic Energy Agency (IAEA) have reached a deal on "the way and the timing" for UN nuclear inspectors to service cameras installed at Iran's nuclear facilities. This patchwork agreement has kept alive the possibility of recovering a complete picture of Iran's nuclear program and of reviving the Iran nuclear deal since Iran cut inspector access in February. It is also the first real sign of cooperative engagement by Iran since President Ebrahim Raisi came to power in August.

The Iran nuclear deal, also known as the Joint Comprehensive Plan of Action, is the latest experiment in how much UN nuclear inspector access states will tolerate. However, it is under exceptional stress from those who believe military coercion is more effective than systems of denial in stemming proliferation. Days after the least competitive presidential election in the Islamic Republic's history, a drone attack at a centrifuge production facility on June 23 damaged the IAEA's monitoring and surveillance equipment. While the Israeli government did not comment on the attack, the Iran Centrifuge Technology Company, located in the city of Karaj, was reportedly "on a list of targets that Israel presented to the Trump administration early last year." Now, Iran has allowed the IAEA to service cameras in every location but the Karaj site.

Acts of sabotage are diametrically opposed to the global nuclear verification regime because states need to believe that punishment will cease if they comply with the agreed-to framework. Further, failure to revive the nuclear deal could remove the possibility of applying the verification tools gained to other proliferation challenges like North Korea or the next nuclear threshold state. The loss of these techniques would undermine efforts to improve the global nonproliferation regime. As the United States' experiences in leaving Afghanistan make clear, accurate intelligence is critical to making informed decisions and avoiding a crisis. The wrong assumptions can have dire consequences.

Verification evolution: Iraq and the old gold standard

The current nuclear verification protocols are the strongest in history and prioritize the non-diversion of nuclear materials over sovereign jurisdiction; however, many of these legal instruments were born out of crisis and remain voluntary, not mandatory. For instance, the investigative powers of the IAEA were substantially expanded by the creation of the Additional Protocol in 1997 to ensure that states' declarations are both correct and complete.

This protocol has its origin in the Middle East. In the aftermath of the 1991 Persian Gulf War, the IAEA realized it could not detect if nuclear material used in a civilian nuclear program was diverted to a covert nuclear weapons program. International inspectors were stunned to find Iraq's nuclear program, under Saddam Hussein, could produce enough fissile material for a nuclear weapon in 12-18 months, instead of the previous prediction of four to five years. This revelation was the impetus to create the Model Additional Protocol in May 1997, which substantially increased the IAEA's oversight of a comprehensive safeguards agreement.

It took the case of a militarily defeated country to create conditions for more vigorous oversight by the IAEA of a clandestine nuclear program with only a general safeguards agreement. The honor code previously relied upon for monitoring international safeguards was shattered by the Iraq experience. Still, the IAEA has no power to enforce safeguards or penalize those who fail to comply; it can exercise only the authority it is given. These limitations have led some states to act against the assurances of the IAEA with disastrous consequences.

Without access to the full range of data that would be available under a rigorous verification regime, the United States used unsubstantiated and incorrect intelligence claims to back its assertion that Iraq had resurrected its nuclear weapons program despite the assessment of the IAEA. The 2003 invasion would prove that Iraq had not, in fact, reconstructed its weapons program.

Today, 137 states have brought an Additional Protocol into force, but for those countries that have not accepted the protocol—like Argentina, Brazil, Egypt and Saudi Arabia—no one can be sure whether their civilian nuclear programs divert materials for weapons use. In the case of Iran, the Additional Protocol was implemented in 2015 on a provisional basis as outlined in the Iran nuclear deal and planned to be fully adopted in 2023. It has not been fully implemented since late February.

The additions of the Iran nuclear deal

The consistent revision and evolution of the global nuclear order is arguably its greatest success. The adoption of the comprehensive safeguards' agreement, Additional Protocol, and the numerous multilateral institutions to protect, restrict, and monitor all nuclear commerce have strengthened the confidence in IAEA assessment. But those mechanisms were not enough to satisfy concerns about the Iranian nuclear program. Despite its politicization in Congress, the Iran nuclear deal represents the next-generation nuclear verification design to prevent any country from cheating its way to a nuclear weapon in a hurry.

Specifically, the Iran nuclear deal caps the quantity and level of enrichment of uranium as well as the number and sophistication of the centrifuges that are operating and limits heavy water production. It also provides continuous monitoring of centrifuges and centrifuge rotor tubes, continuous access to Natanz, the monitoring of the production or acquisition of any uranium ore concentrate and enhanced managed access, meaning the IAEA can inspect a suspected violation.

The deal also instilled two key principles that should be universalized. First, a civilian nuclear program should be commensurate to its energy or related needs. Second, the IAEA has the right to monitor a ban on "weaponization" activities, which are activities related to developing or procuring equipment for developing nuclear weapons. This is the first agreement ever that defines a set of prohibited activities associated with weaponization, and it set up a procurement channel to monitor the materials and technologies Iran seeks to acquire that could be diverted to a secret program. These blocking efforts and verification tools are the most robust in the world, but extending the timeline for these activities, known as the sunset clauses, or applying them to other countries will require reviving the nuclear deal and preventing further acts of nuclear sabotage.

These measures, at least until the deal expires, will provide a high degree of confidence that weapons-related activity is not occurring. They could also be promoted as a model for other countries wanting to give confidence in the peaceful nature of their own nuclear facilities. Presently, the IAEA is investigating several locations for the presence of nuclear particles of "anthropogenic" origin, meaning materials that have been processed beyond their natural state, but this should not be sufficient grounds for losing monitoring altogether. Iran could assuage such concerns in the future through voluntary transparency, if it is sincere in its contention that it has halted progress toward nuclear weapons. It is in Iran's national self-interest to assure the world they have no secret nuclear agenda.

Politicization of technical assurances

Imagine if every country in the world were subject to continuous monitoring of sensitive nuclear facilities and provided access upstream in the fuel cycle to activities such as mining, milling and conversion. Such access would demonstrably reduce the likelihood that materials gained for ostensibly civilian purposes could be siphoned off to a clandestine program. However, failure to revive the deal risks relegating these additional measures to history.

If the politics of the Iranian nuclear program are too challenging, then the new verification tools will not be useful to solve a real crisis if one crops up in Iran or elsewhere. The great arms control theorist and developer of game theory Thomas Schelling opened his book *Arms and Influence* with the reflection: "One of the lamentable principles of human productivity is that it is easier to destroy than to create." Let's hope the groundbreaking verification and monitoring tools of the Iran nuclear deal are not a casualty of human initiative.

__Samuel M. Hickey__ is a research analyst at the Center for Arms Control and Non-Proliferation. His areas of focus include the geopolitics of nuclear power developments in the Middle East region, nuclear diplomacy, and non-proliferation.

This Is the Devastating Global Effect a Nuclear War Would Have on Earth's Air

By David Nield

Source: https://www.sciencealert.com/these-are-the-devastating-effects-that-smoke-from-a-nuclear-war-would-have

Oct 15 – It's clear that a nuclear war would be catastrophic for us and our planet – but just *how* catastrophic? A new study models the impact that smoke from the fall-out of a nuclear conflict would have on our atmosphere – and the results are predictably bleak.

The models used here are some of the most up-to-date and detailed ever put to the task, and it factors in the complex chemical reactions that would happen in the stratosphere, one of the lower levels of Earth's atmosphere.

What the new findings point to is that damage to the environment could be more severe and last longer than previous studies have found, factoring in damage from the initial heating effect of nuclear explosions as well as the subsequent ozone layer loss.

"Although we suspected that ozone would be destroyed after nuclear war and that would result in enhanced ultraviolet light at the Earth's surface, if there was too much smoke, it would block out the ultraviolet light," says climate scientist Alan Robock, from Rutgers University in New Jersey.

"Now, for the first time, we have calculated how this would work and quantified how it would depend on the amount of smoke."

The team analyzed the impact of both a regional and global nuclear war, with 5 megatons and 150 megatons of soot released respectively. A global war would leave an average ozone layer loss of 75 percent over the course of 15 years, the researchers found, with a regional war resulting in a 25 percent ozone layer loss over a period of 12 years.

According to the study, although the smoke would block the Sun's rays initially, stronger bursts of ultraviolet light would follow within a few years – allowed to hit the surface of Earth through damage to the ozone layer.

Both the initial blast, through chemical reactions with nitrogen oxides, and the smoke itself via heating and reduction of photochemistry which interfere with natural atmospheric interactions, would contribute to the loss of ozone.

With variations in UV light linked to everything from skin cancer to agriculture processes to the survival of entire ecosystems, having much more of it arriving on our planet would have profound consequences for anyone and anything that survived the initial blasts. A global war would be worse, but a regional war would still be devastating. "Conditions would switch dramatically, and adaptations that may work at first won't help as temperatures warm back up and UV radiation increases," says atmospheric scientist Charles Bardeen, from the National Center for Atmospheric Research (NCAR) in Colorado. "Just as the smoke is clearing up, you would get this blast of UV with completely different impacts on human health and agriculture."

The earliest nuclear war models from the 1980s predicted a nuclear winter, with smoke from the blasts and subsequent fires blocking out the Sun and its warmth. Later models have since considered how rising temperatures as well as direct damage might impact the ozone layer through the heating of the stratosphere. It's important to bear in mind that nuclear arsenals continue to change as well: countries like India and Pakistan have most likely gained more weapons and more powerful weapons, while for the US and Russia, the trend is reversed.

This study aims to incorporate as many of these different considerations as possible to show the potential differences between global and regional nuclear war – with the end result being that there's no escape from the effects over subsequent decades, no matter where you are on Earth. "In addition to all the fatalities that would happen almost immediately, the climate effects and the UV effects would be widespread," says Bardeen. "These aren't local to where the war occurs. They're global, so they would affect all of us."

▶▶ **The research has been published in** *Journal of Geophysical Research: Atmospheres*.

David Nield *is a Contributing Journalist at ScienceAlert. He's a freelance journalist who has been writing about science and technology for more than 20 years. Dave's work has appeared in a wide range of publications, including Wired, Popular Science, The Guardian, and Gizmodo, and he has been reporting for ScienceAlert across a variety of subjects since 2015. Dave currently lives in Manchester in the northwest of England, having previously got a 2:1 English Literature degree from the University of Durham in the UK.*

Quick Detection of Uranium Isotopes Helps Safeguard Nuclear Materials

Source: https://www.homelandsecuritynewswire.com/dr20211015-quick-detection-of-uranium-isotopes-helps-safeguard-nuclear-materials

Oct 15 – Analytical chemists at the Department of Energy's Oak Ridge National Laboratory have developed a rapid way to measure isotopic ratios of uranium and plutonium collected on environmental swipes, which could help International Atomic Energy Agency analysts detect the presence of undeclared nuclear activities or material.

“This method builds on a commercial microextraction probe to directly sample solids and subsequently extract the analytes from a surface and into a flowing solution,” said ORNL’s Benjamin Manard. He led the proof-of-concept study, which demonstrated that this sampling mechanism was effective at extracting actinide material (e.g., uranium and plutonium) from environmental swipes. The paper made the front cover of the journal *Analytical Chemistry*.

This innovation could help IAEA’s Network of Analytical Laboratories, or NWAL, which includes ORNL, analyze samples collected from facilities worldwide. DOE NWAL coordinator and co-author Brian Ticknor said, “The microextraction method, if it achieves suitable precision and accuracy, could enable higher sample throughput and faster turnaround time.”

The pen-sized microextraction probe in Advion’s Plate Express product uses a “wet vacuum” to mobilize material from a swipe surface. Manard’s team couples the probe to an instrument that subjects the extracted material to a plasma — an ionized gas hotter than the surface of the sun — and measures the mass-to-charge ratios of the ions generated from the sample.

“It truly is an integrated system,” Manard said. An analyst places a swipe on the extraction stage, selects a region of interest and initiates the process by pressing a button. The microextraction probe lowers onto the swipe, seals it to the stage surface and delivers an acid solvent that dissolves any actinides present in the swipe. Then the solution containing the actinide moves into a mass spectrometer for analysis. “With just a click of a button, you’re going from a solid sample on a swipe to an isotopic measurement,” he said.

With this novel approach to assaying solids, co-author Kayron Rogers of ORNL made a series of swipe samples containing varying amounts of reference standards. The team was able to detect as little as 50 picograms of uranium — 80 million times lighter than a grain of sand. Moreover, the researchers made precise and accurate measurements of the ratios of major and minor isotopes of elements in nuclear reference materials. In a subsequent study, they applied the technique to the analysis of plutonium.

“The benefits of this methodology could extend beyond nuclear material analysis, to many applications requiring direct elemental analysis,” Manard said.

Traditionally, analysts’ ash inspection samples in a furnace before acid digestion and lengthy chemical separations. The process from ashing to analysis could typically take up to 30 days. “The goal of this project was to cut down on those steps in the beginning — ashing and dissolution,” Manard said. “If we could sample the swipe directly, we don’t have to go through the process of trying to turn a swipe into a liquid.”

The researchers work in ORNL’s Ultra-Trace Forensic Science Center, a service center and research facility providing expertise and state-of-the-art inorganic mass spectrometry instrumentation. “This project brings together ideas and technologies developed at ORNL that could provide the next revolutionary change to environmental sampling methodology,” said co-author Cole Hexel, who leads the lab’s Chemical and Isotopic Mass Spectrometry Group.

The researchers are excited about experiments to be conducted over the next two years that will examine the versatility of the methodology.

An innovative approach led by co-author Shalina Metzger is to put a chromatography column between the microextraction probe and the mass spectrometer and have actinide-containing solutions flow through connective tubing. Whereas the column would allow uranium to flow through, it would retain plutonium for later elution and measurement. The approach would improve elemental sensitivity and identification.

During their studies, the researchers found that nitric acid degraded the microextraction probe head. Future experiments will seek to optimize solvent conditions for extracting actinides in various chemical forms. “We’re also using ORNL’s unique 3D-printing facilities to fabricate components with polymers that are more resistant to the extraction solvent,” Manard said.

Ultimately, the ORNL researchers hope to develop the capability to differentiate individual analytes collected on a swipe to provide a holistic snapshot of an inspected facility’s activities. Their coupled microextraction and mass spectrometry methodology shows promise as a revolutionary approach toward that aspiration. Manard’s team is hopeful that the coming years of research will prove fruitful and turn this goal into a reality.

Radiation warning signs to be installed along Russia’s Techa River

Source: https://www.neimagazine.com/news/newsradiation-warning-signs-to-be-installed-along-russias-techa-river-8039610

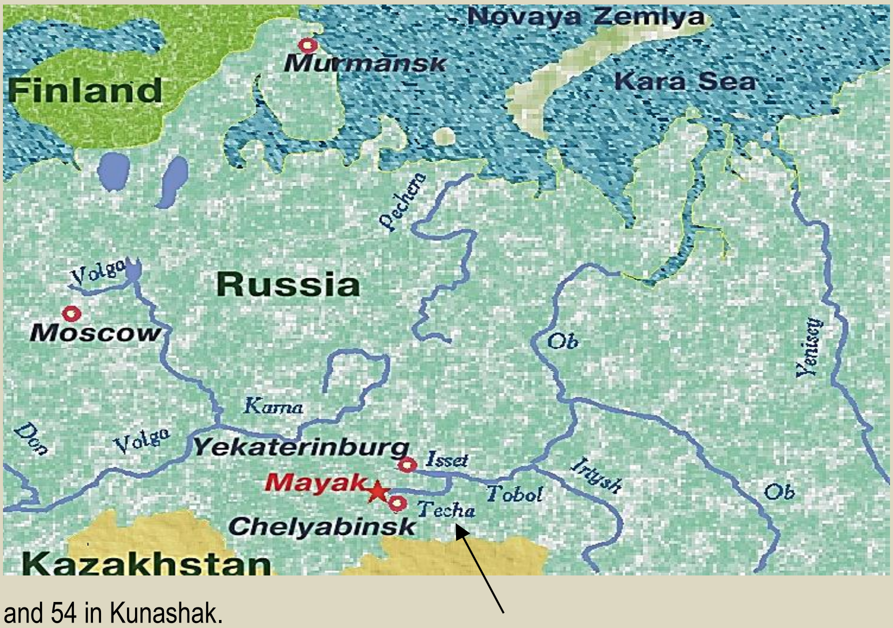
July 2020 – Some 300 radiation warning signs are to be installed along the Techa River, which is adjacent to the radiochemical plant at Russia’s Mayak production association in Ozersk, Chelyabinsk region, Mayak reported. Mayak produces nuclear weapons components and isotopes, and stores and reprocesses used nuclear fuel.

When the site was established in the years after World War III and during the early years of the nuclear arms race, secrecy was paramount and safety was not a consideration – a factor common to all the nuclear weapons states at that time. There were no adequate technologies for recycling of radioactive

waste, which was dumped directly into the Techa River. For three years (1949-1951) some 3m curies of radionuclides were dumped in this way. In 1951, the discharge was stopped, and the waste was collected in a cascade of reservoirs.

The Techa River remains contaminated, long after Mayak stopped dumping waste but the radiation is relatively low. The only inhabited village down the river is called Brodokalmak and is about 85km downstream from Ozersk, and 50km away from a bridge crossing the river. Halfway between the bridge and Brodokalmak is the abandoned village of Muslyumovo, which was inhabited until about a decade ago, when state nuclear corporation Rosatom offered to relocate its 2,500 residents.

According to the results of an auction, the application and price offer of Mayak for this work are recognised as priority. Work on the installation of signs will be carried out in four municipalities of the Chelyabinsk region - in Argayash, Sosnovsky, Krasnoarmeysky and Kunashak regions. Contracts are being signed with each municipality to carry out the work. Under the terms of the contracts, 27 warning signs will be installed in the Argayash region, 66 in Sosnovsky, 153 in the Krasnoarmeysky, and 54 in Kunashak.



The priority locations for the installation are the entrances and approaches to the Techa River from nearby settlements, as well as roads and railways crossing the river. The signs will be located at a distance from each other - from the Techen cascade of water bodies to the border with the Kurgan region. Until November 1, 2020, as determined by the terms of the contracts, 300 signs will be installed containing a warning about the radiation hazard and information on the main restrictions established on the Techa River.

"All the work on the installation of warning signs is carried out in accordance with the measures included in the special environmental programme "Rehabilitation of radiation-contaminated areas of the Chelyabinsk Region for 2010–2020", said Pavel Andronnikov, Head of Planning and Environmental Monitoring at Mayak PA .

All signs will be 500 x 1000 mm with the use of retroreflective materials similar to road signs. Contract preparatory work has already begun. Surveyors of the industrial safety service, together with employees of the Mayak ecology service, are performing geodetic linkage of places for installing signs in accordance with the coordinates determined by the technical specifications. This work is necessary to accurately determine installation sites, as well as to provide technical feasibility of work.

Nuclear War's Smoke Would Cause Climate Change, Threatening Global Food Supplies

Source: https://www.homelandsecuritynewswire.com/dr20211019-nuclear-wars-smoke-would-cause-climate-change-threatening-global-food-supplies

Oct 19 – Nuclear war would cause many immediate fatalities, but smoke from the resulting fires would also cause climate change lasting up to 15 years that threatens worldwide food production and human health, according to a study by researchers at Rutgers University, the National Center for Atmospheric Research and other institutions.

Scientists have long understood that nuclear weapons used on cities and industrial areas could initiate large-scale fires whose massive amounts of smoke injected into the stratosphere could cause global climate change, leading to the term "nuclear winter."

But in the new study, researchers for the first time used a modern climate model, including aerosols and nitric oxide emissions, to simulate the effects on ozone chemistry and surface ultraviolet light caused by absorption of sunlight by smoke from regional and global nuclear wars.

This could lead to a loss of most of our protective ozone layer, taking a decade to recover and resulting in several years of extremely high ultraviolet light at the Earth's surface and further endangering human health and food supplies.

"Although we suspected that ozone would be destroyed after nuclear war and that would result in enhanced ultraviolet light at the Earth's surface, if there was too much smoke, it would block out the ultraviolet light," said one of the study's authors Alan Robock, a Distinguished Professor in the Department of Environmental Sciences at Rutgers University-New Brunswick. "Now, for the first time, we have calculated how this would work and quantified how it would depend on the amount of smoke."

The study's results showed that for a regional nuclear war between India and Pakistan that would generate five megatons of soot, the enhanced ultraviolet light would begin within a year. For a global war between the United States and Russia generating 150 megatons, it would only begin after about eight years. For intermediate amounts of smoke, the effects would fall between these extreme cases.

For a global nuclear war, heating in the stratosphere and other factors would cause a 15 year-long reduction in the ozone column, with a peak loss of 75 percent globally and 65 percent in the tropics. This is larger than predictions from the 1980s, which assumed large injections of nitrogen oxides but did not include the effects of smoke.

For a regional nuclear war, the global column ozone would be reduced by 25 percent with recovery taking 12 years. This is similar to previous simulations but with a faster recovery time due to a shorter lifetime for soot in the new simulations.

"The bottom line is that nuclear war would be even worse than we thought, and must be avoided," Robock said. "For the future, in other work, we have calculated how agriculture would change based on the changes of temperature, rain and sunlight, but have not yet included the effects of ultraviolet light. In addition, the ultraviolet light would damage animals, including us, increasing cancer and cataracts."

►► **The study appears in the** *Journal of Geophysical Research – Atmospheres*.

Turkey's Nuclear Dreams are a Nightmare for the International Community

By Konstantinos Apostolou-Katsaros

Source: https://greekcitytimes.com/2021/09/13/turkeys-nuclear-dreams-are-a-nightmare-for-the-international-community/

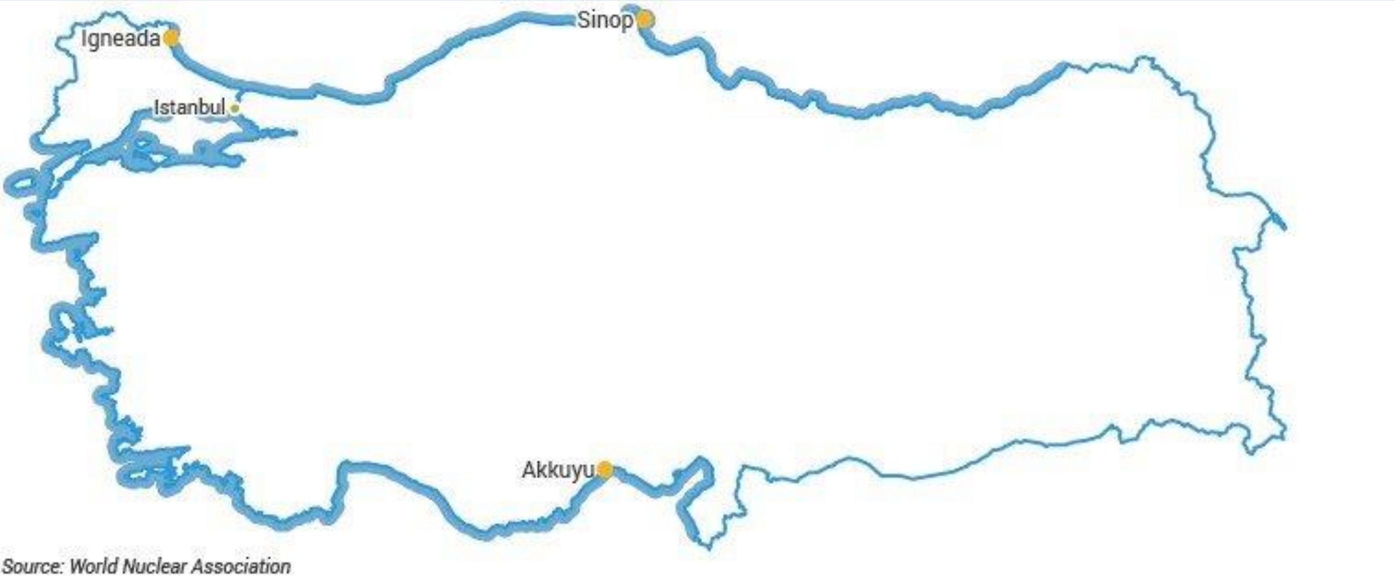
Sept 13 – Turkey's role in the Greater Middle East is under international scrutiny after asserting its intention to become a regional middle power in the emerging multipolar international system. To achieve this it gradually moves away from the West (and the North Atlantic Alliance) in an attempt to pivot east (Eurasia). Purchasing the Russian made S-400 missile system was the onset of this risky foreign policy shift that is becoming progressively a headache for its Western allies. Turkey's ambitions however are restrained by the lack of a nuclear arsenal which would serve as a vehicle to its independence from the NATO shield.

Nuclear Proliferation

The significance that Ankara attributes to nuclear weapons is evident from the relevant statement of Turkey's President Recep Tayyip Erdoğan in September 2019 at the Economic Forum of Central Anatolia. "Some countries have missiles with nuclear warheads, not one or two. But (they tell us) we can't have them. This, I cannot accept" he stated and added "we have Israel nearby, as almost neighbors. They scare (other nations) by possessing these. No one can touch them." The Turkish President concluded saying "we are working on this", thus implying that they their efforts to acquire a nuclear arsenal is already in progress. The Turkish President also clarified his intentions to the UN General Assembly in 2019, when he criticized the "Treaty on the Non-Proliferation of Nuclear Weapons" (which Turkey signed in 1980), since it prohibits countries such as Turkey to develop nuclear weapons. It should be stated that Turkey has signed the "Comprehensive Nuclear-Test-Ban Treaty" back in 1996. However, the revisionist goals of the Turkish leadership, yield little hope on Turkey keeping its obligations on both treaties.

Will Turkey soon become a nuclear-weapon state?

"I hope it will not happen, but Turkey seems to be in quest of it" said Dr. Moritz Kütt, a nuclear weapons expert and researcher at the Institute for Peace Research and Security Policy of Hamburg University. He also added that "nuclear weapons will not calm the security situation; instead they will bolster up Turkey's 'ego'. Nuclear bombs guarantee a place in the forefront of geopolitics. An idea that Erdoğan likes a lot." More concerned appeared the Israeli political scientist Yakov Kedmi who clarified that, it is only a matter of time before Ankara acquires a nuclear arsenal and it is impossible to prevent this. It is also reminded that on February 15, 2010, former Israeli Prime Minister Benjamin Netanyahu had warned former Greek Prime Minister George Papandreou that, Turkey already had the capability to become a nuclear-weapons state.



Source: World Nuclear Association

This concern intensified after aljazeera.com brought to light information which suggested that Islamabad intends to covertly support Turkey's nuclear-weapons program.

Such alarm bells have been ringing since 2015, when German secret services discovered that Turkey appeared to be following Iran's footsteps. It was revealed that President Erdoğan demanded back in 2010 to secretly start the construction of uranium enrichment facilities. In addition, there are suspicions that Turkey has already attained enriched uranium originating from a former Soviet republic. Notably, Turkey was also involved in the activities of Pakistani nuclear smuggler Abdul Qadeer Khan, who sold thousands of centrifuges (their electronic systems came from Turkey) between 1987 and 2002 in Iran, North Korea and Libya.

The ballistic missiles and space program objective

The prerequisite of a nuclear weapons program is the ballistic missile program which aims to develop missiles that will carry nuclear warheads. The Turkish-made Short Range Ballistic Missiles (range >1000km) are already in production while there are reports of producing missiles with a range of over 1000km. In addition, emphasis should be given to the announced Turkish space program.

Firstly, because it will support the volume of data related to the satellite navigation of the Turkish UAVs, at the same time with the ballistic missiles.

Secondly, because it will facilitate the development of missiles with a range of 3500km or greater (Medium Range Ballistic Missiles or larger).

The threat imposed on the states that lay within this range is obvious without considering the possibility of launching the ballistic missiles from surface ships or submarines. Thus the Turkish space program should be closely monitored to clarify whether it is covertly used to support its nuclear weapons program.

Equal distances from Russia-USA, Closer to Pakistan

The construction of the Akkuyu Nuclear Power Plant (as well as those planned to be built in Sinope and in Eastern Thrace) is certainly not coincidental either. This aims to reduce Turkey's energy dependence on one hand (in 2020, approximately 72% of its energy demand was met through imports) and on the other hand, it serves as an induction in the nuclear expertise. Dozens of Turks are already studying Nuclear Engineering at Russian universities since 2015.

Russia has every reason to provide the know-how for the construction of Turkey's Akkuyu Nuclear Power Plant in an attempt to hinder NATO's unity. However, the Russian-Turkish opportunistic cooperation will not feed the latter's ambition in attaining nuclear weapons. Their competing interests collide in many cases. Russia wouldn't want to see a nuclear arsenal in such close proximity to its borders. The leader of the Liberal Democratic Party of Russia Vladimir Zhirinovsky is convinced: if Iran and especially Turkey have nuclear weapons, they will turn against Russia. This does not suggest that Turkey will not achieve its aim. On the contrary it means that Turkey will have to overcome many obstacles set by important states with interests in the wider region, such as Israel, France, Egypt, Saudi Arabia and the UAE. Above all, Turkey will have to face the growing conflict of interest with the US. There are many reasons upon which Turkey will not be tolerated as nuclear-weapon state. As abovementioned, this will instigate its geostrategic autonomy, causing the existing Euro-Atlantic security architecture to disintegrate. In addition, it will trigger a nuclear arms race in the wider region. All of these destabilization fears have long been addressed by the US.

Consequently Turkey's alleged choice to approach the co-religionist (and less pro-Western under the leadership of Imran Khan) and willing Pakistanis for supporting its nuclear-weapons program (1 , 2 , 3 and 4), does not come as a surprise, since it has little or no other option in this venture. The two Sunni forces share the same strategic goals in the Mediterranean and India which derive from their close historic and economic ties. Their defense cooperation agreements (1 , 2 , 3 , 4 , 5 , 6 and 7) are already expanding as a result of the events in Afghanistan which contributed to further strengthen their relations (1 , 2 and 3). The director of the Middle East Center for Reporting and Analysis, Jonathan Speyer, stresses that "Ankara's strong and burgeoning strategic ties to Pakistan are causing international concern regarding the possibility of a transfer of nuclear weapons knowledge between the two countries. Turkey already has the will and the raw materials. This knowledge is the factor it currently lacks."

Drifting apart from the West

Nonetheless, Turkey's eagerness to embark on a nuclear-weapons program should be seen in the bigger context. There are clear indications that the Eurasianist ideology creeps in Turkey's top-ranking policymakers. Analysts identify this ideology as a Turkish version of the Ba'athism in the Arab world. The Eurasianists argue that Turkey's interests lie outside the Western world and therefore should join the "anti-imperialist" camp led by Russia and China.

When speaking about Afghanistan, Turkish president Recep Tayyip Erdoğan said: "Imperial powers entered Afghanistan; they have been there for over 20 years. We also stood by our Afghan brothers against all imperial powers." A similar statement made by the Pakistani Prime Minister Imran Khan, revealed the common grounds of the two Sunni forces in their ideological (and religious) beliefs. He said that the Taliban are "breaking the chains of slavery." Some would argue that both statesmen are influenced by the jihad theorist Sayyid Qutb (author of the influential book "Milestones") and his idea of victimization of Muslims by foreigners or "imperialists". He believed that western nations are attempting to undermine Islamic empowerment thus jihad is the tool to liberate the "suppressed" Muslims from the "imperial powers" (see also 1 , 2 , 3).

Conclusions

It is evident that the alleged new venture of Turkey in the nuclear weapons field is in all cases a cause of serious concern for its Western allies. Its decision to drift away (1 and 2) from the North Atlantic alliance and become a strategically autonomous Eurasianist power, presupposes the acquisition of a nuclear arsenal. This will lead to a reflexive nuclear arms race of key states in the wider sensitive region, hindering the already fragile balances and undermining the existing Euro-Atlantic security architecture. Such prospect cannot be reversed by false hopes on a softer policy after a leadership change in the Turkish elections of 2023, or worst by transactionalism that will boost Turkey's confidence. It is arguable that Turkey's overambitious geopolitical balancing act is pushing the limits of its diplomatic, economic and military capabilities. Therefore, restraining its activities in these fields (especially its military hardware / technology as well as the space, missile and nuclear programs) by the states affected most and the US, is most likely to weaken its eagerness and tame its revisionist goals.

▶▶ **Read also:** Turkey and the Bomb

Konstantinos Apostolou-Katsaros *is a special analyst- consultant. His area of interest is in Foreign Affairs and Greek-Turkish relations. He holds a Ph.D. and M.Sc. from the School of Environment and Technology of Brighton University (UK) where he worked as a Lecturer and Research Associate.*

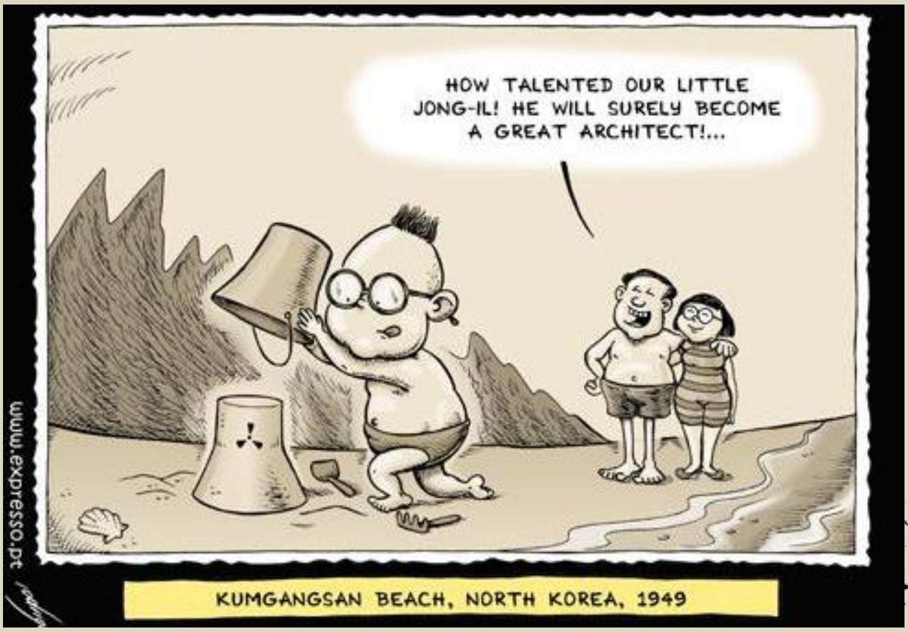
EDITOR'S COMMENT: The close relationship between Turkey and Pakistan brings to mind, speaking about nuclear weapons' ambitions, the well-known saying "there is no smoke without a fire". According to a Greek website "*German newspapers reported in 2013 that Turkey had already set up a secret nuclear power center where Turks and Pakistanis were working on uranium enrichment. These facilities were in areas full of forests in Turkey but were discovered after a wave of wildfires hit the country and the Mediterranean region last summer*." In addition, according to Indian mass media "*a meeting took place on December 22-23, 2020 in which Pakistani Defense Minister Mian Muhammad Hilal Hussain and Deputy Chief of Staff of the Turkish Army Selcuk Bayraktaroglu represented the two countries. There are many indications that the delivery of nuclear weapons to Turkey was discussed! The meeting was also attended by Ismail Demir, head of the Turkish Defense Industry, and Temil Kotil, CEO of Turkish Aerospace Limited (TAI). General Sahir Shamshad of the Pakistan Army also met with Lieutenant (?) Wali Turkchi. Sources said that the transfer of missile technology between the two countries was discussed, as well as the purchase of Turkish UAVs from Pakistan*." Of course, time will show if all this worrying information is true or false. But what if it is true?

Dissertation

Deception in Covert Nuclear Weapons Development

A Framework to Identify, Analyze, and Mitigate Future Long-Term Deception Efforts

Brian J. Gordon


HOW TALENTED OUR LITTLE JONG-IL! HE WILL SURELY BECOME A GREAT ARCHITECT!...
www.expresso.pt
KUMGANGSAN BEACH, NORTH KOREA, 1949

International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

EXPLOSIVE NEWS

What is tiffin bomb, the new security threat in Punjab | Exclusive

Source: https://www.indiatoday.in/india/story/tiffin-bomb-punjab-pakistan-border-terrorism-exclusive-1856503-2021-09-24

Sept 24 – A new security threat has emerged in Punjab in the form of tiffin bombs ahead of the festive season and assembly election. In the last two months, five such tiffin bombs have been recovered in different parts of Punjab.
Police sources said a major tragedy has been averted due to prompt response by the cops based on specific intelligence.

On Thursday, Punjab Police claimed to have busted a terror module backed by Khalistan Tiger Force. Three operatives were arrested with a tiffin bomb from Bhikhiwind village of Tarn Taran district, which is located nearly 10 km from the India-Pakistan border.
The police also recovered a consignment of arms and explosives consisting of two pistols, one grenade and a packet containing explosives near Chungan village, all of which were dropped using a drone.

A tiffin bomb looks like a regular lunchbox but is rigged with an Improvised Explosive Device (IED).

Moreover, it has also been found that explosives recovered by the Delhi Police Special Cell from six people who were allegedly part of a "Pakistan-orchestrated ISI terror module" were dropped by drones from Pakistan in Punjab.

What is a tiffin bomb?

A tiffin bomb is a lunchbox rigged with an Improvised Explosive Device (IED). It is basically a tiffin carrier which is used by workers or school-going children to store their lunch.
There have been at least eight-nine tiffin bombs recovered in Punjab.

"This is a strategy by Pakistan to escalate violence in the state and cause communal tensions," a senior Punjab Police officer said.
NSG's National Bomb Data Centre (NBDC) has been to the state at least half a dozen times to analyse the material concealed in the tiffin carriers. Their findings have only confirmed what was long suspected -- a clear Pakistan imprint.
"These tiffin bombs are made in Pakistan, the signature of fabricature is with the Khalistan network. The bombs have RDX which are well fabricated with proper foundry casing," top sources in the NSG told India Today.
A security grid officer said a 500-700 gram RDX can cause major damage in a 10-foot area. "The idea is to send in explosives and use the innocuous looking tiffin to be planted in a crowded place during the upcoming festival season in order to cause panic and stampede-like situations to cause further harm. In most cases, there is no ideology. Pakistan ISI is using petty criminals and drug smugglers to send in the 'explosive consignment through drones'," the officer said.

One module a week busted since August 8

One of the first such tiffin bombs was recovered on August 8 from a village in Amritsar. Hand grenades and 100 rounds of 9 mm pistol ammunition were also recovered.

According to police, two thermocol boxes wrapped with plastic tapes were dropped by drones near Bharopal village located near the Indo-Pak border. The case has since then been handed over to the National Investigation Agency (NIA).

"It is likely that all these are linked, but it may be difficult to prove," an NIA official said.

NSG said there was a "commonality" in all the recoveries.

Since August 8, a module has been busted once per week. Kapurthala Police recovered two hand grenades, a tiffin bomb and other explosive material in Phagwara on August 20. A third tiffin box was used to blow off an oil tanker in Ajnala on August 8.

A motorcycle rigged with explosives that went off in Fazilka district was to be parked at a crowded area in Jalalabad as part of the plot. The motorcycle exploded in Jalalabad, killing its 22-year-old rider.

Use of drones to smuggle weapons across border

The NIA investigation into the first weapon-dropping case in Punjab has been an eye-opener for security agencies. The case was recorded in 2019 from Chohla Sahib in Punjab's Tarn Taran.

A CID inspector had received information of a huge cache of arms and ammunition, fake Indian currency notes being dropped inside Indian territory through drones. As luck would have it, the drone malfunctioned and crashed on August 19, 2019.

The location of the villages for dropping weapons was given by Akashdeep Singh, who is now lodged in Amritsar jail. He was given a contact of Gurmeet Singh alias Bagga in Germany, a close associate of Ranjeet Singh alias Neeta. They had links to Pakistan.

The conspiracy was plotted on WhatsApp. "The location was given by the local criminal for some money," an official said.

With the upcoming festival season and election season, security agencies and Punjab Police are on tenterhooks to thwart any such plan by Pakistan-backed operatives again.

Indian scientists develop cost-effective device to rapidly detect explosives

Source: https://www.tribuneindia.com/news/nation/indian-scientists-develop-cost-effective-device-to-rapidly-detect-explosives-315644

Sept 24 – Indian scientists have developed a thermally stable and cost-effective electronic polymer-based sensor for rapidly detecting nitro-aromatic chemicals used in high-energy explosives.

The detection of explosives without destroying them is essential for protection, and criminal investigations, minefield remediation, military applications, ammunition remediation sites, security applications. Chemical sensors play a vital role in such cases.

Though explosive poly-nitroaromatic compounds can usually be analysed by sophisticated instrumental techniques, the requirement for quick decision-making in criminology laboratories, reclaimed military sites or to detect explosives in possession of extremists often require simple and cheap field techniques which are non-destructive in nature.

Non-destructive sensing of nitroaromatic chemicals (NACs) is difficult. While earlier studies are based mostly on photo-luminescent property, detection of the basis of a material's conducting property has not been explored so far. Detection on the basis of conducting property helps in making a handy detection device where results can be seen with the help of a LED.

To overcome such disadvantages, a team of scientists led by Dr Neelotpal Sen Sarma from the Institute of Advanced Study in Science and Technology, an autonomous institute of the Department of Science and Technology, has developed an **electronic layer-by-layer (LBL) polymer detector consisting of two organic polymers, which undergoes a drastic change in impedance in the presence of very low concentration of NACs vapour within few seconds.** "An electronic sensing device build around a polymer gas sensor can quickly detect the explosive on-site," said Dr Sarma. The tri-layer polymer matrix was found to be very efficient molecular sensor for nitroaromatic chemicals. The sensor device is quite simple and reversible in nature and its response does not alter with varying operating temperature in presence of other common chemicals and humidity. The device can be operated at room temperature, has a low response time and negligible interference from other chemicals. The fabrication is a very simple, is negligibly affected by humidity, and the cholesterol-based polymers used are biodegradable.

How Big Was the 2020 Beirut Explosion?

Source: https://www.homelandsecuritynewswire.com/dr20211008-how-big-was-the-2020-beirut-explosion

Oct 08 – On 4 August 2020, one of the largest non-nuclear explosions in history pulverized a Beirut port and damaged more than half the city. The explosion resulted from the detonation of tons of ammonium nitrate, a combustible chemical compound commonly used in agriculture as a high-nitrate fertilizer, but which can also be used to manufacture explosives.

Since that time, the explosive yield estimates varied widely, and in some cases, were inconsistent with what would be expected based on the amount of ammonium nitrate stored at the Beirut harbor. In addition, the crater size, seismic magnitude and mushroom cloud height seemed to be inconsistent.

Lawrence Livermore National Laboratory (LLNL) physicist Peter Goldstein has studied how water saturation of the explosive, ground and possibly water and debris from the near-source environment can help reconcile differences in the yield estimates obtained using these different measurements. Official records indicate that roughly 2.7 kilotons of explosive material were stored at the Beirut harbor warehouse where the explosion occurred. The detonation of these materials resulted in a large crater and seismic measurements suggested it was possible that the yield was at least a few kilotons and possibly much greater. However, there were other estimates that suggested the yield was quite a bit smaller, possibly as little as half a kiloton.

Goldstein's research, which appears in *Countering WMD Journa*, analyzes the crater dimensions, seismic magnitude estimates and the cloud height of the explosion and shows that all the data are consistent with a yield of around a kiloton when water/saturation is accounted for. "Water in the near-source environment can have a significant effect on many observations, including crater formation, cloud rise, seismic magnitudes and blast wave effects," he said.

Goldstein used crater-size observations from satellite imagery and empirical data for scaled crater radii from past chemical and nuclear explosions to estimate the yield.

"The evidence suggests that the relatively large crater radius is due to a high degree of saturation of the ground beneath the explosion. It is likely that this saturation increased coupling of shock wave energy to the surrounding material and reduced the effective stress/strength of the material," he said.

He also found that yield estimates based on seismic body-wave magnitude, the maximum debris cloud height and the observed crater depth corroborated the estimates based on crater radius.

Confidence in the reliability of these models is critical for emergency response planning to mitigate potential consequences from accidents such as the Beirut explosion or deliberate acts that could involve improvised nuclear devices or radioactive dispersal devices.

This research also is relevant to nuclear explosions. It suggests that features of the near-source environment can have a large effect on shock/blast waves, seismic motions and crater formation, as well as cloud rise and fallout effects. The effects also propagate into things like the yield estimate. Goldstein said he expects near-source features like water to have a significant effect on other explosion phenomena, including radiation transport and post-detonation debris formation.

Beirut port blast claims another victim, 13 months later

Source: https://www.thenationalnews.com/mena/lebanon/2021/09/28/beirut-port-blast-claims-another-victim-13-months-later/

Sept 28 – A man injured in the Beirut port explosion has succumbed to injuries 13 months after the explosion.

Ibrahim Harb, 35, suffered serious head injuries after 2,500 tonnes of ammonium nitrate exploded at the port in August last year, leaving him in a coma for three months.

He then spent almost a year at a rehabilitation centre, drifting in and out of consciousness until his family moved him home last week. He was there for three days before dying on Monday night.

Mr Harb was laid to rest in Beirut on Tuesday, in an emotional funeral. His death raised the number of people killed in the port explosion to at least 215.

“May God punish whoever was behind it. What else can we say?” his brother Mazen told AP.

Mr Harb, an accountant, had been working at his office in downtown Beirut when the blast happened. He leaves behind a fiance.

Ahmad Mroue, who runs the Lebanese NGO Maan, which works with victims of the blast, said that the death coming on the same day as the suspension of the port blast investigation only underlined the unwillingness of Lebanon's political class to see justice served.

“It’s really sad that we lost another person. Unfortunately, the politicians in this country count them only as numbers, they don’t look at them as human beings. They deserve justice,” he said. “What happened yesterday, just before Ibrahim died was really sad because again we see how politicians are treating the investigation and the judge – the main thing they are doing now is blocking justice.”

The port blast was suspended for a second time after a former minister lodged a complaint, questioning the lead judge’s impartiality.

Members of the Lebanese Internal Security Forces lay flowers in front of a memorial to the victims of the explosion in Beirut's port last year.

Nouhad Machnouq, a former interior minister, filed the complaint on Monday, saying that Tarek Bitar, who is heading the investigating, was acting beyond his remit.

Mr Machnouq, who is one of four former ministers facing questioning in relation to the blast, requested the removal of Mr Bitar, prompting the investigation's freezing.

The suspension prompted outrage among families of the blast's victims, yet lawyers of Maj Gen Abbas Ibrahim, the head of the influential General Security agency, accused Mr Bitar of populism in running the investigation.

"It is unfortunate that Judge Bitar experienced the disappointments of the legal breaches that he reaped during his populist management of the port explosion file," he said in a statement.

He accused Mr Bitar of acting to "dilute the truth and underline it with fictitious heroics".

The investigation has been beset by delays and complaints, with high-profile figures repeatedly refusing to show up when summoned for questioning.

Earlier this month, former prime minister Hassan Diab left the country to visit family in the US, missing his scheduled questioning.

Marathon bomber faces death sentence in high court

Source: https://texasnewstoday.com/marathon-bomber-faces-death-sentence-in-high-court/492764/

Oct 09 – The Biden administration **will try to convince** the Supreme Court this week to revive the death penalty for the convicted Boston Marathon bomber Johar Zarnaev.

Tsarnaev's guilt for the deaths of three people in a shocking bombing near the finish line of the 2013 marathon is not an issue for judges to hear on Wednesday.

Also, even if the federal execution is suspended and President Joe Biden calls for the abolition of the federal death penalty, courts are unlikely to ponder the government's aggressive pursuit of a death sentence against Tsarnaev.

Instead, the main focus is that Tsarnaev's lawyer supports the jury's claim that his brother Tameran is the mastermind of the attack and his impressive younger brother is somehow less responsible. There is evidence that you want to hear it. Evidence suggests that Tamaranza Lunaev was involved in the killing of three people in Waltham, a suburb of Boston, on the 10th anniversary of the 9/11 terrorist attacks.

Last year, the United States Court of Appeals in Boston ruled that a judge had mistakenly ruled out evidence and dismissed Zarnaev's death sentence. There is a second problem with this case. Whether the judge has done enough to ask the jury about the exposure of the bombing to widespread news coverage.

The Trump administration, which has executed 13 executions in the last six months, immediately appealed. When the new administration did not show a change of view, the court agreed to consider the case.

Tsarnaev's lawyer has never objected to him and his brother firing two bombs near the finish line of the marathon on April 15, 2013. Christol Campbell, a 29-year-old restaurant manager from Medford. Eight-year-old Martin Richard, who was going to see a marathon with his family, was killed. More than 260 people were injured.

Sean Collier, a police officer at the Massachusetts Institute of Technology, was shot dead in a car during a four-day search for a bomber. Boston police officer Dennis Simmons also died a year after being injured in a confrontation with a bomber.

Police captured bloody and injured Johar Zarnaev in Watertown, a suburb of Boston. He was hiding in a boat parked in the backyard hours after his brother died. Tamerlan Tsarnaev, 26, was involved in a gun battle with the police and was run over by his brother during his flight.

Tsarnaev, now 28, has been convicted of all 30 charges against him, including plots and the use of weapons of mass destruction and the killing of Collier in an attempt to flee the Tsarnaev brothers. The Court of Appeals upheld everything except some of his convictions.

A convicted murderer who is appealing to a jury for lifelong detention rather than voting for execution has room to provide evidence that he believes is less likely to be sentenced to death.

According to defense lawyers, the 2011 killings were at the heart of their claim that Tsarnaev was deeply influenced and exacerbated by his respected brothers, who had already shown the potential for extreme violence. They said the younger brothers were less responsible for the marathon mayhem.

"Therefore, the evidence makes it very likely that Jowhaar acted under the radical influence of Tameran and Tameran led the bombing," said Ginger Anders, a leading figure in the Supreme Court of Tsarnaev. Submitted to the High Court.

As part of that, the administration did not challenge his brother's leadership role, claiming that the defense lawyer was able to make that claim. Nevertheless, the jury sentenced Tsarnaev to death, written by Chief of Justice Brian Fletcher.

"We chose to launch a terrorist attack on children and other innocent spectators in the marathon, and the jury held him responsible for that choice," Fletcher wrote.

The explanation for Tameran's involvement in the previous murder came from a friend, Ibragim Todashev, who was interviewed by investigators after the marathon attack. Todashev told authorities that Tamerlan recruited him to rob three men and they tied them up with duct tape before Tamerlan cut his throat to leave no witnesses.

With a strange twist, he was shot dead after authorities said he had attacked an agent while Toda Chef was being interrogated in Florida. The agent who killed Todashev eliminated all criminal misconduct.

Jowhaar also told a college friend that his brother was involved in the murder of Waltham and committed "jihad" there, a lawyer representing the friend told the prosecutor. No one has been charged with triple murder.

However, prosecutors said the evidence linking the killings of Tameran and Waltham was unreliable, unrelated to Jowhaar's participation in the marathon attack, and only confused the jury. The judge who oversees the trial agreed.

Nevertheless, authorities had previously used Todashev's statement to apply for a warrant to search Tameran's car after the bombing, looking for blood, DNA, and other evidence associated with the three murders.

After defending their credibility to obtain a warrant, Anders called the explanation of the government statement an unreliable "breathtaking face."

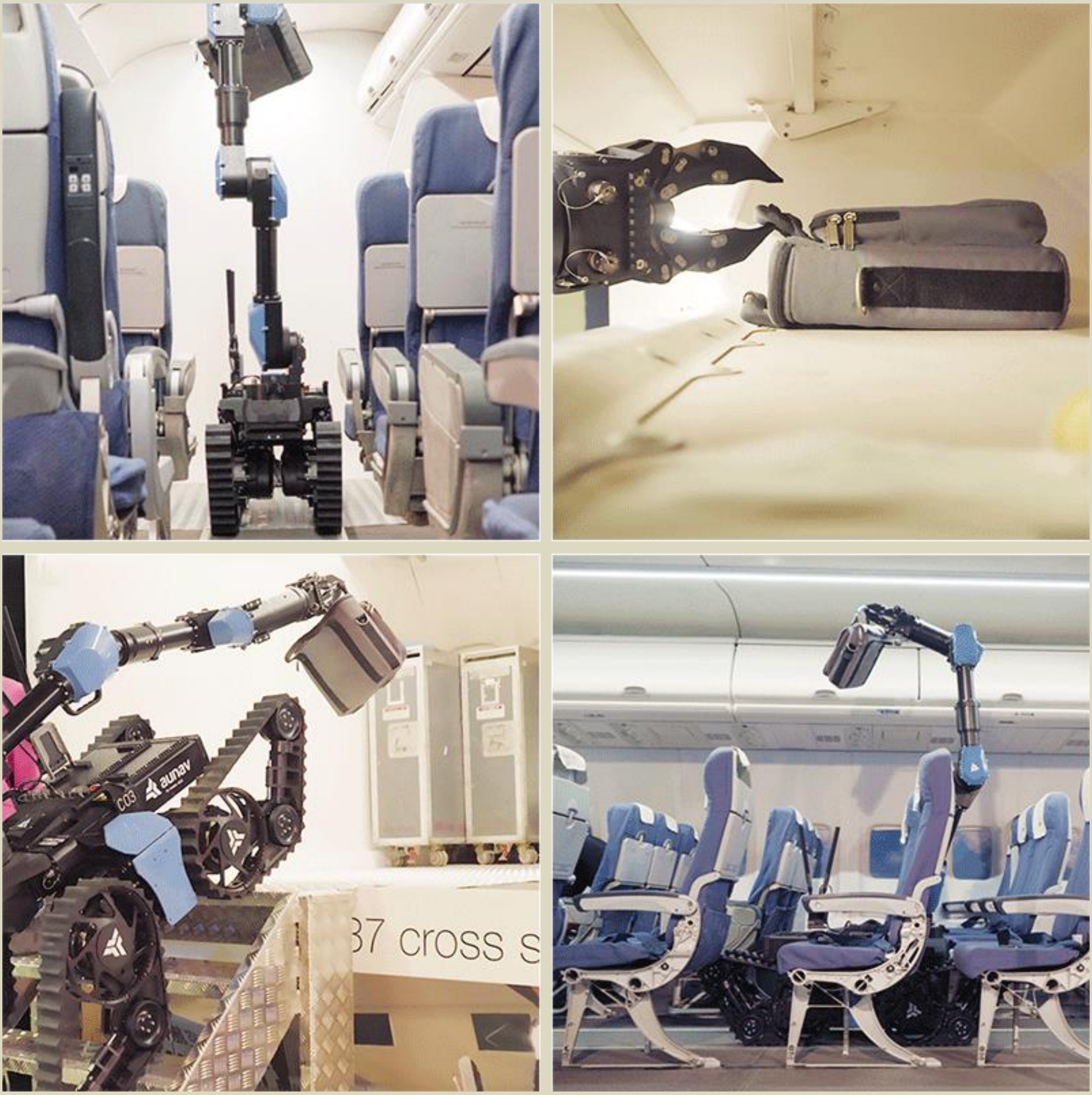
The Justice Department said various standards were applied and when seeking a search warrant, federal agents did not say that all the words Todashev said were true. The Tsarnaev court ruling will increase the likelihood of a new ruling trial that will force victims and their families to relive the horrific time if the administration wants to retry the death penalty. Two years after the attack, the parents of the youngest victim wrote an essay printed on the cover of The Boston Globe, urging the Justice Department to abandon the pursuit of the death penalty. Dennis and Bill Richard wrote that years of complaints that left Zarnaev's name in the news would continue to relive them with trials and prevent them from beginning to heal. "As long as the defendant is in the limelight, we have no choice but to live the story told in his language, not us. The moment the defendant disappears from our newspapers and television screens, we live with our lives. It's the moment to start the process of rebuilding the family, "they write.

EDITOR'S COMMENT: Civilized behavior to terrorists is an insult to the victims.

aunav.NEO HD

Source: https://aunav.com/en/product/aunav-neo/

Aunav.NEO HD is the only EOD/IED/CBRN robot with a variable geometry system which allows its width to be increased or decreased automatically in a few seconds.



The combination of its variable geometry and self-stabilization system, allows the aunav.NEO HD to adapt to any operating scenario imaginable, including narrow airplane aisles, buses or subways and underground tunnels to wading through debris or traversing wide-open spaces. **One robot fit all.**

Added to this versatility is easy transport, thanks to the simple and quick disassembly of its components, and the great strength and power of its main arm, which enables it for a wide variety of EOD/IED/CBRN missions.

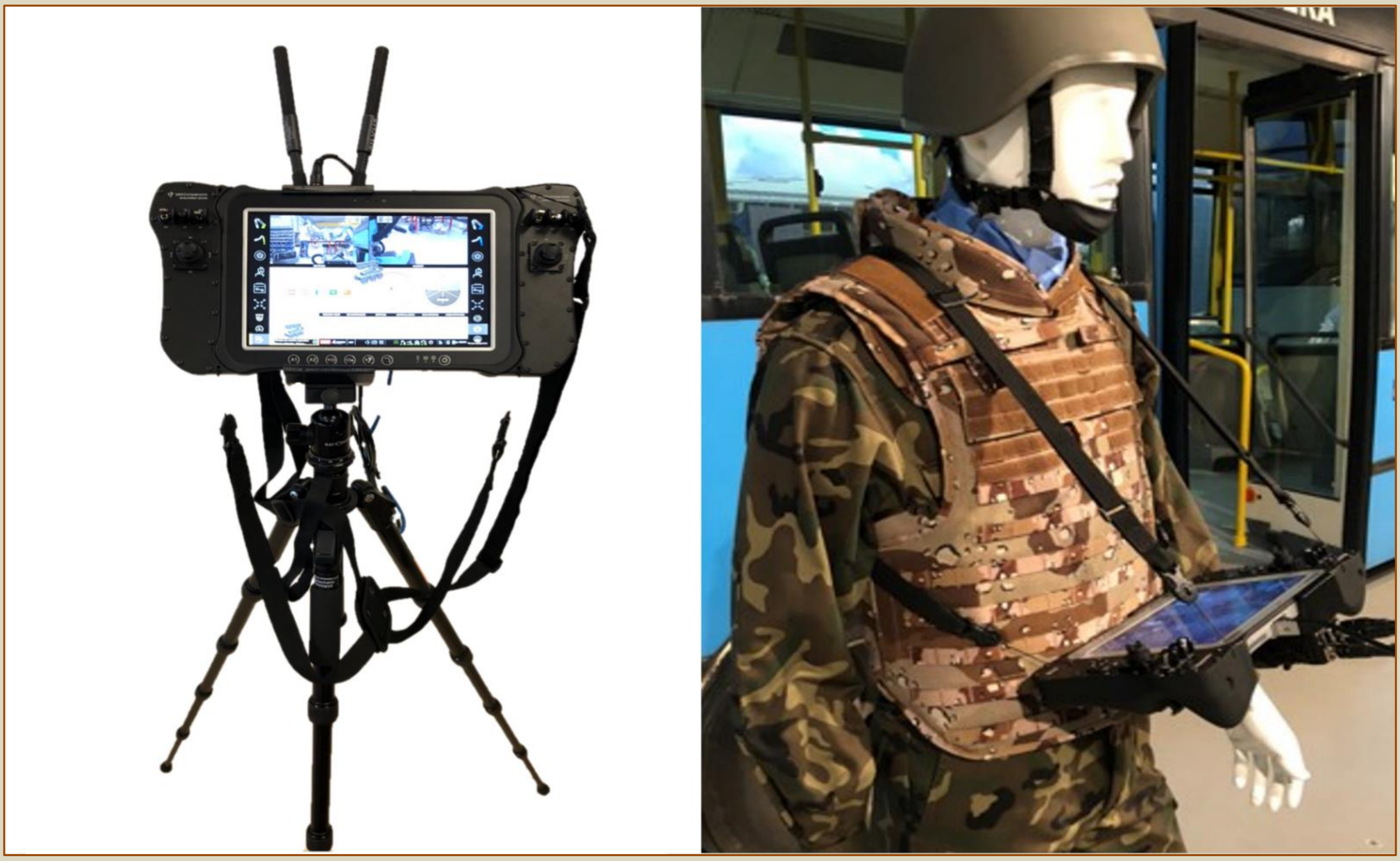
The advanced remote operation control unit provides the robot with autonomous capabilities that reduce operating times. aunav.NEO HD is also available in the aunav.NEO configuration, even lighter.

Variable geometry system

The robot automatically adapts its width from 400 mm to 680 mm to optimize its mobility and stability in narrow or wide spaces.

Control unit

Designed to cradle a Tablet PC, it integrates an ergonomically distributed set of buttons and joysticks on both sides of the base which ensures an easy, intuitive control of the robot. A compact, light-weight design guarantees the operators mobility. It provides an operational range of between 700m and 3km depending on the topography. Up to 8 cameras can simultaneously be displayed in real-time with a 3D drawing continually showing the exact position of each of the robot´s various joints.



AND DON'T FORGET TO PICK UP A GOAT FOR DINNER ON YOUR WAY HOME
LYNCH

ICI International CBRNE Institute

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

CYBER NEWS

C²BRNE DIARY

UK plans to invest £5 billion in retaliatory cyber-attacks

Source: https://www.bleepingcomputer.com/news/security/uk-plans-to-invest-5-billion-in-retaliatory-cyber-attacks/

Oct 04 – The United Kingdom has revealed plans to invest £5 billion in bolstering national cybersecurity that includes creating a “Cyber Force” unit to perform retaliatory attacks.

Fighting back

Cyber-warfare is being embraced as the “fifth domain” of international conflict and is being incorporated in the core functional aspects of nations, including the military. This includes having the same level of funding and attention as more traditional divisions.

As the UK's Secretary of State for Defense Ben Wallace points out in an interview with The Telegraph, Britain isn’t just looking to strengthen its stance against threats, but also to build up its capacity to launch retaliatory assaults.

The UK's goal is to strike back on ‘tier one’ attacks, targeting crucial sectors of hostile states such as Russia, China, and North Korea. As Wallace points out, Britain will be one of the very few countries in the world that will have the capacity to mount offensive cyber-attacks at such a scale, essentially discouraging any future attempts against them.

Typical targets could include electric power stations, telecommunication service providers, and various basic infrastructure entities where any service disruption would result in a large-scale impact and notable adverse economic effects.

Addressing a persistent threat

As Mr. Wallace revealed, some foreign states are waging cyber warfare on Britain on a daily basis, so responding to this aggressively is within the rights that underpin international laws. One of the examples that the official gave during the interview is dismantling servers that are used for ransomware deployment, spyware, or IoT malware.

A notable incident that came up as an example of how catastrophic these attacks can be comes from 2017, when the WannaCry worm crippled parts of the NHS (National Health Service). The Secretary of Defense sees this as an critical event but underlines that Britain hasn’t had a tier-one cyberattack that caused significant catastrophe yet.

Creating the National Cyber Force center is meant to help keep things this way, acting as a deterrent for those eyeing Britain as a lucrative target candidate. This is the same approach that the U.S. has openly taken recently.

The new digital warfare center will be based out of Samlesbury, Lancashire and jointly run by the Ministry of Defense and the GCHQ. Wallace states that the new division should be fully operational by 2030, with more details revealed by Boris Johnson, UK’s Prime Minister, at the upcoming conference of the Conservative Party in Manchester.

One thing to note is that none of the above is novel in the sense that Britain has been engaging in offensive cyber campaigns against the Islamic State, pedophiles, and various foreign hacking groups since at least 2018.
However, the £5 billion investment is meant to build upon these sporadic campaigns and create the ground for permanent deterrent operations against external threats and foreign adversaries.

What are the latest cybersecurity standards?

By Ruben Bonan
Source: https://www.cybersecurity-review.com/what-are-the-latest-cybersecurity-standards/

Cybersecurity standards are the agreed-upon techniques and protocols used by organisations to minimise the risk of and deal with the consequences of cyberattacks. Most cybersecurity protocols focus on prevention through various tools, policies, best practices and technologies and can be applied to networks, applications, services and also people. These standards are usually made to comply with specific industry regulations, but most businesses should adopt a voluntary framework even if they're not obliged to do so.
Cybersecurity standards help make it easier for businesses to keep their data secure and to standardize security measures, making it more difficult for cybercriminals to thrive. These standards are often tailored for specific countries or industries as there can be different regulations or issues to be aware of.
With a greater proportion of the workforce now working remotely, companies have to face new cybersecurity challenges. Cloud-based secure access services such as the Perimeter 81 SASE Platform help ensure that businesses are able to deal with these challenges while allowing their employees to work remotely and securely.

Why Are Cybersecurity Standards Important?
In recent years, there have been a growing number of cyberattacks, particularly those involving ransomware and these attacks can have a devastating effect on a business no matter its size. Ransomware attacks involve malware that locks a user or series of users out of their files. The only way that users can get their files back is by paying the ransom demanded by cybercriminals.
These attacks have become more common in recent years, and it's estimated that criminals have made hundreds of millions of dollars as a result. Cyberattack methods are rapidly evolving and growing more complex at the current moment. Every day, cybercrime has cost businesses around the world 16.4 billion dollars, with a ransom attack happening every eleven seconds.

Cybersecurity Regulations
Of course, not only do the cybercriminals get their ransom, but in many cases, they also fail to unencrypt the files, or they steal and sell the files to the highest bidder. As a result, cyberattacks can be extremely damaging to a company, and many businesses are also at risk of fines due to data protection laws if they suffer from a data breach caused by hackers.
Due to the potential damage that they can face, companies in industries across the world are now beginning to take cybersecurity very seriously. All businesses should have some kind of framework in place to help reduce the risk of a cybersecurity attack, and contingency plans should also be made so that staff know what to do in case of an attack.

Commonly Used Cybersecurity Standards
We've written up this list of the latest and best cybersecurity standards that all businesses should be implementing to keep themselves and their data secure.

SOC 2 Report
A System and Organisation Controls (SOC) report provides assurances about a company's security policy. The report looks at whether a system is protected from physical and logical unauthorised access while also checking that data is stored and protected as it should be. Lastly, the SOC2 report also considers whether the system is available for use, and this report is created following a 12-month audit

from a third party. A SOC 2 report is often required by regulatory bodies and governments to ensure that a company is complying with data protection laws.

ISO/IEC 27001 and ISO/IEC 27002

The ISO/IEC 27001 and ISO/IEC 27002 are international cybersecurity standards that provide a complete information security management system. Using these standards, a firm can manage the security of its assets such as financial data, intellectual property, employee information, and information provided by third parties. In many cases, these standards are required by law, but there are a wide range of IOS/IEC standards available, some of which are tailored to specific industries.

ETSI EN 303 645

The ETSI EN 303 645 was the first globally applicable standard for consumer Internet of Things devices. The Internet of Things (IoT) refers to the network of interconnected devices that utilise sensors, software and other technology to help make our lives easier. While IoT has grown in popularity, there have been a lot of concerns raised about cybersecurity. This standard aims to prevent large-scale, common assaults against smart devices that they see every day. Rather than awkwardly bolting security measures on at the end, this standard defines how to embed proper cybersecurity into IoT products from the start.

***Ruben Bonan** is the Founder of Marketing Marvel, an industry-leading Digital Marketing company. Through their services, Marketing Marvel helps organizations develop their brand awareness and increase their revenues by generating high-quality leads.*

U.S. Unveils New Cybersecurity Requirements for Rail, Air

By Jeff Seldin

Source: https://www.homelandsecuritynewswire.com/dr20211007-u-s-unveils-new-cybersecurity-requirements-for-rail-air

Oct 07 – The United States is taking new steps to make sure the country's air and surface transportation sectors will not be crippled by ransomware or cyberattacks.

Homeland Security Secretary Alejandro Mayorkas announced the measures Tuesday at a virtual cybersecurity conference, warning that recent incidents such as the SolarWinds hack and the Colonial Pipeline ransomware attack showed that "what is at stake is not simply the way we communicate or the way we work, but the way we live."

The new security directives target what the Department of Homeland Security and the Transportation Security Administration describe as "higher risk" rail companies, "critical" airport operators, and air passenger and air cargo companies.

Cybersecurity Coordinators

Mayorkas said that going forward, the rail companies will have to name a cybersecurity coordinator who will report any incidents and create contingency plans in the case of a cyberattack.

The aviation companies will also be required to appoint a cybersecurity coordinator and report incidents to the DHS's Cybersecurity and Infrastructure Security Agency.

Similar cybersecurity directives are already in place for 2,300 critical maritime companies that, starting this month, will have to submit plans to identify and address cyber vulnerabilities.

The U.S. Coast Guard is also working with the International Maritime Organization to require that passenger and cargo vessels arriving in U.S. ports have plans to deal with cyber emergencies.

"Whether by air, land or sea, our transportation systems are of utmost strategic importance to our national and economic security," Mayorkas said.

Spike in Ransoms Paid

Top U.S. officials, including Mayorkas and FBI Director Christopher Wray, have warned that cyberattacks and ransomware attacks, in particular, have become a persistent threat.

"Last year, victims paid an estimated $350 million in ransoms, a 311% increase over the prior year, with the average payment exceeding $300,000," Mayorkas told U.S. lawmakers at a hearing last month.

"We're now investigating over 100 different types of ransomware, each with scores of victims," Wray added.

U.S. officials have blamed Russia for many of the attacks, saying that despite Moscow's assurances, they have seen few indications the Kremlin is doing anything to address the problem.

Russian officials deny any role in the recent, high-profile ransomware attacks.

Speaking at a separate cybersecurity forum Tuesday, the head of U.S. Cyber Command warned the problem with ransomware is likely to persist.

“Our adversaries are targeting everyone,” General Paul Nakasone told the Mandiant Cyber Defense Summit. “What was once viewed as criminal behavior has become a national security issue.”

To help facilitate the fight against cyberattacks and ransomware attacks, U.S. lawmakers are considering several bills that would require private companies to report intrusions and attacks on the government.

“We’re optimistic the legislation will pass,” Mayorkas said Wednesday at the annual Billington CyberSecurity Summit.

“I think we’re at a point, seeing the arc of cybercrimes and the cyberthreats, that really there’s an urgency to it,” he said.

Jeff Seldin *is VOA national security reporter.*

The next big cyberthreat isn't ransomware. It's killware. And it's just as bad as it sounds.

By Josh Meyer (USA Today)
Source: https://news.yahoo.com/next-big-cyberthreat-isnt-ransomware-090022232.html

Oct 12 – Even as most Americans are still learning about the hacking-for-cash crime of ransomware, the nation’s top homeland security official is worried about an even more dire digital danger: killware, or cyberattacks that can literally end lives.

The Colonial Pipeline ransomware attack in April galvanized the public’s attention because of its consumer-related complications, including long lines at gas stations, Homeland Security Secretary Alejandro Mayorkas said in an interview with USA TODAY's Editorial Board last week.

But, "there was a cyber incident that very fortunately did not succeed," he added. "And that is an attempted hack of a water treatment facility in Florida, and the fact that that attack was not for financial gain but rather purely to do harm.”

That attack on the Oldsmar, Florida, water system in February was intended to distribute contaminated water to residents "and that should have gripped our entire country,” Mayorkas said.

It’s no surprise that it didn’t. USA TODAY and others reported on that hack, but it came amid a flurry of reports of other, bigger cyberattacks such as the SolarWinds intrusion of U.S. government agencies, technology firms like Microsoft and cybersecurity companies. .

But Mayorkas and other cybersecurity experts say the Oldsmar intrusion was just one of many indications that malicious hackers increasingly are targeting critical parts of the nation's infrastructure – everything from hospitals and water supplies to banks, police departments and transportation – in ways that could injure or even kill people.

“The attempted hack of this water treatment facility in February 2021 demonstrated the grave risks that malicious cyber activity pose to public health and safety," Mayorkas told USA TODAY in a follow-up exchange. "The attacks are increasing in frequency and gravity, and cybersecurity must be a priority for all of us.”

Weaponized technology

Like Mayorkas, private-sector computer security experts recently have begun issuing warnings that so-called cyber-physical security incidents involving a wide range of critical national infrastructure targets could potentially lead to loss of life. Those include oil and gas manufacturing and other elements of the energy sector, as well as water and chemical systems, transportation and aviation and dams.

And with the rise of consumer-based products like smart thermostats and autonomous vehicles, Americans are now living in a “ubiquitous Cyber-Physical Systems world” that has become a potential minefield of threats, said Wam Voster, senior research director at the security firm Gartner Inc.

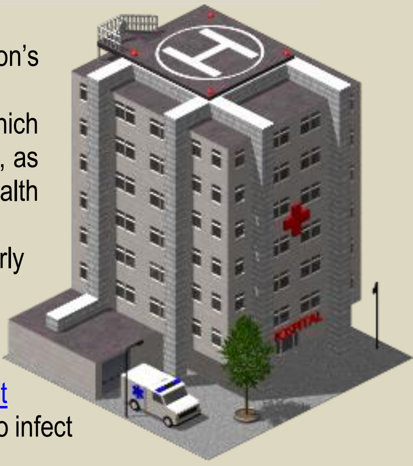
In a July 21 report, Gartner said it was seeing enough evidence of increasingly debilitating and dangerous attacks that by 2025, “cyber attackers will have weaponized operational technology environments to successfully harm or kill humans.”

“The attack on the Oldsmar water treatment facility shows that security attacks on operational technology are not just made up in Hollywood anymore,” Voster wrote in an accompanying article.

Another example, Voster wrote, was the Triton malware that was first identified in December 2017 on the operational technology systems of a petrochemical facility. It was designed to disable the safety systems put in place to shut down the plant in case of a hazardous event.

“If the malware had been effective, then loss of life was highly likely,” Voster wrote. “It is not unreasonable to assume that this was an intended result. Hence ‘malware’ has now entered the realm of ‘killware.'"

A frightening target: Hospitals



So far, few incidents have come to light in which hackers succeeded in shutting down parts of the nation's critical infrastructure in ways that might have contributed to someone's death or serious injury.

However, U.S. officials are especially concerned about the rash of ransomware attacks on hospitals, which have had to divert patients and cancel or defer critical surgeries, tests and other medical procedures, as was the case in a nationwide cyberattack on Universal Health Services, one of the nation's largest health care providers, in September 2020.

In hospital hacks, patients could die or suffer life-threatening complications but it would be nearly impossible to find out unless medical centers willingly offered that information, said a senior Department of Homeland Security official speaking on the condition of anonymity because he was not authorized to discuss ongoing security concerns.

A year ago, the FBI, DHS and the Department of Health and Human Services issued a warning about such attacks on hospitals, describing the tactics, techniques, and procedures used by cybercriminals to infect systems with ransomware for financial gain.

"CISA, FBI, and HHS have credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers," the alert said. "CISA, FBI, and HHS are sharing this information to provide warning to healthcare providers to ensure that they take timely and reasonable precautions to protect their networks from these threats."

Authorities believe the problem may be significantly larger than has been reported, in part because private companies and even government agencies often don't report ransomware hacks of their operational systems. Failure to report such attacks fuels the fast-growing criminal market in ransomware attacks, which can bring hackers millions in payouts, the DHS official said, "and it doesn't help us learn the latest techniques and tactics used by the hackers."

In Alabama, a woman sued a local hospital earlier this year, alleging that its failure to disclose a cyberattack on its systems resulted in diminished care that caused her baby's death.

Last year, an apparently misguided hacker attack caused the failure of information technology systems at a major hospital in Germany. That forced a woman who needed urgent admission to be taken to another city for treatment, where she died.

In both cases, the hospitals and doctors involved have denied allegations that they were responsible and no proven link between the hacks and the deaths were made.

Liability for loss of life

Cybersecurity experts have begun warning government and corporate leaders that they could be held financially or even legally liable if breaches of computerized systems they oversee are found to have had a human impact.

"In the U.S., the FBI, NSA and Cybersecurity and Infrastructure Security Agency (CISA) have already increased the frequency and details provided around threats to critical infrastructure-related systems, most of which are owned by private industry," Katell Thielemann, research vice president at Gartner said in a report in September 2020. "Soon, CEOs won't be able to plead ignorance or retreat behind insurance policies."

The firm estimated that the financial impact of cyber-physical security attacks resulting in fatal casualties will reach over $50 billion within a few years.

"Even without taking the actual value of a human life into the equation," Gartner concluded, "the costs for organizations in terms of compensation, litigation, insurance, regulatory fines and reputation loss will be significant."

Who are the hackers?

While ransomware attacks continue to dominate the headlines, Mayorkas has quietly begun sounding the alarm about cyber intrusions like the one in Florida in which money wasn't the primary motive.

U.S. cybersecurity officials have long known that water facilities and other critical infrastructure have been vulnerable for many, many years," a senior DHS official said. "What made this one different was that there was an intruder who consciously exploited that vulnerability with malicious intent."

"It is also significant because it is one of the few incidents where malicious cyber activity is crossing the line and can actually threaten the lives of people," the official said, for instance by increasing the level of potentially toxic chemicals in the water supply. He said Mayorkas has mentioned the attack in meetings with state and local security officials.

Homeland Security officials would not comment on who might have been behind the Florida attack, including whether it was linked to a foreign power.

Several nations, including Iran, Russia and China have penetrated key elements of U.S. critical infrastructure, but there have been few instances of them taking any action.

U.S. officials believe more and more foreign governments and non-state actors are engaging in malicious cyber-activity – sometimes together – in ways that make it nearly impossible to attribute the attacks, or to determine whether they were driven by profit, political motives or both.

In 2015, an Iranian activist group claimed responsibility for a cyberattack two years earlier that gave it access to the control system for a dam in the suburbs of New York. In a criminal indictment, the Justice Department later said that seven Iranian hackers penetrated the computer-guided controls of the dam on behalf of that country's military-affiliated Revolutionary Guards Corps as part of a broader cyberattack against 46 of the United States' largest financial institutions.

DHS officials told USA TODAY that the water treatment facility indicated that the malicious actor attempted to change chemical mixtures to unsafe levels as part of the water treatment process. An operator detected the changes and corrected the system before it affected the water supply, those officials said.

"Independent of who was behind it, the fact that someone decided to exploit that vulnerability and was able to do it means that other attackers would be able to do it as well," the DHS official said.

Microsoft Blames Iran-Linked Hackers for Attacks on US and Israeli Defense Companies

Source: https://interestingengineering.com/microsoft-blames-iran-hackers-for-attacks-on-defense-companies

Oct 12 – Since July 2021, Microsoft Threat Intelligence Center (MSTIC) has been tracking a new activity cluster that is targeting U.S. and Israel-based defense companies, maritime businesses with a presence in the Middle East, and ports of entry in the Persian Gulf, the company said in a blog post. Analyses of this activity have led the company to believe that it is supported by the Iranian state.

MSTIC assigns DEV-#### names to emerging and unknown clusters of threat activity until a time it has high confidence about the origins or the actor behind them. This string of activities has been assigned a DEV-0343 designation and has been found to be active mostly between Sunday through Thursday, between 7:30 AM and 8:30 PM Iran Time (04:00:00 and 17:00:00 UTC), the company said in the blog post.

The targets are not just defense companies

DEV-0343 activity has targeted defense companies that produce military-grade radars, drone technology, satellite systems, and emergency response communication systems to support the U.S., EU, and Israel governments. It has also targeted maritime and cargo transportation companies with operations in the Middle East. Among its targets are also "customers in geographic information systems (GIS), spatial analytics, regional ports of entry in the Persian Gulf," the blog post said.

The hackers are using the password spray technique — where the same passwords are cycled across a range of usernames to log in to the networks without being locked out. This is enabled by Firefox or Chrome browser emulators which are obfuscated using an average of 150-1000 unique Tor IP addresses, the company said.

So far, Microsoft has detected such attacks on more than 250 Office 365 tenants focused on two endpoints, Autodiscover and ActiveSync on its Exchange services. However, less than 20 tenants were compromised and the company has contacted the customers to notify them and take necessary actions to secure their accounts.

Microsoft believes that the pattern of actions points towards this activity originating from Iran. Access gained from these attacks is likely to help Iran compensate for its developing satellite program, the blog post said.

Microsoft recommends that customers enable multifactor authentication to mitigate compromised credentials, use passwordless solutions like its Authenticator, review and enforce recommended access policies and block incoming traffic from anonymizing services, where possible.

Nation-State Cyber Attacks – Recent Trends

Source: https://i-hls.com/archives/111044

Oct 15 – Russia accounted for 58% of nation-state cyberattacks observed in the past year, according to a recent Microsoft study. Most of these attacks targeted government agencies involved in foreign policy, national security, or defense.

Covering the period from July 2020 to June 2021, the Microsoft Digital Defense Report 2021 claims that attacks from Russian nation-state actors are "increasingly effective," jumping from a 21% successful compromise rate last year to a 32% rate this year. Also, the rate of targeting government agencies for intelligence gathering has climbed from 3% of their targets a year ago to 53% in 2021.

Which other players were behind cyber-attacks? After Russia, the largest volume of attacks have come from North Korea (23%), followed by Iran (11%), China (8%), and South Korea, Vietnam, Vietnam, and Turkey (a new entrant) all with less than 1% representation.

The top three countries targeted by Russian nation-state actors were the U.S., Ukraine, and the UK.

While espionage is the most common goal for nation-state attacks, some attacker activities reveal other goals, including Iran, which quadrupled its targeting of Israel in the past year, according to techworm.net citing the report.

Meanwhile, China is also using its intelligence gathering for a variety of purposes and has been targeting entities in India, Malaysia, Mongolia, Pakistan, and Thailand to glean social, economic, and political intelligence about its neighboring countries.

Cybercrime – especially ransomware – remains a serious and growing plague in this year's report. The top five industries targeted in the past year based on ransomware engagements by Microsoft's Detection and Response Team (DART) are consumer retail (13%), financial services (12%), manufacturing (12%), government (11%), and health care (9%).

The U.S. is by far the most targeted country, receiving more than triple the ransomware attacks of the next most targeted nation. The U.S. is followed by China, Japan, Germany, and the United Arab Emirates (UAE).

US schools gave kids laptops during the pandemic. Then they spied on them

Source: https://www.theguardian.com/commentisfree/2021/oct/11/us-students-digital-surveillance-schools

Oct 11 – When the pandemic started last year, countless forms of inequality were exposed – including the millions of American families who don't have access to laptops or broadband internet. After some delays, schools across the country jumped into action and distributed technology to allow students to learn remotely. The catch? They ended up spying on students. "For their own good", of course.

According to recent research by the Center for Democracy and Technology (CDT), "86% of teachers reported that, during the pandemic, schools provided tablets, laptops, or Chromebooks to students at twice the rate (43%) prior to the pandemic, an illustration of schools' attempts to close disparities in digital access."

The problem is, a lot of those electronics were being used to monitor students, even combing through private chats, emails and documents all in the name of protecting them. More than 80% of surveyed teachers and 77% of surveyed high school students told the CDT that their schools use surveillance software on those devices, and the more reliant students are on those electronics, unable to afford supplementary phones or tablets, the more they are subjected to scrutiny.

"We knew that there were students out there having ideations around suicide, self-harm and those sorts of things," a school administrator explained to the CDT researchers. "[W]e found this [student activity monitoring software]. We could also do a good job with students who might be thinking about bullying … [I]f I can save one student from committing suicide, I feel like that platform is well worth every dime that we paid for [it]."

Thousands of school districts across the United States have installed surveillance software on school-provided devices to monitor their students' online interactions. If a student emails or chats with another student saying they've been thinking of hurting themselves or that there is trouble at home, an AI bot or a human moderator watching over the messages in real time can send an alert to a teacher or administrator, allowing the teacher to jump in within minutes and ask if everything is OK.

These programs, such as Bark, Gnosis IQ, Gaggle, and Lightspeed, can cost the schools tens of thousands of dollars to implement, and they can be set up to search for language and online behavior indicating the possibility of violent tendencies, suicidal ideation, drug use, pornography use, or eating disorders.

I can certainly understand why schools would jump on technology they think might prevent teen suicide, bullying, and the like. The pandemic has been hard on everyone, and increased isolation and uncertainty is particularly hard on kids and teenagers. Students are reporting an increase in self-harm incidents and aggressive impulses since the beginning of lockdowns, and shoving everyone back together for a new school year is going to require adjustments. The only problem is that we've tried this before, in a different form. Everyone's proposed solution to the advent of school shootings was, "Well, let's just watch these little deviants much more closely." Metal detectors at the entrance to schools became the norm, police had a more visible presence, and security cameras went up in classrooms and hallways.

That was a big business; schools spent billions of dollars on security infrastructure that mostly proved to be ineffective. And the results were, well, you'll never guess! Kids felt unsafe, Black students were followed and harassed most frequently, and punishments increased as educational outcomes worsened. And, while some schools have started questioning whether their contracts with the police create more harm than good, others are simply adding digital surveillance to their physical systems.

Students from disadvantaged backgrounds are less likely to have private electronics not subject to surveillance, and will have less privacy when it comes to doing the perverted embarrassing things all teenagers do. And if students' references to drug use or pornography or violent thoughts might be forwarded to law enforcement, it will be, as usual, the kids already subjected to a greater number of interactions with police and social workers and other forms of monitoring and punishment who will suffer the increased attention.

Although schools and parents are quick to voice concerns over privacy, it remains unclear whether the result of all of this monitoring is safety – and if so, safety for whom? Safer for students? Surveys suggest students are mostly aware they are being monitored but are not fully cognizant of the extent. Many of these programs boast that teachers have direct access to the screens of their students, even after school hours are over. Teachers and administrators can hijack control of the computers remotely, closing problematic tabs and overriding their keyboards. Does that make kids feel safe?

Then there is the tricky question of the promise of "intervention". The goal of the surveillance, according to the software companies, is to allow for a problem to be spotted and intervened with early on. That intervention can lead to the presence of police and social workers, each with their own difficult histories when it comes to involvement in private homes. And information about the child's attempts to access outside help might be forwarded to their possible abuser: their parents. The Rape Abuse Incest National Network (Rainn) reported that during the pandemic more than half of their callers seeking assistance and counsel were minors, who were more likely to be trapped in their homes with abusive family members under stressful circumstances.

The software companies' other big promise about monitoring children for problems is that mental health professionals can be alerted and services provided. But again, the outcomes for mental healthcare with children varies wildly. Children with Medicaid coverage are more likely to be prescribed anti-psychotics and other debilitating medication than get access to talk therapy.

It's not clear whether students are going to benefit from this surveillance, or if it is merely going to reduce schools' liability when an act of violence or self-harm takes place. If teens are in need of help, it seems obvious that the best way to protect them is to ensure they have trusted adults in their lives they can turn to. A snooping AI is no substitute for that.

Teens deserve privacy for the same reasons the rest of us do: to not have our rights trampled on, feel paranoid and be disciplined for minor transgressions. Besides, teens need their privacy to create confusing memes and frantic new TikTok dances. It's their job to freak out adults; we need to give them the space to do it.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

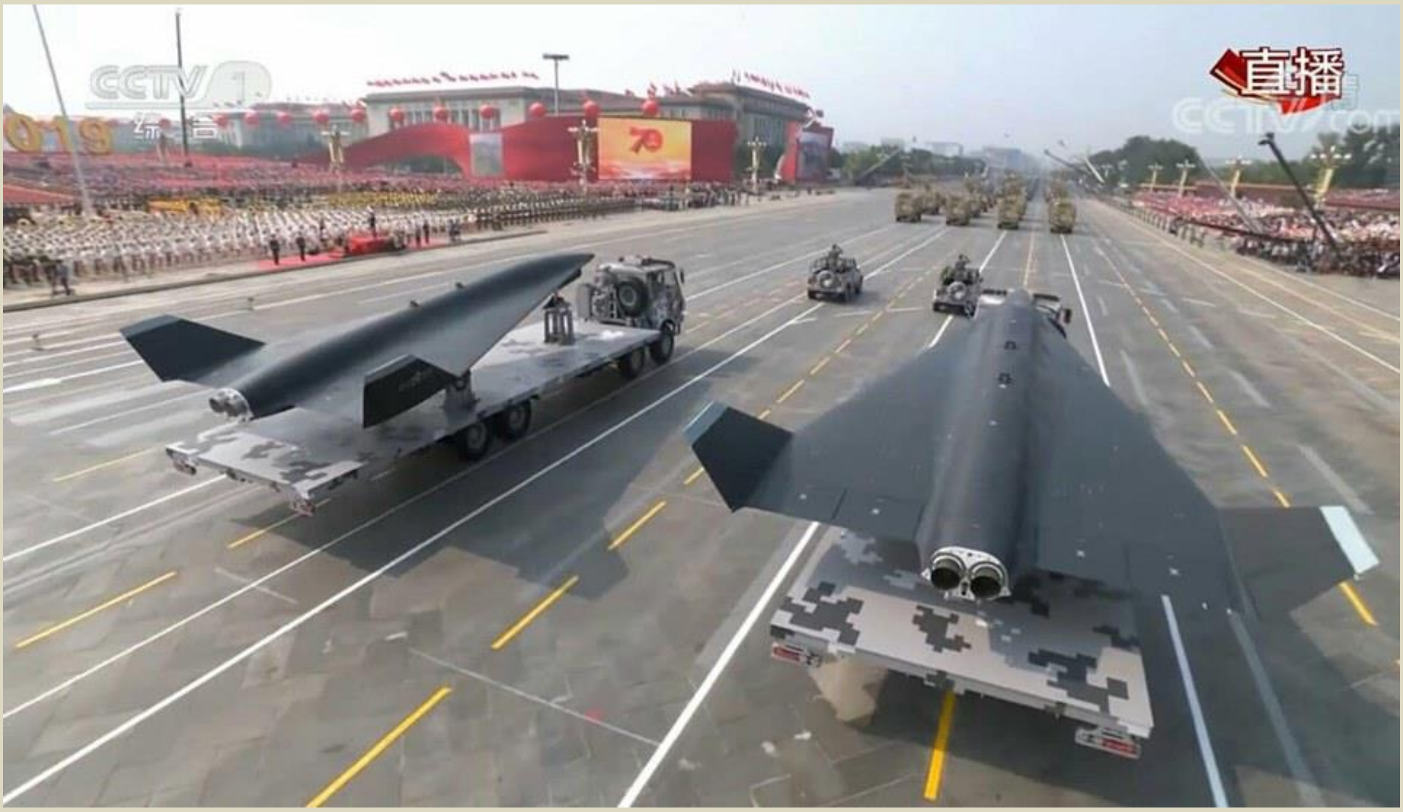
HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Chinese Hypersonic UAV Under Development – Is it a Threat?

Source: https://i-hls.com/archives/110768



Sept 24 – Chinese researchers claim that they have made significant progress on a classified hypersonic drone model. In a work published in a peer-reviewed paper in the journal Tactical Missile Technology, Beihang University's Dai Fei and his team confirm the existence of a Chinese military program to design an unmanned aerial vehicle (UAV) capable of traveling at hypersonic speeds. **Hypersonic speed is one that greatly exceeds the speed of sound, which is Mach 5 and above.**

The product tested by the researchers could be an advanced modification of the supersonic **Wuzhen 8** drone unveiled during China's 2019 National Day military parade, or an entirely new prototype unit that's under development, according to nationalinterest.org.

The team's alleged technical breakthrough is based, in part, on advancements in navigation algorithms that make it possible for UAVs to anticipate optimal landing routines and control their speed with subtle S turns. As explained by Dai's team, one of this project's many complications is that a UAV traveling at staggering speeds of Mach 5 must turn off its engines well in advance in order to land safely.

The research raises technical and military questions, such as the potential of such UAVs to target U.S. fifth-generation fighters. However, **it is not clear that China possesses or is even developing technology to arm hypersonic drones with weapons of any kind**, let alone ones suited for engaging fighters as survivable as the F-22 and F-35 fighters. If this prospective new drone is, in fact, an advanced modification of the Wuzhen 8, then it should be noted that the latter is a reconnaissance craft that likely has no payload.

The Pentagon has repeatedly expressed interest in this domain in recent years, with recent reports noting that tech startup Hermeus is developing a reusable hypersonic drone — dubbed "**Quarterhorse**" (photo above left) – for the US Air Force. There is also Lockheed Martin's mysterious and long-awaited SR-72 hypersonic reconnaissance UAV, scheduled to fly by the mid-2020s.

Meet This Remotely Operated Counter-Drone System

Source: https://i-hls.com/archives/110741

Sept 21 – In recent conflicts, there has been an increase in the usage of drones and loitering munition against various military targets. T he employment of this type of equipment has made low-level conflicts more lethal.

MSI-Defence Systems (MSI-DSL) and Milrem Robotics have joined forces to develop a step-change in countering mini-UAV, loitering munitions or other small difficult to detect airborne targets.

The system utilizes THeMIS unmanned ground vehicles (UGV) integrated with Remote Weapon Systems (RWS) and Electrical Optical Sensor Systems.

The highly mobile, unmanned C-UAS systems will be capable of carrying payloads from 7.62 to 30 mm and will also be able to find and engage larger air threats as well as ground targets, even if armored. All without the operator being exposed to the threats.

Utilizing unmanned ground systems with intelligent functions to counter these new threats helps increase force protection, provide flexibility to tactical units to engage aerial and/or land targets, and ultimately reduce loss of life, according to businesswire.com.

Drones to monitor Central Asian uranium legacy sites

Source: https://www.world-nuclear-news.org/Articles/Drones-to-monitor-Central-Asian-uranium-legacy-sit

July 01 – A new technology using drones is set to be deployed for the remote monitoring of radiation measurements at former uranium mining and processing areas in **Kazakhstan, Kyrgyzstan, Tajikistan** and **Uzbekistan**. The Unmanned Aerial Vehicles (UAVs) equipped with gamma spectrometers have been developed by a German consortium in collaboration with the International Atomic Energy Agency.

RUSSIA
Astana
KAZAKHSTAN
GEORGIA
Caspian Sea
ARMENIA
AZERBAIJAN
UZBEKISTAN
Bishkek
KYRGYZSTAN
CHINA
Tashkent
TURKMENISTAN
Ashgabat
TAJIKISTAN
Dushanbe
IRAN
PAKISTAN
INDIA

Netherlands – Researchers create drone swarms that can detect gas leaks, other threats

Source: https://www.nextgov.com/emerging–tech/2021/07/researchers–create–drone–swarms–can–detect–gas–leaks–other–threats/183826/

July 16 – A new research paper documents the creation of the first autonomous small drone swarm that detects gas leaks as well as other possible chemical threats and can map rooms without the aid of GPS. The research may be particularly relevant to the military, which is increasingly interested in small drones that perform well together with little human control and in tight places where GPS can't reach – like underground – as well as drones that can be used in situations where chemical weapons or other hazards pose a threat to humans.

Safe Airspace in the Age of Drones

Source: https://www.homelandsecuritynewswire.com/dr20211005-safe-airspace-in-the-age-of-drones

Oct 05 – When you think of a story about federal agencies joining forces, "feel good" might not necessarily be the descriptor you'd reach for. But, in this case, we at the think we're onto something.

Here is a story from DHS Science and Technology Directorate (S&T) which includes cool technology and the best minds in government research and development coming together to keep our country, and the skies above it, safe.

We are all familiar with drones, or as they are more formally called, Unmanned Aircraft Systems (UAS). They are becoming more and more ubiquitous, and are being used for everything from backyard fun to military operations. Relatively inexpensive, small, and easy to deploy, they can be controlled with a specialized remote control, an app on your phone, or they may be programmed to autonomously follow a predetermined mission. And, as the technologies for UAS continues to improve, so has the potential for them to be used in illegal and dangerous ways.

In order to deal with these emerging threats, novel and innovative technologies need to be researched, developed, tested, and deployed—which is why S&T launched two unique efforts related to UAS Traffic Management (UTM) and Air Domain Awareness (ADA).

UTM is an S&T-funded initiative that supports the integration of drones into the National Airspace System (NAS). The primary objective of this project is to establish airspace flight corridors, geo-fencing, route planning, terrain avoidance guidance, and weather alerts (among other capabilities) that will enable the safe and secure integration of UAS into our NAS.

"UTM began at the National Aeronautics and Space Administration (NASA) Ames Research Center in 2013 with a research project," says S&T technical subject matter expert Tim Bennett. "A NASA engineer had an idea for an innovative way to approach the problem using software and started with $5,000 of funding from NASA."

ADA, on the other hand, prioritizes the development and implementation of aerial surveillance technologies that can detect, track, and identify low-flying (defined as ground level to 500 ft in the air) aircraft and determine their potential threat level.

Most UAS are small, making them difficult to detect. Effective ADA systems need to be able to accurately detect and identify these aircraft in all sorts of terrain, including deserts, scrubby foothills, mountains, forests, cities, coastlines, and anywhere else they could be flying. ADA systems, in concert with an integrated UTM system, need to be able to identify what is legally flying and what is not. A combined system is needed that can provide the kind of air traffic management for UAS that the Federal Aviation Administration (FAA) has for our current manned aircraft.

The success of the initial work brought additional funding, and the project has continued to grow as the scope of the problem and the need for a solution has increased. Congress has also recognized the importance of this effort and has appropriated funds.

A unique and inspiring part of this story is the way that multiple government agencies, each with a need for a similar solution, have come together to create a single platform.

Because UTM and ADA are relevant to many federal government components, there was interest in the projects from not only NASA, but other agencies such as the Department of Defense (DoD), the FAA, the Department of the Interior (DOI), and the Department of Homeland Security (DHS). Each agency has its own operational use case for UTM and ADA and saw the value in having a single system that could be designed, tested and approved. This system could then provide a standard stream of data which could be displayed to suit the individual missions.

"In my 40 years of working on UAS, I have never seen federal government come together like this," says Bennett. "The agencies meet once a month, and S&T has been a part of the ongoing process."

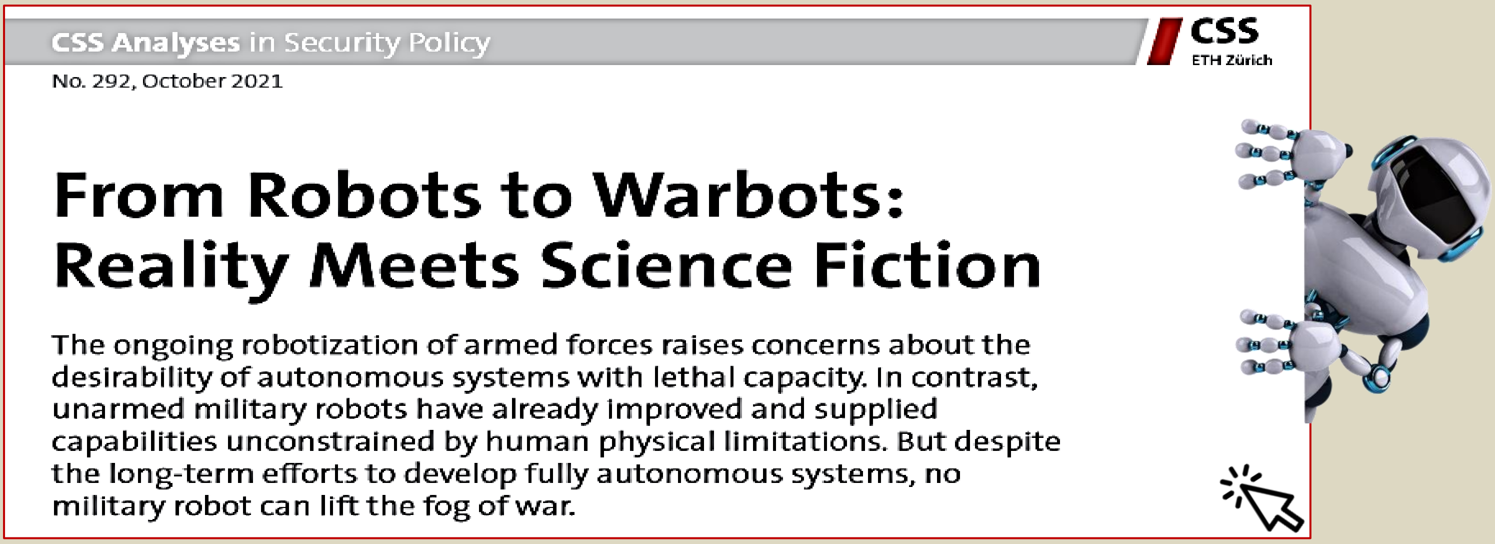
Two ADA demonstrations were held this year to evaluate relevant aerial surveillance technologies and their potential to detect, track, and ID aircraft in key locations at our northern border. These field tests were orchestrated and observed by representatives of the disparate agencies that are collaborating on the project, and the demonstrations were standardized so that platforms could be compared head-to-head.

The first demonstration was held in April in North Dakota to test the technologies in lowland plains terrain, and the second demonstration was held last month in Montana to test the technologies in mountainous terrain. For both demonstrations, targets included UAS under 55 pounds, ultra-light manned aircraft, and small fixed and rotary aircraft.

Conducted during both day and night, the demonstrations operated beyond-visual-line-of-sight and were performed at different altitudes and angles of approach from varying launch locations.

“When you consider metrics such as time, risk, and ability, the combination of UTM with ADA will be a game changer for DHS drone operations—including the delivery of medical supplies, responding to 9-1-1 calls of hazardous materials, bomb threats, suspicious packages, and locating lost persons,” said Bennett.

S&T says that in the not-too-distant future, ADA and UTM technologies could be monitoring the border, national parks, sensitive national security targets, military installations, coastlines and even high-interest events such as the Super Bowl, thanks to this ongoing whole-of government effort to keep us all safe.



CSS Analyses in Security Policy

No. 292, October 2021

CSS ETH Zürich

From Robots to Warbots: Reality Meets Science Fiction

The ongoing robotization of armed forces raises concerns about the desirability of autonomous systems with lethal capacity. In contrast, unarmed military robots have already improved and supplied capabilities unconstrained by human physical limitations. But despite the long-term efforts to develop fully autonomous systems, no military robot can lift the fog of war.

Dominika Kunertova *is a Senior Researcher in the Global Security Team at the Center for Security Studies (CSS) at ETH Zürich.*

Drug Cartels Carry Out Drone Bombings, Evade Jammers

Source: https://www.forbes.com/sites/davidhambling/2021/10/01/drug-cartels-carry-out-drone-bombings-evade-jammers/

Oct 01 – International drug cartels are using drone bombings in increasingly bold assassination attempts, both for their psychological impact and to bypass normal security. Two recent incidents highlight the trend: one attack on a house, another on a prison.

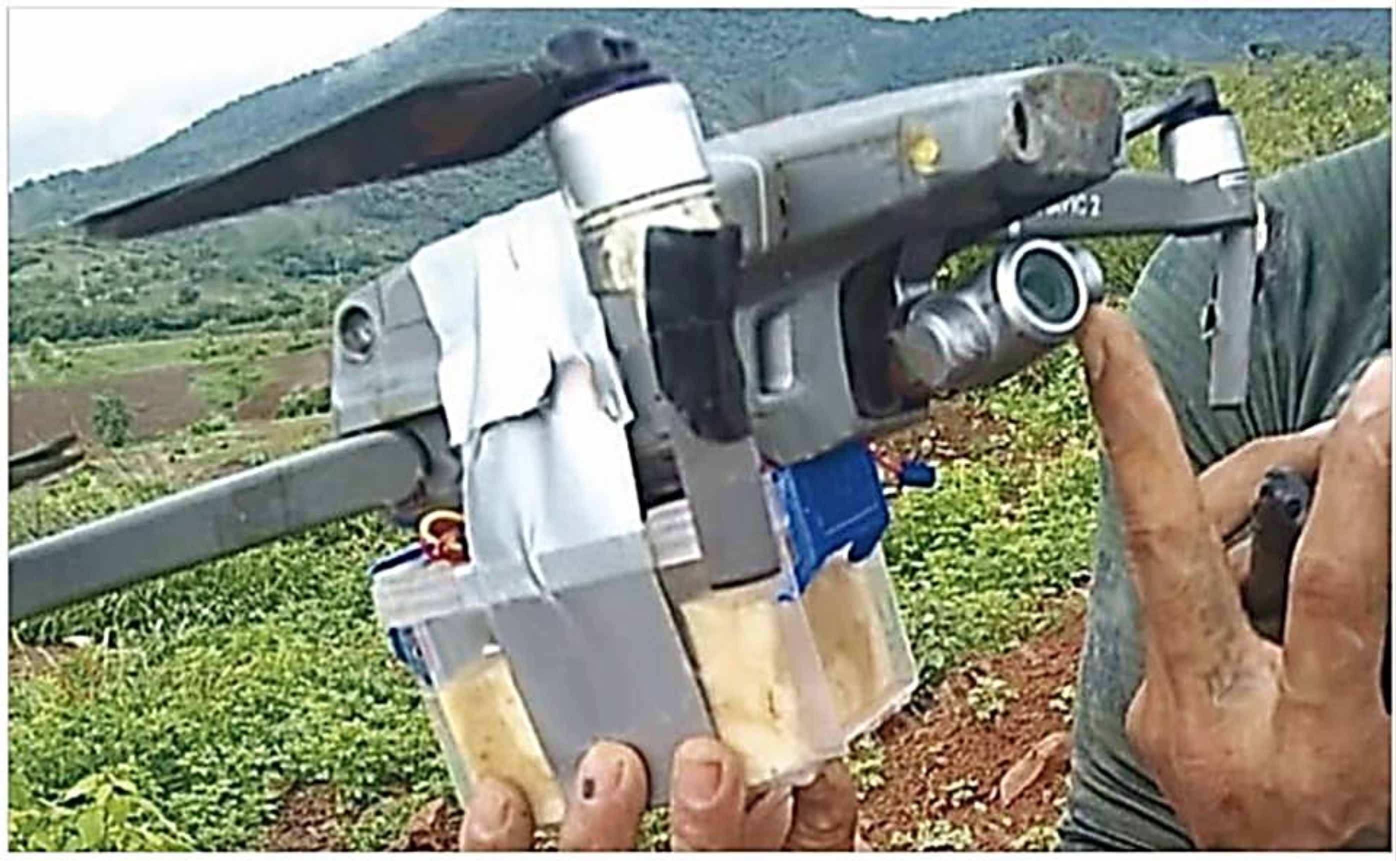
The Mexican Jalisco New Generation Cartel (CJNG) is estimated to control a third of the illegal drugs entering the U.S., and has had drone bombs in its arsenal since 2017. Initially these were consumer quadcopters with explosives taped to them — effectively home-made guided missiles. These weapons were mainly used against other gangs, although in April, a CJNG drone attack injured two police officers.

The latest incident took place in the municipality of Loma Blanca in the city of Tepelcatepec in Michoacán on Sept. 23: video shot from a drone shows it releasing a bomb which strikes a house below. The drone was later recovered and was found to have the initials CJNG RR on it. The RR apparently refers to Ricardo Ruiz, known as ‘El RR,’ leader of the CJNG’s Grupo Elite in Michoacán. It is not known who the house belonged to or whether there were casualties.

The evolution from kamikaze attacks to bombings is a familiar one.

“We saw a similar shift with Islamic State usage some years ago where they evolved from single use IED drones which point detonated to multi-use standoff drones which engaged in aerial bombardment,” Dr. Robert J. Bunker, director of research and analysis at C/O Futures, LLC, told me. “The standoff bombardment capability allows the CJNG to conserve it drone fleet capability and not burn through it.”

ISIS made extensive use of such drone bombers in Iraq and Syria and has carried out hundreds of successful attacks on buildings, vehicles and groups of people with drone bombs typically made from modified 40mm grenades. The CJNG also has extensive military hardware, but appears to be making their bombs from scratch.



Earlier CJNG drone bombs like this one from 2017 were taped to the drone. Now they are capable of dropping grenades.
Mexican Federal Police

“We have recently come across forensic evidence of IED bomblets that were manufactured for drone use in an arms cache seized from that cartel,” says Bunker.

Like ISIS, the CJNG appears to have released the video as a means of terrorizing opponents. Conveniently, drones capture video footage of the attacks they carry out.

“The release of the imagery of the bombardment by CJNG is significant because it shows that the cartel now recognizes the propaganda and psychological warfare potentials,” says Bunker.

The CJNG previously crashed a bomb-laden drone that did not explode beside the empty house of a law enforcement official in 2018. The new approach may prove far more effective for intimidation.

Unknown but possibly related perpetrators carried out a more dramatic attack in Ecuador on Sept. 13. Prison service (SNAI) authorities reported that three drones flew over a penitentiary at El Litoral dropping bombs. The explosions were loud enough to be heard by local residents but caused no casualties.

The attack was assumed to have targeted gang members in the block which was bombed.

“The attack would be aimed at the leaders of the gangs,” said the SNAI on Twitter. “It is serious, we are in the middle of a war between international cartels."

The level of gang violence in Ecuadorean prisons is astonishingly high: in one day of mayhem last month 116 inmates were killed with machetes, guns and grenades. During the drone assault, some inmates fired back at the drones.

Reportedly local gangs allied with the Mexican Sinola Cartel are in conflict with others supported by the CJNG who are attempting to take over the drug business in Ecuador. There is no indication of who sent the drones, but, as Bunker notes, at present they appear to be a CJNG signature weapon.

Drones are so frequently used to smuggle contraband into prisons – last month an inmate in Italy was shot with a gun believed to have been brought in by drone – that many prisons now have jammers, including in Ecuador. Jorge Haz, the director of the El Litoral penitentiary, told local media, "the drones presumably used a type of technology which was not detected by the existing inhibitors in that prison institution."

If accurate, this indicates that the operators anticipated and countered the jamming. This might have meant upgrading the radio controls, or sending the drones on a pre-programmed flight path.

The escalating use of drones, and the possibility that they might simply fly through existing defenses, is further evidence that the threat of improvised drone weapons needs to be addressed urgently.

Iran smuggling high-tech drones to militant allies, opposition group says

Source: https://www.washingtontimes.com/news/2021/oct/6/iran-smuggling-high-tech-drones-militant-allies-op/

In this photo released on Tuesday, Jan. 5, 2021, by the Iranian army, drones are displayed prior to a drill, in an undisclosed location in Iran. The Iranian military began a wide-ranging, two-day aerial rill in the country's north, state media reported, featuring combat and surveillance unmanned aircraft, as well as naval drones dispatched from vessels in Iran's southern waters. (Iranian Army via AP)

Oct 06 – Iran's theocratic regime has ramped up its drone manufacturing operation in recent years and is now smuggling an increasingly sophisticated slate of the weaponized remote-control aircraft to allied militant groups around the Middle East, according to intelligence gathered by a leading Iranian dissident group.

The Iranian military's embrace of drones, or unmanned aerial vehicles (UAVs), has given Tehran an expanding edge in asymmetric warfare across the region while U.S. sanctions have otherwise crippled the capabilities of its conventional air forces, the National Council of Resistance of Iran said Wednesday.

The dissident group gave a presentation to journalists at the Mayflower Hotel in Washington, revealing what it characterized as "newly disclosed information" about the scope and nature of the Iranian program, including a matrix of eight drone development complexes.

"The UAV program of the Iranian regime is the primary weapon used for terrorism and warmongering and destabilizing the region, and certainly this is supplying proxies in the region with those UAVs," said Alireza Jafarzadeh, the deputy director of the U.S. branch of NCRI.

The group has critics and followers in various countries and is known for openly supporting regime change in Tehran.

“There are two elements involved in the [drone] production. One is the Ministry of Defense, and the other one is the Aerospace Force of the Revolutionary Guards,” Mr. Jafarzadeh said. He circulated data obtained and compiled by the Mujahedeen-e-Khalq (MEK), an NCRI-affiliated group with members operating inside Iran.

Mr. Jafarzadeh’s claims were not immediately verifiable and the MEK has a controversial history in Washington, but the group appears to have sources deeply embedded within the Iranian defense community. MEK members are credited with significant revelations about Iran’s covert weapons activities, most notably its nuclear and ballistic missile programs.

The Wall Street Journal published an expose Wednesday that quoted U.S., European and Israeli defense sources as saying Tehran’s ability to develop and deploy drones rapidly is changing the security equation in the volatile region.

The components of Iran’s drones are widely available, although some designs mimic those of the Israeli and U.S. militaries. The Journal cited a confidential assessment produced for the British government by C4ADS, a Washington-based think tank that says Iran has armed its Houthi allies in Yemen with drones using a network of commercial companies around the world.

A matrix of drone-makers

Mr. Jafarzadeh’s presentation outlined a matrix of drone and parts manufacturers that he said are active inside Iran and are aligned with or directly controlled by the Iranian military or the Islamic Revolutionary Guards Corps.

Among those Mr. Jafarzadeh named are Ghazanfar Roknabadi Industries, Quds Air Industries, Fajr Industries Group, Iran Aircraft Manufacturing Co., Shahid Basir Industry, Bespar Sazeh Composite Co., Paravar Pars Co. and an unidentified special drone production operation in the Iranian city of Semnan.

Paravar Pars, according to documents circulated by the NCRI, belongs to the aviation research unit of the IRGC’s Imam Hossein University and “copies … and builds UAVs, ultralight planes, and drones and also installs cameras and other equipment on drones.”

Mr. Jafarzadeh outlined how the crux of the drone development program is tied to the “logistics directorate” of Iran’s elite Quds Force, a key branch of IRGC. He said the directorate manages the shipping of finished drones and drone components to militant groups allied with Tehran in Syria, Iraq, Lebanon and Yemen.

“It is a very interesting and very important part of the whole operation of the Quds Force,” Mr. Jafarzadeh said. “They actually have a smuggling office, whose job is to basically smuggle, whether the finished product of UAVs or the parts [using] air, land and sea pathways to send these weapons to their proxies in these countries.”

Reports of drone strikes carried out by Iranian forces or proxies in recent months often have been vague and difficult to confirm. An attack in July targeted the Israeli-linked British tanker Mercer Street in the Arabian Sea.

A Pentagon investigative team announced in August that it believed the drone used in that attack was produced in Iran and was loaded “with a military-grade explosive.” Details on who operated the drone were never clarified.

In late August, at least eight people were wounded in a drone strike that Yemen-based Houthi militants carried out against Saudi Arabia’s Abha International Airport. The Houthi forces have received considerable backing from Tehran in Yemen’s bloody civil war. Similar strikes have proved vexing for U.S. forces based in nearby Iraq, where drone attacks carried out by Shiite militia groups with deep ties to Iran have added another layer of complexity.

After an early-September drone strike near U.S. forces stationed at Irbil International Airport in northern Iraq, Reuters reported that witnesses heard at least six explosions. That suggests the aircraft used in the attack may have been carrying multiple miniature missiles.

The news agency noted that the airport in Irbil, the capital of Iraq’s autonomous Kurdish region, had come under attack several times over the year leading up to the incident, including by drones carrying explosives.

Iran denies any involvement in the attacks in Iraq, but U.S. officials have blamed the strikes on Iran-aligned militias that have vowed to fight until roughly 2,500 U.S. military forces leave the country. The U.S. troops are in Iraq to support Iraqi military operations against the Islamic State terrorist group.

Sanctions battle

The Iranian drone activity was revealed amid speculation that the Biden administration may be preparing to ease sanctions on Iran as part of an effort to lure the regime into diplomatic talks toward restoring aspects of the Obama-era Iranian nuclear deal.

Mr. Jafarzadeh said the U.S. should be pushing to increase sanctions, not ease them. He said sanctions are “a significant tool in limiting the resources of the Iranian regime in making them pay the price.”

“If the regime is allowed to do such an extensive [drone] operation … without any consequences, they only get encouraged,” he said. “If they constantly hear that ‘We’re open for negotiations, let’s sit down and talk’ and repeatedly hear that instead of being penalized and feeling consequences for the terror and mayhem and destruction they have created in the region, that certainly is not helpful.”

Others have argued that sanctions may have little impact on an Iranian drone program that relies less on the procurement of sophisticated military equipment than on establishing networks for acquiring consumer-level drone equipment and then militarizing it in clandestine facilities.

"Sanctions may not be able to affect Iran's program in a way that improves security for local populations or U.S. citizens or military personnel working and living in the Middle East," said Kirsten Fontenrose, a former top National Security Council official focused on the Middle East.

Ms. Fontenrose, who now heads the Scowcroft Middle East Security Initiative in the Atlantic Council's Middle East Programs, noted in an analysis published by Defense One that a June attack on a U.S. State Department facility in Baghdad was carried out by a drone "built cheaply with off-the-shelf components, including a motor made in Japan and an inexpensive commercial Global Navigation Satellite System antenna with a built-in compass."

"Other parts," she wrote, "come from black-market salvagers of drone test and attack debris, who would not be affected by sanctions."

Ten injured in 2 drone attacks at Saudi's King Abdullah airport

Source: https://www.reuters.com/world/middle-east/ten-injured-drone-attack-saudis-king-abdullah-airport-spa-2021-10-08/

DAMMAM
SAUDI ARABIA
NAJRAN
JAZAN
YEMEN

Oct 09 – Ten people were injured in two explosives-laden drone attacks at King Abdullah airport in the southern Saudi city of Jazan late on Friday and early on Saturday, the Saudi-led coalition said.

The military coalition intervened in Yemen in 2015, backing forces of the ousted government of President Abdrabbuh Mansur Hadi and fighting the Iran-aligned Houthi group.

Six Saudis, three Bangladeshi nationals and one Sudanese were injured in the first attack, Saudi state media said, citing a coalition spokesman. Some of the airport's facade windows were shattered in the attack, the spokesman said.

A second explosives-laden drone was intercepted early on Saturday, the coalition said, without giving details on any injuries or damages.

Air traffic in King Abdullah airport was normal, state TV said.

There was no immediate claim of responsibility by the Houthis. The group regularly launches drone and missile attacks targeting the gulf kingdom.

Counter-UAV Tactical Responses – Insights from US DoD Experiment 2021

By Or Shalom
Source: https://i-hls.com/archives/110978

Oct 07 – In recent years, the threat of unmanned aerial vehicles on critical infrastructures and vessels has been a growing security challenge. The use and realization of these advanced technologies for observation and operational intelligence gathering, along with the conversion of capabilities of injury and physical damage, require preparation, formulating responses, and thwarting threats.
The 2019 attack on Aramco installations in Saudi Arabia caused heavy damages to infrastructure and production capabilities, dwindling to half of the daily extent. This incident clearly demonstrated the risks as well as the hurdles in disaster recovery. This is also relevant to UAV attacks on vessels at mid-sea. These incidents have demonstrated that in addition to cyberattacks there is also the possibility of a physical attack, including a remotely operated attack.
In addition to coping with long-range suicide explosive UAVs, there is also the need for tactical responses to confront local UAVs and drones. During the Heathrow and Gatwick airports incidents in the UK, drones succeeded in disrupting and even halting airport operations, including flight cancellations. These incidents have led to a rethinking regarding the need for advanced technological systems and their acquisition in order to intercept UAVs and drones.
Choosing the right response must be based on the analysis of possible tactical threats with regard to a certain perimeter. For example, the insight that system deployment in the field, e.g. radars or large-area jamming systems, can help neutralize longer-range threats.
In November 2019, the US Secretary of Defense appointed a DoD representative in an attempt to focus efforts and lead collaborations in the following major aspects:

- **Enhancing capabilities through innovation**
- **Developing hardware-based or other (sof tware) capabilities** in order to cope with the threat and neutralize adversary capabilities.
- **Broadening collaborations with allies to deal optimally with the threats.**

In the tactical arena, advanced anti-drone solutions are available. These include, among others, kinetic-based systems or systems that integrate blocking or jamming capabilities against drones. Blocking and jamming are sometimes influenced by problematic (urban) environments, safety constraints, possible consequences of technological blocking in the area, skilled human resources, etc. So adequate alternatives must be considered.

For example, risk analysis regarding drone threats to prison installations will take into account the terrain, as well as statistical data and the popular use of drones for weapon and hazardous materials smuggling, or operational intelligence gathering. This will form the basis for the specification of blocking- and jamming-based neutralizing systems.
In the critical infrastructures arena and open outdoors, rapid destruction systems and kinetic capabilities are preferable. Sometimes, there are environmental constraints. Such was the case of the drone incident involving Angela Merkel, Chancellor of Germany. The units securing VIPs and state leaders must prepare for similar scenarios.
During August and September, the Pentagon completed testing in a desert region in Arizona, designed to find a tactical, commercial solution. The following models were included:

- **Northrop Grumman's XM1211**
- **Smash Hopper from Smart Shooter**
- **Dronebuster Flex force**
- **IXI's DroneKiller**
- **MKIII DroneGun**

During the three-week testing, kinetic and electronic warfare-based systems (the DroneKiller and DroneGun). Of interest was the definition for low-cost solutions, up to $15,000, for stationary or gun posts (for manual use) with cost up to $37,000 per system.
The testing demonstrated impressive results and reflected the capabilities of the professional teams to make improvements according to feedback from the testing.

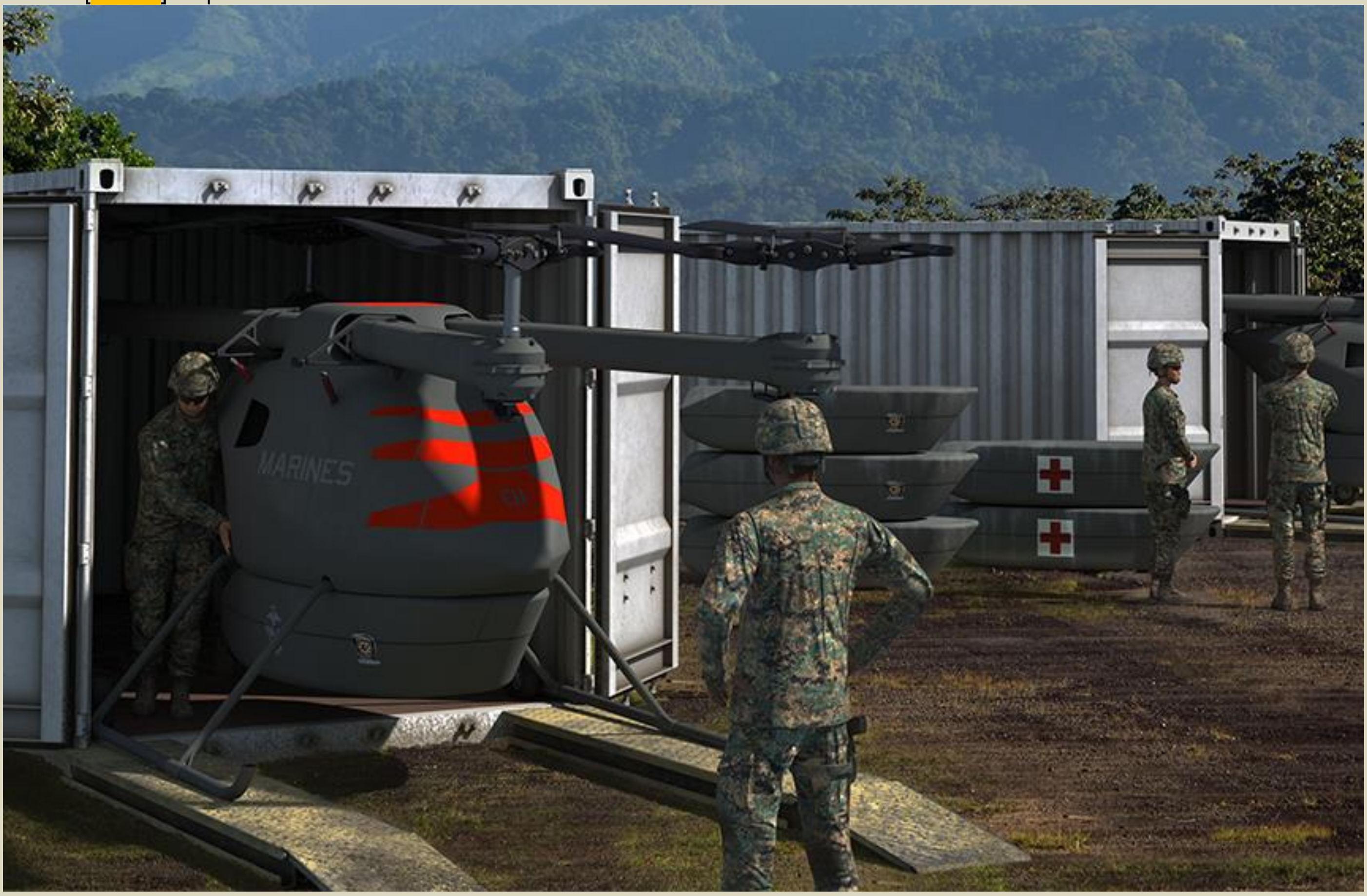
Sources include:

- ✓ Department of Defense: Counter Small Unmanned Aircraft Systems Strategy
- ✓ Eliyahu Mashhadi, Yossi Oren, and Gera Weiss Ben Gurion University of The Negev, Israel, Can the operator of a drone be located by following the drone's path?

***Or Shalom** is a security and cyber expert and consultant to government ministries and defense industries, international business development consultant for companies in the fields of HLS and cyber and leads centers of excellence and advanced training programs in Cyber and HLS for various organizations in the civilian, security, industry, and academic sectors. He holds a master's degree, as well as civil and national qualifications in the realm of HLS and Cyber Security. He has experience in security, innovation, planning, and characterization of technological security systems, HLS, and Cyber preparedness*.

Logistics UAV for Military Missions Unveiled

Source [+video]: https://i-hls.com/archives/111184



Oct 15 – Logistical missions require special capabilities, especially in the field of unmanned systems. A new logistics unmanned aerial vehicle has been unveiled by the US company Kaman. The KARGO UAV is the newest addition to the company's family of purpose-built, autonomous unmanned systems designed for expeditionary logistics.

Built with the U.S. Armed Forces' future operating concepts in mind, the KARGO UAV offers a rugged design for easy transport and deployment. The system's compact form-factor fits in a standard shipping container and is designed to be unloaded and operated by as few as two people.

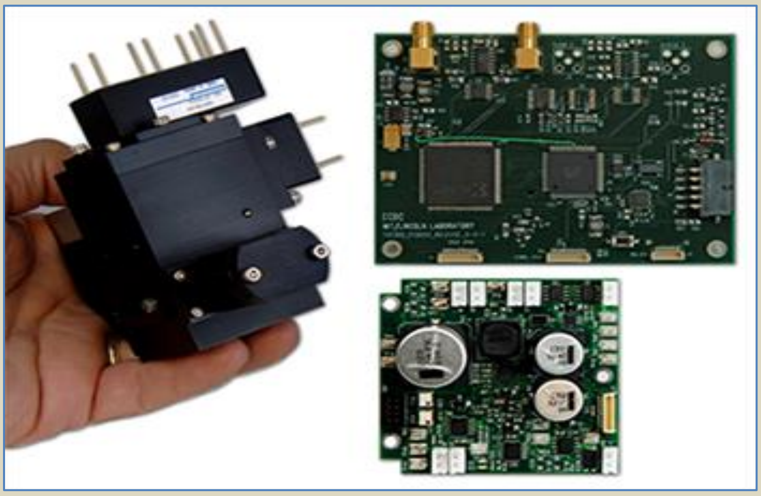
The UAV is purpose-built to provide deployed Marines, Sailors, Airmen, Soldiers, and Coast Guard autonomous resupply in the lethal, fluid combat environment that future military operations will entail or for regular logistics missions, according to the company.

The UAV also has multiple commercial applications and is part of a growth strategy involving a family of purpose-built KARGO vehicles for multiple and repeatable missions.

The KARGO UAV leverages commercial off-the-shelf components as well as thousands of hours of automated and autonomous flight data from Kaman's K-MAX TITAN program, to reduce schedule and technical risk, according to suasnews.com.

Flying UAV Laboratory (COTS system)

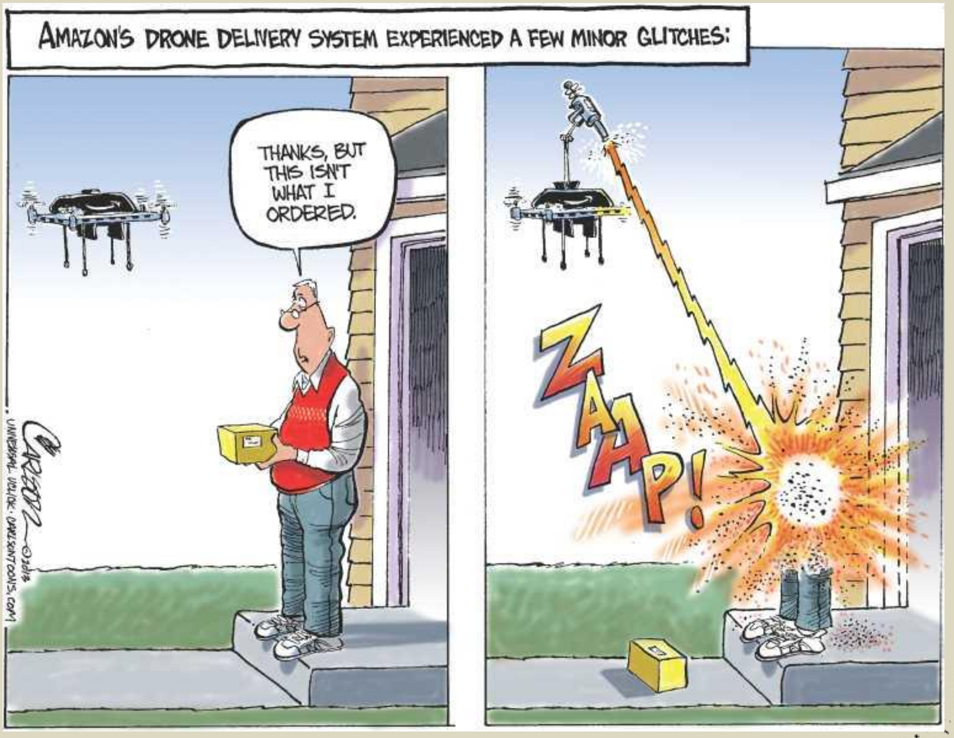
Source: http://www.resrchintl.com/Flying_UAV_Lab.html



Research International has developed a pioneering UAV-based product called the "Flying Laboratory" that has full CBRN monitoring capabilities. A second-generation ion mobility spectrometer (IMS) is mounted onboard to provide toxic gas detection. Up to 20 chemical warfare agents and toxic industrial gases can be detected at part per billion to part per million concentrations.

Biodetector hardware based on ultraviolet-stimulated biofluorescence.

A UV particle fluorometer is used to detect any unusually high biological aerosol levels, and a gamma spectrometer is used in combination with two Geiger counters to detect and identify nuclear materials and monitor radiation levels. One of the Geiger tubes is used for monitoring general background radiation levels, while the second, capable of detecting either alpha, beta or gamma radiation, is mounted so that it monitors radiation emitted from particulates captured by an aerosol sampling filter included in the payload.


AMAZON'S DRONE DELIVERY SYSTEM EXPERIENCED A FEW MINOR GLITCHES:
THANKS, BUT THIS ISN'T WHAT I ORDERED.
ZAAP!
Carlson ©2013 UNIVERSAL UCLICK · CARLSONTOONS.COM

ICI International CBRNE INSTITUTE
C2BRNE DIARY
CBRNE-Terrorism Newsletter
W O M D
HOTZONE SOLUTIONS GROUP
EMERGENCY
RESPONSE
F.D.N.Y.

Risk Communication: Plan with the Whole Community

Source: https://www.domesticpreparedness.com/updates/risk-communication-plan-with-the-whole-community/

Sept 28 – During a disaster, communication becomes especially critical. Language, accessibility, or other barriers can affect many individuals' ability to receive, understand, and act on emergency information.

The ability of a community to communicate accurate emergency information, alerts, warnings, and notifications saves lives. Timely and effective messages can inform people on actions to stay safe, take shelter, or evacuate.

What is in the messages and who communicates them to the community is an important element of risk communication.

Why It Matters

There is widespread evidence that emergencies disproportionately impact individuals with disabilities and others with access and functional needs.

The term "access and functional needs" refers to individuals with and without disabilities, who may need additional assistance because of any temporary or permanent condition. That condition may limit their ability to act in an emergency. Individuals with access and functional needs do not require any kind of diagnosis or specific evaluation. These may include but are not limited to

- individuals with disabilities,
- individuals with limited English proficiency,
- individuals with limited access to transportation,
- individuals with limited access to financial resources,
- older adults, and
- others deemed "at risk" by the Pandemic and All-Hazards Preparedness and Advancing Innovation Act (PAHPAIA) or the Secretary of the U.S. Department of Health and Human Services.

FEMA's whole community approach promotes community participation in emergency planning, response, recovery, and mitigation activities. Integrating community partners into the emergency planning process can help planners better understand and address the needs of the community. These stakeholders should be included in the development of risk communication messages to ensure they are accessible, understandable, and actionable.

Emergency Planning Can Save Lives

During widespread evacuations, transportation systems may be overwhelmed. Understanding the transportation needs of the whole community ahead of an incident will help identify key partners and prioritize communication. Community partners can help widely disseminate messaging to the populations they serve on actions for how to stay safe.

Parents drop off their kids at schools every day assuming they will come home within roughly 8 hours. Yet, in 2014, many Atlanta parents experienced a disaster they never would have predicted.

Icy conditions created by a winter storm paralyzed traffic just as schools were closing. Thousands of children were stranded at schools and on buses. Some children were rescued by firefighters and the National Guard after many cold and hungry hours on buses. More than 2,000 children spent the night at schools across the metro area.

Some parents spent hours behind the wheel trying to get to their children. Others walked miles through the snow to reunite with children.

Research indicates that over one-third of American households with children are not familiar with their school's emergency plans. Even more do not know where schools would evacuate their children to during a disaster.

Emergency action plans help everyone know what to do, who to call, and where to reunite in a disaster.

A New CDC Resource for Emergency Planners

CDC developed a toolkit to help emergency planners, such as those for school districts, develop communication plans that consider the needs of people with disabilities and others with access and functional needs. The Access and Functional Needs Toolkit is organized in two sections. Section 1 provides examples of groups who may be at greater risk or disproportionately affected in an emergency. This section includes noteworthy practices, key considerations, tips, and resources for effective communication with these groups. A second section outlines a process and recommended action steps to integrate a network of community partners into risk communication strategies. It provides customizable tools and instructions, templates, worksheets, and noteworthy partner engagement practices. The resources can help create documentation to institutionalize partner engagement practices and identify areas for improvement.

Government agencies and community organizations can use the toolkit's worksheets and templates to guide their emergency plans and communication strategies.

HOTZONE SOLUTIONS **GROUP**

hotzonesolutions.org