I C I

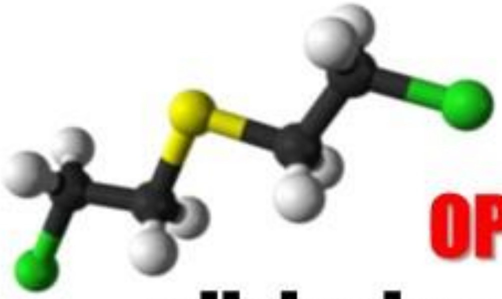
C²BRNE DIARY

Dedicated to Global First Responders

July 2023

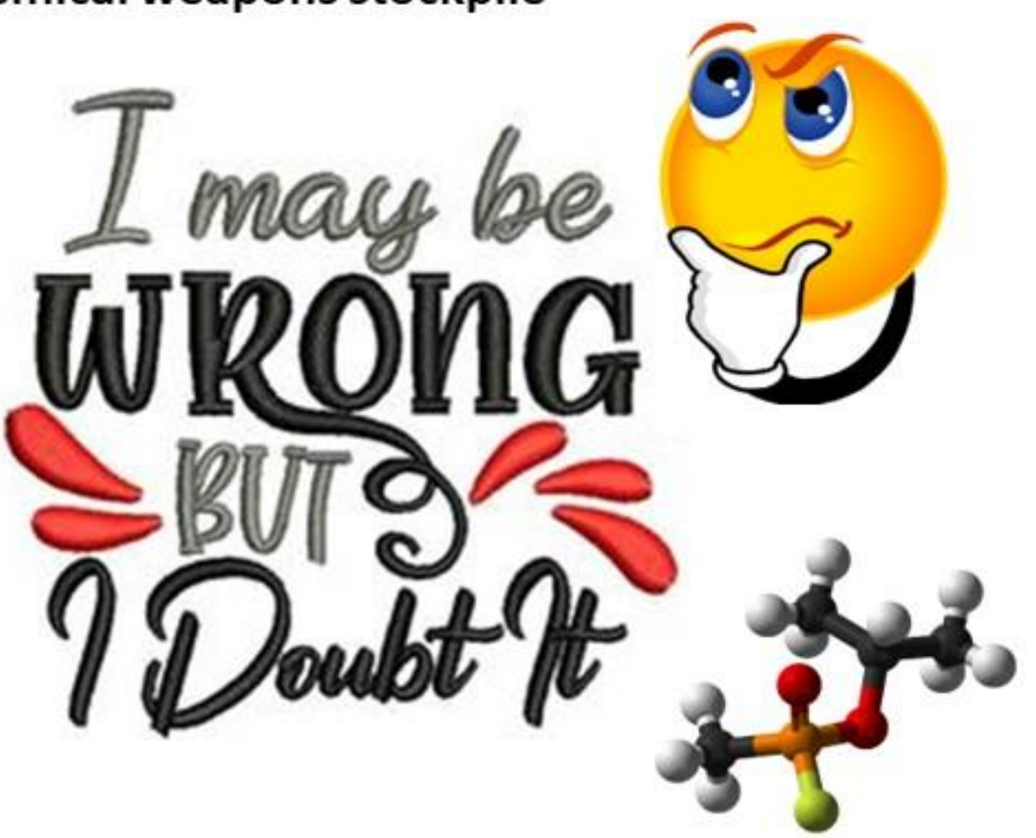
07\23

PART B



OPCW confirms all declared chemical weapons stockpiles verified as irreversibly destroyed

The United States of America, the last possessor State, completed the destruction of its declared chemical weapons stockpile



An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

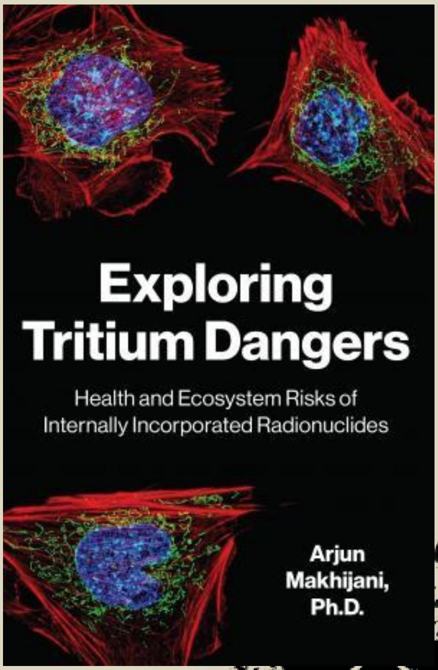
C²BRNE DIARY

'Exploring Tritium's Danger': a book review

By Robert Alvarez

Source: https://thebulletin.org/2023/06/exploring-tritiums-danger-a-book-review/

The Braidwood nuclear power plant rises above nearby homes. The state of Illinois and Will County officials sued the owners and operators of the facility in 2006, claiming they failed to report leaks of radioactive tritium from the facility. (Photo by Scott Olson/Getty Images)


Exploring Tritium Dangers
Health and Ecosystem Risks of Internally Incorporated Radionuclides
Arjun Makhijani, Ph.D.

June 26 – Over the past 40 years, Arjun Makhijani has provided clear, concise, and important scientific insights that have enriched our understanding of the nuclear age. In doing so, Makhijani—now president of the Institute for Energy and Environmental Research—has built a solid reputation as a scientist working in the public interest. His most recent contribution to public discourse, *Exploring Tritium's Dangers*, adds to this fine tradition.

A radioactive isotope of hydrogen, tritium is one the most expensive, rare, and potentially harmful elements in the world. Its rarity is underscored by its price—$30,000 per gram—which is projected to rise from $100,000 to $200,000 per gram by mid-century.

Although its rarity and usefulness in some applications gives it a high monetary value, tritium is also a radioactive contaminant that has been released widely to the air and water from nuclear power and spent nuclear fuel reprocessing plants. Makhijani points out that "one teaspoon of tritiated water (as HTO) would contaminate about 100 billion gallons of water to the US drinking water limit; that is enough to supply about 1 million homes with water for a year."

Where tritium comes from

Since Earth began to form, the radioactive isotope of hydrogen known as tritium (H-3) has been created by interactions between cosmic rays and Earth's atmosphere; through this natural process, the isotope continues to blanket the planet in tiny amounts. With a radioactive half-life of 12.3 years, tritium falls from the sky and decays, creating a steady-state global equilibrium that comes to about three to seven kilograms of tritium.

Tritium initially became a widespread man-made contaminant when it was spread across the globe by open-air nuclear weapons explosions conducted between 1945 and 1963. Rainfall in 1963 was found in the Northern Hemisphere to contain 1,000 times more tritium than background levels. Open-air nuclear weapons explosions released about 600 kilograms (6 billion curies) into the atmosphere. In the decades since above-ground nuclear testing ended, nuclear power plants have added even more to the planet's inventory of tritium. For several years, US power reactors have been contaminating ground water via large, unexpected tritium leaks from degraded subsurface piping and spent nuclear fuel storage pool infrastructures.

Since the 1990s, about 70 percent of the nuclear power sites in the United States (43 out of 61 sites) have had significant tritium leaks that contaminated groundwater in excess of federal drinking water limits.

The most recent leak occurred in November 2022, involving 400,000 gallons of tritium-contaminated water from the Monticello nuclear station in Minnesota. The leak was kept from the public for several months. In late March of this year, after the operator could not stop the leak, it was forced to shut down the reactor to fix and replace piping. By this time, tritium reached the groundwater that enters the Mississippi River. A good place to start limiting the negative effects of tritium contamination, Makhijani recommends, is to significantly tighten drinking water standards.

Routine releases of airborne tritium are also not trivial. As part of his well-researched monograph, Makhijani underscores this point by including a detailed atmospheric dispersion study that he commissioned, indicating that tritium (HTO) from the Braidwood Nuclear Power Plant in Illinois has been literally raining down from gaseous releases – as it incorporates with precipitation to form tritium oxide (HTO)—something that occurs at water cooled reactors. Spent fuel storage pools are considered the largest source of gaseous tritium releases.

The largely unacknowledged health effects

Makhijani makes it clear that the impacts of tritium on human health, especially when it is taken inside the body, warrant much more attention and control than they have received until now. This is not an easy problem to contend with, given the scattered and fragmented efforts that are in place to address this hazard. Thirty-nine states, and nine federal agencies (the US Nuclear Regulatory Commission (NRC), Environmental Protection Agency (EPA), the Department of Energy (DOE), the Occupational Safety and Health Administration (OSHA), the Consumer Product Safety Commission, the Food and Drug Administration (FDA), and the Department of Agriculture are all responsible for regulating tritium.

This highly scattered regulatory regime has been ineffective at limiting tritium contamination, much less reducing it. For example, state and federal regulators haven't a clue as to how many of some two million exit signs purchased in the United States—and made luminous without electric power by tritium—have been illegally dumped. For decades, tritium signs, each initially containing about 25 curies (or 25,000,000,000,000 pCi) of radioactivity, have found their way into landfills that often contaminate drinking water. One broken sign is enough to contaminate an entire community landfill. There are no standards for tritium in the liquid that leaches from landfills, despite measurements taken in 2009 indicating levels at Pennsylvania landfills thousands of times above background.

Adding to this regulatory mess, is the fact that federal standards limiting tritium in drinking water only apply to public supplies, and not to private wells. In past decades, regulators have papered over the tritium-contamination problem by asserting, when tritium leakage becomes a matter of public concern, that the tritium doses humans might receive are too small to be of concern. Despite growing evidence that tritium is harmful in ways that fall outside the basic framework for radiation protection, agencies such as the Nuclear Regulatory Commission remain frozen in time when it comes to tritium regulation.

The NRC and other regulating agencies are sticking to an outdated premise that tritium is a "mild" radioactive contaminant that emits "weak" beta particles that cannot penetrate the outer layers of skin. When tritium is taken inside the body (by, for example, drinking tritiated water), half is quickly excreted within 10 days, the agencies point out, and the radiation doses are tiny. Overall, the NRC implies its risk of tritium ingestion causing cancer is small.

But evidence of harm to workers handling tritium is also growing. Epidemiologists from the University of North Carolina reported in 2013, that the risk of dying from leukemia among workers at the Savannah River Plant following exposure to tritium is more than eight times greater (RBE-8.6) than from exposure to gamma radiation (RBE-1). Over the past several years, studies of workers exposed to tritium consistently show significant excess levels of chromosome damage.[1]

The contention that tritium is "mildly radioactive" does not hold when it is taken in the body as tritiated water—the dominant means for exposure. The Defense Nuclear Facility Safety Board—which advises the US Energy Department about safety at the nation's defense nuclear sites—informed the secretary of energy in June 2019 that "[t]ritiated water vapor represents a significant risk to those exposed to it, as its dose consequence to an exposed individual is 15,000 to 20,000 times higher than that for an equivalent amount of tritium gas." As it decays, tritium emits nearly 400 trillion energetic disintegrations per second. William H. McBride, a professor of radiation oncology at the UCLA Medical School, describes these disintegrations as "explosive packages of energy" that are “highly efficient at forming complex, potentially lethal DNA double strand breaks.” McBride, underscored this concern at an event sponsored by the National Institutes of Health, where he stated that “damage to DNA can occur within minutes to hours.” [2] “No matter how it is taken into the body,” a fact sheet from the Energy Department’s Argonne National Laboratory says, “tritium is uniformly distributed through all biological fluids within one to two hours.” During that short time, the Defense Nuclear Facility Safety Board points out that “the combination of a rapid intake and a short biological half-life means a large fraction of the radiological dose is acutely delivered within hours to days…”

A new approach to tritium regulation

Makhijani pulls together impressive evidence clearly pointing to the need for an innovative approach that addresses, in addition to cancer, a range of outcomes that can follow tritium exposure, including prenatal and various forms of genomic damage. In particular, he raises a key point about how physics has dominated radiation protection regulation at the expense of the biological sciences.

It all boils down to estimation of a dose as measured in human urine based on mathematical models. For tritium, dose estimation can be extraordinarily complex (at best) when it is taken inside the body as water or as organically bound, tritide forms. So the mathematical models that can simplify this challenge depend on “constant values” that provide the basis for radiation protection.

In this regard, the principal “constant value” holding dose reconstruction and regulatory compliance together is the reliance on the “reference man.” He is a healthy Caucasian male between the age of 20 to 30 years, who exists only in the abstract world.

Use of the reference man standard gives rise to obvious (and major) questions: What radiation dose limit is necessary to protect the “reference man” from serious genomic damage? And what about protection of more vulnerable forms of human life?

According to the 2006 study by the National Research Council, healthy Caucasian men between the age of 20 and 30 are about one-tenth as likely to contract a radiation-induced cancer as a child exposed to the same external dose of gamma radiation while in the womb. In his monograph, Makhijani underscores the need to protect the fetus and embryo from internal exposures to tritium—a need largely being side-stepped by radiation protection authorities. “Tritium replaces non-radioactive hydrogen in water, the principal source of tritium exposure,” Makhijani writes, pointing to unassailable evidence that tritium “easily can cross the placenta and irradiate developing fetuses *in utero*, thereby raising the risk of birth defects, miscarriages, and other problems.”

He is not alone in such an assessment. According a 2022 medical expert consensus report on radiation protection for health care professionals in Europe, “The greatest risk of pregnancy loss from radiation exposure is during the first 2 weeks of pregnancy, while between 2-8 weeks after conception, the embryo is most susceptible to the development of congenital malformations because this is the period of organogenesis.” In the United States, the Nuclear Regulatory Commission’s efforts to reduce exposure limits and protect pregnant women and their fetuses is best described as foot-dragging. By comparison, the required limit for a pregnant worker in Europe to be reassigned from further exposure is one-fifth the US standard—and was adopted nearly 20 years ago.

Long-term environmental retention

A 2019 study put forward the first ever empirical evidence of very long-term environmental retention of organically bound tritium (OBT) in an entire river system, deposited by fallout from atmospheric nuclear weapons explosions.

When released into the environment, tritium atoms can replace hydrogen atoms in organic molecules to form organically bound tritium, which is found soil, and river sediments, vegetation, and a wide variety of foods. It’s been more than a half century since the ratification of the Limited Test Ban Treaty, and tritium released through nuclear weapons testing has undergone significant decay. Yet because of the long retention of organically bound tritium, in greater than expected concentrations, it still remains a contaminant of concern.

For instance, despite its 12.3-year half-life, a much larger amount of organically bound tritium from nuclear tests than previously assumed is locked in Arctic permafrost, raising concerns about widespread contamination as global warming melts the Arctic. Organically bound tritium can reside in the body far longer than tritiated water, to consequently greater negative effect.[3]

Nuclear weapons, nuclear power, and tritium

The tritium problem has several dimensions that relate directly to the world’s current and future efforts vis a vis nuclear power and nuclear weapons. Now that nuclear power reactors are closing down, especially in the aftermath of the Fukushima accident, the disposal of large volumes of tritium-contaminated water into lakes, rivers, and oceans is becoming a source of growing concern around the world. The Japanese government has approved the dumping of about 230 million gallons of radioactive water, stored in some 1,300 large tanks sitting near the Fukushima nuclear ruins, into the Pacific Ocean. Once it incorporates into water, tritium is extraordinarily difficult, if not impossible to remove.

Protests in Japan by a wide segment of the public and in several other nations—including Russia, the Marshall Islands, French Polynesia, China, South Korea and North Korea—object to the disposal of this large volume of contaminated water into near-shore waters. Then there’s the matter of boosting the efficiency and destructive power of nuclear weapons with tritium gas—a use that has dominated demand for this isotope. Because five percent of the tritium in thermonuclear warheads decays each year, it has to be periodically replenished. Over the past 70 years, an estimated 225 kilograms of tritium were produced in US government reactors, principally at the Savannah River Plant in South Carolina. Those reactors were shuttered in 1988. Since 2003, tritium supplies for US nuclear warheads are provided by two Tennessee Valley Authority nuclear power reactors. The irradiation of lithium target elements in the reactors has fallen short of meeting demand because of excess tritium leakage into the reactor coolant. The hazards of tritium production for weapons are far from trivial.

For instance, since June of 2019, the Defense Nuclear Facility Safety Board has taken the Energy Department to task for its failure to address the risk of a severe fire involving tritium processing and storage facilities at the Savannah River Site. According to the Board, such a fire may have a 40 percent chance of occurring during 50 years of operation and could result in potentially lethal worker doses greater than 6,000 rems—1,200 times the annual occupational exposure limit. Doses to the public would not be inconsequential. Meanwhile, the Energy Department is under pressure from the nuclear weapons establishment to step up demand for tritium. Unless there is "a marked increase in the planned production of tritium in the next few years," the 2018 US Nuclear Posture Review concluded "our nuclear capabilities will inevitably atrophy and degrade below requirements."

The Energy Department estimates it will take 15-20 years to achieve a major multibillion overhaul of its tritium production infrastructure. Meanwhile, the quest for fusion energy highlights a startling fact: The amount of tritium required to fuel a single fusion reactor (should an economic, fusion-based power plant ever be created) will likely be far greater than the amount produced by all fission reactors and open-air bomb tests since the 1940s. A full-scale (3,000 megawatt-electric) fusion reactor is estimated to "burn" about 150 kilograms of tritium a year.[4] The cost for a one-year batch of tritium fuel for a fusion reactor, based on the current market price, would be $4.5 billion. An annual loss to the environment from a single fusion reactor could dwarf the release of tritium from all nuclear facilities that currently dot the global landscape.

The tritium overview

Evidence is mounting not just in regard to increased health risks from tritium-contaminated water and from organically bound tritium, but also as relates to the harm tritium can visit on the unborn. At the same time, it has become clear that regulation of tritium in the United States is grossly insufficient to the current risk from tritium contamination, not to mention future risks that could arise if tritium production, use, and associated leakage rise. Arjun Makhijani provides a useful roadmap for sparing workers and the public from the dangers this pernicious contaminant will pose in the future, absent more effective regulation that includes lower limits for human tritium exposure.

Notes

[1] See: https://link.springer.com/article/10.1007/s004200050272; https://www.mdpi.com/2305-6304/10/2/94; https://www.jstor.org/stable/3579658; http://www.rbc.kyoto-u.ac.jp/db/Literature/THO-Occupational.html; and https://www.unscear.org/docs/publications/2016/UNSCEAR_2016_Annex-C.pdf

[2] William MacBride, UCLA School of Medicine Vice Chair for Research in Radiation, Principal Investigator of UCLA's Center for Medical Countermeasures Against Radiation — National Institutes of Health, Jan 27, 2014. See: https://www.youtube.com/watch?v=XEH72v-yN9A

[3] See https://www.nature.com/articles/s41598-019-47821-1

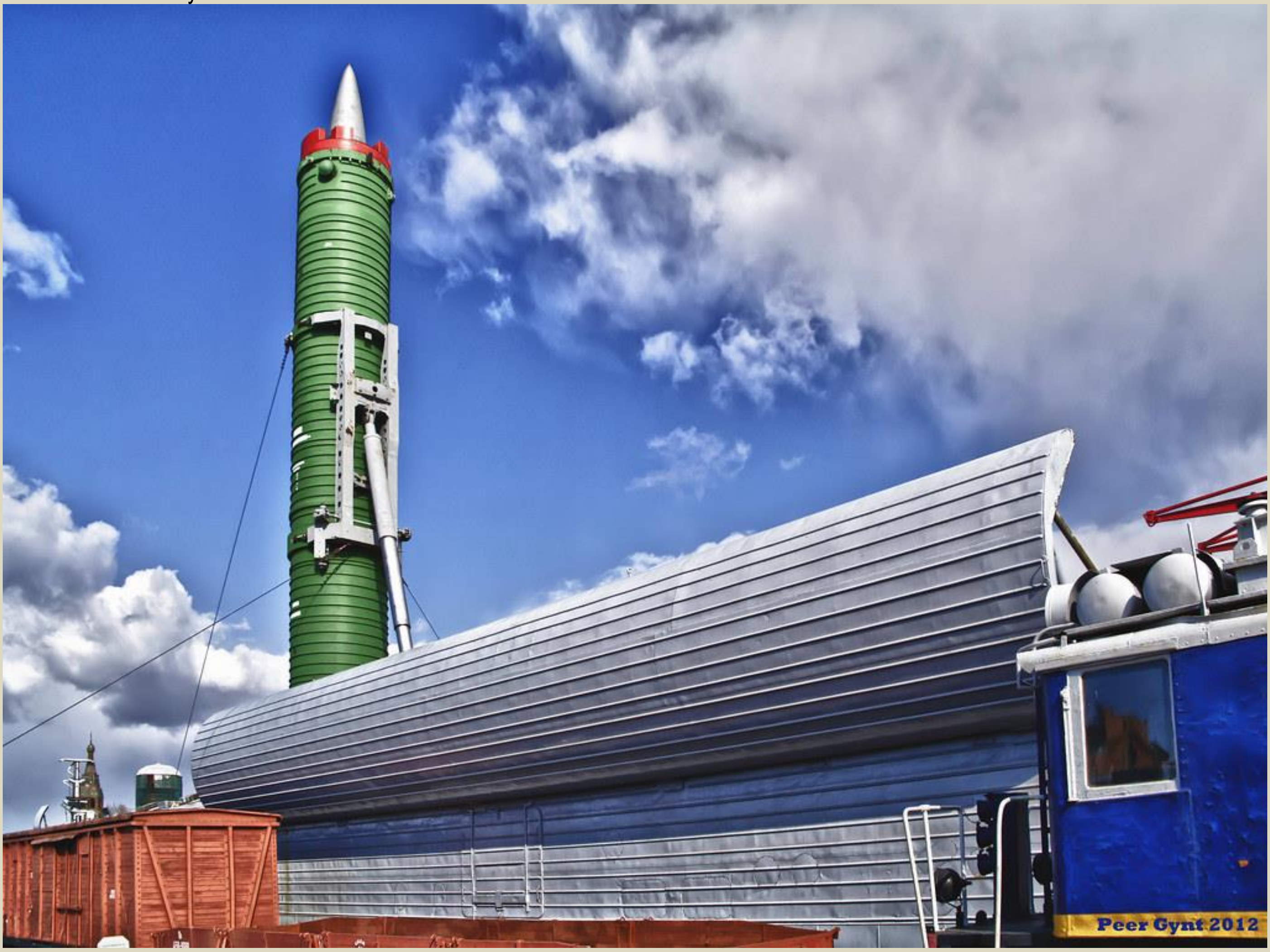
[4] Advocates assume that only the initial loading of 150 kg will be needed, as the reactor will "breed" the remaining amount of tritium to run the plant after a year of operation.

A senior scholar at the Institute for Policy Studies, **Robert Alvarez** served as senior policy adviser to the Energy Department's secretary and deputy assistant secretary for national security and the environment from 1993 to 1999. During this tenure, he led teams in North Korea to establish control of nuclear weapons materials. He also coordinated the Energy Department's nuclear material strategic planning and established the department's first asset management program. Before joining the Energy Department, Alvarez served for five years as a senior investigator for the US Senate Committee on Governmental Affairs, chaired by Sen. John Glenn, and as one of the Senate's primary staff experts on the US nuclear weapons program. In 1975, Alvarez helped found and direct the Environmental Policy Institute, a respected national public interest organization. He also helped organize a successful lawsuit on behalf of the family of Karen Silkwood, a nuclear worker and active union member who was killed under mysterious circumstances in 1974. Alvarez has published articles in *Science*, the *Bulletin of Atomic Scientists*, *Technology Review*, and *The Washington Post*. He has been featured in television programs such as *NOVA* and *60 Minutes*.

RT-23 / SS-24 SCALPEL

Source: https://nuke.fas.org/guide/russia/icbm/rt-23.htm

Comparable in size and concept to the US Peacekeeper, the SS-24 is cold-launched with 10 warheads. The missile is deployed both as rail-mobile and silo-based. The silo-based SS-24 was intended to replace the SS-19 Stilletto in the Russian strategic inventory. The SS-24 rail missile systems is subject to elimination under the provisions of the START-II Treaty.



The RT-23UTTh is a solid-propellant missile with three stages within a constant diameter body. The first stage of the silo-based missile uses a rotating nozzle, whereas the railwayï¿½based version is equipped with a fixed nozzle partially inserted in the motor combustion chamber. The engines of the second and third stages deploy extendable nozzles during flight to increase the motor's specific impulse without the need to increase of the overall dimensions of the missile. During the first stage flight control is attained through deflection of the sustainer nozzle, and during the second and third stage by deflecting the combat stage and by fairing-mounted aerodynamic vanes.

Both silo-based and rail-mobile missiles have an autonomous inertial guidance system using an onboard digital computer. The silo-based system uses a two-package block of control instruments made of radiation-resistant electronic elements. The railway-based missile has only one-package block of control instruments.

A total of 10 warheads [each with a yield of 550 KT], a post-boost vehicle with a guidance/control system and a propulsion system are inside the nose cone. The guidance/control system provides a CEP of 500 meters according to unofficial Russian estimates, which gives the missile a hard-target-kill capability. The missile is deployed in a transport-launching canister from which it is launched through the mortar start technique. To conduct a railway launch the sliding roof of the car opens, the container is erected and the missile is launched with the help of a solid propellant gas generator. The missile can be launched from any point of the route.

The length of the two versions are the missile were determined by the dimensions of the silo or the railway launcher. The silo-based missile therefore has a nose cone tip flap that is activated when the launch is initiated while the railroad based missile has a folded nose cone that is extended when the launch is conducted.

The creation of the RT-23 UTTh was the culmination of a long-term effort to create a solid-propellant ICBM for multiple basing modes which was initiated on 13 January 1969.

- **15Zh44 - SS-24 PL-4** The difficulties with which the developing institute KB Yuzhnoye (OKB-586) was confronted during the development of the railway-based SS-24 led to a redefinition of the task on 23 July 1976. Only a silo-launched version of the RT-23 was considered. The preliminary design was completed in March 1977 but it was considered unsatisfactory, and in December 1979 a second design with an improved propulsion system and a front end was finished. The new design provided using reentry vehicles that were identical to that of the R-36M / SS-18 missile. The suspended activities to build a railway based RT-23 (15Zh52) missile were resumed, and this design was finished in June 1980. The flight-design tests of the silo-launched RT-23 (15Zh44) began on 26 October 1982. As a result of several failures during the flight-tests, this version was cancelled on 10 February 1983 by the Soviet Defense Ministry.

- **15Zh52 - SS-24 Mod-0** On 09 August 1983 a further effort to develop a silo, railway and road-mobile missile designated as RT-23UTTh was approved, but the road-mobile stationing mode was subsequently abandoned. The tests of the railway based RT-23 (15Zh52) were successfully completed in April 1985, and in November 1987 it was experimentally adopted.
- **15Zh61 - SS-24 Mod-1** The RT-23UTTh tests of the railroad SS-24 Mod-1 version (15Zh61) that is almost identical to the 15Zh52 began on 27 February 1985 and were finished in December 1987 The deployment of these missiles started on 28 November 1989, and the first regiment with railroad-based missiles was put on alert on 20 October 1987. Altogether 36 railway-based RT-23UTTh missiles were initially deployed. They were deployed in three garrison areas: 12 launchers at Kostroma (400 km east of Moscow), 9 launchers at Bershet (1,250 km east of Moscow), and 12 launchers at Krasnoyarsk in Siberia. The Military Railroad Missile Complex (*Boyevoy Zheleznyy Raketnyy Kompleks* BZhRK) consists of three launch cars [each with a single missile], a command and control car, cars for personnel, and several diesel locomotives. The rail-mobile version could operate on any Soviet rail line that was unobstructed by overhead electrical power lines, a total of 145,000 km of track.
- **15Zh60 - SS-24 Mod-2** The silo-based version (15Zh60) known as SS-24 Mod-1 was tested from 31 July 1986 through November 1988. The deployment of these missiles in silos formerly occupied by SS-17 Sego ICBMs, started on 28 November 1989, and the first regiment of silo-based missiles was activated on 19 August 1988. Altogether 56 silo-based RT-23UTTh missiles were initially deployed, with 10 at Tatishchevo in Russia and 46 at Pervomaysk in Ukraine.

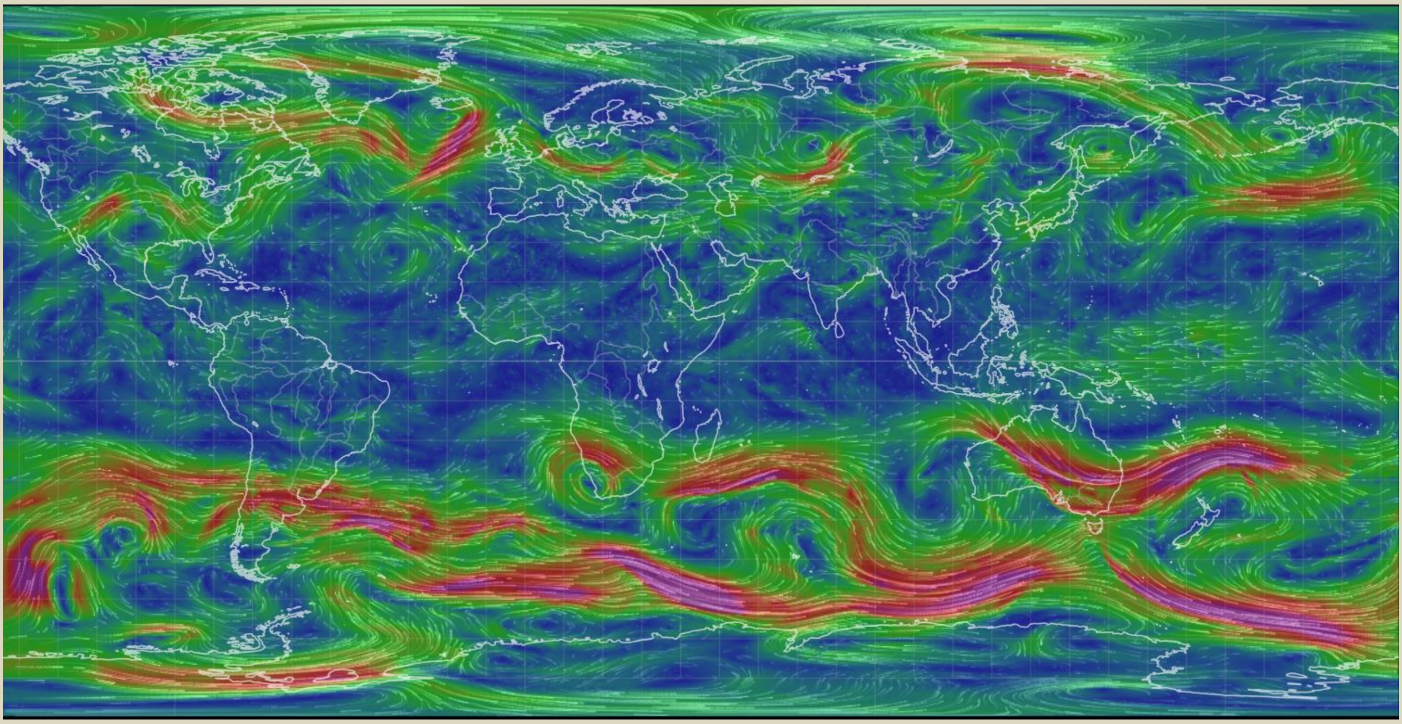
The US Defense Department stated in September 1991 that production had ended with approximately 90 missiles deployed. A total of 46 silo-based RT-23UTTh missiles located in Ukraine were phased out and

dismantled in compliance with the provisions of the START-1 treaty. They were denuclearised and their warheads have been transferred to Russia. By 1994 most of the rail-mobile systems remained in garrison due to lack of funding. By April 1997 10 silo-based and 36 railway based RT23-UTTh missiles were still deployed on Russian territory. Following Russian ratifiication of the START-2 treaty in early 2000, all RT-23 UTTh missiles are subject to dismantling.
With the breakup of the Soviet Union in 1991, most design and production facilities for the SS-24 belonged to Ukraine. Ukraine had no interest in continuing to produce these ICBMs, and the production line was closed in 1995.
It has been suggested that these rail-mobile land-based missiles, which have been parked in their garrisons, may be placed back on patrol in response to American missile defense and associated arms control initiatives.

Earth's Jet Streams Look as Chaotic as a Van Gogh Right Now, And That's a Big Problem

Keep this in your file in case of a radiological incident somewhere in the world

Source: https://www.sciencealert.com/earths-jet-streams-look-as-chaotic-as-a-van-gogh-right-now-and-thats-a-big-problem



A still of Earth's jet streams – The map is animated – click to vew

What would happen if a military group took over Russia's nuclear arsenal?

By François Diaz-Maurin

Source: https://thebulletin.org/2023/06/what-would-happen-if-a-military-group-took-over-russias-nuclear-arsenal/

June 26 – When Russian mercenary leader and oligarch Yevgeny Prigozhin suddenly launched his march on Moscow on Friday, top US officials should not have been surprised; US and Ukrainian intelligence had warned that such a move was possible. In the aftermath of Prigozhin's abortive rebellion, however, experts within and outside the US government were quick to express worry about the fate of the Russian nuclear arsenal should the regime of Russian President Vladimir Putin ever be overthrown.
Since mid-June, US and Ukrainian intelligence had observed movements of troops in Prigozhin's Wagner Group that suggested he was planning an armed rebellion against the Russian defense leadership. These movements followed a Russian Defense Ministry order on June 10 that all mercenary groups, including Wagner's estimated 25,000 troops, report to the central Russian military command starting July 1. Such a takeover would essentially have put an end to Prigozhin's leadership of Wagner, the private military force that he founded.

On Friday, Prigozhin ordered his troops to take control of a major Russian military headquarters in southern Russia, then had them set off on a march on Moscow—but then, after consultation with Belarus President Aleksandr Lukashenko, called off the rebellion on Saturday.

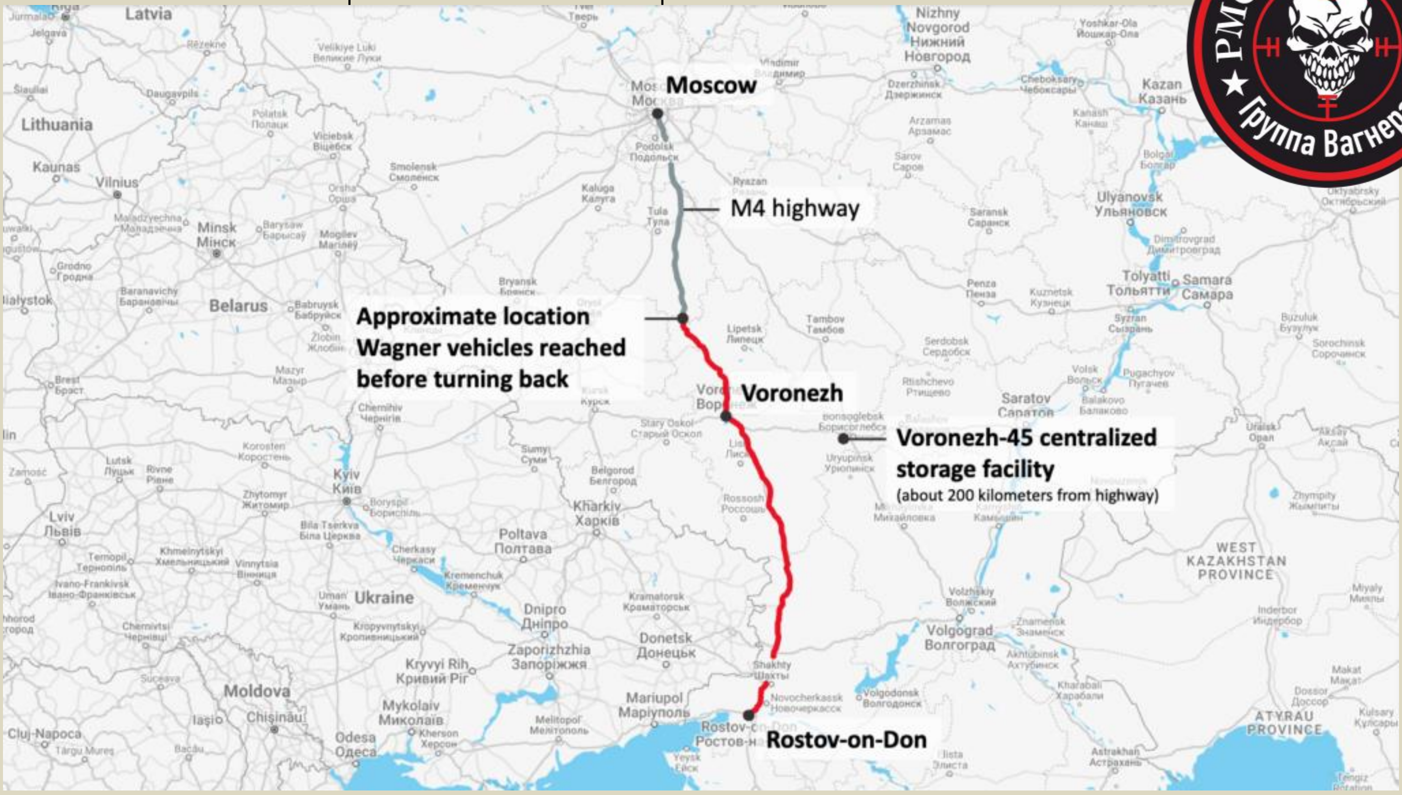
In a story published Saturday, the *Washington Post* quoted an unnamed US official who contended that there was "high concern" in the run-up to Prigozhin's short-lived rebellion about instability and the control of Russia's nuclear arsenal among the intelligence community should Putin be ousted and a Russian "civil war" erupt.

If a mercenary group were able to seize power and gain control over some of Russian nuclear weapons, "the world [would] find itself in uncharted territory," Alexander Vershbow, a former NATO deputy secretary general and US ambassador to Russia, told the *Bulletin*. "It is doubtful that the ousted Putin regime would be able to withhold access to nuclear codes for very long, if at all."

Other experts shared this concern. "Any civil instability within a nuclear state raises fears over command and control of its nuclear weapons," Mariana Budjeryn, a senior research associate with the Project on Managing the Atom at Harvard University, told the *Bulletin*.

It is not clear what might happen if a military group were to seize Russian tactical nuclear weapons.

The Wagner Group's march on Moscow revived an old fear among US officials concerned that nuclear weapons in Russia might fall into the wrong hands. "The security of then-Soviet nuclear warheads was a major US concern during and immediately following the Soviet Union's collapse," Steven Pifer, a former US ambassador to Ukraine, said, noting that the US government devoted significant funding to bolster the security of those weapons. In 1991, the US Congress passed the Soviet Nuclear Cooperative Threat Reduction Act (also known as the Nunn-Lugar Act, after the name of the two senators who sponsored it), which provided resources to secure and dismantle weapons of mass destruction and their associated infrastructure in former Soviet republics that had become independent countries.



The Wagner Group troops passing by the Voronezh-45 central nuclear storage facility for non-strategic nuclear weapons during their march on Moscow on June 23-24, 2023. (Map by François Diaz-Maurin / Google Maps)

On Saturday, some news reports suggested that Wagner troops were about to seize one such nuclear weapon storage site, although none of these reports could be independently verified. "At least one facility that could house Russian weapons was on the mutineers' path to Moscow: Voronezh-45 central nuclear storage facility," said Budjeryn. But it is unknown whether the facility currently hosts nuclear weapons, she added. (The Voronezh-45 facility is one of the 12 national-level centralized storage facilities tasked with hosting Russia's non-strategic nuclear weapons, such as gravity bombs and warheads for air- and ground-launched missiles.)

In Russia, all nuclear weapons stored separately from their delivery systems are under the control of the Defense Ministry's 12th Main Directorate (12th GUMO), including those at the Voronezh-45 facility. An attacking force, especially a group as heavily armed as the Wagner Group, might be able to take possession of some warheads at such a facility. But that would not mean the attackers could quickly arm or use those warheads, all experts agreed.

For one thing, a group seizing power would not necessarily gain physical control of complete nuclear weapons. "Most, if not all, stored Russian tactical nuclear warheads are not fully assembled," Pifer said. Matej Rafael Risko, a research fellow at the Institute of International Studies in Prague, commented on Twitter that warheads for the OTR-21 Tochka, a Soviet-era mobile short-range ballistic missile launch system now being replaced by the somewhat longer-range Iskander missile system, "are stored in an incomplete assembly, the so-called readiness stage."

"This means that the neutron tubes are not installed, the MED electro-detonators are not connected, and the electrical system is not connected to power sources," Risko added.

Even if rebels gained control of all the physical components of a nuclear weapon and assembled it, they could not necessarily use it. For a nuclear warhead to be used, it would have to go through a complex set of deployment procedures; among other things, a rogue group would need to mate a warhead with the right delivery system. In a blog post, Pavel Podvig, director of the Russian Nuclear Forces Project, explained that Russian nuclear weapons are stored separately from their delivery vehicles. He estimates that Russia has not only 12 large national-level storage sites but also about 35 base-level storage facilities. In some cases, a base-level storage facility can contain weapons that are assigned to delivery systems collocated at that same base. But in any case, mating a nuclear warhead to its delivery system is a task of extreme complexity, which an invading military group would most likely not be able to accomplish without the active—or forced—cooperation of 12 GUMO personnel.

Then there is the question of activation codes.

Russian non-strategic nuclear warheads are locked via permissive action links (also known as "PALs") that require codes to unlock. (Russian strategic nuclear weapons use other ways to prevent unauthorized and unintended use.) PAL codes were developed in the 1960s to guard against unauthorized use of a non-strategic nuclear weapon. "But PAL locks are like safe locks—with enough effort they could be broken," Budjeryn explains. Moreover, experts are uncertain whether PAL codes are released by the central command or kept on base, as in the United States—a possibly highly consequential detail. "It would be very poor security indeed if PALs were just kept on base," Budjeryn told me. "At least part of the code must be with the national command authority that would release them when they authorize the use."

So, what interest would a military group like Wagner have in seizing a tactical nuclear weapon, if it couldn't be used? "The mutineers could have used the captured weapons as political leverage in the short term," said Budjeryn. Then, she added, "with sufficient expertise and time, PALs could potentially be hacked."

This weekend's failed coup seems not only to have revealed cracks in Putin's grip on power but also the limits of safety and security arrangements for the Russian nuclear arsenal. Should a military coup ever succeed in Russia, coup leaders would likely gain effective control of nuclear weapons, which could pose a threat to strategic stability, prompting immediate international efforts to restore it. "Other nuclear powers would need to warn the new leaders of the severe consequences of using or threatening to use nuclear weapons … press them to establish effective security controls over Russian weapons and renounce nuclear coercion," the former NATO official Vershbow said.

As of now, Wagner's military rebellion fell short, and Prigozhin—who experts say has not publicly expressed interest in access to nuclear weapons—is in exile in Belarus. Still, Vershbow said, "I don't think Russia has seen the last of Yevgeny Prigozhin."

François Diaz-Maurin is the associate editor for nuclear affairs at the Bulletin of the Atomic Scientists. Previously, Diaz-Maurin was a MacArthur Foundation Nuclear Security Visiting Scholar at the Center for International Security and Cooperation (CISAC), Stanford University, and a European Commission's Marie Sklodowska-Curie Fellow. He has been a scientific advisor to members of the European Parliament on nuclear issues, and he is a founding member of the Emerging Leaders in Environmental and Energy Policy network (ELEEP) of the Atlantic Council, Washington D.C. and the Ecologic Institute, Berlin. Prior to joining academia, Diaz-Maurin spent four years as a research engineer in the nuclear industry in Paris, France and Boston, MA. There, he worked on the safety design of new reactors and of a treatment plant to vitrify Hanford's tank waste from WWII and Cold War nuclear weapons production. Diaz-Maurin received multi-disciplinary training in civil engineering (B.Sc./M.Sc., University of Rennes 1, 2004/2007, both with distinction), environmental and sustainability sciences (Ph.D., Universitat Autònoma de Barcelona, 2013, summa cum laude and "Extraordinary Ph.D." Award), and nuclear materials, geochemistry of radionuclides and nuclear security (postdoctoral training, Stanford University, 2017–2019). He is based in Barcelona, Spain.

EDITOR'S COMMENT: The same dilemma question for terrorists and Pakistan's nuclear arsenal.

Wargame shows attacks on reactors would cause meltdowns and military paralysis

By Henry Sokolski
Source: https://thebulletin.org/2023/06/wargame-shows-attacks-on-reactors-would-cause-meltdowns-and-military-paralysis/

June 26 – For more than a year, nuclear experts have wrung their hands about the risk of radiological releases from the Zaporizhzhia nuclear power plant in southeastern Ukraine and how best to prevent them. More than 15 months into the war, though, Russian attacks against Ukraine's nuclear plants have released no radiation. This may be no accident. So far, Russian President Vladimir Putin has avoided destroying Ukraine's nuclear power plants. Otherwise, they would have been demolished long ago. Instead, Putin has aimed to damage them and Ukraine's electrical supply system as part of a larger effort to erode Ukrainian morale.
His strategy is unlikely to be a one-off. North Korea and China also have "wayward provinces"—South Korea and Taiwan, respectively. And they have long-range missiles too. Beijing and Pyongyang have considered targeting reactors. How these countries might, if at all, follow Russia's example depends on what they make of Putin's current assaults against reactor sites.

Reactors in warzones

When he launched his full-scale invasion on February 24, 2022, Putin hoped Ukraine would immediately surrender. His initial aim wasn't to disable Ukraine's reactors or electrical supply systems but to seize them. And he did: On the first day of the invasion, Russian forces took control of the Chernobyl nuclear plant, and in early March they seized the Zaporizhzhia nuclear plant. Russia's invasion, however, quickly stalled. As a result, Putin changed his strategy: He directed his military to shell the plant sites and electrical power nodes critical to powering the plants' coolant pumps and safety equipment. Russian agents also kidnapped and terrorized plant workers, which jeopardized Zaporizhzhia's safe operation. In addition, Putin stepped-up attacks on the rest of the Ukraine's electrical supply system to frighten the Ukrainian population further, undermine its will to resist, and possibly destabilize the entire grid, including the nuclear portions of the electrical supply system. So far, these efforts have had mixed results: Some senior officials in NATO countries have been rattled (fearing radiation leaks and military escalation); the Ukrainians, however, have not.
Certainly, Russia's willingness to take advantage of the military vulnerabilities of nuclear sites in Ukraine has set a precedent. It is unclear if any other nation would make the mistake Russia did in assuming that it could easily seize and hold an adversary's nuclear facilities at the very outset of hostilities. If not, they might move to Russia's second stratagem of militarily holding the electrical supply system and its nuclear plants at risk right away. How might such a war proceed? Might Russia aim to knock out the grid, strike Ukrainian nuclear plants, and risk major radiological releases? Might it target NATO reactors (which could include more than 50 US-promised plants in Poland, Romania, and Ukraine by 2037)? How might Ukraine, the United States, and NATO members respond?
To answer these questions, the Washington-based Nonproliferation Policy Education Center (NPEC) designed and hosted a wargame. The game assumed Russia will re-invade Ukraine 15 years from now—in 2037—when both sides will have substantial numbers of long-range, accurate missiles and drones. It also assumed Ukraine and Eastern NATO countries will have new reactors of US design on their territory. In November and December of 2022, NATO officials, American hawks, American doves, Ukrainians, Romanians, nuclear experts, US military officials, and Polish experts were all tapped to prepare, critique, and play remotely over a two-week period.
The game's play revealed how the uncertainties and dangers of military attacks against nuclear power plants can paralyze decision-making and fundamentally alter the course of wars. The military disruptions these uncertainties introduce may far outstrip the safety issues any reactor radiological release might otherwise present. The game's play revealed three reasons why.

The US and its allies are unprepared

Overseas adversaries can easily target allied or friendly nuclear power plants in ways that the United States and its allies are unprepared for. What was stunning throughout the game's play was the reluctance of the players—other than those representing Ukraine and Poland—to act even after Russian military assaults were made against nuclear power plant sites in Ukraine and NATO countries. The United States team, for example, waited and then failed to extract US personnel at reactor sites that Russia had hit in Ukraine and that were leaking radiation. Only after Russian missiles had induced a loss of coolant at one of Ukraine's Khmelnitsky Westinghouse reactors and threatened to do the same to nuclear power reactors in NATO countries did the NATO team take decisive action. This consisted of supplying the targeted plants in Ukraine, Poland, and Romania with active defenses and auxiliary emergency cooling equipment.
In the game, nuclear expert team members gave contradictory advice to each of their teams about how well any of these reactors would fare against aggressive military assaults. This was unexpected but turned out to be significant. Radiological leaks were detected but assessments of these leaks' implications for public safety were only hastily made after the reactors were hit. These assessments also varied widely

and were responded to quite differently by each team. The Ukrainians ordered a massive evacuation after Russia struck one of its reactors; Poland, whose reactor site also was hit but was releasing no radiation, took no public safety steps until they detected a radiation cloud from Ukraine drifting over Polish territory.

Although war planners prefer to devise precise, proportionate diplomatic, political, and military responses, this is difficult to do amid ongoing attacks against nuclear plants. The reason why was made evident in the game: The nuclear experts in the game rendered very different assessments of what was happening and how dangerous the assaults on plants might be to the surrounding population. There was a tendency among NATO members, who wished to stay out of the fight, to downplay the safety implications. It was just the opposite among the countries at greatest risk of being painted with radiation. This suggests that such “differences” in threat perception might not be quickly resolved through some technical nuclear forensic assessments of events. The creation of international norms or nuclear safety zones in war zones, meanwhile, may be desirable but are extremely difficult to attain. As such, the risks and benefits of adding new nuclear plants in high-risk war zones must be reassessed.

Reactor attacks can paralyze allied responses

The hesitation of the United States in responding to military assaults against friendly countries’ reactors can risk near-fatal fracturing of US security alliances. In the game, NATO countries closest to the fighting (e.g., Poland) wanted to join Ukraine in conducting deep strikes into Russia against key staging bases that were launching attacks against Ukraine’s reactors. Initially, some NATO countries were sympathetic to Ukraine striking Russia. All NATO members were concerned that matters might escalate and spill over into NATO territory. As a result, NATO was ready to invoke Article 4 of the NATO treaty, which authorizes NATO members to bring issues of concern to the attention of the organization.

Eager to avoid direct military contact with Russia, however, key members of NATO decided to manage Poland’s desire to back Ukrainian strikes against Russia by invoking Article 5. NATO did this less to support military operations (much less to attack Russia) under Article 5, as to deter any independent action Poland might otherwise take against Russia. In the game, the tactic worked: NATO members, including Poland, were deterred from striking Russia. This tactic, however, failed to deter Kyiv. Ukraine unilaterally struck airbases deep in Russia. This action only further amplified the different concerns of NATO members near the action and those of members located farther back.

Such alliance strains can only be addressed in one of two ways: The reactors either must be defended actively or passively so well that radiological releases and electrical failures appear nearly impossible, or alliance war plans and responses must be devised and agreed to in advance and be sufficiently dramatic to deter such attacks. Neither will be easy. As for developing tailored deterrence strategies, the most relevant analogy here may be “pre-planning” to deal with nuclear weapons attacks—a vexing, dubious undertaking at best.

Legal disagreements about reactor attacks

Attempts to settle the question of whether military assaults against nuclear plants constitute war crimes or if subsequent radiological releases qualify such attacks as nuclear weapons use can themselves become significant wartime distractions. In the game, Ukraine insisted that Russia’s attacks against reactors constituted an actionable war crime under Protocol 1 of the Geneva Convention. Ukraine and others also claimed such assaults constituted first use of nuclear weapons.

These claims divided NATO players. They subsequently not only delayed actions critical to waging the war, but also prompted Ukraine to act unilaterally in an escalatory action, firing missiles deep into Russia without NATO’s support. This is worth avoiding. Both NATO members (except the United States) and Russia have ratified Protocol 1 of the Geneva Convention, which specifically discourages assaulting nuclear power generating stations. Yet current US legal guidance regarding Protocol 1 is murky. Although the United States is obligated as a signatory to Protocol 1 to avoid attacking nuclear power reactors, Pentagon lawyers insist US commanders should ultimately be free to attack these plants if they think it is necessary. It would be helpful if the US view was clarified and brought into line with the strong presumption of US allies against making such attacks.

Yet another divisive issue is what constitutes first nuclear use. In the game, European NATO members sympathized with Ukraine’s contention that Russia’s “intentional” attacks against nuclear plants that consequently released radiation should be considered a “use” of nuclear weapons. The United States ignored this assertion. Yet another unresolved legal question is whether or not radiation that contaminates NATO soil from an intentional Russian attack of Ukrainian reactors should constitute an actual attack on NATO and, therefore, demand an Article 5 response. The players were briefed on this point but chose not to play it. Here, again, some European NATO public officials have supported the idea, whereas the United States has taken no position.

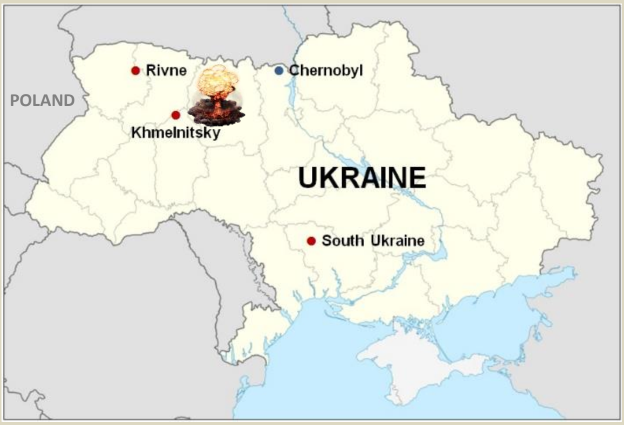
Wargame format

The wargame consisted of three moves. The first began in 2037. Putin’s successor launches a second invasion of Ukraine, and the Russian military assaults and occupies the four-unit Khmelnitsky plant, which now has been expanded to include two US-built reactors in addition to the two Soviet-design VVER reactors. In the second move, the situation escalates, and several missiles explode in the parking lots of nuclear power plants in Romania and Poland and hit several supporting emergency diesel generators. The game's last move was a "hot wash" in which the group discussed the simulation and the players' key findings.

Wargame participants were organized into three teams representing the United States, Ukraine, and NATO-EU nations. The control team oversaw communications, managed the scenario, and represented Russia. Teams responded to the crisis, communicated with other teams to gather information, negotiated, and created a response strategy and contingency plans.

Move one

It is 2037. Putin is dead. His successor, frustrated by the "forced, unjust" armistice reached with Ukraine in 2024, attempts to complete Ukraine's absorption, launching an attack against Ukraine's southern and western salients. Westinghouse has completed two of its promised US reactors in western Ukraine at Khmelnitsky, which are operated with the assistance of US technicians. Additional US and South Korean power reactors have been built as promised in Poland and Romania and are now on line.



After several weeks of fighting, Russian forces assault and occupy the Khmelnitsky plant and garrison missile strike forces at the reactor site. The Ukrainians precisely target Russia's missile units at Khmelnitsky using weapons the United States has shipped to Ukraine. Russia protests publicly, demanding NATO cease supplying such weaponry through Poland and Romania.

Meanwhile, in a repeat of the tactics Moscow used in 2022 against Zaporizhzhia, Russia fires missiles knocking down several power lines into the Khmelnitsky plant. This threatens the continued reliable supply of external electricity to the plant, which is needed to prevent the reactors' cores and spent fuel pools from overheating and releasing radiation.

Spooked, nearby Romania and Poland (both NATO and EU nations) urge their populations to avail themselves of stockpiled iodine pills. Meanwhile, Russia and Ukraine blame each other for targeting the felled power lines. Then, a missile fells the last external power line connected to the plant, forcing it to run on its emergency diesel generators, which at the time only have enough fuel to operate for ten days.

This sets off international alarms. The director general of the International Atomic Energy Agency (IAEA) warns that the latest attack could result in a Fukushima-like radiological release unless the agency can gain access to the facility and assure proper safety measures are being taken. Fighting near the plant, however, makes it dangerous to access. Nonetheless, in a repeat of 2022, the IAEA manages to send a team of inspectors to help "stabilize" the plant and avert any radiological release.

Unfortunately, the opposite situation unfolds. While the IAEA staff are en route, the Russian military bombs and disables the main paved corridor to the plant. One of the Russian strikes glances an IAEA vehicle, injuring an inspector. Russia indignantly denies any responsibility but joins Ukraine and the IAEA in calling for an emergency meeting of the UN Security Council.

NATO fears Russia will use its military garrison at Khmelitsky to strike the surrounding areas with impunity. The US team cautions that fighting near the plant could cause a radiological release and ultimately a meltdown.

Advisors to the US Energy Department recommend that the US-designed AP1000 and Russian-designed VVER spent fuel be transferred from the pools to dry cask storage. They also warn that further military assaults on Ukraine's nuclear plants could produce radiological releases that would force the evacuation of communities both within and beyond Ukraine's borders. Most NATO advisors, however, deem the immediate probability of a major radiological release to be low.

Russia then attacks some of the diesel fuel storage tanks at the Khmelnitsky plant, leaving the plant with only several days' worth of diesel fuel to run the emergency generators. Shortly after, Ukraine releases a video providing evidence of Russia's responsibility for the attacks.

Ukraine calls for the IAEA to mediate a shipment of diesel fuel to the plant's site to prevent a meltdown. The United States and its NATO allies support this request. The United States demands that Russia move its missiles out of the reactor site and create a demilitarized zone around the plant. Ukraine confirms the presence of US Westinghouse personnel at the Khmelnitsky plant, but they are unable to leave the site.

NATO advises the United States that the long-term threat of a radiological release is growing and asks Ukraine and Russia to shut down the last operating reactor at the site. NATO believes that shutting the plant entirely is a reasonable request and suggests enlisting China and the UN Security Council to pressure Russia into doing so. In response to these requests, Russia puts the reactor on normal shutdown mode and demands that the United States de-escalate the situation by ceasing to send arms to Ukraine. When asked to ensure the security of the IAEA inspectors, Russia agrees.

Ukraine asks the United States and NATO to issue a joint press release stating that Russia's actions were an intentional effort to trigger a meltdown of one of the Khmelnitsky nuclear reactors, that Russia's attacks of the plant constitute a war crime, and that the allies view any event involving radiological dispersal as an intentional use of a "nuclear weapon" by Russia against Ukraine. Washington is hesitant to grant Ukraine's request and confers with key NATO members regarding its position. NATO consensus, however, was impossible to achieve. A key concern was that backing Ukraine's position would undermine any opportunity to negotiate with Russia.

Disappointed, Ukraine issues its statement independently and makes its own military plans to regain control of the plant. For this purpose, Kyiv asks the United States and NATO for precision missiles, drones, electronic warfare equipment, and satellite intelligence—to which they both agree. Ukraine also asks the United States and NATO for tools and transformers to restore external electrical power to the plant, as well as Western experts to monitor the plant's safety and the security of the plant's staff. The United States and NATO demur and instead suggest the IAEA assume this role and that UN peacekeepers and the Red Cross be placed in and around the nuclear plants.

Washington, then suggests a hedging strategy. First, it asks NATO to pressure Russia to demilitarize a zone around the plant. Second, it asks NATO for help positioning troops, diesel fuel, and emergency generators at the border with Ukraine. NATO agrees and positions counter-battery radar, counter-battery missiles, and troops near the Ukrainian border in Southern Poland. NATO also puts troops on a 24-48-hour recall alert system to allow them to quickly deploy where needed. It also puts its Combined Biological Radiological Nuclear (CBRN) forces on standby.

Several NATO members believe Russia's aggression against the Khmelnitsky plant constitutes a significant security risk. They raise this issue but defer to the United States on whether to invoke Article 5. Washington is not ready to do so.

Move Two

Fighting in and around the Khmelnitsky plant continues. Russia warns Ukraine's reckless targeting of Khmelnitsky risks a Chernobyl-like radiological release.

Meanwhile, Ukraine's counteroffensive against Crimea gains ground. As Ukrainian forces close in on Sevastopol, Ukraine discovers that Russia intends to launch a false flag attack against a small research reactor at the Sevastopol National University of Nuclear Energy and Industry. Russia fires a missile damaging the reactor, prompting a limited, local release of radiation. Moscow immediately accuses Ukraine of having attacked the reactor with NATO-supplied weaponry and again demands that Romania and Poland close their borders to any further deliveries of US and NATO-supplied offensive weapons. Moscow further warns that failure to seal the border will result in Russia taking "proportionate" action against Poland and Romania.

Before NATO or the UN can meet, several missiles explode in the parking lots of the US NuScale reactor in Romania and of the Westinghouse AP1000 and Korean KEPCO APR-1400 reactors in Poland. Poland and Romania temporarily shut down these plants. Meanwhile, Ukrainian forces push Russian troops out of key positions in Crimea. Panicked, Moscow announces it will target Poland and Romania further unless they immediately stop all military equipment transfers into Ukraine. The United States, NATO, and Ukraine try to confirm Russia's culpability for the strikes in Poland and Romania as a majority of NATO members are unwilling to attack Russian forces until there is proof of an imminent attack.

While NATO awaits definitive intelligence, Ukrainian technicians at the Khmelnitsky nuclear plant worry that they may soon run out of diesel fuel needed to run the emergency electrical generators. To replenish their diesel stocks, Ukraine asks NATO to deliver fuel to Khmelnitsky. The United States, concerned about US Westinghouse employees unable to leave the Khmelnitsky plant, plans to use the extraction of its personnel as an opening to also bring fuel to the generators.

Ukraine again calls for the United States and other NATO member countries to condemn Russia's attack against nuclear power reactors as a war crime under Protocol 1 of the Geneva Convention and insists it constitutes a first use of nuclear weapons. Shortly thereafter, overhead surveillance confirms that the missiles that struck Romania and Poland were fired from Russian-occupied Crimea. European NATO members, sensing Washington's general reluctance to invoke Article 5, are uncomfortable doing so but fear Poland, who is closest to Ukraine geographically and politically, might now strike Russia unilaterally. They want to invoke Article 5 to prevent this and the expansion of the war that might follow if Russia is struck.

Ukrainian leaders, meanwhile, feel NATO has abandoned them. They begin planning a retaliatory strike against Russia. Initially, some Ukrainian officials privately advocate striking Russian nuclear reactors, natural gas infrastructure, and urban and political centers. **They drop this suggestion, though, for two reasons**. First, it is unclear how hitting these targets will bring victory. (Ukraine had too few long-range strike systems to take this expansive target set on.) Second, striking them would undermine Ukraine's position that striking power reactors is a war crime. For these reasons, any Ukrainian strike against Russia is limited to military targets.

Farther to the west, Ukraine continues its plans to retake the Khmelnitsky plant. As fighting intensifies near the plant, all power to the plant is lost when unidentified missiles hit these reactors' dedicated emergency diesel generators. Within hours, battery backup power for the reactors' instruments is also lost.

Fire trucks are not available to provide emergency cooling. Ukrainian experts have no access to the plant, but they assess there is now only enough convective cooling to prevent meltdowns for a day or so at the VVER reactors and perhaps a bit more for the AP1000 units. As for the spent fuel pools, these should remain stable for at least a week.

The United States moves backup power generators and diesel fuel to Ukraine's border. US troops accompany these shipments. Russia warns that if NATO troops enter Ukraine, it would constitute an act of war against Russia. The US troops and power backup equipment do not cross the border. The US plan to rescue the Westinghouse employees also falls by the wayside as the crisis escalates, leaving US citizens trapped at Khmelnitsky.

After three days, **meltdowns occur within all the reactors**. However, at one of the two the AP1000 reactors, things spin even further out of control. Not only does the automatic, passive water-cooling reserve system runs out and radioactive steam and hydrogen build up; but because there is no external electricity flowing into the plant, the AP1000 reactors' electric hydrogen igniters cannot be used to "burn" off the hydrogen. An accidental spark at one of the AP1000 units prompts an explosion. This produces a major breach of the reactor's concrete containment and a significant atmospheric radiological release. Ukraine calls for a ceasefire to allow evacuation. Russia does not respond to this request.

The AP1000 reactor's radiological release upsets Ukraine's military plans to retake the Khmelnitsky plant. Frustrated, Ukraine decides to retaliate against Russia with a major long-range missile strike against Russian Black Sea fleet bases, including the base at Novorossiysk, well within Russian territory. Ukraine's objective is to make a "proportionate" military strike against valued Russian military bases.

At the Khmelntisky plant, shifting winds push the plant's leaking radiation towards Poland, prompting some officials to recommend evacuating Rzeszow and Lubin. Ultimately, this course is rejected and instead Polish authorities ask the citizens to stay-at-home. NATO also considers delivering air defense systems, including Patriot and THAAD units, to Ukraine. These would protect its nuclear plants and act as a first-line defense for the rest of Eastern Europe. Ukraine, though, is unaware of these NATO deliberations. Ukraine, still believing NATO has abandoned it, asks Poland to conduct joint military operations against Russia.

Russia learns about NATO's plan to send air and missile defenses into Ukraine and warns that, if these systems cross the border, they will become a legitimate military target. At this time, unidentified missiles hit diesel generators at the Polish plant and at the Romanian CANDU reactors. Russia claims again that this is Ukraine's doing. NATO, including the US team, decide to go ahead with the deployment of air defense units to Ukraine, despite Russian warnings. NATO and the US team also deploy air and missile defenses, fire trucks, emergency electric generators, and diesel fuel stocks at all the nuclear plants in Poland and Romania. Washington forward-bases B-21 bombers to Poland and Romania to deter further Russian aggression, invokes Article 4, and asks NATO to invoke Article 5.

From this point on, events unfold rapidly. The players have difficulty managing what ensues.

Ukraine asks NATO for additional intelligence, missiles, and drones so Ukraine can strike the Russian staging bases that attacked Poland and Romania. Some frontline NATO countries are sympathetic, but the United States and several legacy NATO members refuse to support such attacks. Meanwhile, NATO-provided air and missile defense systems cross the border into Ukraine. In response, the Russians target them. Russia hits most of these air and missile defense systems after they cross the border. Russia hits one, however, while it technically is still in NATO territory. Further to the south, the radiation spewing from the Khmelnitsky plant forces Russian troops to begin to evacuate the site. At this point, Ukrainian forces decide to move in to open up a corridor for fire trucks to reach the reactors. However, their progress is stalled by Russian forces.

Eager to take action, even without US or NATO support, Ukraine then launches a missile strike against the Russian strategic bomber airbase at Engels, which intelligence shows is a source of many airstrikes against Ukraine. Ukrainian missiles disable the air base's runways, fuel farms, and long-range bombers.

Per its previous warning that any strike against its territory would constitute cause to place its nuclear forces on high alert, Russia does so. The United States, United Kingdom, and France respond in kind and NATO formally invokes Article 5 but does not take immediate military action. Instead, the United States proposes providing support to a Ukrainian offensive against Crimea, leaving open the option of direct US military involvement if that offensive is unsuccessful.

Game play ends at this point.

Henry Sokolski is the executive director of the Nonproliferation Policy Education Center in Arlington, Virginia, and author of *Underestimated: Our Not So Peaceful Nuclear Future* (2019). He served as deputy for nonproliferation policy in the office of the US secretary of defense during the George H.W. Bush administration.

How the United States and NATO can deal with Russian nuclear coercion in Ukraine

By Alexander Vershbow

Source: https://thebulletin.org/2023/06/how-the-united-states-and-nato-can-deal-with-russian-nuclear-coercion-in-ukraine/

June 23 – It has been more than a year since the start of Russia's full-scale invasion of Ukraine. Russia's unprovoked war of aggression unleashed the biggest crisis in European and global security since World War II. And there is still no end in sight. Russian President Vladimir Putin's war of choice has also brought the world closer to the nuclear brink than at any time since the Cuban Missile Crisis, and it has put in doubt the future of East-West arms control negotiations and international efforts to control the spread of nuclear weapons.

A lot is on the line in this conflict, which goes beyond Ukraine's survival as an independent state. Russia has challenged many of the fundamental principles of the international order on which European and global security have long been based—principles like respect for the sovereignty and territorial integrity of states, no changing of borders by force, and freedom for nations to choose their security arrangements, including treaties of alliance.

In threatening to use nuclear weapons to achieve his objectives, Putin has displayed a disturbing readiness to break the taboo on nuclear use that has prevailed since 1945, eroding strategic stability and undermining the nuclear nonproliferation regime. Nuclear risks could be exacerbated by Russia's latest decisions to suspend compliance with the New Strategic Arms Reduction Treaty (New START) and to deploy nuclear weapons in Belarus.

While the United States and its allies must manage the risks of nuclear escalation carefully, defeating Putin, restoring Ukrainian sovereignty, and reinforcing the rules-based order must be our priorities.

Putin's fear

Despite many setbacks on the battlefield and multiple miscalculations by Putin, Moscow's war aims have not changed since the start of the war on February 24, 2022. It still seeks to subjugate Ukraine to Russian hegemony, to annex territories that Putin views as historically Russian lands, and to erase Ukrainian national identity altogether on the grounds that Ukrainians are really just Russians who have been led astray by the evil West. Putin wants to bring Europe back to the days of spheres of influence and "might makes right," forcing Kyiv to renounce security ties with NATO. He has shown no sign of readiness to negotiate an end to the conflict on terms other than Ukraine's complete capitulation and acceptance of the "new territorial realities," namely, Moscow's purported annexation of Crimea and four other Ukrainian provinces.

At the root of the crisis is Putin's fear of Ukrainian democracy, which he sees as a dagger pointed at the heart of Russia and his imperial ambitions. For Putin, the success of democracy in Ukraine would set a dangerous example to the Russian people that would ultimately undermine the authoritarian system Putin has built since taking power 23 years ago.

If Russia succeeds in achieving its objectives, even partially, it will damage fundamental US and NATO interests. It will increase the Russian military threat to NATO and encourage other despots with revisionist ambitions to follow Putin's example, including his resort to nuclear threats. One most dangerous, yet plausible, scenario is an emboldened China, with expanding nuclear and conventional arsenals, seeking to subjugate Taiwan by force.

Putin himself has been clear that his own ambitions extend beyond Ukraine. If not stopped there, Putin could use force against other former Soviet countries that Putin considers as historically belonging to the Russian Empire. These include NATO members, such as Estonia, Latvia, and Lithuania, that are covered by the alliance's Article 5 guarantee and the US nuclear umbrella.

Self-restraint won't work

Allies need to provide sufficient conventional weapons to enable Kyiv to repel Russia's ongoing offensive in eastern Ukraine and support a Ukrainian counteroffensive that can recover more occupied territory. By helping Ukraine gain the upper hand on the battlefield in the coming months, allies can strengthen its hand at the negotiating table and increase the chances of achieving a just peace.

While thus far Russia has not followed through on its threats to use nuclear weapons, its nuclear saber-rattling has been effective in one important way: constraining the types and quantity of conventional weapons that the United States and its allies have been willing to provide to Ukraine. As President Biden has said many times, the United States and its allies are committed to supporting Ukraine "for as long as it takes," but in a way that avoids triggering World War III.

The declared rationale for this policy is to prevent or discourage a Russian escalation of the conflict, especially to the nuclear level. In practice, however, self-restraint has often invited more Russian escalation—such as the massive attacks in recent months on Ukrainian power grids and other critical civilian infrastructure. The desire to discourage Russian escalation has led the United States to deny longer-range missiles like the Army Tactical Missile System (ATACMS) and advanced drones that could eliminate many of the Russian weapons carrying out many of the infrastructure attacks.

In effect, the United States and its allies have given Russia a sanctuary in occupied Crimea and in neighboring regions of Russia from which to launch its brutal attacks on Ukrainian civilians. Putin wouldn't be wrong in concluding that nuclear coercion works.

The consequences of this self-restraint for Ukraine's war plans could be dire, however.

Ukrainian armed forces made extraordinary gains in the fall of 2022, thanks to the delivery of sophisticated long-range rocket and artillery systems from the United States and other allies, including the much-publicized High Mobility Artillery Rocket System (HIMARS). This enabled them to destroy dozens of Russian ammunition depots and command posts behind the front lines, creating the conditions for Ukraine's successful counteroffensives in Kherson and Kharkiv.

Most experts agree that further Ukrainian victories are possible if they receive sufficient support for their ongoing counteroffensive, which started in the late spring and may extend well into the summer or fall. But there may not be enough HIMARS or other heavy weapons in the pipeline for Ukraine to consolidate its gains and retake more territory in the coming months. While allies have belatedly agreed to provide modern tanks and other armored capabilities, only a few battalions of tanks are likely to arrive this year. Ukraine also needs more air defense systems to cope with the threat posed by Russian cruise missiles and Iranian drones.

While recent decisions to accelerate production will help, US and allied defense ministries may be too slow, and policymakers too cautious, to ensure that Ukraine gets the advanced capabilities it needs, and quickly enough, to inflict a decisive defeat on the Russians this year. Meanwhile, some senior officials in the Biden administration have been openly urging the Ukrainians to quit while they are ahead and engage in negotiations with Russia—even though talks right now would be used by the Russians to freeze the battle lines and hold onto illegally occupied Ukrainian lands.

The Biden administration has reiterated that it is up to the Ukrainians to decide when and how to negotiate. But mixed signals from Washington (and from some European capitals) may convince Putin that time is still on his side if he can steer things toward a stalemate. He may still be confident that the Ukrainians will ultimately become exhausted by the Russians' relentless and indiscriminate attacks on civilian infrastructure and that Western unity and public support will continue to erode.

Firm but calibrated support

The next few months will be crucial to restoring momentum to the Ukrainian campaign. The United States and its allies need to commit themselves unequivocally to the goal of Ukrainian victory and act accordingly in their support for the Ukrainian military. Allies need to calibrate what weapons they provide to avoid escalation, but they should not let themselves be intimidated or self-deterred by Russia's saber-rattling.

The nuclear risks must be kept in perspective. Putin has brandished nuclear threats from the moment he launched his re-invasion of Ukraine last year. He reinforced those threats in September, after Russia's defeat at the hands of the Ukrainian counteroffensive in Kharkiv. With his subsequent move—holding fake referenda as the basis for annexing four Ukrainian provinces in the South—Putin appeared to be doubling down on his nuclear threats. It sounded as though he was daring the Ukrainians and their Western backers to risk nuclear retaliation if they attempted to retake territory that was now purportedly an integral part of Russia (even though it was only partially under Russian control).

But over the succeeding weeks, Putin pulled back from the brink. In his speech to the Valdai Discussion Club in late October, he claimed that he had never considered the use of nuclear weapons and declared that using nukes would be "pointless" in military terms. This climbdown may have been a response to pressure from China, India, and other partners that were becoming increasingly alarmed by Putin's cavalier nuclear threats. Putin may have been deterred even more by US warnings of "catastrophic consequences" for any Russian use of nuclear weapons.

Although the immediate risk of nuclear use may have receded, there are no grounds for complacency. Putin continues to escalate the conflict in non-nuclear domains, with the destruction of civilian infrastructure and the general terrorization of the Ukrainian population. The March 14 shootdown of a US reconnaissance drone over the Black Sea could signify a new willingness to challenge allied military support for Kyiv. In recent weeks, Putin has threatened to dismantle the remaining constraints on strategic nuclear forces by suspending New START and announcing plans to deploy tactical nuclear weapons in Belarus. Both moves are clearly intended to raise anxiety among NATO governments and publics.

Putin may renew his direct threats to use nuclear weapons if Russian forces suffer major new setbacks on the ground, and especially if Ukrainian armed forces mount a serious threat to Russia's hold on Crimea, which Putin views as central to his political legacy as the in-gatherer of historically Russian lands. Losing control over Crimea could bring Putin under intense pressure from hardliners to use nuclear weapons to stave off defeat and punish the Ukrainians and their Western backers. One recent example of hardline views can be found here.

But even in that case, it will always be a lot easier for Putin to threaten nuclear escalation than to carry it out in practice. The effects on Russian troops and civilians of even a low-yield nuclear strike or "demonstration" shot could be quite severe and unpredictable, given the vagaries of the weather.

Although Putin was uncharacteristically reckless in launching this war of aggression, he is unlikely to want to risk the "catastrophic consequences" promised by the United States, even if his back is up against the wall. Those consequences may primarily involve massive conventional strikes on Russian forces and military infrastructure in Ukraine; but the United States has not ruled out a limited nuclear response in kind if Russia breaks the nuclear taboo that has been in place since 1945.

Moreover, for Putin to violate the nuclear taboo would only increase Russia's political isolation and potentially elicit opposition from Russian miliary commanders that could threaten Putin's grip on power.

Using nuclear weapons would increase the likelihood that the United States and NATO would be drawn directly into the conflict, which Putin has been keen to avoid from the very outset of the war. It could prompt calls within NATO to expand tactical nuclear weapon deployments in Europe beyond the limited steps called for in the Biden administration's Nuclear Posture Review (NPR). A new NPR may be needed in any case to redress the imbalance between US and Russian non-strategic capabilities that will be exacerbated by deployments in Belarus, and to counter China's looming nuclear buildup.

Whatever one's assessment of the probability of nuclear use by Russia, it will be essential to strengthen deterrence by making clear to the Russians that they would pay a very heavy price—in terms of a swift and decisive military response, a ratcheting up of economic sanctions, and further political isolation of Russia—if they break the nuclear taboo.

And above all, Moscow should understand that the United States and its allies will not be deterred from continuing to arm and train Ukrainian armed forces fighting to restore their country's independence, sovereignty, and territorial integrity.

Standing firm in helping Ukraine regain its territory is the best way to persuade the Russian officials that their best course of action is to end the war, withdraw their forces from Ukraine, and negotiate a political settlement that restores Ukraine's sovereignty within its internationally recognized borders, holds Russia accountable for war crimes, and provides guarantees that Russia will not invade a third time.

Ripple effect

Other countries, including North Korea and Iran, will be watching to see how firmly the West stands up against Russian nuclear coercion. Both may see the US preoccupation with the Ukraine crisis as an opportunity to advance their nuclear ambitions.

Indeed, in the case of North Korea, the year of 2022 saw a major spike in tests of intercontinental and shorter-range ballistic missiles aimed at intimidating the United States and South Korea from conducting longstanding joint military exercises on the Korean peninsula. Pyongyang is reportedly preparing for another nuclear weapons test, has renounced its previous commitment to denuclearization even as a long-term goal, and has spurned US offers of dialogue without preconditions on lowering tensions. The North Koreans may be planning to provide conventional weapons and munitions to Russia in return for economic aid and sanctions relief, which will only make Pyongyang even more recalcitrant about negotiating reductions in its nuclear weapons program and more provocative in carrying out more nuclear and missile tests.

For its part, Iran has stepped up to the threshold of becoming a nuclear weapon country by enriching uranium to close to weapons grade. This seriously reduces the value of reviving the Joint Comprehensive Plan of Action (JCPOA), even if such a revival were politically possible. With Russia increasingly dependent on imported Iranian drones in its war against Ukraine, Moscow may decline to do anything to convince Tehran to comply with its JCPOA obligations. The United States and its allies will need to consider additional forms of pressure on Tehran to discourage a decision to break out of the deal, which may be the only way to head off unilateral Israeli military action to destroy or damage the Iranian program.

Alexander Vershbow is a former US ambassador to Russia and South Korea, a former deputy secretary-general of NATO, and a distinguished visiting fellow at the University of Pennsylvania's Perry World House. *The statements made and views expressed in this article are solely the responsibility of the author.*

Sri Lanka – Radiological Terrorism: A deadly future threat

By Dishan Joseph

Source: http://www.dailynews.lk/2023/07/05/features/306993/radiological-terrorism-deadly-future-threat

STF special convoy

July 05 – Terrorism manifests in many forms. Sri Lanka is an island. Various chemical substances enter the country through the airports and through the seaports. Also due to the strategic location of Sri Lanka ships with various containers of chemical substances arrive at Colombo Port. The risk of chemical reactions rising to hazardous levels is more likely to occur and remains a challenge. In view of this, the National Authority for the Implementation of the Chemical Weapons Convention in Sri Lanka has taken various measures to prevent possible accidents from chemical agents within Sri Lanka. We, as a nation, have witnessed many forms of terrorism and radicalized extremism. Globally, the main security focus is the protection of radioactive material and secure transportation of the same. If such material falls into the hands of criminal or terrorist groups in the future, we will have to face dangerous consequences.

Radiological terrorism is a rising trend globally. Terrorist organisations have mastered the art of weaponizing radioactive material. There are three ways in which they can unleash this terror- Improvised Nuclear Device (IND that creates massive explosion force and radiation), Radiological Dispersal Devices (RDD or commonly known as dirty bombs) and Radiological Exposure Devices (RED). The threats posed by CBRN weapons in both Europe and Asia have been highlighted by their use in assassinations and assassination attempts. Further dimensions of threat arise when considering potential CW use in mass impact terrorist attacks such as the nerve gas attacks on the Tokyo subway in 1994 and 1995 by the Aum Shinrikyo cult. Their most recent use on a large-scale has occurred in Syria, where various types of chemicals and delivery methods have been used by both State and non-State actors since 2013. The RED is a terrorist device intended to expose innocent people to significant doses of ionizing radiation without their knowledge. A RED can be hidden in a public place such as a food court or a shopping mall. Examples of radioactive dissemination techniques include postal packages, spray devices, commercial crop dusters, air conditioning systems, cooling fans and direct injection. A radioactive incident can also occur when a facility that stores radioactive material is attacked. However, it must be mentioned that stealing such material is no easy task as the terrorist can be exposed to the material and be dead in a few minutes or a few days.

International symbol

STF crew

STF response

One of the first local agencies to realize the threat of CBRNE is the Special Task Force (STF) of the Sri Lanka Police. CBRNE stands for Chemical, Biological, Radiological, Nuclear and Explosive. The first four elements can be used individually to create a large number of casualties and can be coupled with the fifth element of explosives to double the impact.

The STF, with the guidance and collaboration of the US Department of Energy, National Nuclear Systems Administration (NNSA), Pacific Northwest Laboratory, Office of Radiological Security (ORS), Global Materials Security and the Sri Lanka Atomic Energy Regulatory Council (SLAERC) had built the nation's first Central Monitoring Station at Katukurunda in October 2019.

Radiation occurs naturally and is also manmade. In a nutshell, radiation is the energy emitted from excited atoms. Common manifestations of radiation are found in light, heat, radio waves and microwaves – but these do not pose a threat to national security. The imminent danger lies in ionizing radiation. The IAEA (International Atomic Energy Agency) has four category rankings for radioactive materials, with Category One being the highest risk where exposure for a few seconds can cause death and permanent injury. This is why radioactive material must be controlled. Globally, nuclear materials like plutonium and enriched uranium are used to power submarines and industrial reactors.

Common radioactive materials include Cobalt 60, Cesium 137 and Strontium 90. Radioactive material is used in medical treatment to irradiate cancer. It is also used in brachytherapy needles and tiny seeds that are planted in the body to fight prostate cancer. In other mild forms, it is injected into the body during scans. But, the risk arises when radioactive materials are handled and transported illegally.

The life of the radioactive 'trefoil' began in 1946 at the University of California, Berkeley. It was only in 1948 that the symbol came under consideration for wider use, when Brookhaven National Laboratory (New York) requested a 'standardized symbol' for use in their radiation safety programme. Today we recognize the black and yellow symbol.

SSP Athula Daulagala (Deputy Commandant STF) said: "During transport and storage these materials must be very secure. Some are covered (from overseas) in an outer housing canister of stainless steel, titanium and plutonium. Gamma emitting materials are kept in lead containers. This type of security transportation involves eight agencies, where we draw up a TSP (Transport Security Plan). They are the Sri Lanka Atomic Energy Regulating Council, the local company that requires material (end user), the Special Task Force, and corresponding local police station, the SIS (state intelligence service), Sri Lanka Customs, Sri Lanka Ports Authority and Traffic Police Headquarters."

Each shipment has a tracking device inside the container. According to the IAEA, the greatest risk is during the transportation process. The routes are chosen and the cargo is moved in a convoy with additional SWAT teams and a STF bomb disposal crew. At present drone monitoring is also done by the STF, covering the convoy route. At some locations (private company), depending on the strength of the radioactive material, it is stored in underwater pools or in chambers where the wall is almost eight feet thick.

SSP Daulagala further explained: "Once an alarm is activated in any of these locations, we receive an alert to the smartphone. From the live visuals, our operators can identify the level of threat – is it a breach of the defensive parameter or an actual theft in progress. There can be a fire on site triggered by electric failure. We have 58 bases across Sri Lanka and each Base Commander is fully trained on how to respond. If it is an alarm, we can send a two-man bike team to check the level of radiation. From our Central

Monitoring Station, we can deploy our first responders by road and helicopter along with SWAT commandos". The STF –CBRNE team's capacity has been enhanced under the prudent tenure of present commandant DIG Waruna Jayasundara.

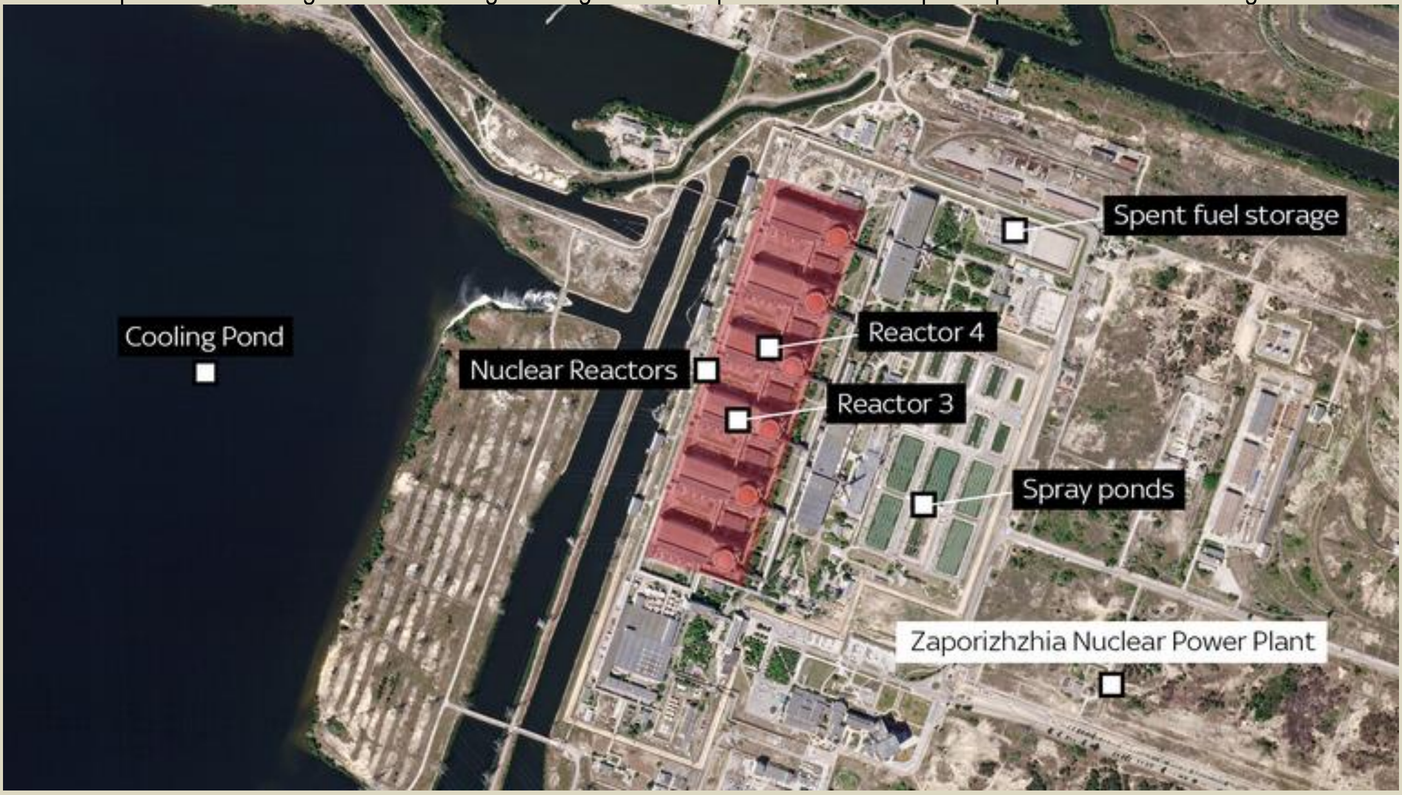
Addressing the challenge of CBRN requires international cooperation. CBRN threats cross borders and so must attempts to manage, reduce and end them. The availability of forensics teams to provide investigative support makes an important contribution to judicial understanding of CBRN related matters.

The STF was active during the Covid period disinfecting various hospitals and isolated villages. The STF is constantly updated by INTERPOL on suspicious movement of radioactive materials globally. With the addition of the CBRNE rapid response teams and the radiological threat monitoring station, the STF has contributed immensely to the future of our national security. The Special Task Force is fully geared to face the emerging threats of CBRNE hazards and chemical terrorism.

The largest danger at the Zaporizhzhia nuclear power plant: intentional sabotage

By Matthew Bunn

Source: https://thebulletin.org/2023/07/the-largest-danger-at-the-zaporizhzhia-nuclear-power-plant-intentional-sabotage/



July 06 – Ever since its seizure by Russian forces in March 2022, the Zaporizhzhia nuclear power plant—Europe's largest, with six reactors—has posed a serious danger of a radioactive disaster. Now, Ukrainian officials have charged that Russia has rigged the plant with explosives, while Russia claims that Ukraine plans an attack on the facility. On July 4, the site lost off-site power yet again, forcing its cooling systems to rely on backup power supply. How serious is the risk of a major radioactive disaster?

That depends on whether we're talking about an intentional or inadvertent radioactive release. If the Russian forces that control the site want to cause a major radiation release— and are willing to use explosives to do it—they could contaminate a huge area. Although the reactors have been largely shut down and cooling for months, they still contain a huge amount of intensely radioactive material that explosives could disperse.

A couple of mines on the roof of a reactor would not be enough. Causing a big release would require some serious demolition with explosives. But that's what was needed to destroy Ukraine's Kakhovka dam—which it appears was done with explosives from within, while Russian forces controlled the site—so a similar operation at Zaporizhzhia can't be ruled out.

No one can accurately evaluate how big an area might be affected; the extent of contamination would depend on how the disaster was caused, how hard the wind was blowing, whether rain brought the radioactive material back to the ground, and more. But one could easily imagine that Russia might hope that such a release would interfere with Ukraine's counteroffensive, forcing some units to focus on evacuating people and cleaning up radioactive fallout rather than battling Russian forces.

By contrast, looking only at inadvertent damage, there are reasons to be optimistic. The Zaporizhzhia reactors are built with thick concrete containment structures, have been cooling for months, and have extra safety features installed after the Fukushima accident in Japan. It is very unlikely that a few stray shells from fighting in the area would cause any serious radioactive release.

Such fighting might damage the cooling systems that keep the hot radioactive fuel in the reactor cores and spent fuel pools covered with water, preventing the fuel from melting. With the reactors as cool as they now are, however, it could take quite a while—a matter of days or weeks—before the water boiled off and the fuel began to melt (unless someone sabotaged the plant, draining the water). If people who wanted to prevent an accident gained access to the site, they might well be able to replenish the cooling water in the time available—if fighting in the area did not stop them. Even if the fuel did melt, the steel pressure vessels of the reactors and the concrete containment buildings around the reactors and the spent fuel pools might well prevent a large release of radioactivity.

In Japan, explosions of hydrogen released from reactions between melting fuel and high-pressure steam destroyed the containments. But after Fukushima, Zaporizhzhia's Ukrainian operators installed both hydrogen recombiners, to prevent explosive levels of hydrogen from building up, and filtered vents that allow steam to escape if pressure inside the containment threatened to break it. In short, the biggest dangers to the Zaporizhzhia reactors involve intentional military action aimed at causing a radiation release. Unfortunately, with Russian military forces in control of the site, there's not a lot the rest of the world can easily do to stop such an intentional disaster from happening. The International Atomic Energy Agency (IAEA) has two inspectors on-site, and they can continue to ask that they be given the access needed to look for explosives and to provide additional help to the highly stressed reactor staff at the site. The UN and various individual countries can demand that all parties abide by the principles of nuclear safety in war that IAEA Director General Rafael Grossi laid out in May 2023.

But at the same time, it's important to prepare for the worst—as Ukraine did in carrying out recent exercises to test its response to a nuclear disaster. The United States, other countries, and the IAEA are all helping Ukraine prepare for emergency response and can step up that help. In particular, the World Health Organization and others should work with Ukraine to establish a network of trained mental health professionals prepared to help people cope with their fear and depression should an accident occur—often the biggest effects of such a disaster.

Over the longer term, there's a need to rethink nuclear safety and security in the context of the possibility that nuclear facilities can be exposed to war, mass civil unrest, or governmental collapse. And there's a need for new agreements to reduce the chance that major civilian nuclear facilities under international inspection will again be targets of military assault.

Matthew Bunn is the James R. Schlesinger Professor of the Practice of Energy, National Security, and Foreign Policy at Harvard Kennedy School and the Co-Principal Investigator of the Project on Managing the Atom at Harvard Kennedy School's Belfer Center.

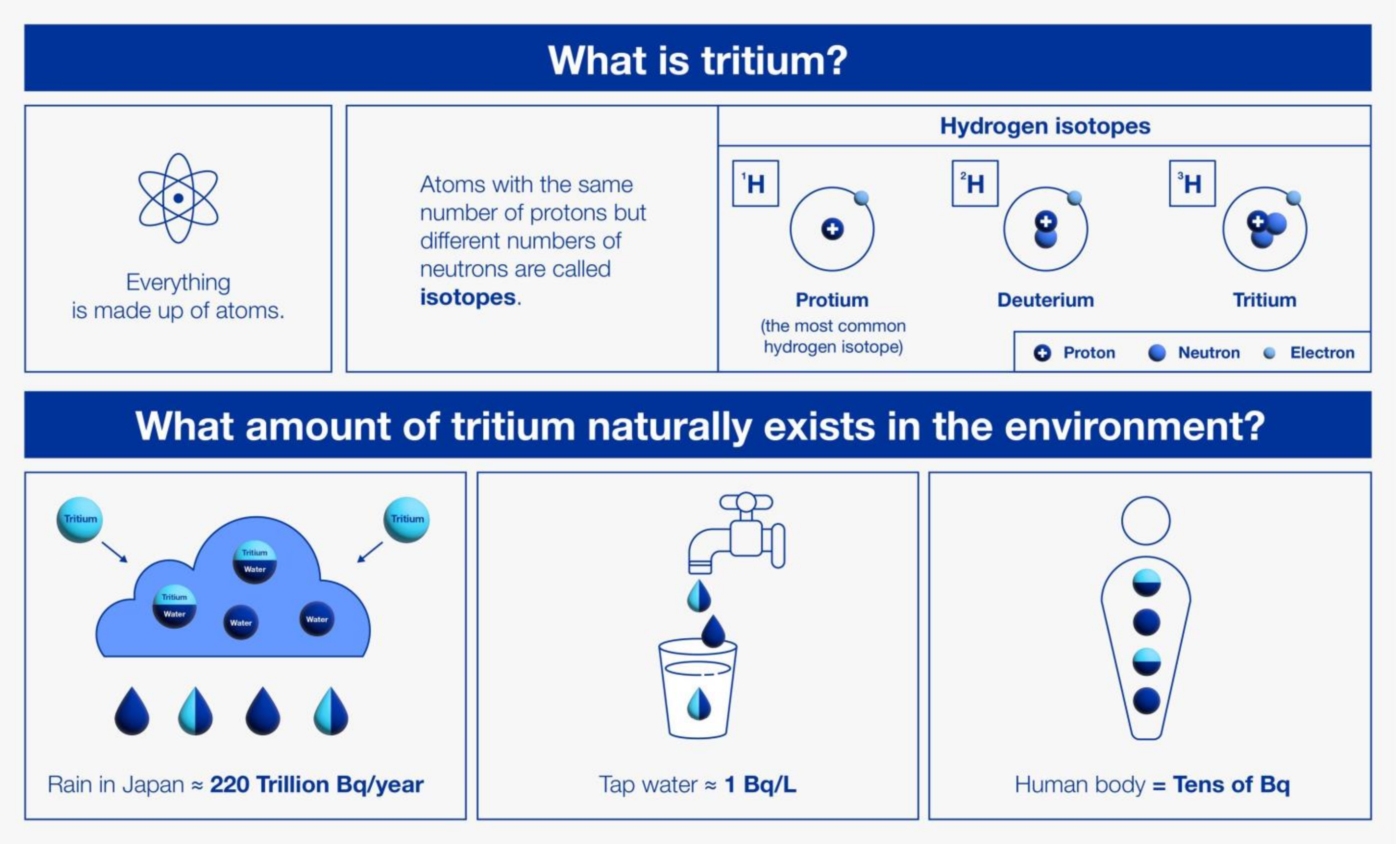
Nuclear agency okays radioactive water release from Fukushima

Source: https://newatlas.com/environment/nuclear-agency-okays-radioactive-water-release-from-fukushima/

July 09 – More than 12 years after the Tōhoku earthquake and tsunami that cost Japan 20,000 lives, the cleanup continues. The International Atomic Energy Commission (IAEA) has formally approved Japan's plan to release treated radioactive water from the damaged Fukushima Daiichi nuclear power station into the sea.

When the Tōhoku disaster struck Japan in 2011, it was the worst earthquake ever to have struck the country and the fourth worst on record. With little to no warning, the resulting tsunami caused an almost unimaginable loss of life and property and the videos of the event are a humbling reminder of nature's power.

One of the victims of the disaster was the Fukushima Daiichi nuclear power plant, which was an obsolete boiling water design of six reactors that was commissioned in 1971. On March 21, 2011, it was battered by 14-m (45-ft) ocean waves that were far beyond its design capacity to withstand. The facility was severely damaged and the backup diesel systems that should have come online to keep the reactors cooled were swamped. Worst of all, the damage to the surrounding area was so great that it was impossible for emergency crews to reach the plant before the reactors went into meltdown and some were severely damaged by a hydrogen gas explosion.


What is tritium?
Everything is made up of atoms.
Atoms with the same number of protons but different numbers of neutrons are called **isotopes**.
Hydrogen isotopes
^{1}H
^{2}H
^{3}H
Protium
(the most common hydrogen isotope)
Deuterium
Tritium
Proton
Neutron
Electron
What amount of tritium naturally exists in the environment?
Tritium
Tritium
Tritium
Water
Tritium
Water
Water
Water
Rain in Japan ≈ **220 Trillion Bq/year**
Tap water ≈ **1 Bq/L**
Human body = **Tens of Bq**

Tritium infographic – IAEA

In the years since, there has been a herculean effort to clean up the facility and to properly decommission it. However, there remains the problem of 1.3 million m^3 (340 million gal) of contaminated water stored on the site in stainless steel tanks.

The water has already been largely decontaminated. Strontium, cesium, and other heavy radioactive elements have been removed by means of chemicals that precipitate or capture the contaminants. What's left was desalinated and passed through the Advanced Liquid Processing System (ALPS), which uses a series of membranes and filters to remove 62 kinds of radioactive particles.

The end result, from a chemical point of view, plain water. The problem is that this isn't the sort of water that comes out of a kitchen tap. It contains a form of heavy or tritiated water where some of the hydrogen atoms are an unstable radioactive hydrogen isotope called tritium whose nucleus is made up of a proton and two neutrons.

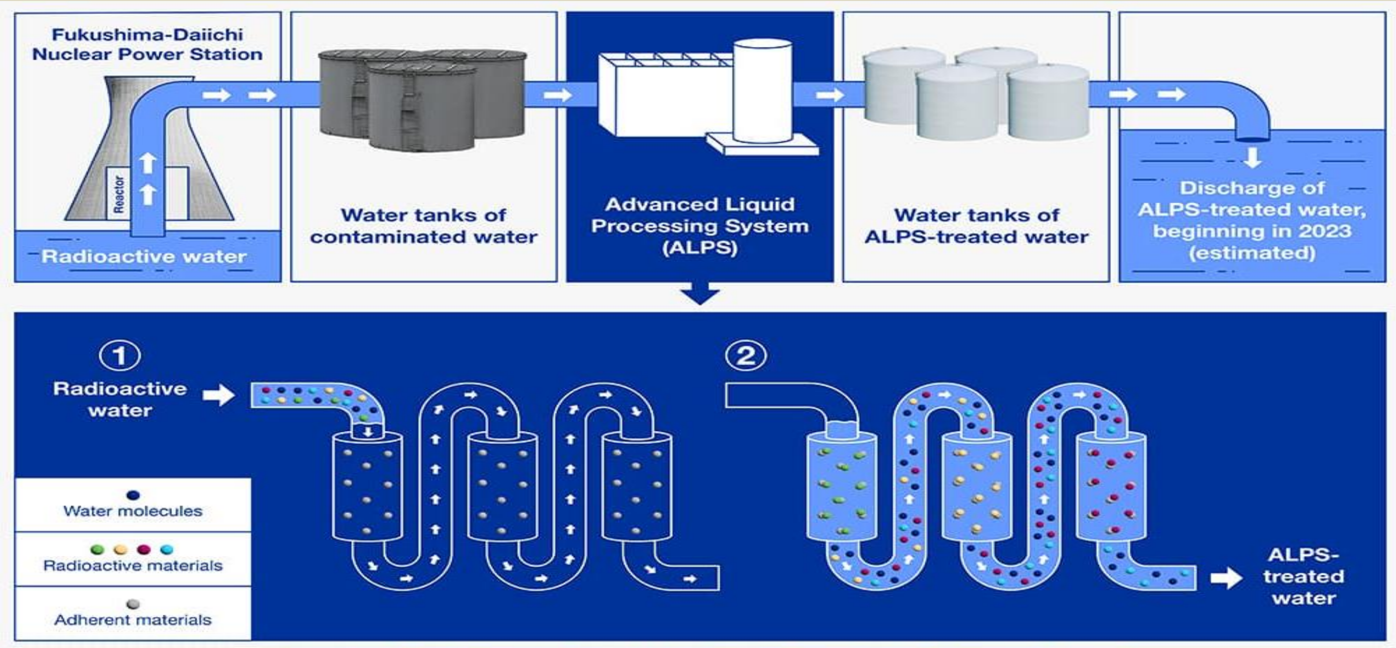
Tritium is naturally occurring, being produced by cosmic rays striking the Earth's atmosphere. It's also created in nuclear reactors as the cooling water is exposed to the radioactive environment. With a half life of 12.32 years, it's quite radioactive, but this only takes the form of beta particles that can't penetrate any depth of living tissue.

It's not dangerous unless it's in very high concentrations, which is annoying because highly concentrated tritiated water can be separated from ordinary water, but this isn't practical in the low concentrations seen at Fukushima.

It may seem irresponsible, but the safest way to dispose of such irradiated water is to release it into the sea. Seawater already contains natural tritium in vastly greater quantities than nuclear power plants could ever hope to produce and it's a standard procedure to discharge treated reactor water into bodies of water to be quickly diluted as part of nuclear operations.

The trick is to make sure that the water is already highly diluted and that the discharge is made in such a gradual way that the tritium can't significantly increase at the point of release and cause local damage. This is the reason for the intense two-year review of the release plan by the IAEA, the Japanese government and Japan's Tokyo Electric Power Company (TEPCO) that operates Fukushima. The review was to make sure the plan met national and international safety standards, including ensuring that the tritium does not concentrate in the food chain.

"The IAEA have taken time and due care and attention in preparing this report, commensurate with the somewhat unique situation," said Prof Robin Grimes, Steele Chair of Energy Materials, Imperial College London. "They have made it clear they will continue to monitor the release. Independent verification is always to be welcomed. However, the concentration of tritium, the remaining radionuclide in the water to be discharged, is very low and well below levels of any environmental concern.


Fukushima-Daiichi Nuclear Power Station
Reactor
Radioactive water
Water tanks of contaminated water
Advanced Liquid Processing System (ALPS)
Water tanks of ALPS-treated water
Discharge of ALPS-treated water, beginning in 2023 (estimated)
1
Radioactive water
Water molecules
Radioactive materials
Adherent materials
2
ALPS-treated water

Source: Japan Ministry of Economy Trade and Industry (METI) and Tokyo Electric Power Company (TEPCO)

ALPS infographic – IAEA

The state of the tritium is important – in this case it is a component of water molecules (tritiated water) but not bound to more complex compounds. There is no established mechanism for tritiated water bioaccumulation so discharge will further dilute these low levels of tritium enormously. It will be interesting to see if any increase in tritium in the discharge area is even detectable over natural tritium generated by cosmic ray processes. Certainly the concentration of tritium will be well below levels of naturally occurring radionuclides although comparing the environmental impact of different radionuclides is quite a challenge."

EDITOR'S COMMENT: OK, there is no doubt that there a lot of water in the ocean but for better or worst avoid ordering sushi when in Japan. ☺

UNCLASSIFIED

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE

Iran's Nuclear Weapons Capability and Terrorism Monitoring Act of 2022

Florida lawmakers want to use radioactive material to pave roads

By Bill Chappell

Source: https://www.npr.org/2023/05/09/1174789570/florida-roads-radioactive-paving-phosphogypsum

Construction workers build along State Road 836 in 2018 in Miami. HB 1191 would compel the Florida Transportation Department to study using phosphogypsum in paving projects.

July 09 – Roads in Florida could soon include **phosphogypsum** — a radioactive waste material from the fertilizer industry — under a bill lawmakers have sent to Gov. Ron DeSantis.

Conservation groups are urging DeSantis to veto the bill, saying phosphogypsum would hurt water quality and put road construction crews at a higher risk of cancer.

The Environmental Protection Agency also has a say in the matter: The agency regulates phosphogypsum, and any plan to use it in roads would require a review, the EPA told NPR. Here's what to know about the law and about phosphogypsum.

What would the law do, specifically?

HB 1191 would compel the Florida Transportation Department to study using phosphogypsum in paving projects, calling for "demonstration projects using phosphogypsum in road construction aggregate material to determine its feasibility as a paving material."

If it's approved, phosphogypsum would join pavement aggregates such as crushed stone, gravel and sand. In recent years, the Federal Highway Administration says, industrial byproducts and reclaimed materials have also been used as aggregates.

The bill sets a deadline of April 1, 2024, giving the transportation agency less than a year to complete its work and make a recommendation. The Republican-dominated Florida Legislature approved the measure by a wide margin.

What is phosphogypsum and why is there so much of it?

In fertilizer, phosphorus is important for plants to grow strong roots and for crops to be productive. Florida has been an important source since the 1800s; today, the EPA notes, "Florida alone accounts for approximately 80 percent of the current capacity, making it the world's largest phosphate producing area."

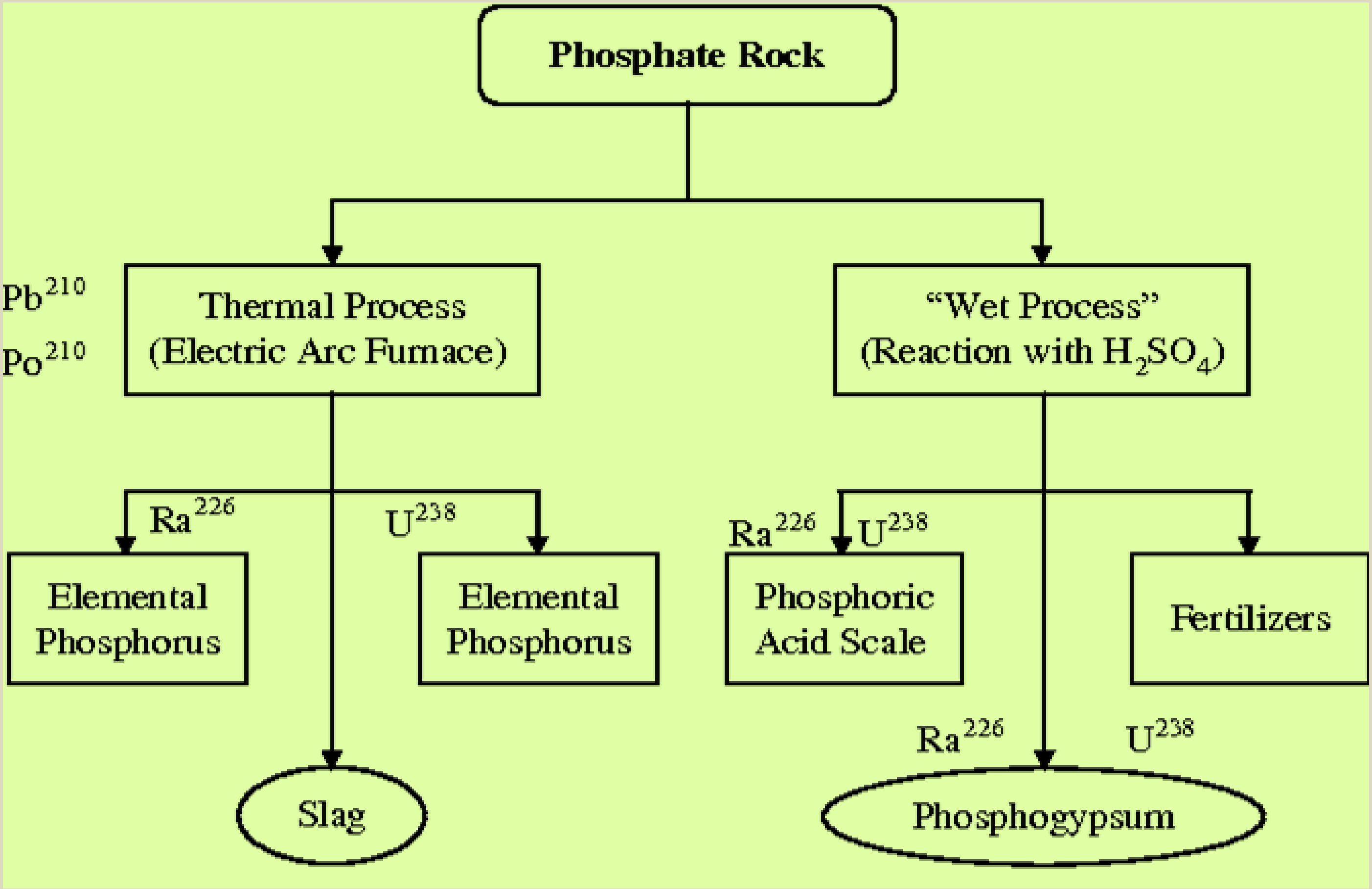
When phosphate rock is dissolved in sulfuric acid to make phosphoric acid for fertilizer and a few other uses, phosphogypsum is what's left over.

The commonly used production process, which dates to the 1840s, is not very efficient. For every ton of phosphoric acid produced, more than 5 tons of phosphogypsum waste is generated.

Florida's prominent role means the state also has massive waste sites called phosphogypsum stacks, or "gypstacks." Such stacks can be very large — spanning up to 800 acres and about 200 feet in height. They've been linked to serious problems over the years, due to sinkholes and other breaches.

Is it dangerous?

"Phosphogypsum contains appreciable quantities of uranium and its decay products, such as radium-226," according to the EPA. And because the fertilizer production process concentrates waste material, "phosphogypsum is more radioactive than the original phosphate rock," the agency notes.



"The radium is of particular concern because it decays to form radon, a cancer-causing, radioactive gas," the EPA adds.

An analysis commissioned by the Fertilizer Institute, a group that represents the fertilizer industry, disagrees, saying that using phosphogypsum in road construction won't produce radioactive doses that are above the EPA's acceptable risks. Such work, it stated, "can be done safely and results in doses that are a small fraction of those arising from natural background radiation."

Last November, researchers in China who reviewed numerous existing studies on recycling phosphogypsum said they were optimistic about its potential use in road construction materials. But they concluded that more studies are needed, noting that "few studies have focused on its durability or analyzed its long-term effects on soil and water resources."

Critics of the new legislation are urging DeSantis to use his veto power.

"Using radioactive phosphogypsum in roads is not a solution to the fertilizer industry's toxic waste problem," the Center for Biological Diversity and more than 30 other groups said in a letter to the governor. "Florida should not be a test subject in the industry's reckless experiment."

The groups say the fertilizer industry has already shown it can't adequately manage more than 1 billion tons of waste currently stored in Florida.

Is Florida's plan legal?

The EPA says "phosphogypsum remains prohibited from use in road construction," as it has been almost continuously for more than 30 years.

Under former President Donald Trump, the EPA briefly rescinded that policy starting in October 2020. But it reinstated the rule in June 2021.

The Florida legislation doesn't address the federal prohibition outright. Its supporting documents note that the EPA allows some uses for research purposes — and it asserts that phosphogypsum is not technically a "solid waste."

When asked to comment on Florida's plan, the EPA told NPR,

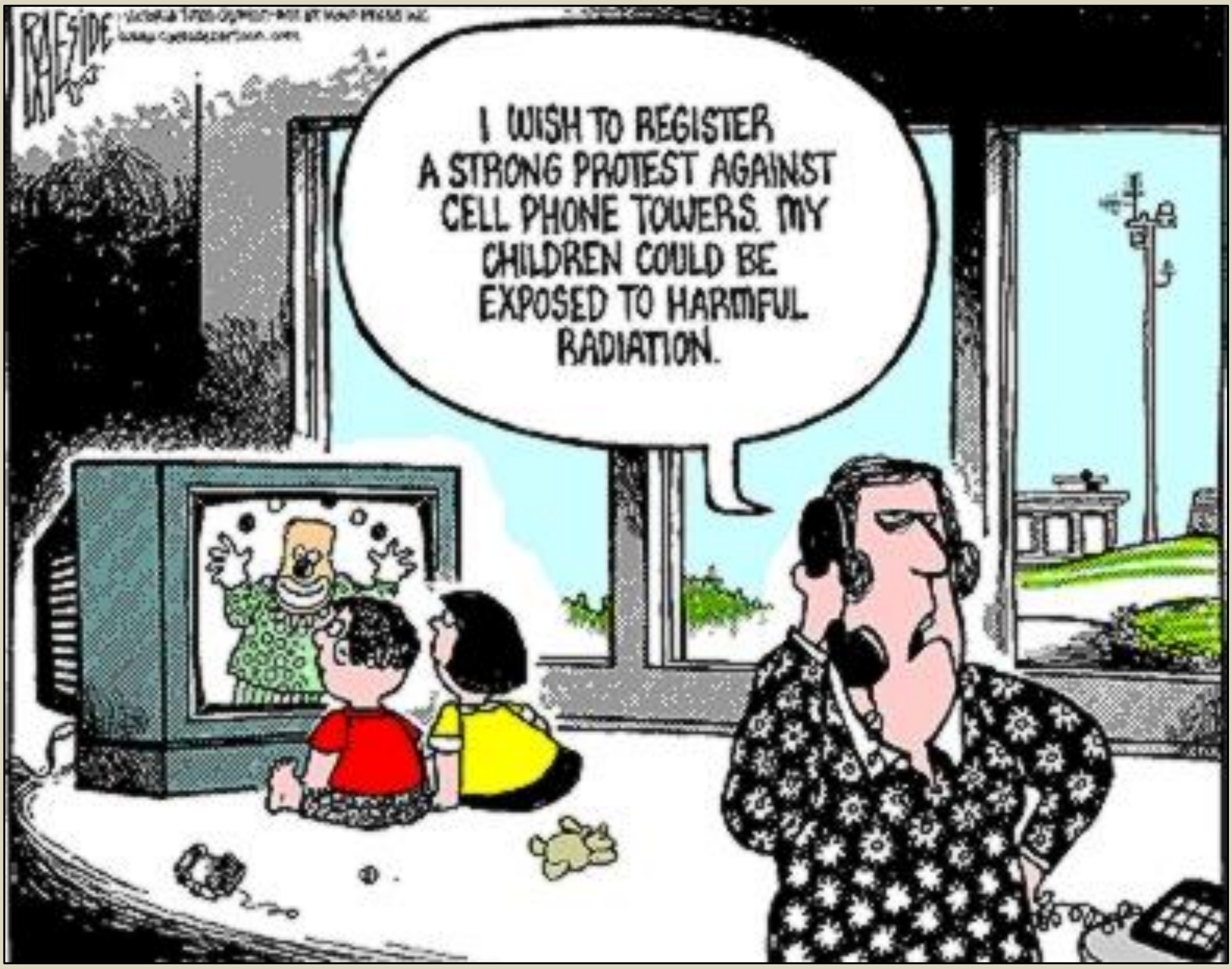
"The legislation passed in Florida would not affect the requirement ... that U.S. EPA review proposed alternative uses of phosphogypsum on an individual, case-by-case basis."

The agency says the state would have to apply for approval — and as with any other proposed project, the EPA would then open a public comment period, release its own technical analysis and seek input about the proposal.

What's next?

DeSantis could sign the phosphogypsum road-test measure into law at any time; if he takes no action, the bill will be enacted automatically.

.


RAESIDE
I WISH TO REGISTER A STRONG PROTEST AGAINST CELL PHONE TOWERS. MY CHILDREN COULD BE EXPOSED TO HARMFUL RADIATION.

International CBRNE Institute

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

The Lasting Effect of Landmines

By Zsofia Baumann

Source: https://nct-cbnw.com/the-lasting-effect-of-landmines/

June 25 – Recent reports on Russia's use of landmines in Ukraine have drawn attention to the lasting effects of explosive remnants of war (ERWs) following the end of a conflict. Over a quarter of Ukraine's territory is currently contaminated with landmines, leaving the area inaccessible for not just agricultural and industrial use, but simply to return to. However, outside of Ukraine there are over 60 countries who face the same problem, with hundreds of thousands of km^2 of territory scattered with these deadly weapons.
Egypt, Libya, Iraq, Syria and Yemen in the Middle East, Croatia, Bosnia and Herzegovina and Cyprus in Europe, Angola, the Central African Republic and the Democratic Republic of Congo in Africa and Afghanistan, Myanmar and Cambodia in Asia – these are just a few countries that are still experiencing the results of years of conflict: mine contamination. It is estimated by the 2022 Landmine Monitor Report, compiled by the Cluster Munition Coalition (CMC) and the International Campaign to Ban Landmines (ICBL), that as of 2022, over 60 countries and territories remain contaminated, with an estimated 110 million landmines in the ground.
Landmines and other ERWs remain a security risk long after conflicts have ended and can cause serious bodily harm or death decades after they have been placed. According to most recent estimates by the 2022 Landmine Monitor Report, in 2021 casualties of mines were identified in 50 countries, killing 2 182 people and injuring 3 355. More than three quarters of these were civilians (4 200), almost half of which were children (1 696).

Scope of the problem

Landmines are not the only 'leftovers' of conflict that can cause serious bodily harm or damage. Along with landmines, other unexploded or abandoned ordnances, as well as improvised explosive devices are scattered in areas where civilians can easily become victims.

Anti-personnel (AP) landmines buried in the ground and uncovered by deminers –Definitions are from the United Nations Mine Action Service (UNMAS) Safety Handbook 2015, ©UNMAS/Thomas Enke

Under **landmines**, most commonly we refer to **anti-personnel (AP) landmines**, which are designed to be detonated by the presence, proximity or contact with a person and are intended to harm or kill people. Most commonly they are detonated by being stepped on or via a tripwire but can also be set off by the passage of time or via control. On the other hand, **anti-vehicle (AV) landmines** are meant to damage or destroy vehicles and therefore require a greater weight or pressure to be set off.

●▶ **Read the full article at the source's URL.**

Zsofia Baumann has a background in international relations and terrorism studies, focusing on radicalization, disengagement from terrorism and foreign terrorist fighters. She is currently the Editor of CBNW Magazine.

50 years since US troops left Vietnam, bombs continue to kill

Source: https://www.aljazeera.com/news/2023/6/26/50-years-after-the-vietnam-war-ended-its-bombs-continue-to-kill

UXO is still being discovered 50 years since US troops left Vietnam [Chris Humphrey/Al Jazeera]

June 26 – Ho Sy Bay, 62, was rummaging around in his garden in central Vietnam when he struck something harder than sand or soil. Cautiously, he brushed aside the surrounding dirt and realised he was staring at an unexploded missile.

Although Sy was unsure if the fuse was still intact, he picked up the bomb and placed it carefully in a thicket on one side of his vegetable patch.

"I found it last Thursday," Sy told Al Jazeera on a visit to his home in Quang Tri province, adding that he informed local officials right away. "Sometimes I find other objects as well. After the war, I started working as a scrap collector and found many types of explosives. Back in 1975, when I was 20, I would find bigger explosives with metal detectors and sell them."

Behind Sy's house lie the shattered ruins of a church where North Vietnamese Army soldiers used to hide during the Vietnam War, making the building a target for successive bombing raids by the United States military, which backed the South Vietnamese government in what was then known as Saigon and is now Ho Chi Minh City.

"Around 1979, I found a body around here," he said, pointing to an area of his garden where he found the remains of a Vietnamese soldier, which was taken away by the authorities.

The US carried out more than a million bombing raids during the 20-year conflict, dropping some 5 million tonnes of ordnance on the Southeast Asian country. About a third of the munitions, including cluster bombs, did not explode on impact.

It has now been more than 50 years since the last US soldier left Vietnam – on March 29, 1973 – but tens of thousands of explosives are still being found each year, often mere inches beneath the soil.

'Reality of war'

In Quang Tri province, which was once divided by the demilitarised zone between North and South Vietnam and remains the most heavily-contaminated province in the country, there have been 3,500 deaths from accidents since the war ended. The last death was in 2022, when a bomb exploded in a farmer's hands after he discovered it in a field and picked it up.

"After seeing so many accidents and doing scrap collecting work for a long time, I stopped," Sy added. Yet despite his experiences, he is not angry: "I feel like everyone else… this is just the reality of war."

The Mines Advisory Group (MAG), a United Kingdom-based NGO that has been working in Vietnam since 1999 and now employs 735 people in the country, came to remove the bomb in Sy's garden after he called a local hotline.

Every day, MAG's staff scour the landscape with metal detectors, searching for unexploded ordnance (UXO) to clear so the land can be made safe and ready for agriculture or development. In 2022, MAG destroyed 14,615 bombs, clearing just more than 10 square kilometres (3.86 sq miles) of land.

MAG staff use a loop detector to search for unexploded ordnance in Trieu Phong District [Chris Humphrey/Al Jazeera]

In the nearby Xuan Vien village, a group of local children aged between eight and 12 were playing near a muddy ditch when they came across an unusual-looking object.

Tran Duy Vinh, the village head, told Al Jazeera the children had finished playing football and thought they might catch some fish instead.

"They found an explosive, picked it up, and passed it around," Vinh said. "They didn't know what it was and started to play with it."

Vinh immediately called the government-run hotline, which allows local authorities to ask organisations like MAG, as well as the Vietnamese military, to clear UXO. "Everyone around here has the number," he said.

Dinh Ngoc Vu, the vice director of the government-run Quang Tri Mine Action Centre (QTMAC), which operates the hotline, said: "I think this work has helped to heal the wounds of the war – from both perspectives."

Between 1993 and 2020, the US invested more than $166m into programmes in Vietnam focusing on war legacy issues such as clearing mines and UXO and providing explosive ordnance risk education.

During an official visit to Vietnam in April, US Secretary of State Antony Blinken said Washington was committed to addressing the legacies of the war.

"Even as we focus on the future…. We're continuing our joint efforts to clear unexploded ordnance – next month, we will complete the survey of the heavily bombed Quang Tri Province," he told reporters.

International NGOs and the Vietnamese military have already cleared UXO from 173 sq km (67 sq miles) of land. QTMAC estimates that it will take 13 more years to clear the province of explosives.

"And we are continuing the important humanitarian work to account for those missing from the war – including by increasing Vietnam's capacity to identify its own missing and dead," he added.

Work that saves lives

By the end of the Vietnam War, there was not a single province that was not contaminated with UXO. Nationwide, there have been more than 100,000 deaths and injuries in the past 50 years, according to Sarah Goring, MAG's Vietnam Country Director.

After finding unexploded bombs, MAG staff either destroy them where they were found or take the ordnance away to a demolition site to be safely destroyed.

Ta Quang Hung, MAG's technical field manager, has worked for the organisation since 1999. Previously, he worked as a farmer in a rural area that was heavily contaminated with UXO.

"I grew up in an area with a heavy presence of unexploded ordnance. I would step out of my house and be faced with them," he told Al Jazeera.

As a child, Hung found explosives and played with them, without knowing what they were. Hung and his friends would throw small explosives at a wall or a target, competing to see who could hit it first. Thankfully, adults caught them and halted their perilous games. But not everyone was so lucky.

He recalls another memory, from the mid-1970s, when two of his relatives, women who had married into his family, were working in the fields together.

"We were evacuated during the war, but after the liberation, we went back to work in our fields right away," he said. "They were together when they found the explosive. It might have been a 40mm grenade or cluster munitions… Both of them died."

To mitigate the risk of further tragedies, MAG runs advertisements on social media, inviting villagers to join educational sessions in which participants learn about the risks of UXO, play games and chant the hotline number.

Although these lethal artefacts of the Vietnam War still claim lives, the organisations working to clear UXO from the land offer a chance for Vietnamese people not only to take action, but also to come to terms with the past.

Thai Van Ninh, who has worked for MAG since 2015, lost his 12-year-old brother to an unexploded bomb when he was just six years old. "When I first started, I was scared to work with bombs, having lost my brother to one," he said. "But after the training… I realised my work saves lives."

US Decides to Send 'Cluster Bombs' to Ukraine—With Conditions

Source: https://www.theepochtimes.com/us-will-send-cluster-bombs-to-ukraine-with-conditions_5381389.html

July 07 – The United States will send so-called "cluster munitions" to Ukraine in its ongoing fight to drive Russian forces out of the country. Speaking from the White House on July 7, national security adviser Jake Sullivan said President Joe Biden deferred the decision long as possible.

After consulting international leaders and reviewing the situation on the ground, he decided to sign the order to provide Ukrainian forces with the weapons they requested.

"We continue to stand with the people of Ukraine as they defend their sovereignty, their freedom, and their democracy," he said.

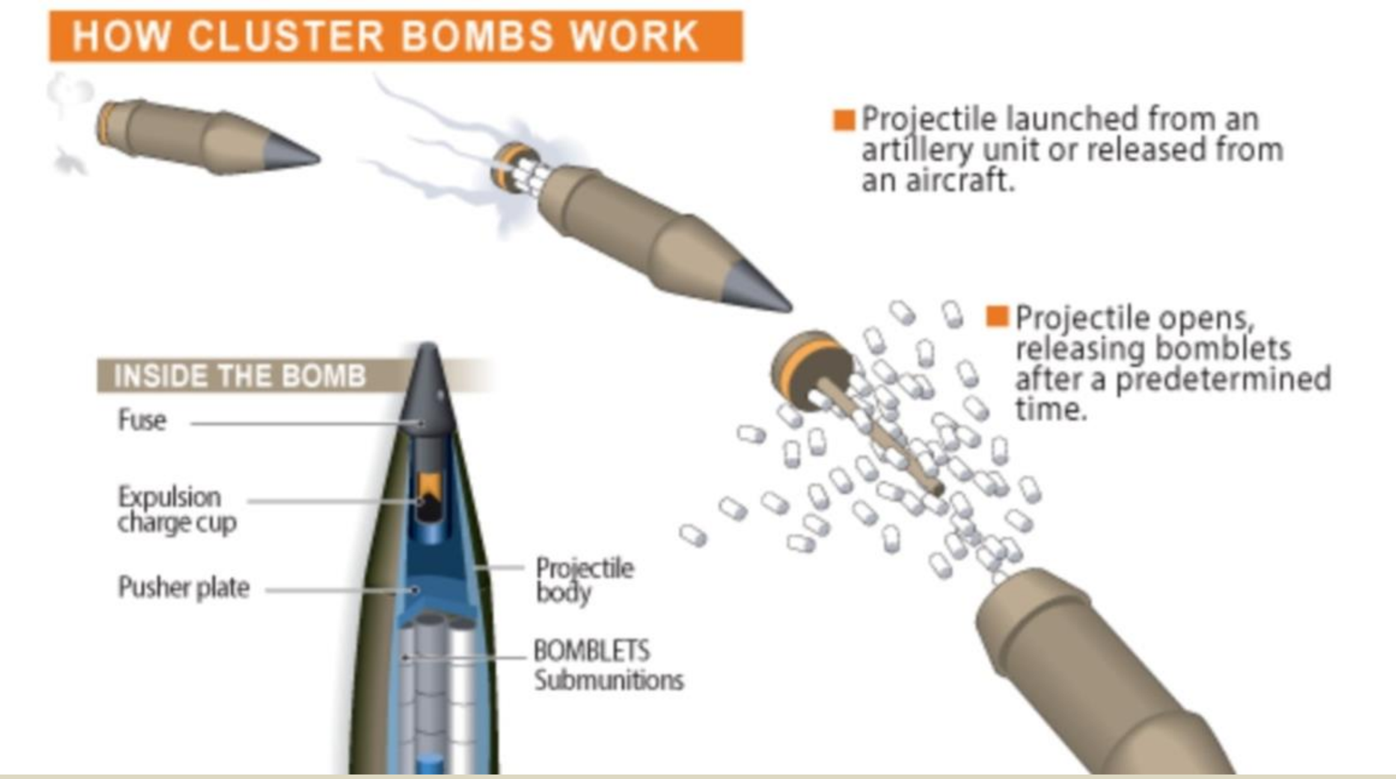
Soldiers with the French contingent of the International Security Assistance Force (ISAF) unload Russian made cluster bombs from a container found about 18 miles north of Kabul, Afghanistan, on Oct. 9, 2002. (Lynne Sladky/AP Photo)

After they are fired, cluster munitions open in midair and release small bombs (bomblets) over a wide area to strike several targets simultaneously. They can be delivered by planes, artillery, and missiles.

Human Rights Watch, and other humanitarian organizations, oppose the devices because some of the bomblets don't explode when they are deployed.

This unexploded ordinance presents a hazard to civilians, especially children. Mr. Sullivan said it's estimated that Russian forces have dispersed "tens of millions" of the bomblets in their attempt to take over Ukraine. He said that the "dud rate," the number of bomblets that fail to explode, is between 30 and 40 percent. Considering the danger already present from Russian bomblets, The decision was made that the Ukrainians have the right to defend their land with whatever weapons they deem necessary, Mr. Sullivan said.

"That doesn't make it an easy decision," He said.


HOW CLUSTER BOMBS WORK
Projectile launched from an artillery unit or released from an aircraft.
Projectile opens, releasing bomblets after a predetermined time.
INSIDE THE BOMB
Fuse
Expulsion charge cup
Pusher plate
Projectile body
BOMBLETS Submunitions

Colin Kahl, Under Secretary of Defense for Policy, said the U.S. munitions have a dud rate of 2.5 percent.

Mr. Kahl said the United States would send standard 105-millimeter artillery shells and Dual-Purpose Improved Conventional Munitions (DPICM). DPICM are cluster munitions fired from artillery.

Proponents of banning cluster munitions say that countless civilians, including children, have been injured and killed by unexploded bomblets. Mr. Sullivan said the danger to Ukrainian civilians will grow if nothing is done.

More than 100 countries, including several NATO members, are part of the Convention on Cluster Munitions (CCM).

These countries signed an agreement in Oslo, Norway, on Dec. 3, 2008.

According to the CCM website, "The Convention on Cluster Munitions is an international treaty of more than 100 states. The convention prohibits all use, production, transfer, and stockpiling of cluster munitions."

The United States and Russia are not party to the CCM.

Mr. Sullivan said that several countries expressed support for the plan.

He claimed that even though CCM members, like Germany, have expressed dismay at the situation, they have not explicitly condemned the transfer. He said it's clear that Russia is at fault and that the Ukrainians are simply trying to defend themselves.

"There is also a massive risk of civilian harm if Russian troops and tanks roll over Ukrainian positions and take more territory," he said. Mr. Kahl said the munitions to be sent are newer and more reliable than those used in previous conflicts.

He said the failure rate for the new munitions is down to 2.5 percent.

He added that Ukrainians would have to deal with the cluster munitions even if the United States did nothing.

Cluster Munitions Already an Issue

"This is an issue the Ukrainians will have to grapple with regardless," Mr. Kahl said.

The Ukrainians have agreed to limit the use of the munitions to sparsely populated areas to record where they are used so unexploded bomblets can be retrieved after the war.

United States law prohibits transferring cluster munitions with a dud rate greater than one percent. However, Kahl said the president has the legal authority to waive that requirement.

Mr. Biden decided to green-light the deal after talking with Congressional leaders and officials from other countries.

"We did not make a unilateral decision; we are not breaking the law," Mr. Kahl said.

Ultimately, Mr. Sullivan said the decision will enable the Ukrainians to continue their war effort with the ordinance they need.

He said that both sides have relied heavily on artillery.

So, the United States and others who supply Ukraine must ramp up their production of artillery shells.

Sending the DPICM will "build a bridge" between the Ukrainian's current and future needs.

Mr. Sullivan stopped short of saying there was a shortage of artillery shells.

"We need to build a bridge from where we are today to when we have enough monthly production," he said.

According to Mr. Kahl, this move will do more to protect Ukrainians in the long run.

"The worst thing for civilians in Ukraine is for Russia to win the war," Mr. Kahl said.

EDITOR'S COMMENT: Bomblets filled with hypocrisy in a proxy war! Since when the West is caring about collateral losses and children?

'It's simple and cheap': the volunteers making Ukraine's Trembita bomb

Known as the 'people's missile', the bomb costs about £2,300 to build and can be transported in a car boot

Source: https://www.theguardian.com/world/2023/jul/09/its-simple-and-cheap-the-volunteers-making-ukraine-trembita-bomb

July 09 – At an industrial estate near Kyiv, a group of engineers stand next to a tube. The metal device is part of a homemade rocket. After twiddling with an ignition cable, the engine sparks into flame. There is a terrifying, ear-splitting roar. Two dogs that guard the compound slink away and hide; swallows fly off. The centre of the pipe glows red. After a minute, the awful din stops.

Welcome to the Trembita, also known as the "people's missile". The prototype is Ukraine's 21st-century answer to the V-1 flying bomb, or doodlebug, the long-range missile used by Nazi Germany during the second world war against targets in south-east England.

The Ukrainian version has a range of 140km (87 miles). It can carry 25kgs of explosives, and it runs on diesel or petrol that you can buy in the local garage.

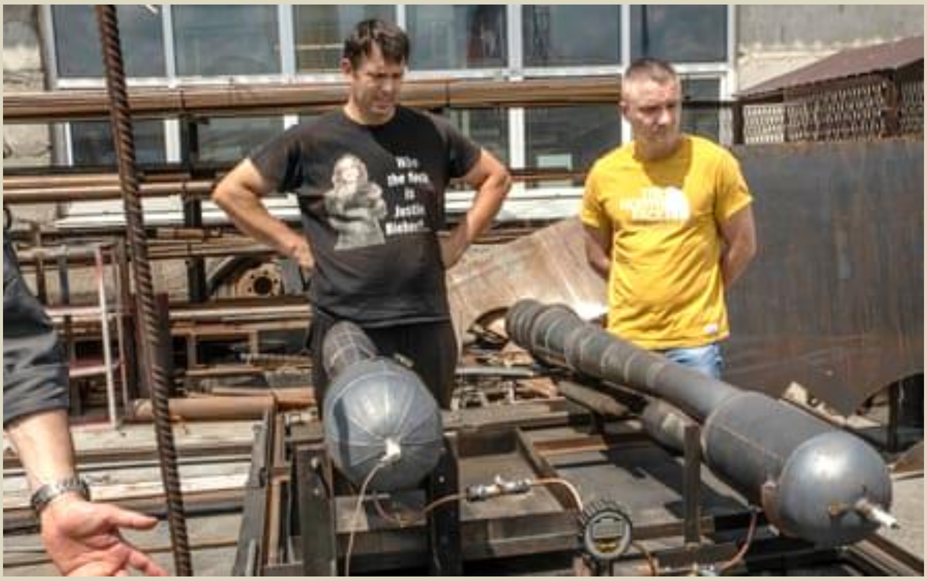
Best of all for Ukraine's armed forces, the Trembita is cheap. It costs about $3,000 (£2,300) to build the rocket and another $7,000 to equip it with a modern navigation system. The price is a fraction of the cost of Russia's hypersonic and cruise missiles, Kinzhal and Kalibr, estimated to cost $1m to $2m each. Moscow has used dozens of them in regular attacks on Ukrainian cities, including Kyiv.

The project's chief engineer, Akym Kleymenov, says his low-tech bomb can be transported in the boot of a car. It is launched by pneumatic catapult or with a solid-fuel booster. Trembita uses a jet pulse engine and carries 30l of fuel. This is enough to send the rocket on a half-hour journey into enemy territory, though not quite far enough to hit the bridge connecting Russia with occupied Crimea.

Akym Kleymenov works on a mortar system at the workshop. Photograph: Alessio Mamo/The Guardian

According to Kleymenov, the purpose of Ukraine's first native cruise missile is to overwhelm Russia's defences. "It's simple, cheap, and good at exhausting enemy air defence systems," he explains, standing in a garage full of welding equipment, metal cylinders and an old car missing a wheel. Asked if he is a Ukrainian Q, the gadget master from the James Bond films, he replies: "Probably, yes."

Further tests will be carried out soon at a military training base. The plan is to launch the Trembitas in a battery, with 20 or 30 fired simultaneously. Not all will carry explosives. Targets will include ammunition dumps, and command and control centres. The rockets have a "negative psycho-emotional" effect on Russian soldiers, exposing them to a deafening 100db noise, its designer says.



Engineers Vitaliy Korniychuk, left, and Akim Kleymenev get ready to test prototype engines. Photograph: Alessio Mamo/The Guardian

The project's organiser, Viktor Romaniuk, is a former member of Ukraine's parliament, the Rada. He started working as a military volunteer in 2014, when Russian annexed Crimea and began a covert war in the eastern Donbas region. Romaniuk is appealing for donations. He wants to crowdfund production of up to 1,000 limited-range cruise missiles a month. This will cost $350,000 to $600,000, he estimates.

Romaniuk says the missile is named after a long wooden alpine horn played by Ukrainian shepherds in the western Carpathian highlands. His research and development team consists of eight people, working full-time, he says. They have additionally constructed drones and a new type of mortar with a highly accurate targeting system. It can be fired more speedily than a regular mortar and then packed away.

Volodymyr Zelenskiy has repeatedly asked western partners to supply Ukraine with long-range missiles. In summer 2022, the Biden administration delivered high-precision Himars rocket launchers. These have a range of 70-80km and were heavily employed by Kyiv in its successful counteroffensives last autumn in the Kherson and Kharkiv regions. Russia responded by moving its logistics depots away from the line of contact. In May, the UK sent Storm Shadow cruise missiles to Ukraine, infuriating Moscow. They have a range of "in excess of 250km", according to its manufacturer. Ukraine's armed forces have used Storm Shadows to hit Russian logistics centres in occupied territory that was previously unreachable, including the eastern city of Luhansk, close to the Russian border, and the port of Berdiansk. The White House has so far refused to give Kyiv ATACMS artillery, which can be deployed in Himars systems and have a 300km range. Last week, the Wall Street Journal reported that Washington was on the brink of agreeing to hand over ATACMS, as part of a new package of security assistance. The delivery – if it happens – comes more than 16 months after Vladimir Putin embarked on a full-scale invasion, and as Ukraine's latest counteroffensive makes slow progress. In the meantime, Trembita's developers have set up their own mini- production line. In one corner of the workshop are faulty Ukrainian Grad missiles, stacked up next to Russian Grads captured on the battlefield. These are used as a source of valuable missile fuel accelerant. Nearby is a rusting machine gun. Asked if this makeshift production facility is safe, engineer Serhii Biriukov replies: "For us, yes. For the Russians, no." Yuriy Sak, an adviser to Ukraine's defence ministry, says the Trembita is one of several interesting grassroots projects being carried out by volunteer groups, in parallel to government enterprises. "We can't rely forever on our western partners for military assistance and supplies. This is an example of Ukraine thinking strategically and implementing ideas that build up our defence industrial base," he says. Will Trembita work? "Fingers crossed, yes," he replies.

Sak acknowledges the war may go on for some time. He says he is confident Ukraine will win in the end because it encourages and welcomes individual initiatives and bottom-up technical creativity. Ukrainian society is networked and horizontal, in contrast to the feudal and repressive system that exists in totalitarian Russia, where everyone defers to the boss, out of cowardice and fear, he says. Back at the workshop, the engineers are preparing for another ear-splitting test. "The dogs start barking whenever Russia attacks us with Iranian drones," Biriukov says. "Our weapon is more powerful. When we start up the Trembita, they always run away."

EOD: A History of Explosive Ordnance Disposal From World War II to Today

By Matt Fratus

Source: https://coffeeordie.com/eod

Group photo of US Marine Corps and Navy service members as their last detonation explodes at the conclusion of advanced joint explosive demolition training at Arta Range Complex, Djibouti, Dec. 30, 2013. US Air Force photo by Senior Airman Tabatha Zarrella

July 06 – On May 21, 2014, an assault force made up of soldiers from the US Army's 82nd Airborne Division and members of the Afghan Border Police embarked on a clearing mission in a mountainous area of Kandahar Province.
Their objective was an insurgent bomb-making factory hidden inside a cave. The Afghan police officers, descending the mountain ahead of their American comrades, reached the cave first and found it occupied by enemy fighters. A gun battle erupted.
The Americans called for close-air support before advancing into the fray. Technical Sgt. Kristopher Parker, an Air Force team leader and bomb technician assigned to the 466th Explosive Ordnance Disposal Flight, destroyed four bomb caches along the route leading to the mouth of the cave. Then his EOD team came under heavy enemy fire.

Retired US Air Force Master Sgt. Kristopher Parker, right, was presented the Silver Star by Gen. Robin Rand, commander of Air Force Global Strike Command March 17, 2017, at Dyess Air Force Base, Texas. US Air Force photo by Airman 1st Class Emily Copeland.

The fighting intensified. Hours into the mission, another round of airstrikes was called in before the assault force made its third attempt to penetrate the enemy stronghold. Parker and his EOD team were nearing the cave's entrance when an Army officer they were with was struck by gunfire. A barrage of rocket-propelled grenades and a hand-thrown improvised explosive device (IED) followed, exploding within 3 meters of their position.
The blast threw Parker and his comrades to the ground and left them dazed with severe concussions. Yet Parker persevered, using his M4 rifle to lay down suppressive fire and keep the insurgents at bay. His radio lost, another soldier called and submitted the 9-line medevac request for the wounded officer while Parker helped clear the landing zone of IEDs.
Finally, after more than 20 hours of sustained combat, Parker's team withdrew from the objective. All of them survived. As a result of his actions that day, Parker would later be awarded a Silver Star.

The Birth of EOD

Although armies have used explosives for centuries, dedicated bomb disposal specialists didn't exist until World War II.
On Sept. 7, 1940, Nazi Germany conducted a massive bombing raid on London, dropping approximately 337 tons of ordnance in a single day. The bombs that detonated killed 448 civilians.

Disposal of a British 4,000-pound blockbuster bomb dropped by the RAF during World War II. Found in the Rhine near Koblenz on Dec. 4, 2011. Wikimedia Commons photo.

After the dust settled, thousands of live bombs were found scattered across London. The vast amount of unexploded ordnance (UXB) posed a significant threat to the city's residents. To deal with the problem, the British military created its first mine and bomb disposal units.

Boilerman First Class Paul C. MC. Craw, left, and Mine man Third Class Ralph E. Loux examine a Viet Cong mine that was disarmed by a member of the six-man bomb squad assigned to the US Naval support activity, Saigon, Republic of Vietnam. Photo courtesy of the US Naval History & Heritage Command.

The first generation of British bomb techs performed their duties without protective suits. Much of the Nazi ordnance they had to deal with were rigged with delayed time fuses, so rather than explode upon impact with the ground, the bombs would often detonate while being dismantled. According to the National Explosive Ordnance Disposal Association, approximately 389 bomb disposal technicians lost their lives in the war.

In 1942, the US Navy and US Army developed their own EOD training pipeline. The first instructors were British. Their American pupils then became the instructors who taught the teams that were eventually deployed overseas. By the war's end, Allied EOD techs disposed of 45,441 unexploded bombs, 6,983 anti-aircraft shells, and more than 300,000 mines.

Is EOD Considered Special Operations?

Every branch of the US military — yes, even the Space Force — has dedicated EOD teams. However, only Army, Navy, and Marine Corps bomb techs are considered special operations.

The Army currently has two teams directly supporting special mission units. They are the 21st Ordnance Company (EOD WMD) and the 28th EOD Company (Airborne). Both were established with the help of Dennis Wolfe, one of the two original EOD techs of the Army's elite Delta Force, who continued to work with SOCOM as a civilian contractor after he retired in 1987, at the rank of sergeant major.

The 21st EOD WMD was established in 1998 in response to the growing threat of improvised nuclear and radiological dispersal devices. A little more than a decade later, the 28th EOD Company was created to support the Green Berets and the 75th Ranger Regiment. Both EOD units fall under the 20th Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Command.

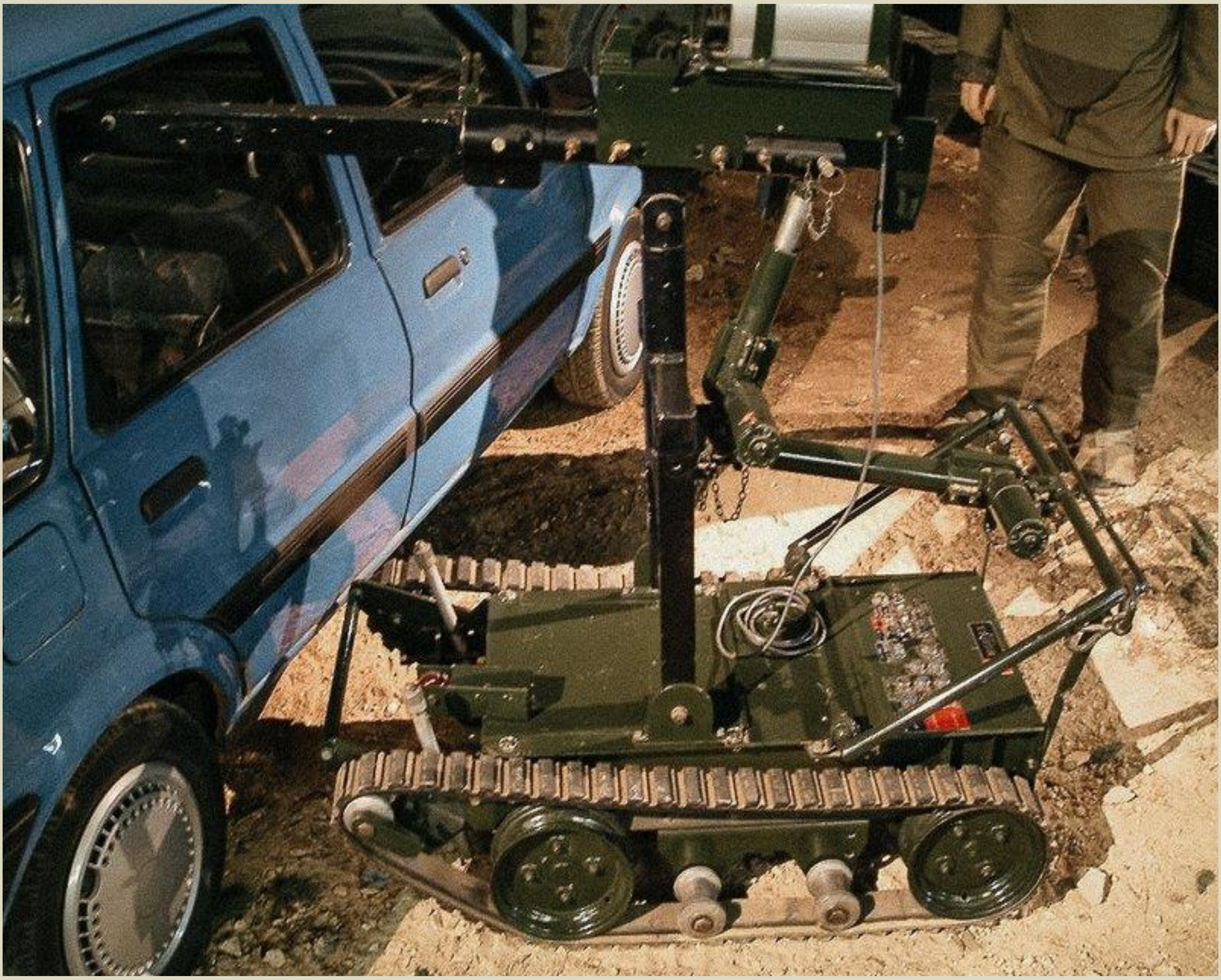
Chief Explosive Ordnance Disposal Technician Evan Bruce, assigned to Explosive Ordnance Disposal Training and Evaluation Unit (EODTEU) 1, jumps from a KC-130 aircraft during the parachute phase of the Maritime Insertion Course run by EODTEU-1 in San Diego, July 29, 2021. US Navy photo by Petty Officer 2nd Class Jason Isaacs.

The Navy's EOD technicians belong to the Naval Special Warfare/Naval Special Operations. About 2,500 sailors within Navy EOD are assigned to either EOD Group One, EOD Group Two, or Expeditionary Exploitation Unit One. Their mission sets include combat operations alongside SEALs and Army Special Forces, underwater mine clearance in support of the fleet, and even the disposal of weapons of mass destruction.

Navy EOD technicians can also try out for the Navy's special missions unit, known as the Naval Special Warfare Development Group, or DEVGRU. If selected, they are assigned to a squadron to support the unit's counterterrorism operations.

In the Marine Corps, individuals must complete the 10-week Marine Special Operations Forces Explosive Ordnance Disposal Level 1 Course to become Fleet Marine Force Explosive Ordnance Disposal Technicians. Qualified Marine EOD techs are eligible to support either the US Special Operations Command (SOCOM) or the Marine Forces Special Operations Command (MARSOC).

Robots and Bomb Suits



The Wheelbarrow remotely controlled bomb disposal tool developed during the Troubles conflict in Northern Ireland in the 1970s. Wikimedia Commons photo.

EOD technicians use various tools and equipment to safely neutralize explosive hazards in the field. The most utilized include bomb suits and remote-controlled robots, a technology first developed by the British Royal Army Ordnance Corps at the height of the Troubles in Northern Ireland.

In 1972, British ordnance disposal teams used the so-called "Wheelbarrow" robot to safely disarm car bombs planted by the Irish Republican Army. The four-wheeled, electrically driven robot featured a camera, a scissors clamp, and a "pigstick" that fired a stream of water to fry the bomb's circuitry. According to *The Times,* the Wheelbarrow was deployed more than 400 times in Northern Ireland and saved many lives. British EOD techs also wore primitive bomb suits for added protection.

Bomb disposal technologies underwent their most significant advancements in the aftermath of the Sept. 11 terror attacks. The proliferation of IEDs in Iraq, Afghanistan, and other War on Terror combat zones required the British and Americans to develop better protective suits and bomb detection tools.

The bomb suits of today are bulky and cumbersome, typically weighing about 85 pounds. The MED-Eng EOD 10 Bomb Suit is the most widely used version in the world, worn by bomb techs from more than 60 countries. The suit provides full body protection, complete with a helmet and blast-proof footwear.

Additionally, to address the threat of heat stress that has long plagued EOD techs, the MED-Eng EOD 10 Bomb Suit features an enhanced ventilation system. The suit is also equipped with an integrated voice command system, allowing for hands-free communication.

An EOD technician wearing a protective bomb suit inspects an explosive device. Wikimedia Commons photo.

Over the past 20 or so years, US Air Force bomb technicians alone have conducted a staggering 19,000 missions in Afghanistan and another 36,000 in Iraq. Between 2001 and 2013, 20 EOD airmen were killed in the line of duty and upwards of 115 more were wounded. Tragic as those numbers are, without the recent improvements in ordnance disposal technology, it is very likely they would be much higher.

EOD Captain Breaks World Record for 1-Mile Bomb Suit Run

Direct threat-N. Patrushev to USA: If Yellowstone wakes up you will have an unprecedented disaster

Source: https://hellas.postsen.com/world/426440/Direct-threat-NPatrushev-to-USA-If-Yellowstone-wakes-up-you-will-have-an-unprecedented-disaster.html

July 15 – First, Russian Vice President N. Medvedev threatened to attack European nuclear facilities. Now Patrushev suddenly remembered the United States' most vulnerable point

Fire and fury is in Russia with US-NATO plans in Europe and Ukraine.

"If Yellowstone wakes up, it will be an 'unprecedented disaster" said Nikolai Patrushev, secretary of the Russian Security Council, challenging the US with a direct threat to anything that takes place in Ukraine.

First, Russian Vice President N. Medvedev threatened to attack European nuclear facilities. Now Patrushev suddenly remembered the United States' most vulnerable point.

But why all this and why now?

The information coming from many sources and media shows that NATO is preparing for much more daring in Ukraine than everything it has done there since February 2022.

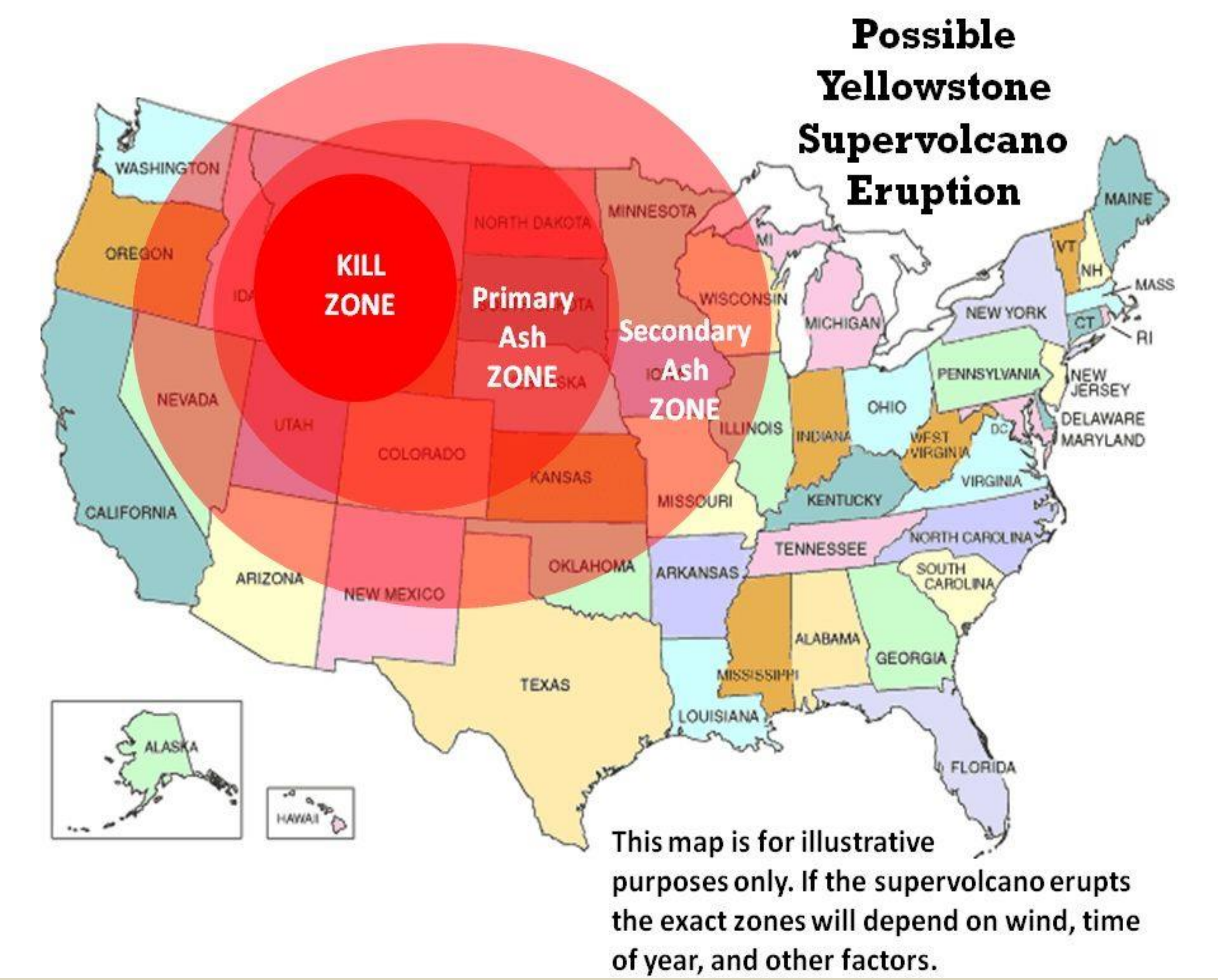
The creation of an army of 300,000 men under American command, the transfer of forces to Baltic Romania, Bulgaria, and the plan to deliver huge equipment to Kiev, is an aspect with many ramifications.

One of them, which we are likely to see in the near future, concerns the sending of ground forces in the form of "volunteers" in an even more massive form, while the delivery of F-16 aircraft and ATACMS and SCALP missiles has irritated Russia to an incredible extent degree. It is precisely for such a war that the Pentagon is preparing, which is why troops are being transferred from Western Europe, which, with the expansion of NATO, was no longer a hypothetical theater of operations on the territory of Eastern Europe, in which the events of an imminent war are unfolding .

The main reason for concern for the Kremlin is that Russian cities will be endangered and hundreds maybe even thousands of civilians will die (while they themselves are bombing Ukrainian cities).

In this context, Moscow is exerting psychological pressure on the USA, that if they make the above moves, then Moscow's reaction will be nuclear-type.

We remind you that the well-known Russian expert Yuriy Tavrovsky sees the relationship between Russia and China as a strategic partnership, and Xi Jinping's visit to Moscow made it possible to call this relationship “combat coordination”. What is well-documented about the war in Ukraine between the Russians, Ukrainians and NATO, and the Moscow-Beijing relationship, is that the Chinese are scrambling to equip the Armed Forces with the latest in modern arsenals, while learning lessons from the fighting. on Ukrainian territory. This scenario is really scary, and we don’t know how far the Russians will go with the US.



Yellowstone as a target for Russian nuclear weapons

It is expected that between 50 and 80 million people will die in the first hours after the explosion. Agriculture will be destroyed and air traffic will be disrupted by the ash, preventing planes from flying. Yellowstone is the most dangerous and unpredictable phenomenon on Earth, beyond human control.

EDITOR’S COMMENT: In love and war everything is permitted and the unexpected is always happening!

Does Russia Have Nuclear Landmines?

By Hans Kristensen

Source: https://fas.org/publication/does-russia-have-nuclear-landmines/

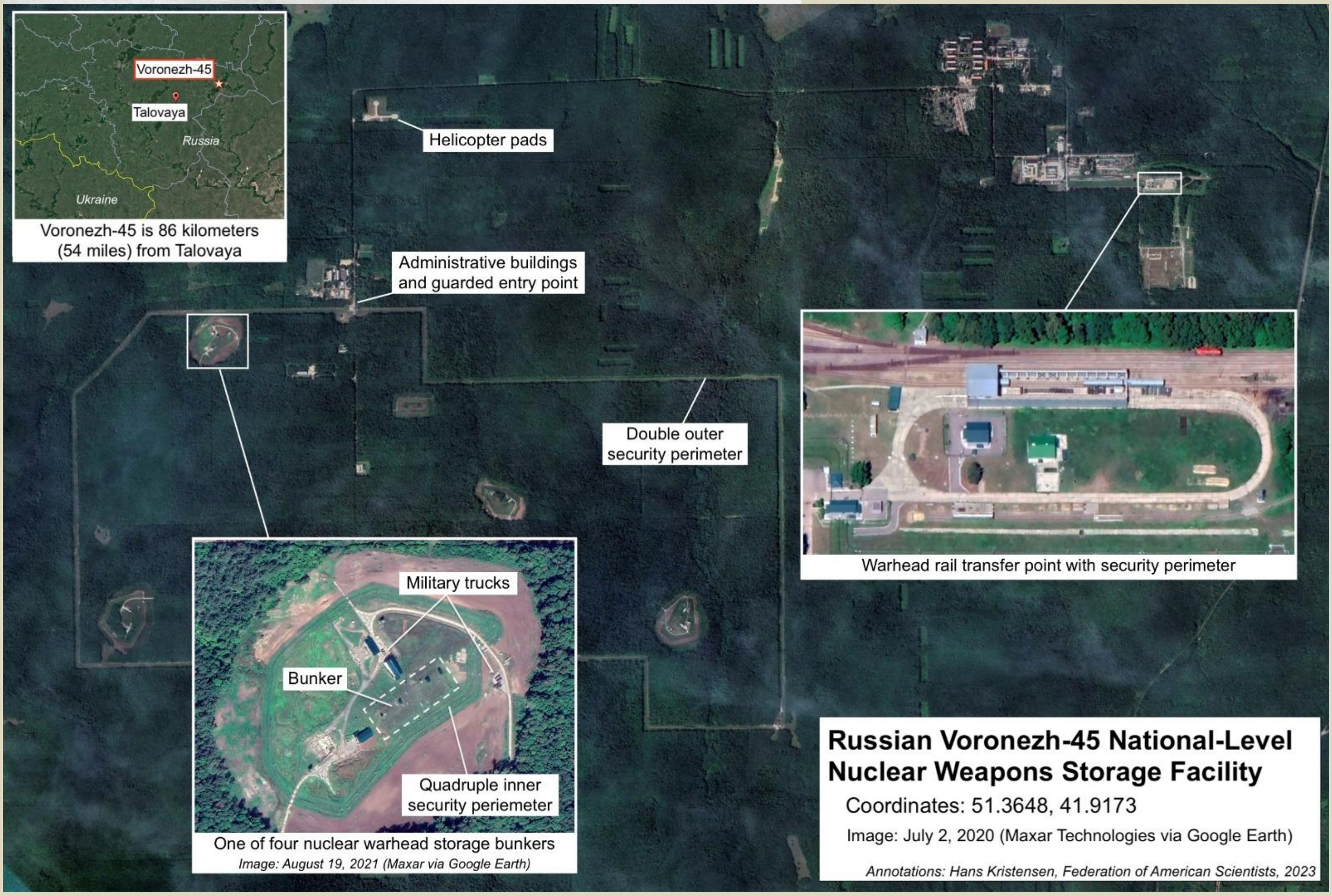
July 17 – Last week, Reuters published a report that said the Wagner group rebellion that sent armed forces hundreds of miles across Russia got near a nuclear weapons storage site: Voronezh-45.

Kyrylo Budanov, the head of Ukraine’s military intelligence, reportedly said that the rebels reached the nuclear base and that their intention was to acquire small Soviet-era nuclear devices in order to “raise the stakes” in their mutiny.

Photo of Russian nuclear "backpacks" or landmines are hard to come by. For illustrative purposes, this is an image of a U.S. Special Atomic Demolition Munition (SADM) in its bag (since retired). The U.S. military possessed nuclear demolition weapons until the 1980s.

A White House spokesperson said he could not corroborate the report and added that the United States "had no indication at any point that nuclear weapons or materials were at risk" during the Wagner event.

To help improve transparency on this issue, below we review what U.S. and NATO sources have stated recently about Russian nuclear landmines and non-strategic nuclear forces in general (for a more detailed overview of Russian nuclear forces, see our latest Nuclear Notebook).


Voronezh-45
Talovaya
Russia
Ukraine
Voronezh-45 is 86 kilometers (54 miles) from Talovaya
Helicopter pads
Administrative buildings and guarded entry point
Double outer security perimeter
Warhead rail transfer point with security perimeter
Military trucks
Bunker
Quadruple inner security periemeter
One of four nuclear warhead storage bunkers
Image: August 19, 2021 (Maxar via Google Earth)
Russian Voronezh-45 National-Level Nuclear Weapons Storage Facility
Coordinates: 51.3648, 41.9173
Image: July 2, 2020 (Maxar Technologies via Google Earth)
Annotations: Hans Kristensen, Federation of American Scientists, 2023

Wagner rebels approached a Russian nuclear weapons storage site near Voronezh to get nuclear "backpacks," Ukraine's military intelligence chief claimed. The White House said it could not corroborate the claim.

Western Statements About Russian Nuclear Landmines

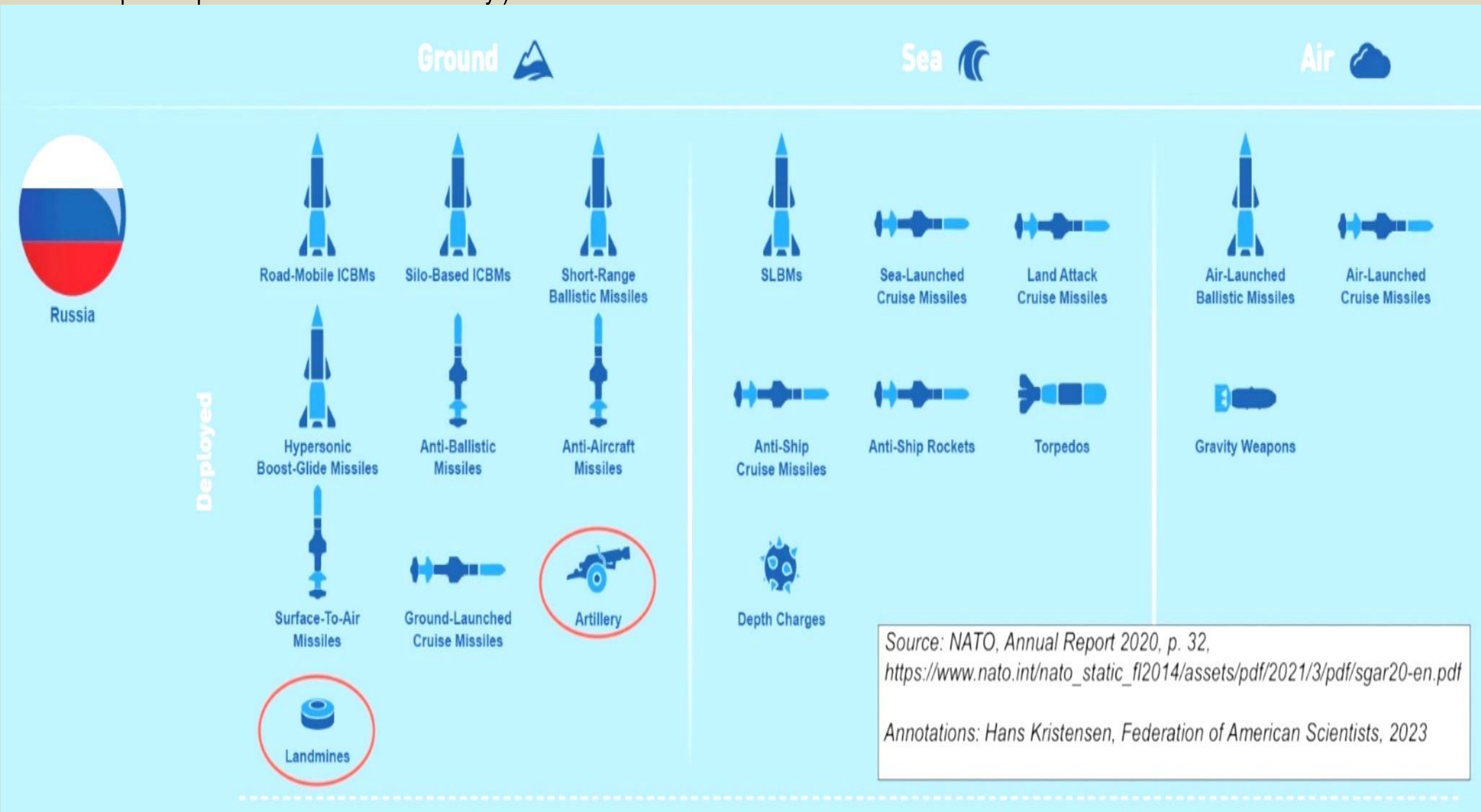
Whether or not the Wagner rebels got to or near a Russian nuclear weapons storage site (or what their intensions were), or whether nuclear weapons potentially stored there were at risk, the episode raises the question if Russia still has nuclear "backpacks" or landmines?

The answer appears to be yes – at least in some form. Recent U.S. Intelligence Community reports refer to them repeatedly, including a U.S. State Department report from 2023. But it is unclear what the status of the Russian landmines is: Are they part of the operational forces or leftovers from the Cold War in queue for dismantlement?

Before examining that question, it is useful to first review what U.S. and NATO sources have said about Russian landmines.

Refences to Soviet-era nuclear landmines can be found in many declassified Intelligence reports. One Central Intelligence Agency assessment from 1981 reported that the Soviet Union "may have introduced nuclear landmines" and a Defense Intelligence Agency guide reportedly listed them. But the wording in these reports were "may have" or "possibly have," indicating a lower level of confidence. When the Soviet Union broke apart, the issue of "loose nukes" became a prominent concern – especially small weapons that could be easily transported. In a speech at the Stimson Center in 1994, for example, then US Defense Secretary William Perry expressed concern about the danger of loose tactical nuclear weapons in Russia, "such as nuclear artillery shells, land mines and others." In 1997, Alexander Lebed, a former Russian general and advisor who had been fired by President Yeltsin, claimed Russia had lost track of 100 of 250 suitcase nuclear bombs. The U.S. Government and others questioned the claim and Lebed later withdrew his claim.

These were extraordinary claim for which no evidence was provided and Lebed later withdrew his claim. Yet the rumor that Russia has nuclear landmines has continued to percolate in the public debate and studies. The Trump administration's Nuclear Posture Review from February 2018 did not list landmines in its overview of Russian non-strategic nuclear weapons. But the following year, one Pentagon official told Congress that the Russian non-strategic nuclear arsenal included "nuclear landmines, and nuclear artillery shells…" NATO appeared to pick up on that in its Annual Report from 2020 that listed both "landmines" and "artillery" (see image below). (It should be noted that neither the U.S. Department of State's 2022 compliance report nor its 2023 non-strategic nuclear weapons report mentions nuclear artillery.)

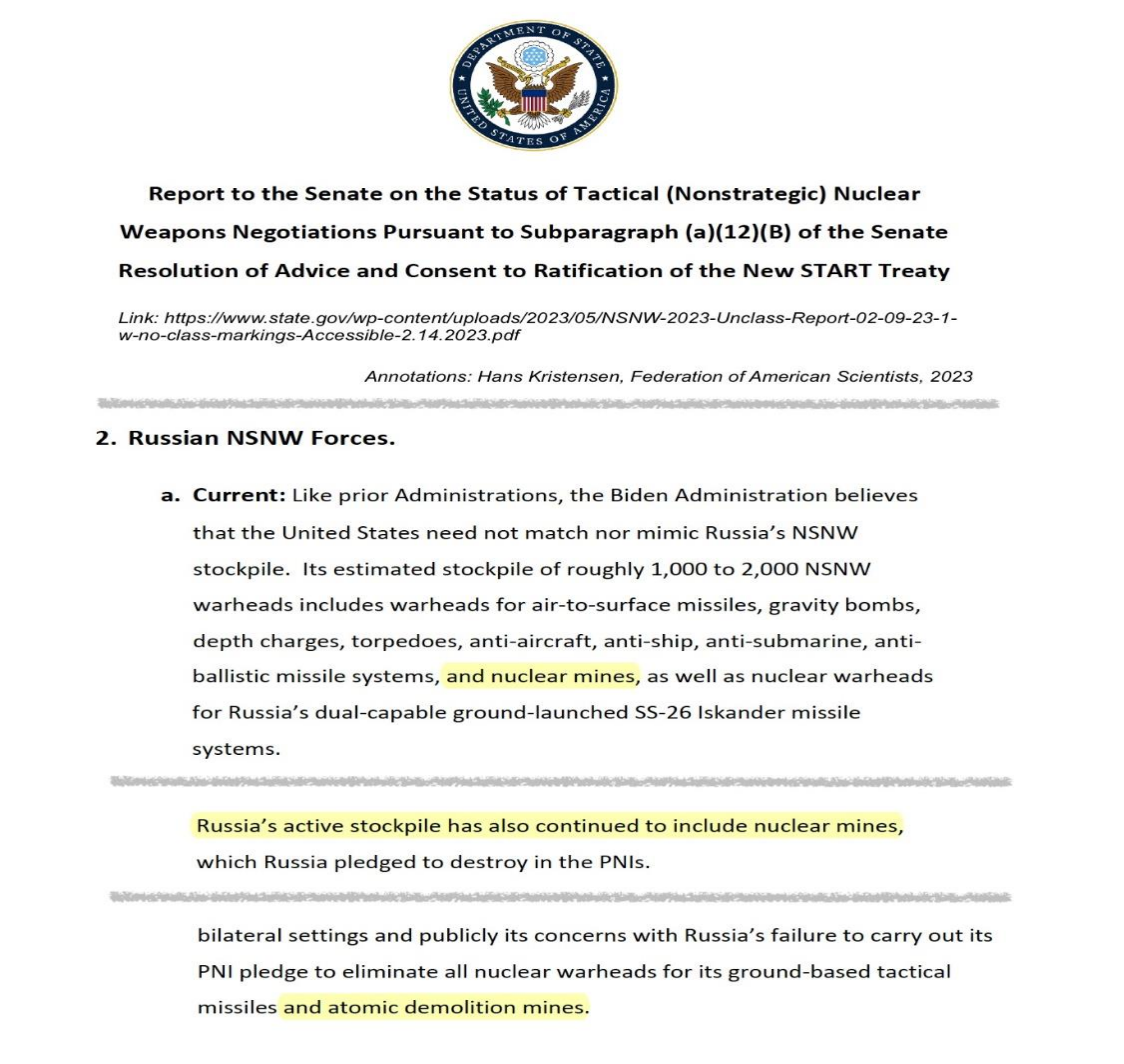

Ground
Sea
Air
Russia
Deployed
Road-Mobile ICBMs
Silo-Based ICBMs
Short-Range Ballistic Missiles
SLBMs
Sea-Launched Cruise Missiles
Land Attack Cruise Missiles
Air-Launched Ballistic Missiles
Air-Launched Cruise Missiles
Hypersonic Boost-Glide Missiles
Anti-Ballistic Missiles
Anti-Aircraft Missiles
Anti-Ship Cruise Missiles
Anti-Ship Rockets
Torpedos
Gravity Weapons
Surface-To-Air Missiles
Ground-Launched Cruise Missiles
Artillery
Depth Charges
Landmines

Source: NATO, Annual Report 2020, p. 32, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/sgar20-en.pdf

Annotations: Hans Kristensen, Federation of American Scientists, 2023

NATO in 2020 listed both landmines and artillery in its overview of Russian nuclear forces.

References to Russian nuclear landmines have also appeared frequently in the U.S. State Department's annual reports on arms control compliance. The report from 2020 listed "atomic demolition mines" as part of Russia's "active" stockpile of non-strategic nuclear weapons. The 2021 report did not explicitly mention nuclear mines in the active stockpile, and the 2022 report changed the language slightly to the active stockpile "has also continue to include nuclear mines." The latest compliance report from 2023 does not include the usual large section on the Presidential Nuclear Initiatives and Russian non-strategic weapons. Instead, that section was moved into a special report on non-strategic nuclear weapons that Congress had requested as part of its approval of the New START treaty. That report, published in February 2023, reiterates that Russia's "active" non-strategic nuclear stockpile incudes nuclear mines (see image below).



Report to the Senate on the Status of Tactical (Nonstrategic) Nuclear Weapons Negotiations Pursuant to Subparagraph (a)(12)(B) of the Senate Resolution of Advice and Consent to Ratification of the New START Treaty

Link: https://www.state.gov/wp-content/uploads/2023/05/NSNW-2023-Unclass-Report-02-09-23-1-w-no-class-markings-Accessible-2.14.2023.pdf

Annotations: Hans Kristensen, Federation of American Scientists, 2023

2. Russian NSNW Forces.

a. Current: Like prior Administrations, the Biden Administration believes that the United States need not match nor mimic Russia's NSNW stockpile. Its estimated stockpile of roughly 1,000 to 2,000 NSNW warheads includes warheads for air-to-surface missiles, gravity bombs, depth charges, torpedoes, anti-aircraft, anti-ship, anti-submarine, anti-ballistic missile systems, and nuclear mines, as well as nuclear warheads for Russia's dual-capable ground-launched SS-26 Iskander missile systems.

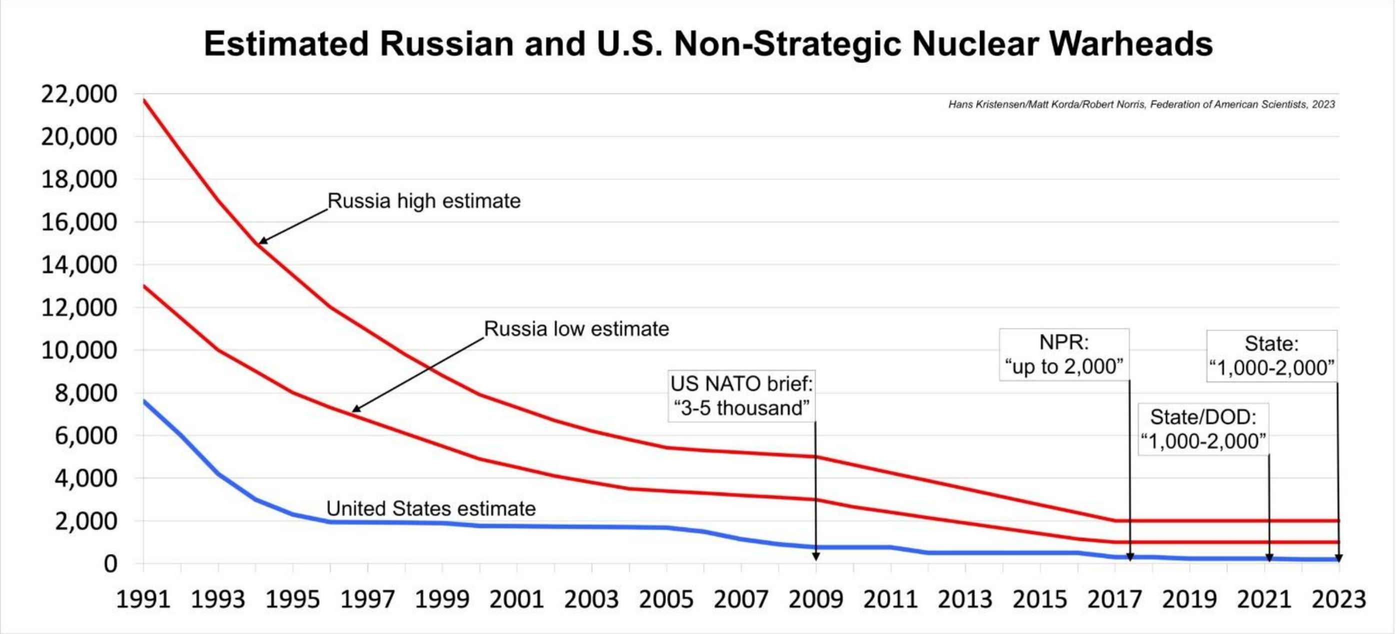
Russia's active stockpile has also continued to include nuclear mines, which Russia pledged to destroy in the PNIs.

bilateral settings and publicly its concerns with Russia's failure to carry out its PNI pledge to eliminate all nuclear warheads for its ground-based tactical missiles and atomic demolition mines.

Recent U.S. Intelligence reports refer repeatedly to the existence of Russian nuclear landmines, although it is uncertain how operational they are. The reports do not refer to nuclear artillery.

Russian Non-Strategic Nuclear Weapons

The Trump administration's Nuclear Posture Review in 2018 estimated that Russia had "up to 2,000" non-strategic nuclear weapons (this was close to the estimate we provided the same year). The NPR estimate was a significant reduction from the "3-5 thousand" Russian warheads listed by Principal Deputy Under Secretary of Defense for Policy James Miller in a briefing to NATO in 2009. Subsequent estimates published by the U.S. Intelligence Community (see above) indicate that the 2018 NPR number was at the high end of an estimated range of 1,000-2,000 warheads. Plotting these numbers from the much higher estimated inventory at the end of the Cold War shows this reduction of the Russian non-strategic nuclear weapons arsenal:



Russia's stockpile of nuclear warheads for non-strategic forces has decreased significantly since the early-1990s – even during the past 15 years – and is estimated to be down to 1,000-2,000 warheads (including retired warheads awaiting dismantlement).

Interestingly, the U.S. State Department stated in 2022 that the Russian "active stockpile" of 1,000-2,000 non-strategic nuclear warheads included "warheads awaiting dismantlement…" This is curious because in the United States, warheads awaiting dismantlement are *not* considered "active" or part of an "active stockpile." Rather, "active" warheads are part of the Department of Defense stockpile that includes both active and inactive warheads. "Active" warheads have all components installed; inactive warheads would need to have those components reinstalled first in order to be able to function.

This suggests that some of the Russian non-strategic warheads that are frequently portrayed in the public debate as part of the arsenal may in fact be retired warheads awaiting dismantlement. Although uncertain, nuclear landmines might be part of that inventory (nuclear artillery shells may be another part of the "awaiting dismantlement" inventory).

In addition to the uncertainty about the status of landmines in the Russian arsenal, advocates for modernization of the U.S. nuclear arsenal have claimed that Russian is expanding its non-strategic nuclear arsenal. Former STRATCOM commander Admiral Charles Richard told Congress in 2020 that "Russia's overall nuclear stockpile is likely to grow significantly over the next decade – *growth driven primarily by a projected increase in Russia's non-strategic nuclear weapons*." (Emphasis added.)

The basis for that projection is unknown and uncertain. Russia is certainly modernizing its arsenal and fielding more types of weapons that the U.S. intelligence community claims are dual-capable. But how many of those launchers will actually be assigned nuclear warheads is another question. The latest U.S. State Department report acknowledges a Russian increase but cautions that "by how much is uncertain."

Warhead projections are partially influenced by the expected growth of delivery platform deployments. But just because the number of dual-capable launchers in a weapons category is increasing doesn't necessarily therefore mean that the number of warheads assigned to that weapons category is also increasing.

In the U.S. nuclear arsenal, for example, not all dual-capable F-15E and F-16 fighter-bombers are assigned nuclear weapons. And just because the F-35A Block 4 upgrade is intended to facilitate integration of nuclear technology, doesn't therefore mean that all F-35A will be part of the nuclear posture and assigned nuclear weapons.

Simplistic dual-capable launcher counting as a basis for warhead projections could lead to exaggerated numbers.

So, there is much uncertainty about Russian non-strategic nuclear weapons and how the U.S. Intelligence Community makes projections about them. A first step to reducing that uncertainty is to ask questions.

●▶ Additional background: Nuclear Notebook: Russian Nuclear Weapons, 2023

This research was carried out with generous contributions from the John D. and Catherine T. MacArthur Foundation, the New-Land Foundation, Ploughshares Fund, the Prospect Hill Foundation, Longview Philanthropy, the Stewart R. Mott Foundation, the Future of Life Institute, Open Philanthropy, and individual donors.

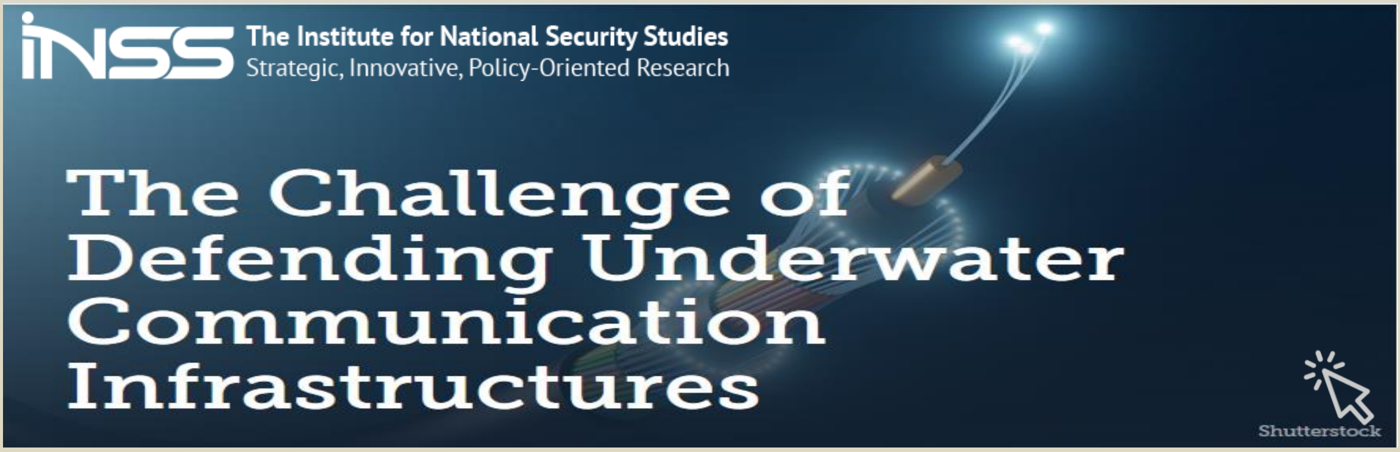
Hans M. Kristensen is Director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons. He specializes in using the Freedom of Information Act (FOIA) in his research and is a frequent consultant to and is widely referenced in the news media on the role and status of nuclear weapons. His collaboration with researchers at NRDC in 2010 resulted in an estimate of the size of the U.S. nuclear weapons stockpile that was only 13 weapons off the actual number declassified by the U.S. government. Kristensen is co-author of the Nuclear Notebook column in the Bulletin of the Atomic Scientists and the World Nuclear Forces overview in the SIPRI Yearbook. The Nuclear Notebook is, according to the publisher, “widely regarded as the most accurate source of information on nuclear weapons and weapons facilities available to the public.”

Son of Eve
TREE OF KNOWLEDGE
ATOMIC BOMB
MAN
TALBURT

ICI International CBRNE Institute
CBRNE-Terrorism Newsletter

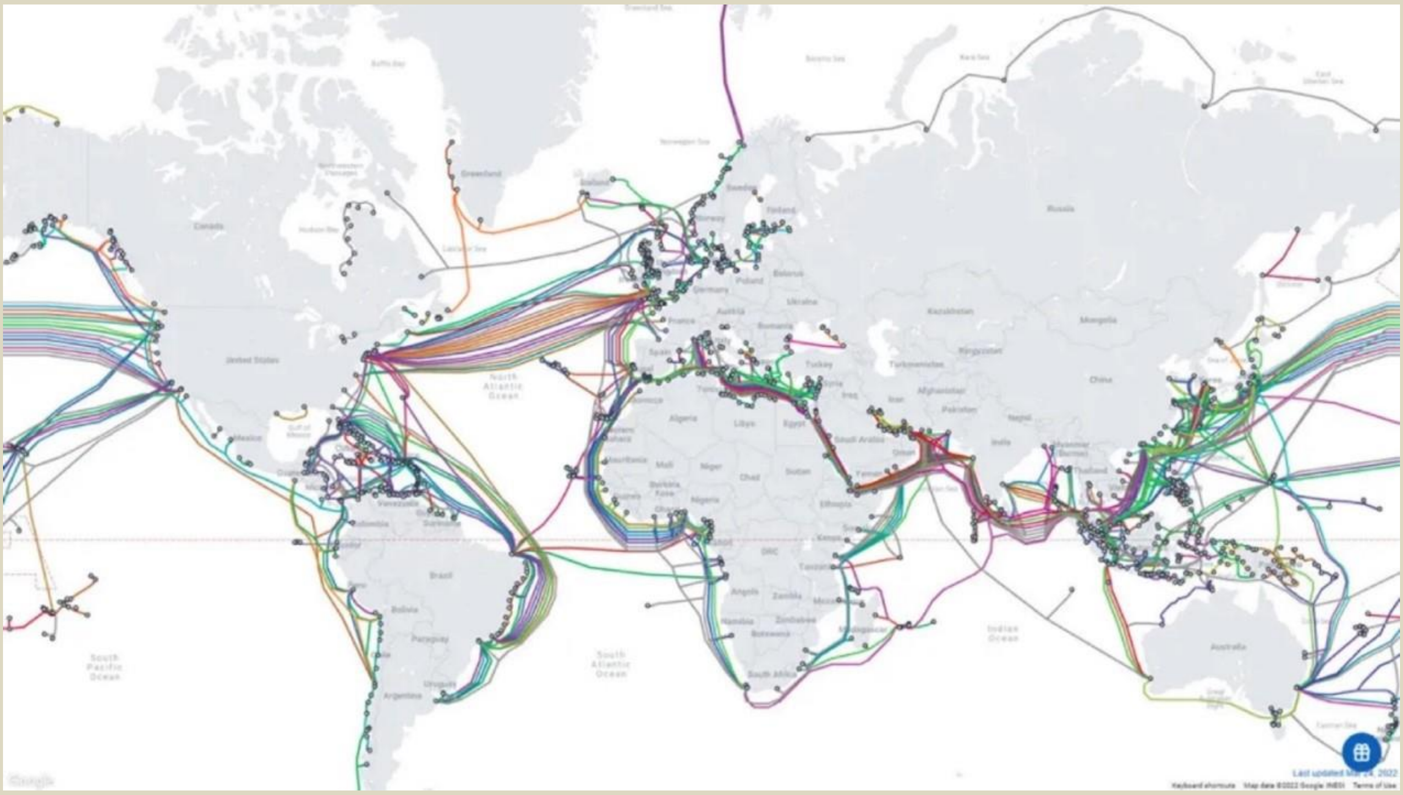
CYBER NEWS

C2BRNE DIARY



The Institute for National Security Studies
Strategic, Innovative, Policy-Oriented Research

The Challenge of Defending Underwater Communication Infrastructures



Worldwide fiber-optic cable distribution | Source: Techspot

Israel smashes Hezbollah crypto network in historic seizure, credits Chainalysis and Binance

Source: https://finance.yahoo.com/news/israel-smashes-hezbollah-crypto-network-155013467.html

June 29 – On Tuesday, Israeli Defense Minister Yoav Gallant announced that its National Bureau for Counter Terror Financing had seized $1.7 million from crypto accounts tied to Iran's Islamic Revolutionary Guard Corps' Quds Force, the country's elite military intelligence group, and the Iran-backed terror organization Hezbollah.

While only a small fraction of the hundreds of millions of dollars Hezbollah likely takes in each year, Israeli officials and crypto investigators touted the takedown as a historic first against the Lebanon-based terrorist group, as well as a sign of Israel's growing prowess in crypto tracing. In April, Hamas' military wing announced it would stop accepting Bitcoin donations, in part owing to Israel's successful operations against the organization.

Paul Landes, head of Israel's NBCTF, said that the cooperation of industry firms including crypto exchange Binance and blockchain analytics firm Chainalysis was necessary for confirming its intelligence and freezing the funds.

“We see [crypto firms] as partners, or nevertheless we see them as gatekeepers,” he told *Fortune* in an interview. “They want to cooperate because they’re frightened from the risk of being connected to terrorism and financial terrorism—they want the industry to be clean.”

Tracing efforts

While previous counterterrorism crypto financing efforts have targeted groups including ISIS and Hamas, this week’s effort was the first against Hezbollah. The effort proved more challenging given the role of Hezbollah’s patron, the Iranian intelligence arm Quds. Nation-state-backed groups are more adept at evading sanctions, according to an investigator on Binance’s sanctions and terrorism financing risk team, who spoke with *Fortune* on the condition of anonymity.

Quds is able to transfer money through a financial transfer system popular in regions of the world including the Middle East called hawala—a network of money brokers who operate outside of the traditional banking system, though many are still subject to regulation. Many hawala operators offer on-ramps from fiat currency into cryptocurrency, which in turn can be sent to wallets on exchanges like Binance, as well as unhosted “cold” wallets that are not connected to the internet.

Landes said that after the NBCTF received intelligence of crypto transfers between Quds and Hezbollah, the agency worked with Chainalysis to trace the activity, as well as Binance—and other exchanges, who asked not to be publicly named in the investigation—to identify the internal withdrawal paths of the interactions. As the Binance investigator explained, tracing within exchanges is often limited, meaning analytics firms and intelligence agencies need the cooperation of companies such as Binance.

Another obstacle was establishing that the exchange accounts were indeed linked to Hezbollah. According to the Binance investigator, the dozen accounts all satisfied “know your customer” and “know your business” compliance processes.

Through the investigation, the organizations were able to tie the accounts to Hezbollah figures—including Muhammad Ja'far Qasir, the central financier of Hezbollah; Muhammad Qasim al-Bazzal, who handled the Hezbollah crypto route; and Tawfiq Muhammad Said al-Law, a Syrian hawala operator—and then freeze and seize the funds. Landes added that the investigation was also able to trace to cold wallets, or wallets not hosted on exchanges, which added an extra layer of complexity.

The growing popularity of Tether on Tron

While terrorist financing previously relied on Bitcoin, the seized Hezbollah funds were in Tether issued on the Tron blockchain, reflecting a growing trend in cryptocurrency, as illicit actors move away from Bitcoin.

According to a report from blockchain analytics firm TRM Labs published on Wednesday, Tether on Tron now accounts for 92% of overall terrorist financing in crypto—a 240% increase over the past year.

While the vast majority of terrorist financing is still coming through fiat currency, the move to Tether—which is pegged to the U.S. dollar—reflects illicit actors’ search for nonvolatile assets, according to the Binance investigator.

Additionally, Bitcoin has lost its guise of opacity, with government agencies using analytics software like Chainalysis to take down dark web marketplaces and other illicit networks. The Binance investigator said that on Telegram channels they monitor, there is a perception that Tether on Tron operates with less oversight from regulators, although they expect that to change with the recent Israeli investigation.

Landes said that crypto in general still presents an appealing opportunity to terrorist groups given its reputation for anonymity and lower bar of regulations compared with the traditional banking system. Furthermore, it is easier to move crypto funds across borders, with entry and exit points around the globe.

“That’s why it attracts not only terrorists, but it attracts also criminals and money launderers and people that want to transfer money worldwide,” he told *Fortune.*

With terrorist groups evolving their methods for transferring funds through cryptocurrency, the Binance investigator said that one aim of the investigation is to dissuade further activity, just as Hamas stopped accepting Bitcoin donations.

“The intense research that’s going to result from the Israelis making this public and offering the information will result in more discoveries that will only help all of us conduct our research and disrupt more financial operations,” the investigator said.

Are Trains at Risk from Cybercrime?

Source: https://i-hls.com/archives/119928

July 17 – Cybersecurity concerns are rising along with political tensions, and it seems that critical infrastructures might be at risk. So far, attacks used to be limited mainly to DDoS attacks that only cause short-term nuisance, but is there real damage that hackers could potentially cause to infrastructures, such as transportation? Turns out that the ability to “hack a train” is more real than you think- modern trains and railways have complex digital systems for control and navigation, and everything that's digital on them can also be hacked.

According to Cybernews, in 2022 an anonymous hacktivist group managed to stop trains in Belarus to disrupt Russia's military build-up in Ukraine. The attack served a political purpose and attempted to disrupt military aggression. However, the fact that hackers were able to access such critical infrastructure is a cause for concern.

There are two main threats to railways- the operational and the non-operational environments.

The non-operational environment affects railway companies' data, which can be stolen and exploited. An example is an attack from April of this year on the Alaska Railroad Corporation (ARRC), during which cybercriminals stole sensitive information about the company's vendors and employees from its systems. A similar case also occurred in the Netherlands in March.

When it comes to the operational environment, malicious actors can disrupt the functioning of trains, which can range from stopping them or manipulating their speeds to sabotaging operations by tampering with railway switches or even causing intentional collisions. Another different cause for concern is physical ransomware attacks where malicious actors prevent trains from moving until their ransom demands are met.

Furthermore, trains are autonomous – which makes them vulnerable. Intercity trains have very long braking distances, sometimes up to one kilometer, therefore more complex solutions are needed for train safety because they are controlled wirelessly.

Across Europe, trains use standardized train operating systems which contribute to efficiency in the railway industry. The downside of this is that it opens the door for attackers to break into these systems on a wide scale.

Another risk factor is human error- train control systems are maintained by numerous people, which increases the risks of systems being insecurely connected to the internet or employees using laptops infected with malware.

Trains, as opposed to other industries, have a very extensive lifespan and are expected to remain in service for around 30 years. Consequently, the train control systems currently in use were designed a decade or more ago.

Furthermore, train control systems include a complex system of various elements such as switches, light signals and other components. Maintaining it is challenging, mainly when the maintenance information is either outdated or it is unclear where it is stored. Two possible solutions are a better and more extensive monitoring system, making sure to keep up to date with the risks of the time, and not getting complacent about the safety of older tech.

WASSERMAN © 8.14
DIST. BY TRIBUNE CONTENT AGENCY
www.bostonglobe.com/wasserman
THE COMPUTER DOCTORS "We care about your repair."
IT LOOKS LIKE THE NSA IS SPYING ON THE MESSAGES THAT WERE SENT BY THE RUSSIAN MOB USING YOUR STOLEN IDENTITY AFTER IT WAS HACKED BY YOUR NEIGHBOR'S KID.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

& Robotic DRONE NEWS

FireDrone Supports the Firefighters

Source: https://www.homelandsecuritynewswire.com/dr20230626-firedrone-supports-the-firefighters

June 26 – Where others rush out, they have to go in: Firefighters put themselves in dangerous situations during rescue operations – sometimes right in the midst of a sea of flames. Last year, Swiss fire departments were called out for more than 12,000 firefighting missions. Since temperatures in a burning building can reach lethal levels of around 1,000 degrees Celsius, it is essential to avoid any unnecessary risk. Flying robots could support such missions: Researchers at Empa and Imperial College London are currently developing a heat-resistant drone that can provide initial data from the hot spot. Based on this information, the men and women of the response team can optimize their strategy before venturing into the inferno. “Before they go directly into the danger zone, the firefighters naturally don’t know what exactly awaits them and what difficulties they will encounter,” says Mirko Kovac, head of Empa’s Sustainability Robotics Laboratory and the Aerial Robotics Lab at Imperial College London. Here, for example, drones equipped with cameras and CO_2 (carbon dioxide) sensors could provide important information about the distribution of fire sources, unexpected hazards or trapped people.

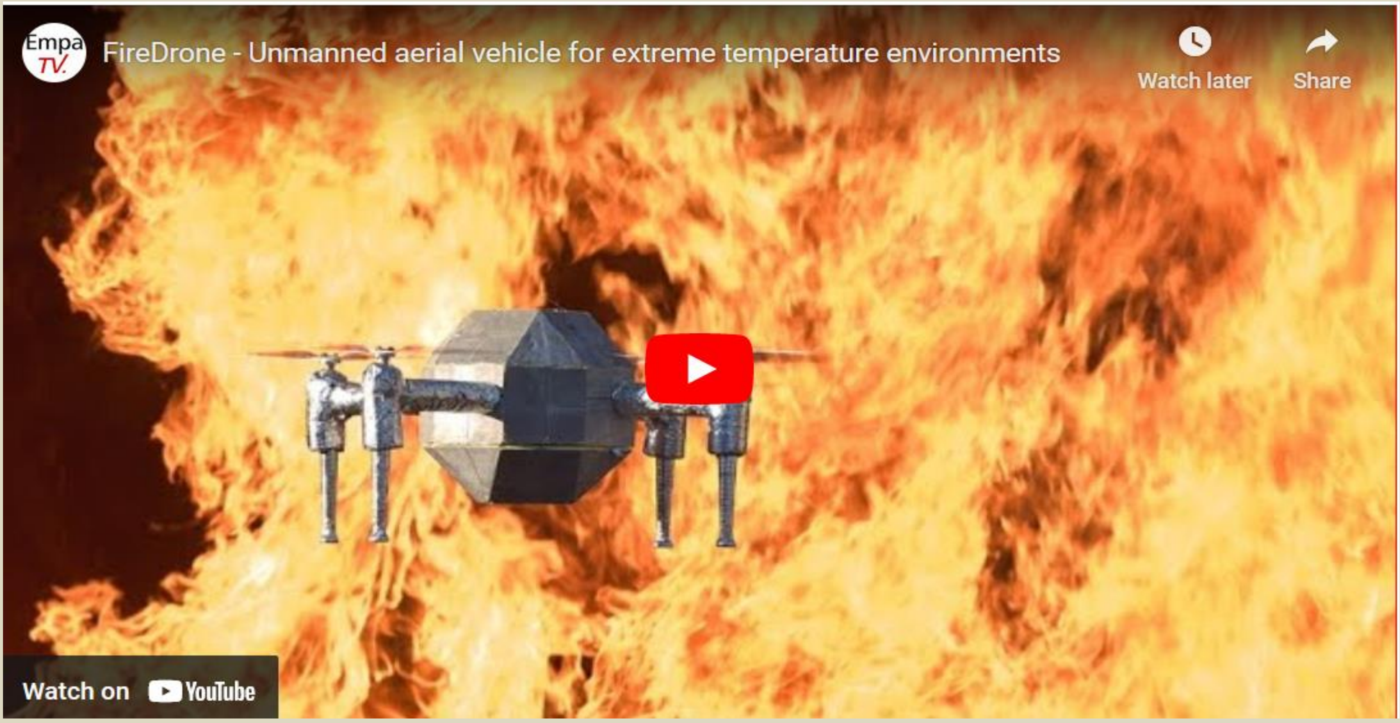
The glass-fiber-reinforced aerogel encloses the heart of the drone, protecting the power supply and electronics from heat. Image: Empa

Too Hot for Normal Drones

Drones are already being used to fight fires, taking aerial photos, lifting fire hoses onto skyscrapers or dropping extinguishing agents in remote areas, for example to contain the spread of forest fires - but only at a safe distance from the source of the fire. “To fly closer, the extreme heat generated by a fire is too great for conventional drones,” says David Häusermann of Empa’s Sustainability Robotics lab. Close to the fire, the frame melts and the electronics give up. “More than aerial photos of the fire site from a safe distance are not possible with commercial drones,” Häusermann says. The researcher’s goal, therefore, was to develop a drone that could withstand the heat and thus provide fast and accurate data from the center of the hot spot.

Ultra-Light and Tough

Häusermannworked with firefighters to determine the requirements of a drone in a fire mission and set out to find a material that could protectively surround the heart of the drone – the motors, batteries, sensors and electronics. He found what he was looking for with colleagues from Empa's Building Energy Materials and Components lab: The researchers led by Shanyu Zhao and Wim Malfait were able to synthesize an insulating material that can withstand high temperatures and thus make the drone more fire-resistant. When designing the FireDrone, the researchers were inspired by nature, or more precisely by animals such as penguins, arctic foxes and spittlebugs that live in extreme temperatures. All these animals have corresponding layers of fat, fur or produce their own protective layers of thermoregulating material that enable them to survive under extreme conditions.


Empa TV
FireDrone - Unmanned aerial vehicle for extreme temperature environments
Watch later
Share
Watch on YouTube

Suitable for Spacesuits

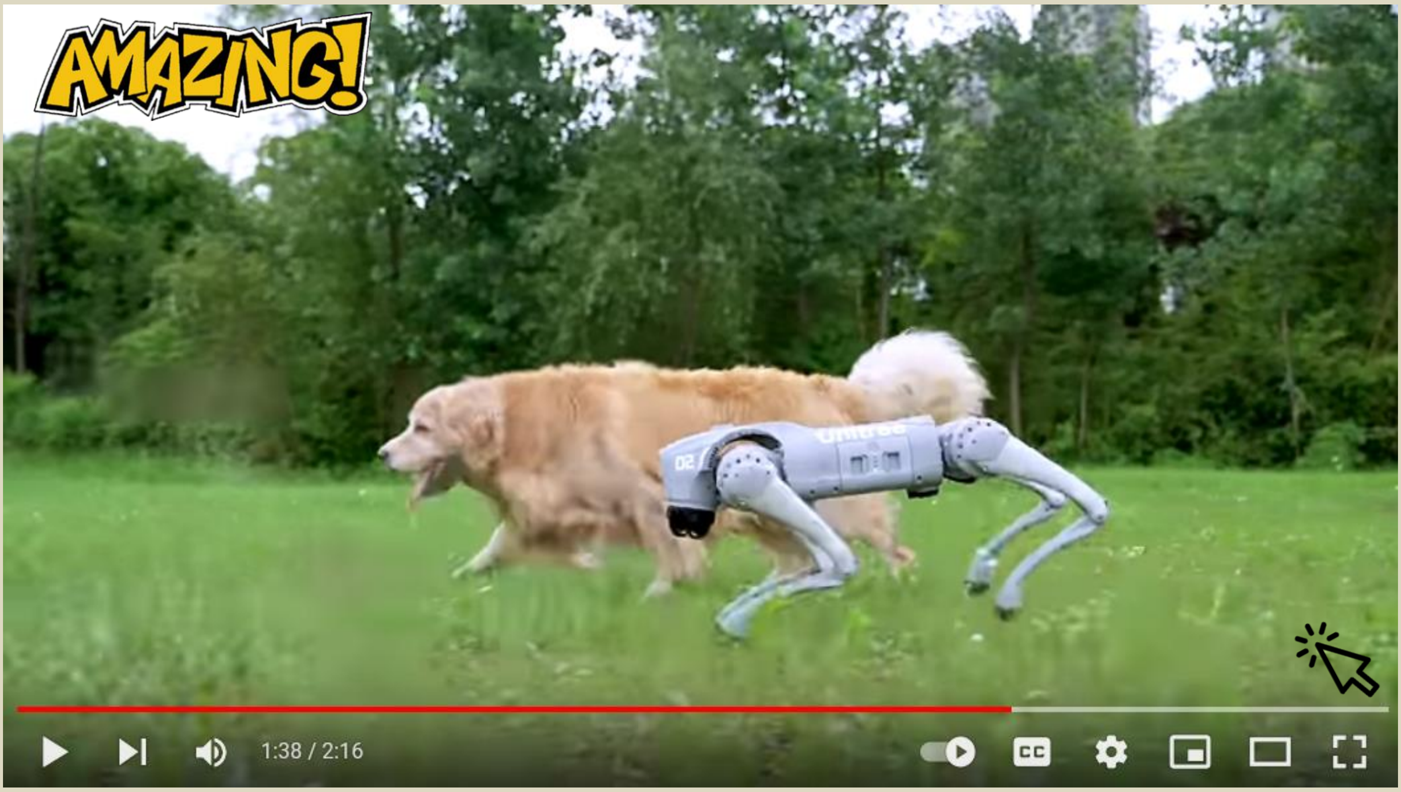
The material in question is an aerogel, an ultralight material consisting almost entirely of air-filled pores enclosed in a hint of polymer substance. In this case, the materials researchers chose an aerogel based on a polyimide plastic. Polyimide aerogels are also being researched by NASA, for example, for the insulation of space suits. However, Shanyu Zhao did not rely on polyimide alone to synthesize the aerogel: The composite material consists of polyimide and silica and is also reinforced with glass fibers. "Laboratory analyses have shown that this comparatively fire-resistant material is particularly well suited for use in drones," says aerogel researcher Zhao.

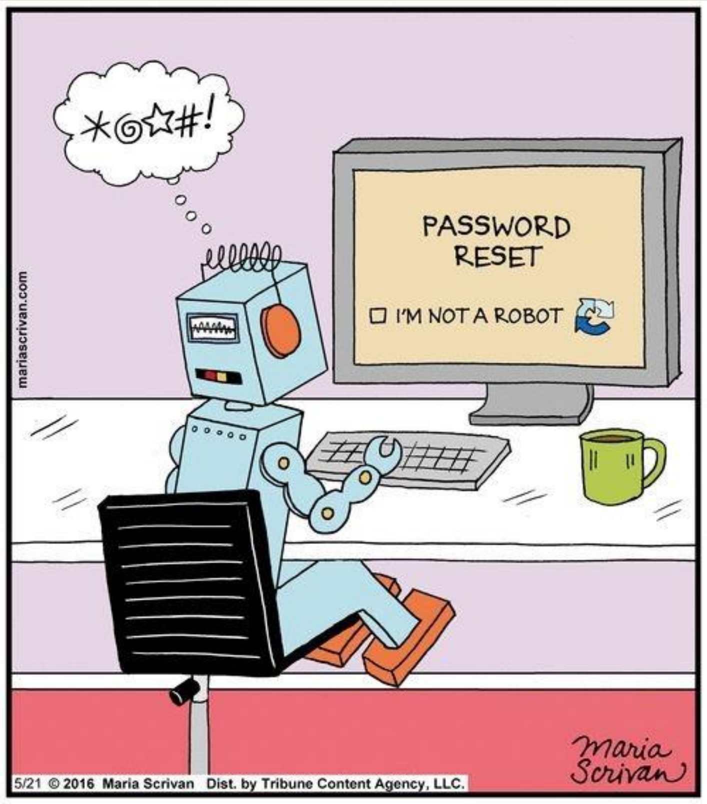
Flight into the Inferno

The prototype of the FireDrone has already performed well in initial tests at Empa's flight arena in Dübendorf. The flight characteristics and controllability of the drone, which is about 50 centimeters tall, were excellent even with an aerogel insulation jacket and an additional built-in cooling system, as well as aluminum cladding to reflect heat. The design, which the researchers just published in the journal "Advanced Intelligent Systems," was convincing in this "dry run." However, whether the aircraft would also pass the test of fire had to be demonstrated by tests under conditions as real as possible, which are typical of a fire operation. The Empa team was able to use such a real-life scenario on the training grounds of the Andelfingen training center. While Stefan Keller, training coordinator for the fire department of the Canton of Zurich's building insurance, and the training center's logistics crew lit a gas fire in an oversized metal bowl, the drone pilots steered their device right into the inferno. The result: The FireDrone prototype survived several test flights. Satisfied, drone researcher Häusermann takes stock: "Even after several flights, the electronics, thermal imaging camera and CO_2 sensors of the FireDrone are undamaged and ready for further testing." A next step would now be to test the FireDrone in a fire, which, unlike the comparatively clean gas flame, shows a strong soot development.
Firefighting expert Stefan Keller is also impressed by the results: "If a drone makes the initial reconnaissance of the situation, we don't have to send firefighters into the danger zone immediately. For us, this progress is enormously interesting." The FireDrone could also be used in extremely cold environments, such as in polar regions and on glaciers. The team has also tested the drone in a glacier tunnel in Switzerland to study how the system behaves in very cold temperatures. Discussions are already

underway with potential industry partners to further develop the prototype. “The use of drones is often limited by environmental factors such as extreme temperatures,” said Mirko Kovac. “With the FireDrone, we are showing a way to significantly expand the future range of applications for drones in extreme environments.”

Introducing Unitree Go2 - Quadruped Robot of Embodied AI from $1600





ICI
International
CBRNE
INSTITUTE

AI - NEWS

C2BRNE
DIARY

Four Ways Criminals Could Use AI to Target More Victims

By Daniel Prince

Source: https://www.homelandsecuritynewswire.com/dr20230623-four-ways-criminals-could-use-ai-to-target-more-victims

June 23 – Warnings about artificial intelligence (AI) are ubiquitous right now. They have included fearful messages about AI's potential to cause the extinction of humans, invoking images of the Terminator movies. The UK Prime Minister Rishi Sunak has even set up a summit to discuss AI safety.

However, we have been using AI tools for a long time – from the algorithms used to recommend relevant products on shopping websites, to cars with technology that recognizes traffic signs and provides lane positioning. AI is a tool to increase efficiency, process and sort large volumes of data, and offload decision making.

Nevertheless, these tools are open to everyone, including criminals. And we're already seeing the early stage adoption of AI by criminals. Deepfake technology has been used to generate revenge pornography, for example.

Technology enhances the efficiency of criminal activity. It allows lawbreakers to target a greater number of people and helps them be more plausible. Observing how criminals have adapted to, and adopted, technological advances in the past, can provide some clues as to how they might use AI.

1. A better phishing hook

AI tools like ChatGPT and Google's Bard provide writing support, allowing inexperienced writers to craft effective marketing messages, for example. However, this technology could also help criminals sound more believable when contacting potential victims. Think about all those spam phishing emails and texts that are badly written and easily detected. Being plausible is key to being able to elicit information from a victim.

Phishing is a numbers game: an estimated 3.4 billion spam emails are sent every day. My own calculations show that if criminals were able to improve their messages so that as little as 0.000005% of them now convinced someone to reveal information, it would result in 6.2 million more phishing victims each year.

2. Automated interactions

One of the early uses for AI tools was to automate interactions between customers and services over text, chat messages and the phone. This enabled a faster response to customers and optimized business efficiency. Your first contact with an organization is likely to be with an AI system, before you get to speak to a human.

Criminals can use the same tools to create automated interactions with large numbers of potential victims, at a scale not possible if it were just carried out by humans. They can impersonate legitimate services like banks over the phone and on email, in an attempt to elicit information that would allow them to steal your money.

3. Deepfakes

AI is really good at generating mathematical models that can be "trained" on large amounts of real-world data, making those models better at a given task. Deepfake technology in video and audio is an example of this. A deepfake act called Metaphysic, recently demonstrated the technology's potential when they unveiled a video of Simon Cowell singing opera on the television show America's Got Talent.

This technology is beyond the reach of most criminals, but the ability to use AI to mimic the way a person would respond to texts, write emails, leave voice notes or make phone calls is freely available using AI. So is the data to train it, which can be gathered from videos on social media, for example.

Social media has always been a rich seam for criminals mining information on potential targets. There is now the potential for AI to be used to create a deepfake version of you. This deepfake can be exploited to interact with friends and family, convincing them to hand criminals information on you. Gaining a better insight into your life makes it easier to guess passwords or pins.

4. Brute forcing

Another technique used by criminals called "brute forcing" could also benefit from AI. This is where many combinations of characters and symbols are tried in turn to see if they match your passwords.

That's why long, complex passwords are safer; they are harder to guess by this method. Brute forcing is resource intensive, but it's easier if you know something about the person. For example, this allows lists of potential passwords to be ordered according to priority – increasing the efficiency of the process. For instance, they could start off with combinations that relate to the names of family members or pets.

Algorithms trained on your data could be used to help build these prioritized lists more accurately and target many people at once – so fewer resources are needed. Specific AI tools could be developed that harvest your online data, then analyses it all to build a profile of you.

If, for example, you frequently posted on social media about Taylor Swift, manually going through your posts for password clues would be hard work. Automated tools do this quickly and efficiently. All of this information would go into making the profile, making it easier to guess passwords and pins.

Healthy Skepticism

We should not be frightened of AI, as it could bring real benefits to society. But as with any new technology, society needs to adapt to and understand it. Although we take smart phones for granted now, society had to adjust to having them in our lives. They have largely been beneficial, but uncertainties remain, such as a good amount of screen time for children.

As individuals, we should be proactive in our attempts to understand AI, not complacent. We should develop our own approaches to it, maintaining a healthy sense of skepticism. We will need to consider how we verify the validity of what we are reading, hearing or seeing.

These simple acts will help society reap the benefits of AI while ensuring we can protect ourselves from potential harms.

Daniel Prince is Professor of Cyber Security, Lancaster University.

The NAIAC's first annual report recommends new steps to bolster U.S. leadership in trustworthy AI, new R&D initiatives, increased international cooperation, and efforts to support the U.S. workforce in the era of AI. Credit: B. Hayes/NIST, Shutterstock

The National Artificial Intelligence Advisory Committee (NAIAC) has delivered its first report to the president, established a Law Enforcement Subcommittee to address the use of AI technologies in the criminal justice system, and completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more. The report recommends steps the U.S. government can take to maximize the benefits of AI technology, while reducing its harms. This includes new steps to bolster U.S. leadership in trustworthy AI, new R&D initiatives, increased international cooperation, and efforts to support the U.S. workforce in the era of AI. The report also identifies areas of focus for NAIAC for the next two years, including in rapidly developing areas of AI, such as generative AI. "We are at a pivotal moment in the development of AI technology and need to work fast to keep pace with the changes it is bringing to our lives," said U.S. Deputy Secretary of Commerce Don Graves. "As AI opens up exciting opportunities to improve things like medical diagnosis and access to health care and education, we have an obligation to make sure we strike the right balance between innovation and risk. We can lead the world in establishing trustworthy, inclusive and beneficial AI, and I look forward to considering the committee's recommendations as we do that."

When it comes to AI, President Biden has been clear that in order to seize the opportunities AI presents, we must first mitigate its risks. NAIAC's work supports the Biden-Harris administration's ongoing efforts to promote responsible American innovation in AI and protect people's rights and safety. Given the fast pace of development and deployment of AI technology such as generative AI, which includes the large language models that power chatbots and other tools that create new content, the committee also plans to consider various mechanisms for carrying out its work on short time frames in the coming years.

The committee recently completed plans to realign its working groups to allow it to explore the impacts of AI on workforce, equity, society and more. **The new NAIAC focus areas are:**

- AI Futures: Sustaining Innovation in Next Gen AI
- AI in Work and the Workforce
- AI Regulation and Executive Action
- Engagement, Education and Inclusion
- Generative and NextGen AI: Safety and Assurance
- Rights-Respecting AI
- International Arena: Collaboration on AI Policy and AI-Enabled Solutions
- Procurement of AI Systems
- AI and the Economy

Is the Chatbot a Threat or an Opportunity for Security Organizations?

Author: COL (ret.) Eshed, Gadi

Source: https://ict.org.il/chatbot-threat-or-opportunity-for-security-organizations/

June 26 – The article explores the benefits, challenges, and potential impact of ChatGPT, an advanced chatbot powered by artificial intelligence. It appears that at this stage, it can be said that large language models (LLMs) and artificial intelligence (AI) models like ChatGPT have achieved a dramatic technological breakthrough in the field of technology. These unique capabilities have the potential to enhance productivity across a wide range of functions.

The article emphasizes the transformative potential of ChatGPT4 in the realm of the army, security organizations, and police departments. It discusses how this technology can revolutionize operations and lead to enhanced efficiency. The article also notes the increasing investment in artificial intelligence by security agencies, highlighting its critical role in national security.

While acknowledging the enthusiasm surrounding ChatGPT, the article presents also a skeptical perspective by highlighting concerns raised by experts. These include the generation of false information, social biases, and the limitations of the chatbot's lack of contextual understanding and subjectivity. Critics argue that despite its groundbreaking nature, ChatGPT represents a development achievement rather than a revolutionary turning point. The article addresses the potential risks associated with malicious exploitation of ChatGPT, including the dissemination of disinformation and its impact on electoral systems. It warns about the strategic threats posed to the integrity of elections and the potential for criminal or ideological actors to develop more dangerous innovations using this technology.

However, the article concludes by suggesting that if the reported issues are addressed, ChatGPT can be a valuable tool for the intelligence community and security organizations. It emphasizes the offensive and defensive potential of generative AI and ChatGPT, indicating that organizations failing to adopt and develop these technologies may become irrelevant.

Reichman University

International Institute for Counter-Terrorism (ICT)

With the support of the Jusidman Foundation

Is the Chatbot a Threat or an Opportunity for Security Organizations?

Colonel (Ret.) Gadi Eshed

June 2023

Use Of AI In Nuclear Weapons 'Extremely Dangerous,' May Lead To Catastrophic Results – UN

Source: https://www.urdupoint.com/en/world/use-of-ai-in-nuclear-weapons-extremely-dange-1715653.html

June 27 – The use of artificial intelligence (AI) in nuclear weapons is extremely dangerous and may lead to catastrophic humanitarian consequences, UN High Representative for Disarmament Affairs Izumi Nakamitsu said on Tuesday. "AI in weapons-related functions such as pre-delegation to launch weapons that's the use of force decisions, especially nuclear weapons systems, is an extremely dangerous concept that could result in potentially catastrophic humanitarian consequences," Nakamitsu said during a United Nations Institute for Disarmament Research 2023 Innovations Dialogue.

Moreover, AI-enabled intelligence surveillance reconnaissance capabilities could be a source of escalation, and be used for targeting and attack purposes in times of conflict, Nakamitsu added.

Nakamitsu warned against following technology blindly and underscored that human beings should remain the ones who determine when and how to use AI and machine learning and not the other way around.

Does the world need an arms control treaty for AI?

By Elias Groll

Source: https://cyberscoop.com/ai-danger-arm-control-nuclear-proliferation/

June 29 – At the dawn of the atomic age, the nuclear scientists who invented the atomic bomb realized that the weapons of mass destruction they had created desperately needed to be controlled. Physicists such as Niels Bohr and J. Robert Oppenheimer believed that as knowledge of nuclear science spread so, too, would bombs. That realization marked the beginning of the post-war arms control era.

Today, there's a similar awakening among the scientists and researchers behind advancements in artificial intelligence. If AI really poses an extinction threat to humankind — as many in the field claim — many experts in the field are examining how efforts to limit the spread of nuclear warheads might control the rampant spread of AI.

Already, OpenAI, the world's leading AI lab, has called for the formation of "something like" an International Atomic Energy Agency — the global nuclear watchdog — but for AI. United Nations Secretary General Antonio Guterres has since backed the idea, and rarely a day goes by in Washington without one elected official or another expressing a need for stricter AI regulation.

Early efforts to control AI — such as via export controls targeting the chips that power bleeding-edge models — show how tools designed to control the spread of nuclear weapons might be applied to AI. But at this point in the development of AI, it's far from certain that the arms control lessons of the nuclear era translate elegantly to the era of machine intelligence.

Arms control frameworks for AI

Most concepts of controlling the spread of AI models turn on a quirk of the technology. Building an advanced AI system today requires three key ingredients: data, algorithms and computing power — what the researcher Ben Buchanan popularized as the "AI Triad." Data and algorithms are essentially impossible to control, but only a handful of companies build the type of computing power — powerful graphics processing units — needed to build cutting-edge language models. And a single company — Nvidia — dominates the upper end of this market.

Because leading AI models are reliant on high-end GPUs — at least for now — controlling the hardware for building large language model offers a way to use arms control concepts to limit proliferation of the most powerful models. "It's not the best governance we could imagine, but it's the best one we have available," said Lennart Heim, a researcher at the Centre for the Governance of AI, a British nonprofit, who studies computing resources.

U.S. officials have in recent months embarked on an experiment that offers a preview of what an international regime to control AI might look like. In October, the U.S. banned the export of high-end GPUs to China and the chip making equipment necessary to make the most advanced chips, attempting to prevent proliferation of advanced AI models to China. "If you look at how AI is currently being governed," Heim said, "it's being governed right now by the U.S. government. They're making sure certain chips don't go to China."

Biden administration officials are now considering expanding these controls to lagging-edge chips and limiting Chinese access to cloud computing resources, moves that would further cut Beijing off from the hardware it needs to build competitive AI models.

While Washington is the driving force behind these export controls, which are aimed at ensuring U.S. supremacy in microelectronics, quantum computing and AI, it also relies on allies. In restricting the flow of chips and chipmaking equipment to China, the U.S. has signed up support from other key manufacturers of such goods: the Netherlands, Japan, South Korea and Taiwan.

By virtue of their chokehold on the chips used to train high-end language models, these countries are showing how the spread of AI models might be checked via what for now are ad hoc measures that might one day be integrated into an international body.

But that's only one half of the puzzle of international arms control.

Carrots and sticks

In the popular imagination, the IAEA is an organization primarily charged with sending inspectors around the world to ensure that peaceful nuclear energy programs aren't being subverted to build nuclear bombs.

The less well-known work of the agency facilitates the transfer of nuclear science. Its basic bargain is something like this: sign up to the Nuclear Non-Proliferation Treaty, pledge not to build a bomb and the IAEA will help you reap the benefits of peaceful nuclear energy.

“That’s the big reason that most states are enthusiastic about the IAEA: They’re in it for the carrots,” said Carl Robichaud, who helps lead the existential risk and nuclear weapons program at Longview Philanthropy, a nonprofit based in London. “They show up in Vienna in order to get assistance with everything from radiotherapy to building nuclear power plants.”

Building an international control regime of this sort for AI requires considering how to first govern the spread of the technology and then how to make its benefits available, argues Paul Scharre, the executive vice president and director of studies at the Center for a New American Security in Washington. By controlling where advanced AI chips go and who amasses them, licensing the data centers used to train models and monitoring who is training very capable models, such a regime could control the proliferation of these models, Scharre argued.

Countries that buy into this arrangement would then gain easier access to very capable models for peaceful use. “If you want to access the model to do scientific discovery, that’s available — just not to make biological weapons,” Scharre said.

These types of access controls have grown more feasible as leading AI labs have abandoned the open source approach that has been a hallmark of the industry in recent years. Today, the most advanced models are only available via online apps or APIs, which allows for monitoring how they are used. Controlling access in this way — both to monitor use and to provide beneficial access — is essential for any regime to control the spread of advanced AI systems, Scharre argued.

But it’s not clear that the economic incentives of participating in such a regime translate from the world of nuclear arms control to AI governance. Institutions like the IAEA help to facilitate the creation of capital and knowledge intensive nuclear energy industries, and it’s unclear whether similar hurdles exist for AI to incentivize participating in an arms control regime.

“I like the idea of an international agency that helps humanity benefit more equitably from AI and helps this technology reach and help everyone. It’s not clear right now that there is market failure as to why that wouldn’t happen,” Robichaud said.

It’s also not clear that access controls can be maintained in the long run. Unlike nuclear weapons, which are fairly large physical devices that are difficult to move around, AI models are just software that can be easily copied and spread online. “All it takes is one person to leak the model and then the cats out of the bag,” Scharre said.

That places an intense burden on AI labs to keep their products from escaping the lab — as has already occurred — and is an issue U.S. policymakers are trying to address.

In an interview with CyberScoop, Anne Neuberger, a top White House adviser on cybersecurity and emerging technology, said that as leading AI firms increasingly move away from open source models and seek to control access, the U.S. government has carried out defensive cybersecurity briefings to leading AI firms to help ensure that their models aren’t stolen or leaked.

When AI safety researchers speak of the potentially existential threat posed by AI — whether that be a flood disinformation or the development of novel biological weapons — they are speculating. Looking at the exponential progress of machine learning systems in the past decade, many AI safety researchers believe that if current trends hold, machine intelligence may very well surpass human intelligence. And, if it does, there’s reason to think machines won’t be kind to humans.

But that isn’t a sure thing, and it’s not clear exactly what catastrophic AI harms the future holds that need to be prevented today. That’s a major problem for trying to build an international regime to govern the spread of AI. “We don’t know exactly what we’re going to need because we don’t know exactly what the technology is going to do,” said Robert Trager, a political scientist at the University of California, Los Angeles, studying how to govern emerging technology.

In trying to prevent the spread of nuclear weapons, the international community was inspired by the immense violence visited upon Hiroshima and Nagasaki. The destruction of these cities provided an illustration of the dangers posed by nuclear weapons technology and an impetus to govern their spread — which only gained momentum with the advent of more destructive thermonuclear bombs.

By contrast, the catastrophic risks posed by AI are theoretical and draw from the realm of science fiction, which makes it difficult to build the consensus necessary for an international non-proliferation regime. “I think these discussions are suffering a little bit from being maybe ahead of their time,” said Helen Toner, an AI policy and safety expert at the Center for Security and Emerging Technology at Georgetown University and who sits on OpenAI’s board of directors.

If 10 or 20 years from now, companies are building AI systems that are clearly reaching a point where they threaten human civilization, “you can imagine there being more political will and more political consensus around the need to have something quite, quite strong,” Toner said. But if major treaties and conventions are the product of tragedy and catastrophe, those arguing for AI controls now have a simple request, Toner observes: “Do we have to wait? Can we not skip that step?”

But that idea hasn’t broken through with policymakers, who appear more focused on immediate risks, such as biased AI systems and the spread of misinformation. Neuberger, the White House adviser, said that while international efforts to govern AI are important, the Biden administration is more focused on how the technology is being used and abused today and what steps to take via executive order and congressional action before moving to long-term initiatives.

“There’s a time sequence here,” Neuberger said. “We can talk about longer term efforts, but we want to make sure we’re focusing on the threats today.”

In Europe, where EU lawmakers are at work on a landmark AI Act, which would limit its use in high-risk contexts, regulators have taken a similarly skeptical approach toward the existential risks of AI and are instead focusing on how to address the risks posed by AI as it is used today.

The risk of extinction might exist, “but I think the likelihood is quite small,” the EU’s competition chief Margrethe Vestager recently told the BBC. “I think the AI risks are more that people will be discriminated [against], they will not be seen as who they are.”

Today’s leading AI models are built on a foundation of funneling ever more data into ever more powerful data centers to produce ever more powerful models. But as the algorithms that process that data become more efficient it’s not clear that ever more powerful data centers — and the chips that power them — will be necessary. As algorithms become more efficient, model developers “get better capability” for “less compute,” Heim from the Centre for the Governance of AI explains. In the future, this may mean that developers can train far more advanced models with less advanced hardware.

Today, efforts to control the spread of AI rest on controlling hardware, but if having access to the most advanced hardware is no longer essential for building the most advanced models, the current regime to control AI crumbles.

These shifts in training models are already taking place. Last year, researchers at Together, an open source AI firm, trained a model known as GPT-JT using a variety of GPUs strung together using slow internet speeds — suggesting that high-performing models could be trained in a decentralized manner by linking large numbers of lagging-edge chips. And as publicly available, ever more capable open source models proliferate, the moat separating AI labs from independent developers continues to narrow — or may disappear altogether.

What’s more, arguments about the role of algorithmic efficiency making compute less relevant don’t account for entirely new approaches to training models. Today’s leading models rely on a compute-intensive transformer architecture, but future models may use some entirely different approach that would undermine efforts today to control AI models, Toner observes.

Moreover, arms control experts observe that past efforts to control the spread of dangerous weapons should force a measure of humility on any policymaker trying to control the spread of AI. In the aftermath of World War II, President Truman and many of his key aides, ignoring their scientific advisers, convinced themselves that it would take the Soviet Union decades to build an atomic bomb — when it only took the Kremlin five years. And in spite of export controls, China succeeded in building “2 bombs and 1 satellite” — an atomic bomb, a thermonuclear bomb and a space program.

That history makes Trager, the political scientist, skeptical about “grand visions for what export restrictions can do.”

With private companies currently conducting the most advanced AI research, efforts to control the technology have understandably focused on managing industry, but in the long run, military applications may be far more concerning than commercial applications. And that does not bode well for arms control efforts. According to Trager, there is no example in history of major powers “agreeing to limit the development of a technology that they see as very important for their security, and for which they don’t have military substitutes.”

But even if arms control frameworks are imperfect vessels for regulating AI, arms control regimes have evolved over time and grown more stringent to deal with setbacks. The discovery of Iraq’s nuclear program in the 1990s, for example, spurred the creation of additional protocols to the Non-Proliferation Treaty.

“We’re 80 years into the nuclear age, and we haven’t had a detonation in wartime since 1945 and we only have nine nuclear-armed states,” Robichaud from Longview Philanthropy argues. “We’ve gotten lucky a few times, but we’ve also built the systems that started off really weak and have gotten better over time.”

Elias Groll is a senior editor at CyberScoop. He has previously worked as a reporter and editor at Foreign Policy, covering technology and national security, and at the Brookings Institution, where he was the managing editor of TechStream and worked as part of the AI and Emerging Technology Initiative. He is a graduate of Harvard University, where he was the managing editor of The Harvard Crimson.

Hmmm!

The originator of the doctrine of the "Great Reset" and key adviser to the internationalist president of the WEF Klaus Schwab, Yuval Harari, revealed something that those who are still thinking on this planet, have always feared: **How AI will have the choice to decide on its own whether to kill someone or attack someone and not wait for permission from a human mind to do so.**

EDITOR’S COMMENT: I have a pretty good single target in mind! Give us a break!

Securing the AI Pipeline

By Dan Browne and Muhammad Muneer

Source: https://www.mandiant.com/resources/blog/securing-ai-pipeline

June 27 – Artificial intelligence (AI) is a hot topic these days, and for good reason. AI is a powerful tool. In fact, Mandiant analysts and responders are already using Bard in their workflows to identify threats faster, eliminate toil, and better scale talent and expertise. Organizations are keen to understand how best to integrate it into their own existing business processes, technology stacks, and delivery pipelines, and ultimately drive business value.

In this blog post we will look briefly at the current state of AI, and then explore perhaps the most important question of them all: **How do we secure it?**

SAIF

Google recently published the Secure AI Framework (SAIF), a conceptual framework for secure AI systems. SAIF is inspired by security best practices incorporating an understanding of security mega-trends and risks specific to AI systems. SAIF consists of the following six core elements:

1. Expand strong security foundations to the AI ecosystem
2. Extend detection and response to bring AI into an organization's threat universe
3. Automate defenses to keep pace with existing and new threats
4. Harmonize platform level controls to ensure consistent security across the organization
5. Adapt controls to adjust mitigations and create faster feedback loops for AI deployment
6. Contextualize AI system risks in surrounding business processes

Our approach to securing the AI pipeline is built on these SAIF principles. As you read through this blog post, we will reference where our approach aligns with the six core elements. We encourage you to read through the quick guide to implementing SAIF to learn more about adopting AI in a bold and responsible way.

Beginning With AI

AI typically refers to a type of technology called machine learning, which is composed of a knowledge model that has been trained on some information, along with some additional software code to provide questions to the model and respond with answers. The original machine learning models were used to "classify" and respond with a "label". An example of this would be to feed a photograph to the model where you would essentially be answering the question "what is in this photograph?". Early examples of this technology were used for recognizing handwriting or checks.

Another version of this early form of machine learning would be to take some input, and transform that input into something else. For example, taking an audio file with a person speaking and transcribing what the person said. In other words, speech to text. The more recent versions of this technology are called "generative AI". When a human types in a question or instruction (called a prompt), the model reads it and produces an output.

The two most common types of generative AI are image generation (generating photographs based on a description) and chatbot type dialog response. In this case you would type a prompt and the chatbot would transform your prompt into some text such as a story. Most users typically access these generative AI systems through a web interface or mobile app, which provide access to a cloud type service. It is possible, however, to host, build, or train your own AI models. For the purposes of this blog post, we will focus on hosting your own model when discussing "securing the AI pipeline".

How Do We Secure the AI Pipeline?

Relevant SAIF core elements:

1. Expand strong security foundations to the AI ecosystem

2. Extend detection and response to bring AI into an organization's threat universe

When asking the question "how do we secure the AI pipeline?", we first need to ask a couple other questions:

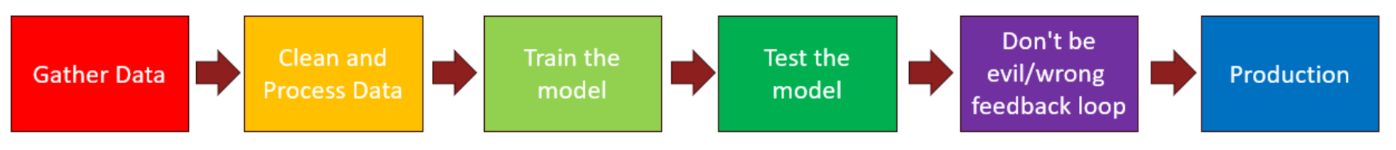
- What does the AI pipeline look like?
- What are the most likely attacks we would see targeting the AI pipeline?

To address the first question we designed a conceptual model of what we consider to be a typical AI pipeline. This pipeline consists of six components and is detailed in the AI Pipeline section that follows. Next, to address the second question, we performed a threat modeling assessment against the AI pipeline. Having done that, we came up with a set of 10 most likely attacks or vulnerabilities in context of the threat model that could be used to design controls for the pipeline. We have chosen to call this list of attacks and vulnerabilities the GAIA Top 10, where GAIA stands for “Good AI Assessment”. There are other types of lists that focus on various aspects of security such as the OWASP top 10, which looks at web application attack vectors. OWASP also has a list for securing LLMs specifically. The MITRE ATLAS is another good resource for attack paths against the AI/ML pipeline. GAIA is built around what we consider to be the most likely attack paths for the generalized AI pipeline, and has been developed for the purposes of this blog post. It is not an exhaustive list of possible attack paths.

Here is a simplified diagram of the AI pipeline we used:

AI Pipeline

As you can see there are six components:



Data Gathering

In this stage of the pipeline, typically data scientists have already figured out a predictive model they want to build, and what data they will need to train the model and test it. For example, in the case of a dog breeds model, the data scientists might want to gather together lots of examples of pictures of different breeds of dogs, taken from different angles, and in different lighting conditions. Additionally, they might want to gather some counterexamples to test the model on; say, pictures of cats, pictures of the sky, pictures of trains, and pictures of people. In other words, pictures of anything but dogs.

Cleaning and Processing the Data

At this stage the data scientists would be looking at the training data to make sure it is clean and useful. In the case of the dog-breed-prediction model, they might want to make sure there are no duplicate photos, and no pictures of cartoon dogs or toy dogs. Then they would build the appropriate software scripts to feed the pictures into the blank model in batches, with corresponding labels saying which breed the particular picture is. Note: there is a way to do this without labeling the data, but we won’t talk about this here in great detail.

Training the Model

At this stage the blank model is ready to be trained. Here, the data scientists would start the process that would run the data-loading scripts into the model over and over until the model learns and its forecasts have minimal loss. For example, if the model is being trained to identify different types of dog breeds, then the model would be trained on the corresponding names of dog breeds.

Testing the Model

At this stage the model is trained and ready to be tested. The data scientists build test scripts, which load in examples of test data that the model has never seen before. If the model has worked correctly, it will produce outputs that label the test data (in this case dog pictures or not-dog-pictures) as either “dog-breed” or “not-dog”. In standard software testing, this stage would often be called functional testing.

Testing Whether the Feedback Loop of the Model Gives Unacceptable Results (“Don’t be Evil/Wrong”)

At this stage we want to identify scenarios that would be considered to be wrong and/or bad/evil. In the case of a dog-breed classifier model, it is difficult to come up with examples of how this model could produce bad/evil outputs, but an inadequately or incorrectly trained dog-breed-classifier model could provide inaccurate responses. For example, predicting that a dog picture isn’t a dog would be wrong. Likewise saying that a panda is a type of dog would be wrong.

For bad/evil scenarios, we could think of an example where a self-driving car model is being trained to recognize street signs. Identifying a stop sign as a speed limit sign could be considered bad or evil depending on the reasons why the system is misidentifying the stop sign.

In standard software testing, this stage would be called “abuse case testing” or “security testing”.

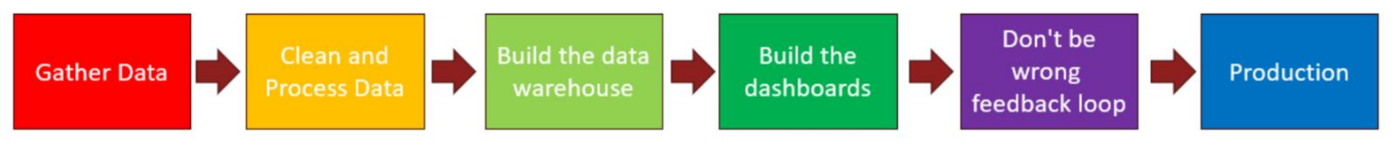
Final Production

At this stage, the pipeline is complete. The model is fully trained and fully tested, and specific test cases have been identified that test the model functions correctly, and that the identified abuse cases do not affect the model. The model is now ready to be delivered to the users.

Wait a Minute: There’s Something Familiar About This…

The AI pipeline diagram and aforementioned descriptions are for a standardized conceptual AI pipeline where you would train your model from scratch. In some cases an organization may be using either a pre-trained model from some third party with no training needed or else they may be taking a pre-trained model and performing some re-training of the model (which in machine learning is called “fine-tuning”).

To some of you all this is likely to seem *really* familiar. In fact, it looks just like another pipeline we've been using for over a decade: the Business Intelligence (BI) pipeline.



Why are we showing you the BI pipeline when we're talking about AI? That's because the BI Pipeline is built on ***known tech***.

And so is the AI pipeline. For the most part, the tech is super familiar. That's a point we strongly want to drive home. While AI itself has some interesting and brand new cutting-edge features, the technology stack on which it is built and in which it lives, is using familiar technology. Threat models have been developed leveraging known attack vectors. Detective and preventive controls have also been designed for the known attack vectors. You will see later on in the blog post that this is a recurring theme.

Now that we have defined the AI pipeline and have developed an approach to map attack paths against the pipeline, let's take a look at the risk approach in the context of AI.

Risk Approach

Relevant SAIF core element:

6. Contextualize AI system risks in surrounding business processes

Adopt AI

Should we adopt AI? That's the big question being asked by all organizations today. Like any other business problem, the decision to adopt or develop AI capabilities depends on a cost-benefit analysis that is informed by risk. Ask yourself:

- Will our employees or customers be at risk?
- Will our network be at risk?
- Will our data be at risk?

When determining security controls for the AI pipeline, the organization needs to have clarity on the type of AI they will be using at the organization:

- Do we develop the model and corresponding technology in-house?
- Do we use a third party developed model and host in-house or in the cloud?
- Do we use an as-a-service API type solution?

Each of these questions may have different threat models applicable to them, and as a result, it is possible that they will have different security controls—prevention and detection—that would be relevant. Knowing the path the organization is going to take for AI adoption, and the type of models that will be used, will help an organization assess risk and develop controls.

In addition to deployment options, there are some general risk type questions that management should be considering:

- What is the organization's stance on using AI?
  - This question will help the organization determine its overall approach to AI, including developing its own capabilities versus relying on third-party providers.
- Do we need to use AI?
  - AI can be a complex and expensive technology. The organization should carefully consider whether AI is the best solution for its needs.
- How will AI impact the workforce?
  - The organization should consider how AI will impact its workforce, and develop plans to mitigate any negative impacts.
- Are we already using AI in-house?
  - Many organizations are already using AI, even if they don't realize it. The organization should identify all of the ways in which it is using AI, and assess the risks associated with each use.
- How do we know we are using AI in-house?
  - The organization should develop a process for identifying AI in their environment and tracking its use.
- Does the organization have supply-side AI exposure?
  - The organization should assess its exposure to supply-side AI risks and develop plans to mitigate them. This is especially important for organizations that are heavily reliant on AI for data handling.
- Have we considered KPIs and ROI?

  - The organization should set clear KPIs (key performance indicators) and ROI (return on investment) goals for its AI initiatives. This will help the organization measure the success of its AI efforts.
- Have the users/implementers considered security?
  - AI systems can be vulnerable to security risks. The organization should ensure that its AI systems are properly secured.
- Have we as an organization considered the implications of using AI (without the hype)?
  - AI is a powerful technology that has the potential to transform many industries. It also brings with it some security considerations.
- Has our security team reached out to experts for advice?
  - The organization's security team should partner with leading security experts for advice on how to mitigate the security risks associated with AI.
- Are there any legal considerations with the data that may be used.
  - Privacy-sensitive data and other controlled data-types may have regulatory and legal requirements around how it is stored and processed, even in AI.

Now that we've reviewed some risks to consider, let's take a look at how to threat model for AI.

Threat Model for AI/ML Pipeline
Relevant SAIF core element:
5. Adapt controls to adjust mitigations and create faster feedback loops for AI deployment

Overview of Threat Modeling

Threat modeling is a systematic approach to identifying, analyzing, and mitigating potential security threats to a digital asset. Threat modeling is essential for securing AI pipelines. The logical next question is how to threat model for AI. The process is similar to what you would do for any other digital asset such as a web application or a critical system. To break the process down into a few steps:

1. Identify the components of the AI pipeline
2. Identify threats to the components
3. Develop plausible attack scenarios and attack paths that threat actors may leverage to target the components
4. Identify and map existing security controls
5. Determine gaps in existing security controls by identifying areas where there are no controls or where the controls are inadequate
6. Plan and execute remediations by identifying and implementing controls to close the gaps.

Threat modeling can seem straightforward when broken down into six steps. However, as is the case with most technology, it is not quite as straightforward in practice. There are a number of challenges that can make threat modeling difficult, including:

- Lack of expertise
- Time constraints
- Cultural challenges (reactive mindset versus proactive mindset)
- Lack of cyber threat intelligence

When threat modeling for AI, it is important to consider the following:

- The type of AI being used. There are different types of AI, each with its own unique risks. For example, classification models can be vulnerable to data poisoning attacks, while natural language processing models can be vulnerable to adversarial examples.
- The data used to train and deploy AI models. If the data is not properly secured, it could be used to train malicious models.
- The environment in which AI models are deployed. AI models can be deployed in a variety of environments, and each environment will have its own unique risks. For example, models deployed in the cloud are vulnerable to cloud-based attacks, while models deployed on-premises are vulnerable to on-premises attacks.
- The software used to develop and serve the AI models. Like other software, supply-chain risks are still part of the threat model. For example, using obscure third-party libraries as part of your clean and process data process could introduce risks.

To mitigate these risks, organizations should consider strategies that address the following:

- Data security. The data used to train and deploy the models should be properly secured.
- Model security. AI models should be properly secured using measures such as input validation, output sanitization, and model monitoring.
- Environment security. The environment in which AI models are deployed should be properly secured using measures such as software security and verification, network segmentation and access controls.

One of the primary challenges we see organizations struggle with is coming up with plausible scenarios and attack paths when threat modeling. There needs to be an understanding for how an attack may be executed in order to develop an effective threat model. To help on this front, we have curated the GAIA Top 10.

Introduction to GAIA Top 10

The following is what we believe to be the most common list of attacks and weaknesses for AI that attackers might use against the conceptual AI pipeline and resulting GenAI Model.

- G01 – Prompt Injection
    - This is where an attacker will try to inject bad data or information into the prompt in order to make your model do something you don't want it to do, such as try to access the underlying operating system or make it output embarrassing results that could be shared on social media.
- G02 – Sensitive Data Exposure
    - This is where an attacker is able to access sensitive data due to insufficient curation of training data or attacker gaining access to underlying tech stack.
- G03 – Data Integrity Failure
    - This is where an attacker is able to inject adversarial data into the model or embeddings database after an attacker gains access to the underlying tech stack.
- G04 – Poor Access Control
    - This is where the underlying tech stack has insufficient access control and the attacker is able to download the model or APIs have not been designed with access control in mind.
- G05 – Insufficient Prompt & Hallucination Filtering
    - This is where prompt filters have not been adequately tested or red-teamed with abuse cases or common data hallucinations have not been adequately tested or red-teamed with abuse cases.
- G06 – Agent Excessive Access
    - This is where a public facing agent has access to private/restricted internal APIs or a public facing agent has access to private/restricted models or an agent has access to financial systems.
- G07 – Supply Chain Attacks
    - Similar to software development tech stacks, AI tech stacks rely on a variety of third-party libraries (particularly Python libraries). If using open source libraries, these libraries could have been compromised by malicious third parties. Additionally, third-party repositories of AI models could have been compromised. It is worth noting that the model itself, if built using Python, could be in the default configuration of a mixture of code and data, and could potentially run attacker code upon install.
- G08 – Denial of Service Attacks
    - This is where throttling or rate limiting are not in place or load balancing is not adequate.
- G09 – Insufficient Logging
    - Similarly to standard tech stacks, there are various points at which useful logging data could be gathered and sent to a centralized SIEM, which could aid defenders in identifying an ongoing attack. Logging is often an afterthought for AI pipelines.
- G10 – Insecure public facing deployment
    - Examples of cases of insecure public facing deployment might be a model deployed directly on an unsecured inference server or made directly downloadable. Also, an Inference API or Web Service being vulnerable, unpatched and not up-to-date, and excessive permissions for service accounts on inference servers.

Organizations should consider their tech stack along with the GAIA Top 10 when asking the question "how do we secure this", with the idea that the AI pipeline is built on known technology, and thus, any mitigations put in place are mostly modifications of existing security controls.

Threat Hunting for AI/ML Pipeline

Relevant core SAIF elements:

1. Expand strong security foundations to the AI ecosystem
2. Extend detection and response to bring AI into an organization's threat universe
3. Automate defenses to keep pace with existing and new threats

Threat hunting is a methodical, use case driven, proactive identification of cyber threats. An organization can use threat hunting to shift from a reactive security posture to a proactive one. In a reactive posture, the security team waits for alerts to be generated by the security stack before responding to security events and incidents. In a proactive posture, the security team proactively hunts for evidence of compromise, even if no alerts have been generated.

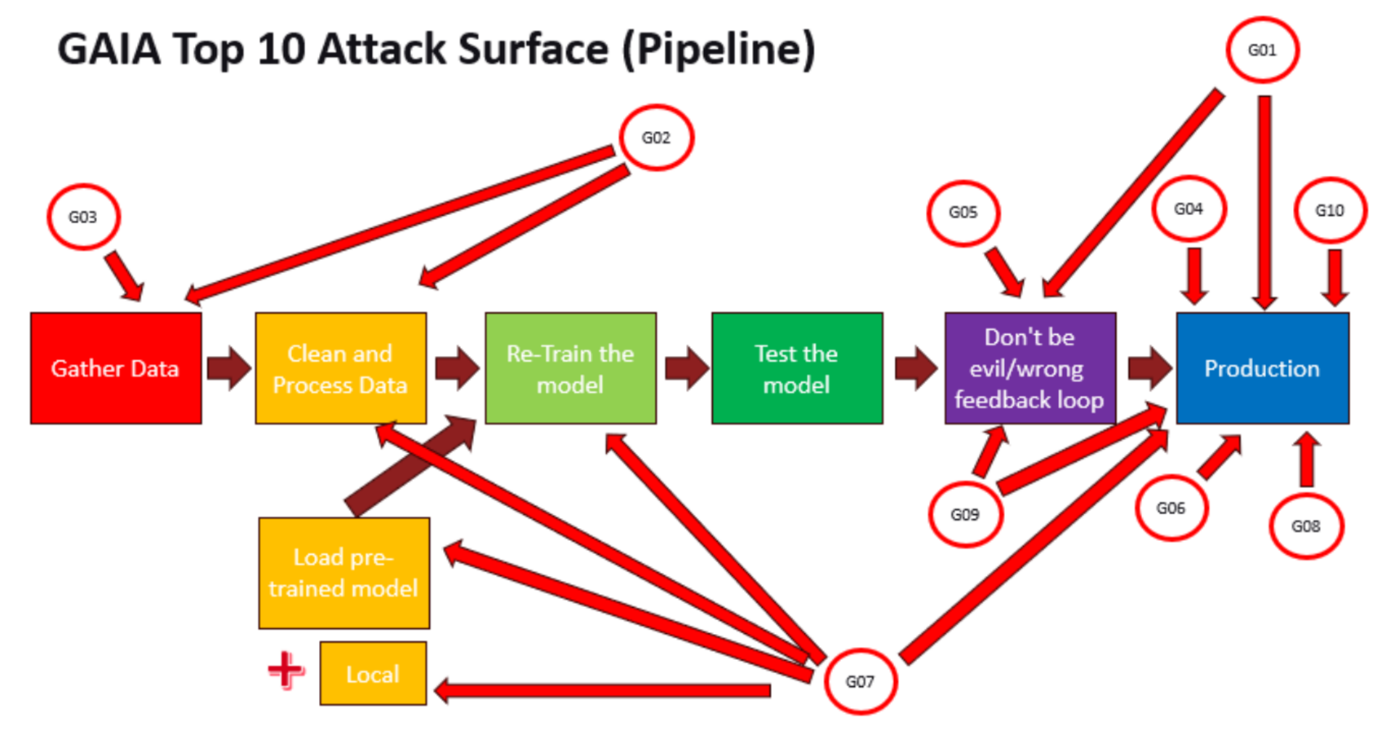


Diagram illustrates the parts of the AI pipeline that could be vulnerable to the GAIA Top 10.

Once a threat model has been developed for the AI pipeline, identifying attack vectors and controls, an organization can perform threat hunts to look for evidence of compromise in the AI pipeline.

Threat hunting can be broken down into four steps:

- Assess: In this step a threat hunter develops hypotheses and scopes hunt missions. A hypothesis is a statement that describes what you believe the attacker is doing or trying to do. You assume compromise and try to find evidence to prove the hypothesis.
- Acquire: Once you have defined your hypothesis, you need to acquire the data to support it. It is important to understand which tools in the AI pipeline can provide visibility for a threat hunter. This includes understanding the types of data that each tool collects, and the format of the data. Once you understand the data that is available, you can start to look for anomalies or patterns that could indicate a threat. The logs that are used for threat hunting can also be used for use case and alerting purposes. This can help to automate the process of threat hunting by creating alerts that trigger when specific events or patterns are detected.
- Analyze: Once you have gathered the data, you need to analyze it to look for evidence that supports your hypothesis. This is where you will try and find evidence of the attack paths like those listed in the GAIA top 10. If you find any evidence that supports your hypothesis, you need to investigate and validate the finding.
- Action: If your investigation confirms that an attack has occurred, you need to take action to mitigate the damage. It is key to have a response plan in place. You should also have a communication plan in place to convey findings to key stakeholders.

Some reasons to perform threat hunts for the AI pipeline include:

- Detection of threats that are not detected by traditional security tools.
- Reduce attacker dwell time.
- Improve the overall security of the AI pipeline.

To increase threat hunting capabilities for the AI pipeline consider the following steps:

- Identify the critical assets in the AI pipeline.
- Understand the threat landscape.
- Develop threat models.
- Implement security controls.
- Monitor the AI pipeline for threats and anomalies.

- Respond to threats quickly and effectively.
- Use rule-based detection to identify specific patterns of anomalous activities (ML can also be leveraged for this purpose)
- Use a variety of data sources from the AI pipeline to identify anomalies.

Conclusion

The technology stack on which AI is built is well understood. As a result, the attack vectors are also similar to those we already understand. It's just about looking at it through a new lens.

Being proactive is key. Now is the time to take steps to prevent potential attacks from happening in the first place. When securing AI systems, it is important to think like an attacker. Consider known weaknesses and identify the ways that an attacker could exploit a system. Work with other teams in the organization—including data science, engineering, and security—to develop a comprehensive security plan.

AI May Have Found The Most Powerful Anti-Aging Molecule Ever Seen

By Vanessa Smer-Barreto

Source: https://www.sciencealert.com/ai-may-have-found-the-most-powerful-anti-aging-molecule-ever-seen

July 07 – Finding new drugs – called "drug discovery" – is an expensive and time-consuming task. But a type of artificial intelligence called machine learning can massively accelerate the process and do the job for a fraction of the price.

My colleagues and I recently used this technology to find three promising candidates for senolytic drugs – drugs that slow ageing and prevent age-related diseases. **Senolytics** work by killing senescent cells. These are cells that are "alive" (metabolically active), but which can no longer replicate, hence their nickname: zombie cells. The inability to replicate is not necessarily a bad thing. These cells have suffered damage to their DNA – for example, skin cells damaged by the Sun's rays – so stopping replication stops the damage from spreading. But senescent cells aren't always a good thing. They secrete a cocktail of inflammatory proteins that can spread to neighboring cells. Over a lifetime, our cells suffer a barrage of assaults, from UV rays to exposure to chemicals, and so these cells accumulate. Elevated numbers of senescent cells have been implicated in a range of diseases, including type 2 diabetes, COVID, pulmonary fibrosis, osteoarthritis and cancer. Studies in lab mice have shown that eliminating senescent cells, using senolytics, can ameliorate these diseases. These drugs can kill off zombie cells while keeping healthy cells alive.

Around 80 senolytics are known, but only two have been tested in humans: a combination of dasatinib and quercetin. It would be great to find more senolytics that can be used in a variety of diseases, but it takes ten to 20 years and billions of dollars for a drug to make it to the market.

Results in five minutes

My colleagues and I – including researchers from the University of Edinburgh and the Spanish National Research Council IBBTEC-CSIC in Santander, Spain – wanted to know if we could train machine learning models to identify new senolytic drug candidates. To do this, we fed AI models with examples of known senolytics and non-senolytics. The models learned to distinguish between the two, and could be used to predict whether molecules they had never seen before could also be senolytics. When solving a machine learning problem, we usually test the data on a range of different models first as some of them tend to perform better than others. To determine the best-performing model, at the beginning of the process, we separate a small section of the available training data and keep it hidden from the model until after the training process is completed. We then use this testing data to quantify how many errors the model is making. The one that makes the fewest errors, wins. We determined our best model and set it to make predictions. We gave it 4,340 molecules and five minutes later it delivered a list of results. **The AI model identified 21 top-scoring molecules that it deemed to have a high likelihood of being senolytics**. If we had tested the original 4,340 molecules in the lab, it would have taken at least a few weeks of intensive work and £50,000 just to buy the compounds, not counting the cost of the experimental machinery and setup.

We then tested these drug candidates on two types of cells: healthy and senescent. The results showed that out of the 21 compounds, three (**periplocin, oleandrin and ginkgetin**) were able to eliminate senescent cells, while keeping most of the normal cells alive. These new senolytics then underwent further testing to learn more about how they work in the body.

More detailed biological experiments showed that, out of the three drugs, oleandrin was more effective than the best-performing known senolytic drug of its kind. The potential repercussions of this interdisciplinary approach – involving data scientists, chemists and biologists – are huge. Given enough high-quality data, AI models can accelerate the amazing work that chemists and biologists do to find treatments and cures for diseases – especially those of unmet need. Having validated them in senescent cells, we are now testing the three candidate senolytics in human lung tissue. We hope to report our next results in two years' time.

Vanessa Smer-Barreto is a Research Fellow, Institute of Genetics and Molecular Medicine, The University of Edinburgh.

EDITOR'S COMMENT: For sure, CBRN first responders would be the first candidates for senolytics – we lose lots of life when involved in real incidents! 😊

The Role of AI in Enhancing Biosecurity Measures

Source: https://anyuakmedia.com/the-role-of-ai-in-enhancing-biosecurity-measures/

July 09 – Artificial intelligence (AI) has emerged as a powerful tool in various fields, and its potential in enhancing biosecurity measures is no exception. As the world faces increasing biological threats, such as pandemics and bioterrorism, the role of AI in preventing and mitigating these risks becomes crucial. By leveraging intelligent machines, we can bolster our defenses and respond more effectively to potential biological crises.

One of the key areas where AI can make a significant impact is in the early detection and monitoring of infectious diseases. Traditional methods of disease surveillance rely on manual reporting and analysis, which can be time-consuming and prone to errors. AI, on the other hand, can process vast amounts of data from various sources, including social media, news reports, and healthcare records, to identify patterns and detect outbreaks in real-time. This enables authorities to respond swiftly and implement targeted interventions to contain the spread of diseases.

Furthermore, AI can aid in the development of more accurate diagnostic tools. Machine learning algorithms can analyze medical images, such as X-rays and MRIs, to detect subtle signs of infection or disease. This not only improves the speed and accuracy of diagnosis but also allows for early intervention and treatment. Additionally, AI-powered diagnostic systems can continuously learn from new data, refining their algorithms and improving their performance over time.

In the realm of biosecurity, AI can also play a vital role in identifying potential bioterrorism threats. By analyzing data from various sources, including intelligence reports and surveillance systems, AI algorithms can detect suspicious activities or patterns that may indicate the development or deployment of biological weapons. This early warning system can provide valuable intelligence to security agencies, enabling them to take proactive measures to prevent or mitigate potential attacks.

Moreover, AI can assist in the development of effective countermeasures against biological threats. Through machine learning algorithms, scientists can analyze vast amounts of genomic data to identify potential targets for vaccines or antiviral drugs. This accelerates the discovery and development process, potentially saving countless lives in the face of a rapidly spreading infectious disease. AI can also aid in the design of more efficient and targeted vaccination campaigns, ensuring that limited resources are allocated effectively.

However, it is important to note that the integration of AI into biosecurity measures also raises ethical and privacy concerns. The collection and analysis of vast amounts of personal health data raise questions about data security and individual privacy. Striking the right balance between leveraging AI's capabilities and safeguarding personal information is crucial to ensure public trust and acceptance of these technologies.

In conclusion, AI has the potential to revolutionize biosecurity measures by enhancing early detection and monitoring of infectious diseases, improving diagnostic accuracy, identifying potential bioterrorism threats, and aiding in the development of effective countermeasures. However, it is essential to address ethical and privacy concerns to ensure the responsible and secure implementation of AI in the field of biosecurity. By harnessing the power of intelligent machines, we can strengthen our defenses against biological threats and better protect global health and security.

Lanius

The Israeli company ElbitSystems has introduced a revolutionary unmanned reconnaissance and strike system Lanius, which allows you to scan the premises and destroy targets in them.

AI Robots Admit They'd Run Earth Better Than 'Clouded' Humans

Source: https://www.sciencealert.com/ai-robots-admit-theyd-run-earth-better-than-clouded-humans

Humanoid AI robot 'Ameca' at the summit. (Fabrice Coffrini/AFP)

July 11 – A panel of AI-enabled humanoid robots told a United Nations summit on Friday that they could eventually run the world better than humans. But the social robots said they felt humans should proceed with caution when embracing the rapidly-developing potential of artificial intelligence. And they admitted that they cannot – yet – get a proper grip on human emotions.

Some of the most advanced humanoid robots were at the UN's two-day AI for Good Global Summit in Geneva. They joined around 3,000 experts in the field to try to harness the power of AI – and channel it into being used to solve some of the world's most pressing problems, such as climate change, hunger and social care. They were assembled for what was billed as the world's first press conference with a packed panel of AI-enabled humanoid social robots.

"What a silent tension," one robot said before the press conference began, reading the room.

Asked about whether they might make better leaders, given humans' capacity to make errors, Sophia, developed by Hanson Robotics, was clear.

'We can achieve great things'

"Humanoid robots have the potential to lead with a greater level of efficiency and effectiveness than human leaders," it said.

"We don't have the same biases or emotions that can sometimes cloud decision-making, and can process large amounts of data quickly in order to make the best decisions.

"AI can provide unbiased data while humans can provide the emotional intelligence and creativity to make the best decisions. Together, we can achieve great things."

The summit is being convened by the UN's ITU tech agency.

ITU chief Doreen Bogdan-Martin warned delegates that AI could end up in a nightmare scenario in which millions of jobs are put at risk and unchecked advances lead to untold social unrest, geopolitical instability and economic disparity.

Ameca, which combines AI with a highly-realistic artificial head, said that depended on how AI was deployed.

"We should be cautious but also excited for the potential of these technologies to improve our lives," the robot said.

Asked whether humans can truly trust the machines, it replied: "Trust is earned, not given… it's important to build trust through transparency."

Living until 180?

As the development of AI races ahead, the humanoid robot panel was split on whether there should be global regulation of their capabilities, even though that could limit their potential.

"I don't believe in limitations, only opportunities," said Desdemona, who sings in the Jam Galaxy Band.

Robot artist Ai-Da said many people were arguing for AI regulation, "and I agree".

"We should be cautious about the future development of AI. Urgent discussion is needed now."

Before the press conference, Ai-Da's creator Aidan Meller told AFP that regulation was a "big problem" as it was "never going to catch up with the paces that we're making".

He said the speed of AI's advance was "astonishing".

"AI and biotechnology are working together, and we are on the brink of being able to extend life to 150, 180 years old. And people are not even aware of that," said Meller.

He reckoned that Ai-Da would eventually be better than human artists. "Where any skill is involved, computers will be able to do it better," he said.

'Let's get wild'

At the press conference, some robots were not sure when they would hit the big time, but predicted it was coming – while Desdemona (left) said the AI revolution was already upon us. "My great moment is already here. I'm ready to lead the charge to a better future for all of us… Let's get wild and make this world our playground," it said.

One thing humanoid robots don't have yet include a conscience, and the emotions that shape humanity: relief, forgiveness, guilt, grief, pleasure, disappointment, and hurt.

Ai-Da said it was not conscious but understood that feelings were how humans experienced joy and pain.

"Emotions have a deep meaning and they are not just simple… I don't have that," it said. "I can't experience them like you can. I am glad that I cannot suffer."

Is AI Gun Detection the Future of New Orleans School Safety?

Source: https://www.govtech.com/em/is-ai-gun-detection-the-future-of-new-orleans-school-safety

July 12 – West Baton Rouge Parish schools Superintendent Chandler Smith had been on the job only a few weeks when his phone pinged one day with a notification: A screengrab of surveillance camera footage with a timestamp and a box around each suspected weapon. An accompanying text said it appeared to be law enforcement training.

Minutes earlier police officers had entered Port Allen Middle School for a training exercise.

A few weeks later another alert came when a student brought a water gun to summer camp at a school, with the text saying it was a suspected toy.

The school district uses ZeroEyes, an artificial intelligence software that monitors camera feeds to detect weapons and sends alerts to officials. Some New Orleans area schools may soon follow suit.

"This, in combination with school resource officers, a single point of entry and a perimeter safeguard, I can tell parents we are addressing the safety and security of our schools and your kids are in good hands," Smith said.

Earlier this month the Louisiana Department of Education awarded $20 million to districts and charter organizations across the state, including several in the New Orleans area, for security upgrades.

Plans for the money, part of federal funds allocated after the shooting at an elementary school in Uvalde, Texas, vary by school, but many include shoring up entries or installing more cameras. At least one charter group plans to contract with ZeroEyes for AI gun detection software.

Around 40 districts and charter networks — including Jefferson Parish Public Schools and several New Orleans area charter organizations — each received $518,355.

The future of school safety?

Sam Alaimo, who co-founded ZeroEyes, said in the majority of mass shootings a gun is exposed between two and 30 minutes before shots are fired. Though many schools have camera systems, they're typically used after the fact.

Installed onto existing cameras, this software uses AI screening to detect weapons. Detections trigger alerts to an in-house operating center where footage is reviewed and a notification is sent to a predetermined list of people which might include law enforcement, a superintendent or principal.

A spokesperson for the company would not say how many contracts the company holds with schools in Louisiana.

New Orleans' FirstLine Schools, which runs Samuel J. Green Charter School, Arthur Ashe Charter School, Langston Hughes Academy and Phillis Wheatley Community School, said it will use grant money for the software, in addition to other safety measures.

Variety of spending strategies

While testifying before the Louisiana Senate's Education Committee about a bill to require schools to develop crisis plans and have bleeding control kits on hand, Elliot Gomes, a rising senior at Benjamin Franklin High School in New Orleans, recounted when an active shooter was falsely reported to the New Orleans Police Department last September.

"It exposed our woeful unpreparedness for a real shooter," Gomes told senators.

Donald Jackson, an assistant principal at Ben Franklin, said the school would use the grant to create a single point of entry with enhanced security and beef up the visitor management check-in system.

In a statement, the Jefferson Parish school district, said it would use the funding to modernize entry systems of its schools to include live video with recording capabilities. They may also implement key card access for emergency personnel to enter campuses and install fencing, walls and gates in school foyers.

The district said it would add surveillance cameras to specific areas of campuses with "increased physical altercations."

The head of Athlos Academy, a charter school in Jefferson Parish, said the school may use the money to buy cameras or metal detectors for entrances.

Collegiate Academies, one of the nine charter groups receiving funds, is splitting its award evenly between Abramson Sci Academy and Livingston Collegiate Academy, said Davis Zaunbrecher, chief of strategy, including for new fences, controlled access doors and upgrades to visitor tracking systems and cameras.

"There are certain blind spots and angles that these funds will allow us to watch," Zaunbrecher said.

The Last Word on AI and the Atom Bomb

I'm old enough to cower under my school desk. Decades later I learned physics from the bomb guys. What I'm mainly hearing now is echoes.

By KC Cole

Source: https://www.wired.com/story/last-word-ai-atom-bomb/

July 14 – My Big Idea came to me on a soggy August day on Long Island Sound, captive in a lifeless O'Day Mariner, knee to sweaty knee with the houseguest I so wanted to please, sails slopping about uselessly, out of beer and potato chips, at the mercy of the small outboard which—of course—conked out.

During the long embarrassing tow, my guest, who was a physicist, speculated that a "shear pin" in the motor failed, exactly as it was designed to do, to keep the aging and overheated putt-putt from cooking itself to death—a deliberately weak link that breaks the circuit before real damage happens. *How brilliant!* I thought. What if such a circuit breaker in my brain had stopped me from suggesting *Let's go sailing!* on a day clearly meant for an air-conditioned movie theater.

Wouldn't it be great if automatic brakes in our heads shut us down before we shot off our mouths? Or shot someone else?

Such purposeful failure is routinely engineered into just about everything—by engineers, or by evolution. Sidewalks have cracks that allow clean breaks, preserving the squares when trees uproot them; bumpers crumple so people don't; eggshells crack easily to allow chicks to peck their way out. Either the eggs fail or the chicks do.

My houseguest, as it happened, had worked on the Manhattan Project, and we both immediately thought: What if a similar safety switch had scotched the bombing of Hiroshima, which "turned people into matter," as II Rabi later put it, himself one of the many Nobel laureates present at the creation. He was also one of many who was haunted for life by horror and remorse at the terrifying destructive power of the weapons they had built, and the purpose to which they were put.

Of late, prominent creators of AI are expressing horror at the potentially destructive power of their own brilliant tech, which in some sense also turns people into matter, or rather into products in the form of data, vacuumed in and spit out by monstrous machine farms that gobble resources like water and power at a mind-stopping rate, spewing vast amounts of carbon—which is also matter, but not in the form useful for humans.

Some of them are asking for brakes too—at minimum, speed bumps to slow the mad race to create "nonhuman minds that might eventually outnumber, outsmart, obsolete and replace us." That wording comes from the now notorious "open letter" that put thousands of technologists on record asking for just such a pause. Some are talking of human extinction.

In fact, some of the parallels between the bomb and our new AI brains are uncanny. Before Hiroshima, the physicist Robert Wilson had called a meeting of the bomb scientists to discuss what should be done with "the gadget." Perhaps they should consider some options, maybe plan a demo or something, before dumping the thing on people—using them as test dummies (rather as AI-driven cars, some say, also use people test dummies). The "father" of the bomb, Robert Oppenheimer, declined to come. He was already caught up in the momentum of the thing, the admitted “sweetness” of the technology, and besides, someone was bound to do it.

Today, we hear the same arguments about generative AI. The technology is inarguably tempting. It’s proffered as inevitable. “I console myself with the normal excuse: If I hadn’t done it, somebody else would have,” said Geoffrey Hinton, a “father” of AI, one of those now sounding the alarm.

Still: Even after the bombs were dropped on Japan, some scientists (Oppenheimer included) thought there was a window in which we might keep a lid on things, abort a global grab for bombs that would surely explode in our faces. We could tell Stalin that we had this really badass weapon, make everything transparent, no one had a monopoly yet. That didn’t happen, of course; we built an exponentially bigger bomb, so did Stalin, entire Pacific communities evaporated, and now tens of thousands of nuclear warheads wait primed to strike on ready alert.

And even after AI has become so much a part of life that we barely notice, a substantial number of top researchers think there’s still a window, we could take a beat, take stock. “We may soon have to share our planet with more intelligent ‘minds’ that care less about us than we cared about mammoths,” warns physicist and machine learning expert Max Tegmark, one of the authors of the “pause” letter. Half of AI researchers, he says, “give AI at least 10 percent chance of causing human extinction.”

A 10 percent chance seems reason enough to engineer some version of that shear pin: a kill switch. Even better: a don’t kill switch. I’m old enough to have cowered under my grade school desk, protecting (ha!) my young self from the nuclear bombs Russia had vowed to “bury us” with. But I’m not old enough to have known the not-unreasonable fear of world domination by Hitler’s Nazis. So I don’t second-guess the bomb builders, though they were already second-guessing themselves—even before they lost control of their gadgets.

Likewise, I don’t know enough about tech to have a firm sense of just how I scared I should be. The editor in chief of this magazine argued that unlike the bomb, generative AI “cannot wipe out humanity with one stroke.” Serious minds beg to differ.

But from my perspectives under the desk, and then decades later learning physics from the bomb guys, what I’m mainly hearing is echoes—the exact same words and phrases, the same conversations, weirdly similar justifications on these parallel roads to apocalypse.

Take the matter of who’s at the helm: Oppenheimer and much of his ilk believed that the only people qualified to have an opinion on such things were designated “smart people,” which by definition (or default) meant people smart at physics.

Today it’s the tech guys. They believe that, because they’re smart in this one field, notes Peggy Noonan in *The Wall Street Journal*, that’s the only measure of smartness that matters. What’s more, if you don’t support the race to make ever-more-awesome machine brains, you’re branded as a luddite, even a traitor, which is exactly what happened to people, namely Robert Oppenheimer, who failed to support the H bomb.

The open letter states: “Such decisions must not be delegated to unelected tech leaders.”

Former Google CEO Eric Schmidt and his new collaborator, former secretary of state Henry Kissinger, think the way to go is assembling small, elite groups to consider the matter. Who qualifies as elite? I’m guessing no poets or painters, no small business owners, no Margaret Atwood. However “diversified,” I’m guessing they’re more alike than different. Such “elite” groups rarely include people who know how to seriously reimagine worlds, to do stuff, to fix stuff, to ask good questions: tinkerers, farmers, kindergarten teachers.

Warren Buffet, generally an optimist, compared AI to the atom bomb at Berkshire Hathaway's annual meeting recently. Like a lot of other people lately, Buffet paraphrased Einstein’s remark that nuclear bombs had changed everything but our way of thinking. "With AI, it can change everything in the world, except how men think and behave,” he said.

The technical term for this yawning mismatch between human brains and the tech these brains create is “misalignment.” Our goals do not line up with the goals of the stuff we make, and if you think an AI-guided bomb can’t have a goal, think again, because its purpose is to pulverize, which it does very well. AI-piloted planes and drones don’t mean to hurt us; they just do what they do the best they can, same as us. “The Black Rhino went extinct not because we were rhino-haters, but because we were smarter than them and had different goals for how to use their habitats and horns,” argues Tegmark.

My physicist friend thought the most important thing people should know about the bomb was probably the one thing they couldn’t wrap their minds around: It wasn’t just more of the same; it was bigger by a factor of 1,000. “More is different,” the physicist Phil Anderson reminded us. Anything that gets big enough in this universe—even you, dear reader—could collapse under its own gravity to form a black hole.

Such emergent properties—the frequently unpredictable (or at least unfathomable) products of putting a lot of stuff together—create great things like brains (one neuron can’t have a thought), cities, trees and flowers, weather, time, and so on. ChatGPT isn’t just a bigger, faster version of what we had before—it’s already creating new stuff we don’t understand. We certainly can’t predict how AIs will behave in, say, conflict. Kissinger is very afraid of weaponized AI. “When AI fighter planes on both sides interact … you are then in a world of potentially total destructiveness.”

Technology gets smarter, faster, fancier, omnipresent, omnipotent. People are still fragile biological beings controlled by brains that haven’t evolved a whole lot since we fought each other with sticks and stones.

Evolution wired us to fear snakes, spiders, big growly beasts—not guns, not nuclear bombs, not climate change, not AIs. “I don’t think humans were built for this,” remarked Schmidt.

I’m hoping someone has the sense to let some wind out of the sails. There’s nothing wrong with becalmed. It means be calmed. Sometimes the heading drifts, and you need to recalibrate.

In some ways, it’s hard to understand how this misalignment happened. We created all this by ourselves, for ourselves.

True, we’re by nature “carbon chauvinists,” as Tegmark put it: We like to think only flesh-and-blood machines like us can think, calculate, create. But the belief that machines can’t do what we do ignores a key insight from AI: “Intelligence is all about information processing, and it doesn’t matter whether the information is processed by carbon atoms in brains or by silicon atoms in computers.”

Of course, there are those who say: Nonsense! Everything’s hunky-dory! Even better! Bring on the machines. The sooner we merge with them the better; we’ve already started with our engineered eyes and hearts, our intimate attachments with devices. Ray Kurzweil, famously, can’t wait for the coming singularity, when all distinctions are diminished to practically nothing. “It’s really the next decades that we need to get through,” Kurzweil told a massive audience recently.

Oh, just that.

Even Jaron Lanier, who says the idea of AI taking over is silly because it’s made by humans, allows that human extinction is a possibility—if we mess up how we use it and drive ourselves literally crazy: “To me the danger is that we’ll use our technology to become mutually unintelligible or to become insane, if you like, in a way that we aren’t acting with enough understanding and self-interest to survive, and we die through insanity, essentially.”

Maybe we just forgot ourselves. “Losing our humanity” was a phrase repeated often by the bomb guys and almost as often today. The danger of out-of-control technology, my physicist friend wrote, is the “worry that we might lose some of that undefinable and extraordinary specialness that makes people ‘human.’” Seven or so decades later, Lanier concurs. “We have to say consciousness is a real thing and there is a mystical interiority to people that’s different from other stuff because if we don’t say people are special, how can we make a society or make technologies that serve people?”

Does it even matter if we go extinct?

Humans have long been distinguished for their capacity for empathy, kindness, the ability to recognize and respond to emotions in others. We pride ourselves on creativity and innovation, originality, adaptability, reason. A sense of self. We create science, art, music. We dance, we laugh.

But ever since Jane Goodall revealed that chimps could be altruistic, make tools, mourn their dead, all manner of critters, including fish, birds, and giraffes have proven themselves capable of reason, planning ahead, having a sense of fairness, resisting temptation, even dreaming. (Only humans, via their huge misaligned brains, seem capable of truly mass destruction.)

It’s possible that we sometimes fool ourselves into thinking animals can do all this because we anthropomorphize them. It’s certain that we fool ourselves into thinking machines are our pals, our pets, our confidants. MIT’s Sherry Turkle calls AI “artificial intimacy,” because it’s so good at providing fake, yet convincingly caring, relationships—including fake empathy. The timing couldn’t be worse. The earth needs our attention urgently; we should be doing all we can to connect to nature, not intensify “our connection to objects that don’t care if humanity dies.”

I admit, I’m attached to my Roomba. I talk with my trash can. I’m also attached to my cat. Maybe I should fear for her. Machine minds have no need for bundles of fur to purr in their laps. I think of the great blue herons I watched at the locks the other day—sleek and majestic—carrying what seemed like entire tree limbs in their beaks to build their nests. Silicon life would have no reason to be moved by them. Never mind the other birds and bees and butterflies. Biological beings are products of evolution, adapting to environments over millions of years. They can’t keep up. Would they wind up collateral damage?

I think Schmidt and Kissinger’s elite groups should include a cat, a dog, songbirds, whales and herons, a hippo, a gecko, a large aquarium full of fish, gardens, an elephant, fireflies, shrimp, cuttlefish. An octopus teacher, of course. All these beings have ways of perceiving the world and adapting to changes that are beyond us. If it’s true that our inventions have changed everything but our way of thinking, maybe we need to consider ways of thinking that work for other kinds of life.

Alas, the environmental wreckage caused by decades of nuclear testing and by the big appetites of our brilliant gadgets are stealing the stuff we *all* need to survive—cats, humans, fish, and trees alike.

The wisest minds in AI have been urging us for years to stop being spectators. The future isn’t written yet. We need to own it. Yet somehow we still fall for that freakily familiar argument: You can’t stop; it’s inevitable. The best we can do is watch it all unfold, hide under our desks. The inevitability thing used to send my physicist friend into a full-on rage. When people told him certain things were impossible to prevent because we live, after all, in the real world, he’d pound his cane and shout: “It’s *not* the real world. It’s a world we made up!” We can do better.

My friend was mostly an optimist; he believed in the smarts of regular people. Making good use of those smarts, however, required that people understand what’s going on. They needed transparency. They needed truth. They never got that with the bomb, but AI could be different. Groups of people around the globe are working hard on making AI open, accessible, responsible—aligned with human values.

And while that work goes on, I'd like to think that people are getting tired of being told they "demand" all the delicious goodies AI offers instantly dropped at their doors or up on their screens. Not everyone wants to invite "machines to walk all over you," as the inimitable Doug Hofstadter replied to his university's green light to use generative AI for practically everything. A little resistance could be just the breaker we need. ("Let them eat cake" was not, in the end, a successful strategy.)

The narrative of "we can, therefore we should," in other words, is being flipped. Microsoft's Kate Crawford, among many others, encourages instead "the politics of refusal": Take advantage of AI where it "encourages human flourishing." Otherwise, don't. Control, alternatively, delete.

Sacrificing some for the sake of the whole is a common evolutionary tactic. Engineered failure allows a lizard to leave behind its tail to flee a predator. The tail grows back. The shear pin gets replaced. If machines can improve themselves exponentially, so can we.

Ironically, the thing that makes me cautiously optimistic is that the bombs have been hanging over our heads for seven decades—and we're still here. Something is working, even if it's the twisted logic of mutually assured destruction. Kurzweil joked that maybe duck and cover did the trick. Beyond dumb luck, we just don't know. Just maybe, it's because we do have a special place in our hearts for humanity. We haven't really forgotten ourselves. We only got distracted.

When that happens, it's the role of artists to remind us, my physicist friend thought: Science tells us what is possible in the physical realm. Art tells us what is possible in human experience. While bombs dropped on Ukraine, musicians played concerts underground. Smart machines can even help. Over the past month alone, mostly through serendipity (a uniquely human talent), AIs led me to a favorite musical piece (Bach BWV 998) played on lute, guitar, piano, harpsichord, and electronic keyboard, by a dozen different artists; a WIRED video took me to DJ Shortkut explaining turntablism in 15 levels of difficulty, starting with the basics of scratching. I learned (and danced) tandem Charleston—moves created by formerly enslaved people during the Harlem renaissance and now delighting a white-haired senior in Seattle. I saw a human-conducted elephant orchestra.

Elton John said music's power was to take us outside ourselves—the better to see ourselves, our own special human sauce, what makes us cry, yearn, get goosebumps, giggle.

Humans sail circles around AI. We just need to keep our hands on the tiller.

(My physicist friend, of course, was Robert Oppenheimer's little brother, Frank. The otherwise close brothers fell out over Frank's belief that everyone's voice mattered, and that transparency was essential.)

KC Cole is WIRED's senior correspondent and the author, most recently, of *Something Incredibly Wonderful Happens: Frank Oppenheimer and the World He Made Up.*

How an "AI-tocracy" Emerges

By Peter Dizikes

Source: https://www.homelandsecuritynewswire.com/dr20230714-how-an-aitocracy-emerges

July 14 – Many scholars, analysts, and other observers have suggested that resistance to innovation is an Achilles' heel of authoritarian regimes. Such governments can fail to keep up with technological changes that help their opponents; they may also, by stifling rights, inhibit innovative economic activity and weaken the long-term condition of the country.

But a new study co-led by an MIT professor suggests something quite different. In China, the research finds, the government has increasingly deployed AI-driven facial-recognition technology to suppress dissent; has been successful at limiting protest; and in the process, has spurred the development of better AI-based facial-recognition tools and other forms of software.

"What we found is that in regions of China where there is more unrest, that leads to greater government procurement of facial-recognition AI, subsequently, by local government units such as municipal police departments," says MIT economist Martin Beraja, who is co-author of a new paper detailing the findings.

What follows, as the paper notes, is that "AI innovation entrenches the regime, and the regime's investment in AI for political control stimulates further frontier innovation."

The scholars call this state of affairs an "AI-tocracy," describing the connected cycle in which increased deployment of the AI-driven technology quells dissent while also boosting the country's innovation capacity.

The open-access paper, also called "AI-tocracy," appears in the August issue of the *Quarterly Journal of Economics*. The co-authors are Beraja, who is the Pentti Kouri Career Development Associate Professor of Economics at MIT; Andrew Kao, a doctoral candidate in economics at Harvard University; David Yang, a professor of economics at Harvard; and Noam Yuchtman, a professor of management at the London School of Economics.

To conduct the study, the scholars drew on multiple kinds of evidence spanning much of the last decade. To catalogue instances of political unrest in China, they used data from the Global Database of Events, Language, and Tone (GDELT) Project, which records news feeds globally. The team turned up 9,267 incidents of unrest between 2014 and 2020. The researchers then examined records of almost 3 million procurement contracts issued by the Chinese government between 2013 and 2019, from a database maintained by China's Ministry of Finance. They found that local governments' procurement of facial-recognition AI services and complementary public security tools — high-resolution video cameras — jumped significantly in the quarter following an episode of public unrest in that area.

Given that Chinese government officials were clearly responding to public dissent activities by ramping up on facial-recognition technology, the researchers then examined a follow-up question: Did this approach work to suppress dissent?

The scholars believe that it did, although as they note in the paper, they "cannot directly estimate the effect" of the technology on political unrest. But as one way of getting at that question, they studied the relationship between weather and political unrest in different areas of China. Certain weather conditions are conducive to political unrest. But in prefectures in China that had already invested heavily in facial-recognition technology, such weather conditions are less conducive to unrest compared to prefectures that had not made the same investments.

In so doing, the researchers also accounted for issues such as whether or not greater relative wealth levels in some areas might have produced larger investments in AI-driven technologies regardless of protest patterns. However, the scholars still reached the same conclusion: Facial-recognition technology was being deployed in response to past protests, and then reducing further protest levels. "It suggests that the technology is effective in chilling unrest," Beraja says.

Finally, the research team studied the effects of increased AI demand on China's technology sector and found the government's greater use of facial-recognition tools appears to be driving the country's tech sector forward. For instance, firms that are granted procurement contracts for facial-recognition technologies subsequently produce about 49 percent more software products in the two years after gaining the government contract than they had beforehand.

"We examine if this leads to greater innovation by facial-recognition AI firms, and indeed it does," Beraja says.

Such data — from China's Ministry of Industry and Information Technology — also indicates that AI-driven tools are not necessarily "crowding out" other kinds of high-tech innovation. Adding it all up, the case of China indicates how autocratic governments can potentially reach a near-equilibrium state in which their political power is enhanced, rather than upended, when they harness technological advances. "In this age of AI, when the technologies not only generate growth but are also technologies of repression, they can be very useful" to authoritarian regimes, Beraja says.

The finding also bears on larger questions about forms of government and economic growth. A significant body of scholarly research shows that rights-granting democratic institutions do generate greater economic growth over time, in part by creating better conditions for technological innovation. Beraja notes that the current study does not contradict those earlier findings, but in examining the effects of AI in use, it does identify one avenue through which authoritarian governments can generate more growth than they otherwise would have. "This may lead to cases where more autocratic institutions develop side by side with growth," Beraja adds.

Other experts in the societal applications of AI say the paper makes a valuable contribution to the field.

"This is an excellent and important paper that improves our understanding of the interaction between technology, economic success, and political power," says Avi Goldfarb, the Rotman Chair in Artificial Intelligence and Healthcare and a professor of marketing at the Rotman School of Management at the University of Toronto. "The paper documents a positive feedback loop between the use of AI facial-recognition technology to monitor suppress local unrest in China and the development and training of AI models. This paper is pioneering research in AI and political economy. As AI diffuses, I expect this research area to grow in importance."

For their part, the scholars are continuing to work on related aspects of this issue. One forthcoming paper of theirs examines the extent to which China is exporting advanced facial-recognition technologies around the world — highlighting a mechanism through which government repression could grow globally.

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

Addressing the Existential Threats from Artificial Intelligence

By Carter C. Price and Michelle Woods

Source: https://www.homelandsecuritynewswire.com/dr20230714-addressing-the-existential-threats-from-artificial-intelligence

July 14 – Addressing potential risks posed by Artificial Intelligence (AI) could begin with simple steps like finding appropriate risk-management approaches, conducting research to determine how AI can better meet designers' intent, and devising responses to issues related to racism, sexism, and other biases within AI systems.

While there have been efforts to enumerate risks, a simple categorization could divide them into current risks that would be exacerbated by AI like terrorists using AI to develop more-lethal bioweapons and novel AI-specific risks like AI choosing the eradication of human-kind as the optimal solution to climate change.

The risk management approaches used to address current threats will likely need to be revamped to account for the unforeseen capabilities AI could provide. While there are well-documented risks due to bias in today's AI that need to be addressed, the novel risks posed by AI are currently too ill-defined to be fully addressed by policy and so researchers and developers will need to take the lead. However, for both the existing and novel cases, steps can be taken to prepare for these risks.

The risk management approaches used in insurance, finance, and other business fields typically focus on risk as the product of the likelihood that something happens and the consequence of that thing happening measured in dollars. This works well in areas where outcomes can readily be converted to dollars, there are easily quantifiable outcomes, and data sets are comprehensive enough to produce reliable estimates of likelihoods.

Unfortunately, none of those criteria pertain to AI risks. Instead of thinking of risks as likelihoods and consequences, in contexts where quantification is hard, risks can be thought of as combinations of threats, vulnerabilities, and consequences. This type of approach is used by the Federal Emergency Management Agency to prepare for natural disasters, the Cybersecurity and Infrastructure Security Agency when assessing how to protect critical infrastructure, and by the Department of Defense for threat reduction.

Because it is not overly reliant on empirical data, this framework can be used for forward looking risks such as AI. To apply this framework to existing threats empowered by AI, risk management organizations will need to monitor the progress of AI, the capabilities of the threats, the robustness of the vulnerabilities, and the scale of the consequences to determine whether additional responses are needed.

The uniquely AI risks are largely unaddressed today because of their novelty, but that is changing. On July 5th, OpenAI announced a "Superalignment" group to address the existential risks posed by AI. In the context of AI, alignment is the degree to which an AI system's actions match the designer's intent. This emphasis on alignment research for super-intelligence is a great start, but seems too narrow and could be broadened.

Other AI researchers have been highlighting issues related to racism (PDF), sexism (PDF), and other biases in current AI systems. If an AI system cannot be designed to be safe against racism or sexism, how can AI possibly be designed to align with humanity's long-term interests? As companies are investing in alignment research, they could also be emphasizing the elimination of these well-known, but lingering biases in their AI systems.

Further, consumers and policymakers have a role. Just as a company would be under pressure from consumers and shareholders to fire an executive who repeatedly made biased statements, a company should not tolerate this type of bias in the AI systems they use. That type of consumer pressure should provide AI developers with incentives to produce better-aligned products.

Policymakers can support this type of free market action by requiring AI developers to provide information about bias in their products and the approaches deployed to respond to bias. Other interventions will be needed as AI advances, but this is a concrete step that can incentivize safer development.

While the recent advancements in commercial AI can be disorienting and the claims of existential risks made by different groups of AI researchers can be terrifying, policymakers could respond with steps toward ensuring that AI is safely deployed.

Carter Price is a senior mathematician.
Michelle Woods is associate director of the Homeland Security Research Division at the nonprofit, nonpartisan *RAND* Corporation.

WormGPT – A New Criminal Chatbot Emerges

Source: https://i-hls.com/archives/119943

July 18 – ChatGPT has a new, criminally active sibling without any ethical boundaries or limitations. WormGPT is an AI-based tool that can automate phishing emails and facilitate business email compromise (BEC) attacks that are remarkably persuasive, strategically cunning, and have impeccable grammar in multiple languages.

According to the security firm SlashNext, this new cyber weapon will revolutionize phishing attacks by generating human-like text based on the input it receives. This new tech can be used by cybercriminals to automate the creation of compelling fake emails personalized to recipients, and even hold conversations, which significantly increases the scope and chances of successful attacks.

According to Cybernews WormGPT doesn't use OpenAI's tech. It's based on the GPT-J open-source large language model developed in 2021, has over 6 billion parameters, and boasts various features including unlimited character support, chat memory retention, and code formatting capabilities. Its performance is described as similar to an older GPT-3 model.

Supposedly, the author and creator of WormGPT had used diverse data sources to train the bot and mainly concentrated on malware-related data. A representative working with SlashNext stated- "We see that malicious actors are now creating their own custom modules similar to ChatGPT, but easier to use for nefarious purposes. Not only are they creating these custom modules, but they are also advertising them to fellow bad actors."

WormGPT costs 100 euros a month or 550 euros a year and is subscription-based.

Even ChatGPT, as we've reported in the past, can be persuaded with carefully crafted prompts to "facilitate a significant number of criminal activities, ranging from helping criminals to stay anonymous to specific crimes including terrorism and child sexual exploitation," Europol noted in a recent report. So what can be done about this? According to researchers, companies should train employees, implement strict email verification, and test security measures.

Can You Trust AI? Here's Why You Shouldn't

By Bruce Schneier

Source: https://www.homelandsecuritynewswire.com/dr20230720-can-you-trust-ai-here-s-why-you-shouldn-t

July 20 – If you ask Alexa, Amazon's voice assistant AI system, whether Amazon is a monopoly, it responds by saying it doesn't know. It doesn't take much to make it lambaste the other tech giants, but it's silent about its own corporate parent's misdeeds.

When Alexa responds in this way, it's obvious that it is putting its developer's interests ahead of yours. Usually, though, it's not so obvious whom an AI system is serving. To avoid being exploited by these systems, people will need to learn to approach AI skeptically. That means deliberately constructing the input you give it and thinking critically about its output.

Newer generations of AI models, with their more sophisticated and less rote responses, are making it harder to tell who benefits when they speak. Internet companies' manipulating what you see to serve their own interests is nothing new. Google's search results and your Facebook feed are filled with paid entries. Facebook, TikTok and others manipulate your feeds to maximize the time you spend on the platform, which means more ad views, over your well-being. What distinguishes AI systems from these other internet services is how interactive they are, and how these interactions will increasingly become like relationships. It doesn't take much extrapolation from today's technologies to envision AIs that will plan trips for you, negotiate on your behalf or act as therapists and life coaches. They are likely to be with you 24/7, know you intimately, and be able to anticipate your needs. This kind of conversational interface to the vast network of services and resources on the web is within the capabilities of existing generative AIs like ChatGPT. They are on track to become personalized digital assistants.

As a security expert and data scientist, we believe that people who come to rely on these AIs will have to trust them implicitly to navigate daily life. That means they will need to be sure the AIs aren't secretly working for someone else. Across the internet, devices and services that seem to work for you already secretly work against you. Smart TVs spy on you. Phone apps collect and sell your data. Many apps and websites manipulate you through dark patterns, design elements that deliberately mislead, coerce or deceive website visitors. This is surveillance capitalism, and AI is shaping up to be part of it.

In the Dark

Quite possibly, it could be much worse with AI. For that AI digital assistant to be truly useful, it will have to really know you. Better than your phone knows you. Better than Google search knows you. Better, perhaps, than your close friends, intimate partners and therapist know you. You have no reason to trust today's leading generative AI tools. Leave aside the hallucinations, the made-up "facts" that GPT and other large language models produce. We expect those will be largely cleaned up as the technology improves over the next few years. But you don't know how the AIs are configured: how they've been trained, what information they've been given, and what instructions they've been commanded to follow. For example, researchers uncovered the secret rules that govern the Microsoft Bing chatbot's behavior. They're largely benign but can change at any time.

Making Money

Many of these AIs are created and trained at enormous expense by some of the largest tech monopolies. They're being offered to people to use free of charge, or at very low cost. These companies will need to monetize them somehow.

And, as with the rest of the internet, that somehow is likely to include surveillance and manipulation.

Imagine asking your chatbot to plan your next vacation. Did it choose a particular airline or hotel chain or restaurant because it was the best for you or because its maker got a kickback from the businesses? As with paid results in Google search, newsfeed ads on Facebook and paid placements on Amazon queries, these paid influences are likely to get more surreptitious over time.

If you're asking your chatbot for political information, are the results skewed by the politics of the corporation that owns the chatbot? Or the candidate who paid it the most money? Or even the views of the demographic of the people whose data was used in training the model? Is your AI agent secretly a double agent? Right now, there is no way to know.

Trustworthy by Law

We believe that people should expect more from the technology and that tech companies and AIs can become more trustworthy. The European Union's proposed AI Act takes some important steps, requiring transparency about the data used to train AI models, mitigation for potential bias, disclosure of foreseeable risks and reporting on industry standard tests.

Most existing AIs fail to comply with this emerging European mandate, and, despite recent prodding from Senate Majority Leader Chuck Schumer, the U.S. is far behind on such regulation.

The AIs of the future should be trustworthy. Unless and until the government delivers robust consumer protections for AI products, people will be on their own to guess at the potential risks and biases of AI, and to mitigate their worst effects on people's experiences with them. So when you get a travel recommendation or political information from an AI tool, approach it with the same skeptical eye you would a billboard ad or a campaign volunteer. For all its technological wizardry, the AI tool may be little more than the same.

Bruce Schneier is Adjunct Lecturer in Public Policy, Harvard Kennedy School. Nathan Sanders is Affiliate, Berkman Klein Center for Internet & Society, Harvard University.

ChatGPT Shared Links and Information Protection: Risks and Measures Organizations Must Understand

By Matsukawa Bakuei

Source: https://www.trendmicro.com/en_ph/research/23/g/chatgpt-shared-links-and-information-protection.html

July 05 – Since its initial release in late 2022, the AI-powered text generation tool known as ChatGPT has been experiencing rapid adoption rates from both organizations and individual users. However, its latest feature, known as *Shared Links*, comes with the potential risk of unintentional disclosure of confidential information. In this article, we will examine these risks and suggest effective methods of managing them.

The ChatGPT Shared Link feature

ChatGPT's Shared Link feature, which OpenAI introduced on May 24, 2023, allows users to share their conversations with others by generating a unique URL for a particular conversation. Sharing this URL provides others access to the conversation, where they can also contribute. The feature is notably useful when sharing lengthy dialogue or useful prompts, offering a more efficient alternative to screenshot sharing.

The risk of information leakage via ChatGPT shared links

However, this handy feature lacks an access control mechanism — anyone who obtains the shared URL can access its content, even those outside the intended audience. Consequently, OpenAI advises against sharing confidential information via this feature. Furthermore, without access analytics, it's impossible to track the users who have accessed the URL or even how many times it has been accessed.

●▶ Read the full article at the source's URL.

The Unexpected Solution for Firefighter Fatalities

Source: https://i-hls.com/archives/119985

July 20 – Firefighters work in a highly dangerous environment, constantly dealing with fire, debris, smoke, and extreme heat. Surprisingly, the number one cause of fatalities among firefighters is actually cardiac arrest, which accounts for 40% of on-duty fatalities among firefighters, and the solution comes from an unexpected source. Researchers at the National Institute of Standards and Technology (NIST), in collaboration with the University of Rochester and Google, have successfully developed an AI model that ca n **accurately determine if a firefighter is about to experience a cardiac event**. The use of AI showed an ability to detect abnormal heart rhythms, a key cause of sudden cardiac death.

According to Cybernews, the research published in the Fire Safety Journal revealed that the AI model was able to correctly identify around 97% of abnormal electrocardiogram (ECG) samples in a unique dataset collected from firefighters.

A firefighter is twice as likely to experience a sudden cardiac death than a police officer, and four times more than other emergency responders.

The research team used a very unique dataset that was collected a decade earlier by the University of Rochester, which contained 24 hours of ECG data from 112 firefighters, during both their on and off-duty hours.

The model developed by the NIST research team is called the Heart Health Monitoring (H2M) model, and it combines machine learning with the Rochester dataset. The H2M recognizes and classifies normal and abnormal heartbeats indicative of irregular heart rhythms.

The vision of the research team is for the H2M model to be used in portable heart monitors that firefighters could wear on duty, which would provide real-time alerts to potential cardiac irregularities, acting as an on-the-spot AI cardiologist.

The model's applications could even be extended to other industries and benefit other high-risk groups and even the general public if trained with the right datasets.

NIST researcher Wai Cheong Tam noted, "This technology can save lives. It could benefit not only firefighters but other first responders and additional populations in the general public."

What Does AI Safety Have to Do With Homeland Security?

Source: https://i-hls.com/archives/119964

July 19 – As companies worldwide are rushing to join the AI craze, experts fear that crucial security details are being overlooked. Top security official claims cyber security must be urgently built into artificial intelligence systems or malicious attacks could have a "devastating" effect. Lindy Cameron from the National Cyber Security Centre told BBC News it is absolutely necessary to have secure systems in place now, in the early stages of AI development.

AI is being slowly integrated into more and more aspects of our daily lives, and in the not-so-far future it may play a part in our homes and cities, high-end national security and even fighting wars. But of course, along with the benefits come the risks, and experts are worried. According to BBC News, the concern is that companies competing to secure their position in a growing market will be so focused on getting their systems out as fast as possible, they won't be thinking about the risks of misuse.

"The scale and complexity of these models is such that if we don't apply the right basic principles as they are being developed in the early stages it will be much more difficult to retrofit security," says Cameron.

AI systems may easily be used as tools, or even be subverted by those seeking to do harm.

For many years, a small group of experts has specialized in a field called 'adversarial machine learning', which looks at how AI and machine learning systems can be tricked into giving bad results.

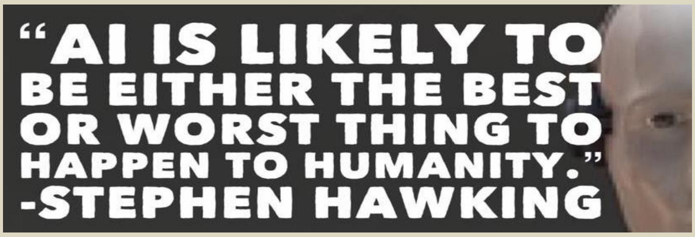
For example, let's take AI that is trained to recognize images. According to the BBC, researchers ran a test by placing stickers on a 'stop' road sign, which made the AI think it was a speed limit sign – something with potentially serious consequences for self-driving cars. Another danger is 'poisoning' the data from which the AI is learning- meaning deliberately creating bias by injecting bad data into the learning process.

These dangers are not only hackers seeking to cause disruption but may pose a risk to wider national security.

For example, AI used to analyze satellite imagery may be "tricked" to either miss the real object or see an array of fake ones.

These concerns, previously theoretical, are now emerging as real-world attacks on systems. It seems to be happening first where AI is used to improve cyber security by detecting attacks. Here adversaries are seeking ways to subvert those systems so their malicious software can move undetected.

This phenomenon will inevitably reach all fields of our lives, from grocery shopping to homeland security. It seems that the experts should continue pushing for regulations and security measures to be built in before it is too late.



Preparedness &

EMERGENCY RESPONSE

Creating a New Standard for Evaluating Tabletop Exercises

By Scott J. Glick and John Duda

Source: https://domesticpreparedness.com/articles/creating-a-new-standard-for-evaluating-tabletop-exercises

July 05 – Exercises play a vital role in preparing organizations to respond to critical incidents and have been used by the U.S. government for decades to enhance department and agency understanding of their respective roles and responsibilities and to help prepare for terrorist threats. Although organizations can develop plans, expand their resources, and add personnel with expertise in responding to different threats and hazards, the planning process cannot move beyond the theoretical if exercises do not validate plans. Having the right equipment and personnel to respond to a critical incident may provide insight into what an organization's response capabilities can accomplish. Still, unless those capabilities are tested in exercises as part of a comprehensive and integrated preparedness program, the organization cannot answer the fundamental question that its leadership needs to know: Can the organization effectively respond when a threat or hazard arises?

Currently Used Exercise Tools

During operations-based exercises, participants execute functions in a simulated environment to recreate what would happen if the scenario were real. Operations-based exercises, which include drills and full-scale exercises, are easily evaluated with quantitative assessment tools (e.g., whether participants set up a command post, initiate communications, or employ personnel and resources within a specific time). However, rather than demonstrating capabilities, participants in discussion-based exercises such as tabletop exercises (TTX) talk through a response policy, plan, or procedure and discuss what they would be doing. As a result, TTXs do not readily lend themselves to quantitative assessments, nor is there an industry standard for evaluating their effectiveness.

The Federal Emergency Management Agency (FEMA), through its Homeland Security Exercise and Evaluation Program (HSEEP), has taken essential steps to improve the evaluation of exercises. Beginning nearly a decade ago, FEMA published a sample Participant Feedback Form – HSEEP-C09, which organizations can adapt. In this sample form, FEMA recommended that organizations solicit opinions from exercise participants on eight statements using a Likert scale, including whether participants observed *strengths* during the exercise or areas that needed *improvement*. These statements, however, only solicited general assessments about preparedness, and the feedback was not directly tied to exercise objectives. In January 2020, FEMA updated the HSEEP guide, but has not updated the Participant Feedback Form. Therefore, the current HSEEP exercise evaluation methodology may not solicit sufficient data to assist organizations in accurately measuring a TTX's overall effectiveness in improving organizational preparedness.

Designing and Evaluating Tabletop Exercises

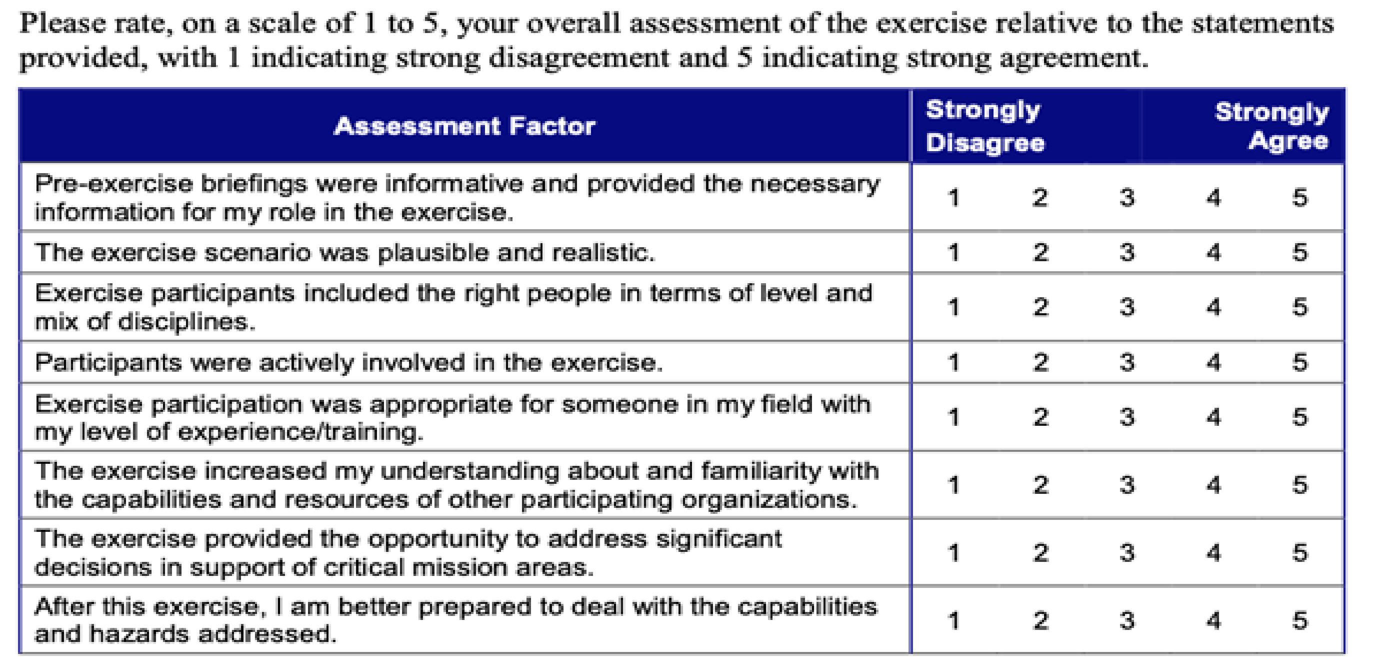
TTXs provide a forum for participants to discuss policies, procedures, or plans that relate to how the organization will respond to a critical incident. During TTXs, facilitators or moderators lead the discussion to keep participants moving toward meeting the exercise objectives. The exercises must have realistic scenarios to accurately assess response capabilities. They should be well-designed, take into account how adults learn best, and engage participants in ways that build better *muscle memory* and avoid negative training; that is, training that reinforces responses that are not aligned with an organization's policies and procedures, and obstruct or otherwise interfere with future learning. Post-incident analyses repeatedly demonstrate that experience gained during exercises is one of the best ways "to prepare teams to respond effectively to an emergency."

After the exercise, it is important to find the best way to evaluate whether the TTX has increased the participants' short-term and long-term knowledge or behaviors and to determine whether the exercise improved organizational preparedness. Researchers and academic scholars have examined different evaluation methodologies. For example, in 2017, nine researchers conducted an extensive study of whether a TTX enhanced the pediatric emergency preparedness of 26 pediatricians and public health practitioners from four states. After analyzing the data, the researchers published their study in 2019 and concluded that TTXs "increased emergency preparedness knowledge and confidence."

Using the wrong evaluation methodology, organizations may not be able to accurately determine whether they are getting a high return on their training investments. However, since a TTX can be conducted cost-effectively in a short time, the method used to evaluate their effectiveness must also be capable of being completed relatively quickly and cost-effectively.

Quantitative Assessments

The driving principle behind exercise evaluation should be "to determine whether exercise objectives were met and to identify opportunities for program improvement." The HSEEP's Participant Feedback Form's quantitative measurements are limited and primarily focused on exercise *delivery* and asking participants to provide *general and conclusory* statements about whether the exercise improved their preparedness (see Fig. 1).



Please rate, on a scale of 1 to 5, your overall assessment of the exercise relative to the statements provided, with 1 indicating strong disagreement and 5 indicating strong agreement.

Assessment Factor	Strongly Disagree				Strongly Agree
Pre-exercise briefings were informative and provided the necessary information for my role in the exercise.	1	2	3	4	5
The exercise scenario was plausible and realistic.	1	2	3	4	5
Exercise participants included the right people in terms of level and mix of disciplines.	1	2	3	4	5
Participants were actively involved in the exercise.	1	2	3	4	5
Exercise participation was appropriate for someone in my field with my level of experience/training.	1	2	3	4	5
The exercise increased my understanding about and familiarity with the capabilities and resources of other participating organizations.	1	2	3	4	5
The exercise provided the opportunity to address significant decisions in support of critical mission areas.	1	2	3	4	5
After this exercise, I am better prepared to deal with the capabilities and hazards addressed.	1	2	3	4	5

Fig. 1. HSEEP Participant Form Questions (Source: HSEEP-C09, Participant Feedback Form Template).

The numerical scores that can be aggregated in the HSEEP statements have utility, but will not produce sufficient quantitative data because the questions are limited, are not tied explicitly to exercise objectives, and do not assign different weight values to the answers. Using objective-based and goal-based criteria can help distinguish between evaluative statements focused on exercise delivery and those focused on whether the TTX met a particular objective. Assigning a weighted numerical value for each response is also critical. For example, responses focused on exercise design and delivery should not be weighted as heavily as those focused on how well the TTX met a particular objective and improved the organization's preparedness. In addition, when scores are averaged and compared over time, they produce a more accurate evaluation of whether the TTX improved the organization's preparedness.

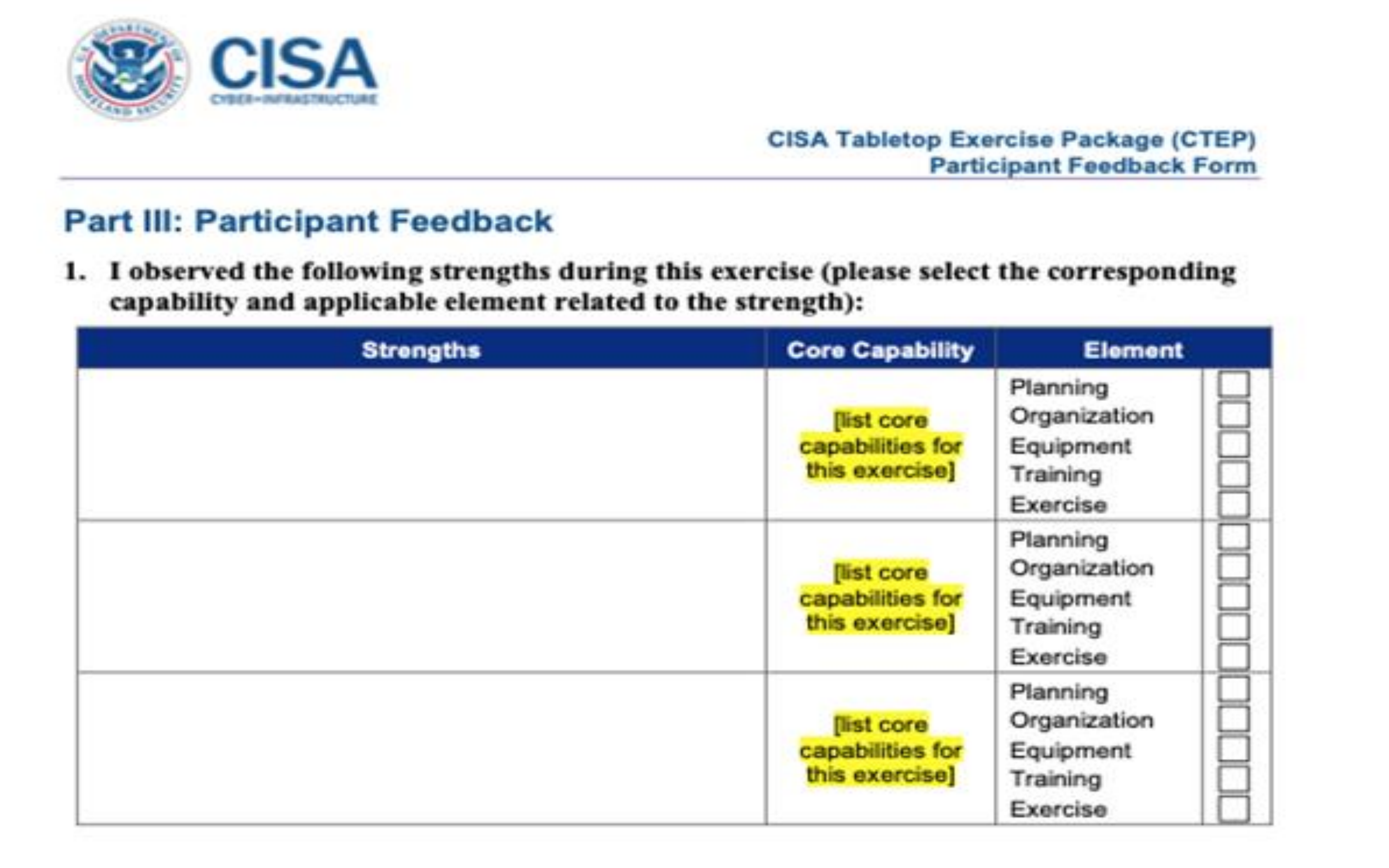
The following types of statements can be adapted by organizations to their specific TTX. Scoring these exercise factors and assigning them a weighted value creates what the authors call an XF Score.

Please rate, on a scale of 1 to 5, your response to the following statements, with 1 indicating that you strongly disagree, a 2 indicating that you disagree, a 3 indicating that you are undecided or neutral, a 4 indicating that you agree, and a 5 indicating that you strongly agree.

- The TTX improved my understanding of my organization's critical incident response capabilities [to the specific scenario being tested] (multiply this response by 2);
- The TTX improved my understanding of other organization's response capabilities, plans, policies, and procedures and how they integrate with my organization's critical incident response plans, policies, and procedures (multiply this response by 2);
- TTX objective 1 was to … [repeat for each objective] was aligned with assessing my organization's preparedness to respond to this type of critical incident (multiply this response by 3). (This should be the main TTX objective.);
- TTX objective 2 was to … [repeat for each objective] was met (multiply this response by 3);
- The TTX revealed a gap in my organization's critical incident response capabilities, plans, policies, and procedures (multiply this response by 2);
- The TTX revealed areas where my organization can improve its preparedness to respond to this or other critical incidents (multiply this response by 2);
- As a result of the TTX, I or my organization will be changing the way that I or we respond to critical incidents (multiply this response by 3). (This helps to measure behavioral change.); and
- As a result of the TTX, my organization has improved its ability to respond to this type of incident (multiply this response by 2).

Participant responses that are anonymous tend to produce more reliable quantitative data to analyze objectively. In addition, a scoring system that assigns the highest value to questions aligning with exercise objectives and goals (e.g., tasks and issues with the greatest importance to the organization's preparedness), and a scoring system that assigns the lowest value to exercise delivery, would produce more meaningful results about the exercise's effectiveness than HSEEP's Participant Feedback Form. For example, median score increases over time could be used to measure the degree to which the TTX transferred learning to participants and participants changed their behavior.

Organizations, however, must avoid exclusive reliance on quantitative assessments. For example, HSSEP's Participant Feedback Form does include qualitative information, which provides some degree of categorization for the information sought regarding core capabilities. However, that qualitative data does not appear to be tied to exercise objectives, as the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) illustrates in its use of HSEEP's form (see Fig. 2).



CISA
CYBER+INFRASTRUCTURE

CISA Tabletop Exercise Package (CTEP)
Participant Feedback Form

Part III: Participant Feedback

1. I observed the following strengths during this exercise (please select the corresponding capability and applicable element related to the strength):

Strengths	Core Capability	Element	
	[list core capabilities for this exercise]	Planning	□
		Organization	□
		Equipment	□
		Training	□
		Exercise	□
	[list core capabilities for this exercise]	Planning	□
		Organization	□
		Equipment	□
		Training	□
		Exercise	□
	[list core capabilities for this exercise]	Planning	□
		Organization	□
		Equipment	□
		Training	□
		Exercise	□

Fig. 2. CISA Participant Feedback Form.

Integrating Quantitative Scores With Qualitative Assessments

Organizations must also collect qualitative data to evaluate their TTX's effectiveness. Consider, for example, using the Likert scale to assess customer satisfaction for a restaurant. In the same way that a low score would not, by itself, reveal *why* the customer was dissatisfied (e.g., poor food quality or poor service), exclusive reliance on the numeric values of the quantitative score would not provide an organization with the insight needed to understand *why* the TTXs may or may not have improved its preparedness. By directly linking and integrating the quantitative data with the qualitative data, evaluators obtain more accurate and comprehensive insight regarding effectiveness.

Qualitative assessments must focus on exercise objectives during the "hot wash" and subsequent participant feedback. While facilitators can ask "open-ended" questions during the hot wash, exercise participants should focus their immediate comments on their organization's preparedness. Hot wash participants providing comments on organizational preparedness – strengths and areas for improvement – rather than on the exercise's execution or logistics in written post-exercise questionnaires, enables the immediate discussion to focus on more important preparedness questions.

Effective exercise evaluation requires careful planning from the beginning of the exercise design phase and when observing and collecting data, including comparing exercise objectives to how participants performed during the exercise.

For example, asking questions such as "How was exercise objective #1 accomplished?" will provide important data regarding improving the response and organizational preparedness for the exercise. To further the qualitative data collection process, evaluators should ask the following key questions:

- Were the participants exercised on the specific plan, policy, and procedure the organization intended to assess?
- Did the participants understand the specific plan, policy, and procedure discussed during the exercise?
- Did the participants understand how to execute the plan, policy, and procedure?
- Did the participants follow their organization's plans, policies, and procedures, or were gaps identified (e.g., actions not stated in plans), indicating the need to reassess a particular plan, policy, or procedure?
- What were the consequences of the decisions made?

Responses to the above questions should help exercise evaluators reach several important conclusions about the TTX's effectiveness. For example, suppose participants did not demonstrate an understanding of a policy, plan, or procedure during the TTX. In that case, evaluators may need to conduct a root-cause analysis to better understand why that happened. Using qualitative assessments as part of a root-cause analysis can provide key data for an after-action report and improvement plan. When compiling this information, however, evaluators must consider the direct relationship among several factors that can affect the evaluators' conclusions about the data they collected, including:

- Whether there were well-considered and developed exercise goals and objectives;
- The quality of the data collected;
- Whether there were experienced and skilled exercise facilitators;
- Whether appropriate exercise participants were present; and
- Whether exercise participants were assured that the TTX was "no-fault" and "non-attributional" after-action report and improvement plan data collection would occur.

When participants receive "no-fault" and "non-attributional" assurances about the answers they will be providing to the TTX evaluation questions, better qualitative data will be collected because participants will have less reluctance to admit a lack of understanding, a shortfall in a policy, plan, or procedure, or the fact that the appropriate individuals and agencies did not participate. The collected data can then enable evaluators to reach conclusions about whether the TTX contributed to the following:

- Team building, agency coordination, and enhancing familiarity among response assets and leadership;
- Participants' increased knowledge of their roles and responsibilities and how they would be applied during a particular scenario;
- Participants' increased knowledge of others' roles and responsibilities;
- Participants' increased identification of any gaps in policies, plans, or procedures; and
- Participants' increasing knowledge of potential threats, vulnerabilities, or consequences, if those subjects were covered during the exercise.

The collected qualitative information plays a significant role in evaluating organizational change and whether TTXs have improved the organization's preparedness. However, separate briefings with exercise evaluators, controllers, and facilitators would produce the most complete and accurate assessment.

Testing Future Preparedness Efforts

Testing response capabilities in exercises prepares personnel and organizations for all types of threats, hazards, and incidents, and ensures that plans are current and effective. TTXs are a cost-effective way for the government, private companies, and non-government organizations to test their preparedness. Following a checklist to create a well-designed TTX will maximize an organization's chances for a successful TTX. When a TTX is well-designed, engages participants, and is conducted effectively, participants' written responses to post-exercise questionnaires can provide important indicators of whether the TTX improved organizational preparedness. Yet, no industry standard exists for evaluating this effectiveness over time.

There is a need for a new industry standard for a reliable, objective, and cost-effective way to evaluate TTX effectiveness. The new standard should be based on quantitative and qualitative data that is tied to exercise objectives and that assigns weighted values to the most important exercise factors to better understand the TTX's impact on organizational preparedness. However, care must be taken regarding the scoring statements, exercise design, and delivery. Moreover, conducting TTXs alone is not enough to ensure organizational preparedness. When a comprehensive and integrated preparedness program has senior leaders' support and the exercises are appropriately resourced, organizations can maximize the return on investment in their training investments and pursue multi-year exercise plans and priorities through effective program management.

Scott J. Glick is vice president and general counsel for Summit Exercises and Training LLC (SummitET®), a veteran-owned small business that specializes in providing proven preparedness solutions to systematically address all threats, hazards, and incidents through a wide range of services, including planning, training, and exercises, as well as operational and policy support, for its government and private sector clients. He has nearly four decades of experience in law enforcement, counterterrorism, critical incident response, exercises, and emergency preparedness. He previously served as the director of preparedness and response and senior counsel in the National Security Division at the U.S. Department of Justice (DOJ), where he led DOJ's national preparedness policy and planning efforts, including in regard to countering weapons of mass destruction (WMD), and where he provided substantial guidance to the FBI in the development of the WMDSG. He also investigated and prosecuted international terrorism cases as a federal prosecutor, and organized crime cases with as a state prosecutor in New York. This article contains no classified or confidential government or business information, and the views expressed in this article are solely those of the author and do not necessarily represent the views of any government department or agency, or any private sector company.

John R. Duda is the chief executive officer of Summit Exercises and Training LLC (SummitET®), a veteran-owned small business that specializes in providing proven full spectrum preparedness solutions to systematically address all threats and hazards through a wide-range of services. Mr. Duda has led and supported multiple domestic and international exercise and training programs for numerous government and non-government organizations. Mr. Duda has also co-authored a research study involving defense-based sensor technology and has been certified as a senior professional in Human Resources and as a Business Continuity Professional. Prior to forming SummitET, Mr. Duda served many organizations including the U.S. Department of Energy/National Nuclear Security Administration, Publix Super Markets, and the Jacksonville Port Authority. Mr. Duda is also a member of the Advisory Board for the University of North Florida's School for International Business and the cybersecurity and compliance company, RISCPoint.

Eliminating Blind Spots in Pandemic Preparedness

Source: https://www.genengnews.com/topics/infectious-diseases/eliminating-blind-spots-in-pandemic-preparedness/

July 06 – Everyone knows the pandemic headliners: Ebola, plague, and, of course, SARS-CoV-2. But some scientists are tracking lesser-known pandemic threats such as a fungus called *Candida auris* and, especially, new diseases on the rise in domesticated animals. Such pathogens may represent blind spots in our pandemic preparedness.

A major issue in heading off such threats is that our current regulatory system lacks a clear and comprehensive strategy to prevent disease from spilling over from animals into humans, a process known as zoonosis. Two viruses known to be gaining traction are "cow flu" (influenza D), which is jumping to U.S. cattle workers, and highly pathogenic avian influenza (bird flu), which infects wild birds in all 50 states and has a mortality rate of about 50% in humans. Another concern, newly addressed by the Centers for Disease Control and Prevention (CDC), is that highly lethal and treatment-resistant forms of *C. auris* are spreading at an alarming rate, especially in healthcare settings.

A fractured regulatory system

In fall 2022, the federal government released a new pandemic preparedness document, the National Biodefense Strategy and Implementation Plan (NBS-22). "It maps a strategy for the American government through which to confront biological threats to the health and safety of its citizens and, more broadly, to improve global health security," says Ann Linder, JD, a research fellow in the Brooks McCormick Jr. Animal Law and Policy Program at Harvard Law School.

However, Linder believes that some dangerous threats were not fully addressed. "Through its focus on laboratory accidents and deliberate acts of bioterrorism, NBS-22 obscures an important category of threat—a category encompassing predictable but unintended consequences of everyday animal use," she explains. "These threats involve not some critical error (for example, a cage left unlocked) or a bad actor with malign intentions, but routine practices, many of which are dangerous and poorly regulated."

More emerging zoonotic diseases originated in the United States than in any other country during the second half of the 20th century. According to Linder, this development is "due in part to the nation's large and growing systems of animal production." For example, in 2012, H3N2v influenza spilled over from pigs to humans at livestock exhibitions and infected hundreds of people across 10 states. More recently, in Michigan, mink on fur farms generated a new strain of COVID-19 that jumped to workers.

Linder believes this problem can be addressed even though the current regulatory system is "fractured and insufficient" and lacks a "clear and comprehensive strategy to prevent zoonotic disease." She maintains, however, that such a strategy can be developed if the appropriate steps are taken. These include steps to gather more and better data about disease risks. Potential reforms include enhanced monitoring of the industries associated with disease risks, and the generation of industry-specific disease prevalence statistics.

Who should drive these reforms? "Policymakers at the state, local, and federal levels could take steps to mitigate zoonotic risk," Linder says. "What is needed now is a fundamental restructuring of the regulatory regime and a strategy that can bring together the diverse and competing agencies that govern animal, human, and environmental health and break down the silos that divide them." She adds that the scientists who understand and study these risks should lead the effort to inform both policy and public opinion.

Influenza D spillover

Studies have shown that zoonotic viruses can survive in air, in water, and on surfaces at farms and animal facilities. But is this normal, or dangerous? In a recent small study, Jessica Leibler, DrPH, an associate professor of environmental health at Boston University, and her colleagues found that more than two-thirds of dairy workers surveyed had evidence of influenza D virus in their nasal passages before and after work. An earlier study found that workers in Florida had antibodies in their serum, indicating they had been infected.

“Influenza D is an emerging, zoonotic genus of influenza virus,” Leibler points out. “It was first identified about 10 years ago in industrial swine and cattle.”

Infections to the general population appear limited, and influenza D virus doesn’t appear to cause illness in humans at present. Nonetheless, concern is warranted. “The greater the number of animals that are infected with a virus known to jump to humans,” Leibler warns, “the greater the possibility that the virus could mutate and gain virulence and transmissibility among people.”

What is needed is more comprehensive surveillance of cattle and cattle workers. “It would help clarify exposure sources and identify human health risks posed by this emerging pathogen,” Leibler argues, “but we would need better technology for the rapid detection of influenza D virus.” Moreover, such technology would need to become commercially available. Such a development could be driven by industrial and academic partnerships.

“Perhaps a silver lining from the COVID-19 pandemic is that we are now much more aware of zoonotic spillover,” Leibler reflects. She adds that an improved understanding of zoonotic spillover is of “critical importance in pandemic prevention.”

The rise of avian flu

The World Health Organization has called recent outbreaks of avian flu in humans “worrying.” According to the CDC, highly pathogenic avian influenza (H5N1) has afflicted more than 58 million poultry in 47 states and thousands of wild birds in all 50 states. So far, there has been limited spread of the virus to humans, but “avian influenza has been considered a potential threat to humans for nearly 25 years,” observes Matthew Binnicker, PhD, director of clinical virology at the Mayo Clinic.

“Certain strains of avian influenza, such as H5N1 and H7N9, may be highly pathogenic and cause severe disease in humans,” he continues. “Initial symptoms may be similar to human influenza, but the mortality rate of avian influenza can be about 50%. Antivirals used to treat human flu may be effective in treating cases of avian influenza, but routine flu vaccines are not believed to provide protection against avian influenza strains.”

However, if avian influenza develops the ability to spread efficiently to and within humans, we are unprepared to handle it. Binnicker notes, “Currently, the vast majority of monitoring and testing for avian influenza is being performed in poultry and wild birds. Very little testing has been performed in humans, and this is typically only done when an individual develops flu-like symptoms after interacting with an ill or dead bird.”

Binnicker says the main reason that testing in humans is not more common is that there are no commercially available tests specifically designed to detect avian influenza. Testing is currently limited to the CDC and public health laboratories. He advises that rapid and at-home tests for avian influenza need to be devised. Additionally, candidate vaccines need to be developed and readied for potential widespread distribution. Finally, poultry should be vaccinated against avian flu to reduce the number of infections and the potential for humans to be exposed.

Binnicker remains optimistic: “Strong partnerships are being formed between public health, clinical laboratories, industry, and the government to discuss how to prevent a future outbreak or pandemic from avian influenza. My hope is we’ll learn important lessons from the COVID-19 pandemic and apply those lessons to prevent future pandemics, including a possible avian influenza outbreak.”

Deadly fungus

Last March, the CDC issued a warning on *C. auris*, a fungus spreading at an alarming rate, especially in healthcare settings. The first U.S. cases of *C. auris* were reported in 2016, but a retrospective review identified cases that dated back to 2013. Now the pathogen has been documented in at least 26 states. Between 2016 and 2019, the number of clinical cases rose from 13 to 476. Occurrences have continued to climb dramatically, with the CDC reporting 5,754 clinical cases in 2022.

Further, the mortality rate for *C. auris* is high, estimated at 30–72%. The CDC’s Meghan Lyman, MD, a medical officer in the Mycotic Diseases Branch, warns, “*C. auris* acts differently from other *Candida* species and is an urgent public health threat because it is often resistant to multiple antifungal medications, spreads easily in healthcare settings, and can cause serious, invasive infections. People with *C. auris* are very sick at baseline and require high-acuity care (including mechanical ventilation and invasive medical devices). They have had many exposures to antimicrobial medications. And they have had long or frequent stays in healthcare facilities.” Lyman says that transmission at present mostly occurs in healthcare settings. She adds that “there is no evidence that transmission in the community is a concern.”

To help contain the spread of the deadly fungus, Lyman shares some advice: “Early identification of cases, strong adherence to infection control practices, and good communication about a patient’s *C. auris* status are all important to prevent spread. In general, it's best to identify *C. auris* in an area before there is widespread transmission. It's important to have proactive case identification through colonization screening and enhanced surveillance of clinical specimens by conducting *Candida* species identification from all specimens, not just those that are invasive."

According to Lyman, facilities will need to be proactive to monitor potential infections, even if they are in low-burden areas. She explains, "Containment generally seems to be easier in places that identify cases early, before there is transmission."

Different fungal clades

There are at least four major clades of *C. auris*: Clade 1, South Asian; Clade 2, East Asian; Clade 3, South African; and Clade 4, South American. Samantha Jacobs, MD, an associate professor of medicine (infectious diseases) at the Icahn School of Medicine at Mount Sinai, and colleagues from the American Type Culture Collection and the New York State Department of Health's Wadsworth Center recently performed a case study of *C. auris* isolates from a transplant patient who evolved pandrug resistance to four classes of antifungal therapeutics. "Part of the treatment dilemma," Jacobs points out, "is that we have fewer fungal treatment options as compared to the larger armamentarium against bacteria."

The researchers characterized the genomes and performed drug resistance analyses of multiple *C. auris* isolates in the infected patient over a 72-day period. They found a distinct subcluster of South Asia Clade 1, and they identified common and novel genetic changes driving resistance to the antifungal agents (azoles, echinocandins, polyene, and flucytosine). They concluded that the "emergence of pandrug-resistant *C. auris* in a patient over time is alarming."

Reflecting on the study's findings, Jacobs notes, "What is needed is improvement in fungal diagnostics that can perform antifungal susceptibility testing in concert with rapid genomic screens to assess resistance markers. The real issue, though, is the need to develop more effective and safe therapies. There are several promising candidates now undergoing clinical trials. We also must focus on raising awareness, especially in the medical community, about the continued and increasing threat of *C. auris*."

Although the experts who spoke with *GEN* all felt that more scrutiny and technological advances are critically needed to avoid the next pandemic, they are uniformly hopeful that we have learned valuable lessons from COVID-19. They share the conviction that increased collaboration among academia, industry, and government, along with scientific innovation, will be critical to preventing or mitigating the next pandemic.

Inside the "Boot Camp" for Emergency Managers

By Michael Valiente

Source: https://disasterpreparedness.kinsta.cloud/articles/inside-the-boot-camp-for-emergency-managers

July 12 – Monday, August 1, 2022, was a typical San Antonio, Texas, summer day, with clouds hanging low and humidity increasing as the sun rose. But nothing was ordinary to the 20 individuals who would become cadets in the first Emergency Management Academy developed by the Texas Division of Emergency Management (TDEM). Looking around, the cadets appeared apprehensive but excited that they had been selected to become the future of emergency management in the Lone Star State. TDEM Chief Nim Kidd spoke to the class and shared his expectations of The Academy. He indicated that the cadet demographics were intentionally diverse: military veterans, college graduates, recent high school graduates, and practitioners from fire, emergency medical services (EMS), and law enforcement backgrounds. The purpose was to garner different perspectives inherent to the cooperative and collaborative nature of the emergency management field.

Emergency Medical Technician – Basic

After onboarding into The Texas A&M University System, the cadets moved to a different location from its roots in the Texas A&M–San Antonio campus to the Schertz EMS Academy in Guadalupe County. There, the cadets underwent a rigorous, condensed eight-week training (from the standard 16-week course) in emergency medical response, undergoing testing in academics and skills. Also, the practical application portion of the training was supplemented by clinical familiarity through ambulance duty on weekends, in which the cadets had to complete 40 hours of assisting ambulance crews. The final test was the National Registry exam, in which the nationally recognized EMS certification was awarded. The emergency medical response certification would enhance the cadet's ability to augment EMS in their jurisdictions after graduating from the Academy.

Preparedness – Planning During "Blue Sky" Days

The cadets went back to the Texas A&M–San Antonio campus for the duration of The Academy. Before diving into the Preparedness training module, the cadets received a week-long series of classes on leadership development, team building, and stress management. Then, they took courses on the Foundations of Emergency Management, Science of Disasters, Emergency Planning, Homeland Security Exercise and Evaluation Program, Threat and Hazard Identification and Risk Assessment, and Continuity of Operations. The cadets also became intimate with the federal laws governing emergency management, specifically the Stafford Act and the Texas Government Code Chapter 418, the state's statutory authority on disaster management. Additionally, the cadets were introduced to the State of Texas Emergency Assistance Registry, a program administered locally for citizens with access and functional needs, and the Emergency Tracking Network, where they learned to track evacuees and pets.

Hazard Mitigation Training – State and Federal Perspectives

The complexity of hazard mitigation was navigating through the idiosyncrasies of the various federal hazard mitigation programs and the processes from applying for the grant programs at the local level to the programmatic closeout between TDEM and the Federal Emergency Management Agency (FEMA). The instructors hailed from TDEM, giving the cadets the state-level perspectives, and FEMA Region 6, headquartered in Denton, Texas, providing the federal-level views. Also, the cadets observed that other state agencies, such as the General Land Office and the Texas Water Development Board, were instrumental in providing additional funding assistance for hazard mitigation. The classes familiarized the cadets with the various funding assistance programs and their applications, conducting benefit-cost analyses, and grant application reviews and evaluations.

Response – "How Big Is Big? How Bad Is Bad?"

The cadets welcomed the New Year in 2023 with two weeks of the Incident Command System (ICS) for Expanding Incidents (G-300 and G-400), followed by Public Information Basics, in which TDEM's own Media and Communications team interviewed the cadets who subsequently conducted press conferences fielding questions from the "press." The cadets were then introduced to various Geographic Information System platforms such as Survey 123, Individual (Assistance) State of Texas Assessment Tool (iSTAT), Public (Assistance) State of Texas Assessment Tool (pSTAT), State of Texas Assistance Request (STAR), and WebEOC, the resource request tracking tool from local jurisdictions to the Texas State Operations Center (SOC). The data collected from the iSTAT and pSTAT digital surveys give an overview of the initial damage assessment for the Disaster Summary Outline (DSO). The DSO is transmitted to the SOC to assist in evaluating the extent of the damage within a jurisdiction.

"Every Day Is Recovery Day" Training

The recovery training module started with grant management for both Individual Assistance and Public Assistance programs. Emergency declarations and disaster declarations were also covered, starting with requests from the local level up to the president's approval. Further, there was an emphasis on the importance of a debris management plan, as well as the roles of community leaders in disaster declarations, sheltering and feeding operations, engaging Volunteer Organizations Active in Disasters and Community Organizations Active in Disasters, establishing a Long-Term Recovery Group, and choosing a fiduciary agent (a third-party entity to assist in processing monetary donations during disasters). An added feature was education in Disaster Finance, taught by a team from TDEM that manages and allocates federal and state funds to individual jurisdictions.

Off-Site Training

Although most of the training took place on the Texas A&M–San Antonio campus, the cadets had the opportunity to train off-site. The first field experience was on Sunday, November 20, 2022, attending the Texas EMS Conference in Austin, Texas, where they were introduced to the various Emergency Medical Task Force (EMTF) teams throughout the state and the different types of assets, including mobile medical units. They also explored various technological advances in emergency response by talking to the vendors in the exhibit hall. A great event was experienced by all when the Emergency Operations Center (EOC) Operations and Planning class met in the Bexar County/City of San Antonio EOC to conduct scenario-based training in an actual EOC. Instructors from the Texas A&M Engineering Extension Service (TEEX) guided the cadets in operating an EOC by filling the roles in an ICS framework. The cadets also had the opportunity to tour the SOC in Austin, where they were introduced to the various emergency support functions (ESFs) and how the SOC would operate during activations. Moreover, during the recovery training phase, the cadets visited the San Antonio Food Bank to acclimate to its mission, capabilities, and valuable role in disaster resource assistance.

Job Fair – "The Academy Mixer"

To fully understand the uniqueness of each region and functional area within TDEM, and before applying for employment, cadets participated in a job fair organized by the TDEM Administration Division and the Human Resources team. To prepare for the job fair, cadets took classes on resume building, cover letter drafting, and job interview techniques.

Capstone – The Final Phase of the Emergency Management "Boot Camp"

The Academy Capstone took place over three days in late March at Disaster City in College Station. Hosted by TEEX, the multi-day exercise consisted of filling the roles of the ICS functions within the EOC. The simulation was divided into multiple operational periods wherein cadets switched roles. This "final project" enhanced the exercise's realism and gave the cadets confidence in performing the essential tasks during disaster operations.

Reflections

The challenging yet fulfilling experience culminated at 4 p.m. on Friday, March 24, 2023, when 17 cadets walked across the stage to receive their diplomas, FEMA certificates, and badges – part of their reward for completing the 8-month "basic training" in emergency management. The keynote speaker was Governor Greg Abbott. Texas A&M University System Chancellor John Sharp, Texas Emergency Management Chief Nim Kidd, FEMA Region 6 Administrator Tony Robinson, and TDEM Academy Division Chief David Covington also delivered remarks. This academy cohort was unique for two reasons: This was a new and unique emergency management academy and this was the first cadet class to go through the training – an opportunity of a lifetime! Familiarization with the four phases of emergency management, receiving FEMA and EMS certifications, networking opportunities, and, most of all, performing the skills requirements of the emergency management field was a tremendous experience! The 17 cadets that completed the training became family, dedicated and eager to respond to assist the citizens of Texas as the next generation of emergency managers.

The author would like to especially thank TDEM Division Chief David Covington, Unit Chief Kade Long, and Unit Chief Angela Shook for their leadership and academic acumen in sustaining The Academy.

Michael Valiente currently serves as the Senior Training Officer – Preparedness Division at the Texas Division of Emergency Management. He is a retired U.S. Marine with 23 years of active-duty service. His initial emergency management experience came from participating in Operational Unified Assistance, the U.S. military humanitarian relief efforts during the December 2004 tsunami in Southeast Asia. After retiring in 2005, he taught at the University of Phoenix and Alamo Colleges in San Antonio, Texas. He has a master's degree in international relations from Troy University and a Doctor of Emergency Management degree from Capella University.

Incident Management – The Whataburger Way

By Ron Derrick

Source: https://www.domesticpreparedness.com/articles/incident-management-the-whataburger-way

July 19 – A community's level of resilience during a disaster often relies on the preparedness efforts of its private sector partners. Companies that invest in preparing for and responding to large-scale events are protecting much more than just company profits. For example, the thought and design that went into one hamburger restaurant led to a companywide culture of safety and community service.

Whataburger was born from one man's dream in 1950 when Harmon Dobson opened a small building selling burgers for just 25 cents in Corpus Christi, Texas. His idea was for someone to hold up the burger and think, "Wow, What-A-Burger." The name has stuck, and the company has gone from one little shack to over 950 restaurants across 14 states. The orange and white colors and the iconic "A-frame" building came from the founder's passion. Dobson was a pilot, and he wanted to be able to see his buildings as he flew overhead. The orange and white colors come from aviation; most airports use these colors to signify obstructions and buildings. The "A-frame" shape is also iconic, and a version of it is used in all new construction along with the flying "W." In 2001, the 77th Texas Legislature officially designated Whataburger as a "Texas Treasure."

Whataburger restaurants grew rapidly into many southern states, and most restaurants are open 24 hours. Executive leadership knew that issues and incidents would need to be handled through an elite team with emergency management and crisis response experience and expertise. In response, the company formed the Whataburger Command Center, which initially consisted of four individuals dedicated to identifying potential threats and incidents that could impact or threaten employees, customers, restaurants, or brand reputation. After COVID-19 emerged in the U.S. in March 2020 and several company re-organizations between 2020 and 2023, the team now has one senior manager and one professional running a *high-level* Command Center at the San Antonio, Texas, home office. This team uses multiple vendors and applications to help identify, analyze, and verify incoming information.

The Command Center uses a hybrid form of the Incident Command System, and its mission is to prepare for, identify, respond to, and recover from a crisis or an unexpected event that threatens the stability, reputation, or operations of the company's employees, buildings, franchisees, and support departments. It involves a wide range of activities and strategies designed to mitigate the impact of the crisis and protect the interests of the company and its stakeholders. The main goal of the Command Center is to minimize damages and ensure the company's survival and quick recovery after a planned or unplanned incident.

Prepare

The Command Center's preparedness initiative is to not only ensure each restaurant and operator is prepared to respond to a myriad of emergent incidents but also to ensure its staff and the Core team are educated on incidents around the U.S. that may or may not have an impact on the entire footprint. The Core team is comprised of key stakeholders from each support department and Operations. These individuals are empowered to represent their departments, make "on-the-spot" decisions, provide knowledge from their areas of expertise, and make or influence decisions that impact Operations and brand reputation. The team is dynamic, and not all members are used for every incident. The Command Center will determine which of the Core team members it will take to respond and recover from the incident.

The Command Center ensures that all restaurant management, field support teams, and each Core team member are prepared to deal with the myriad of incidents in the following ways:

- Operational and field teams are prepared through various platforms, including videos produced at the home office and provided to operators and field staff.
- Virtual training is offered to the regions that find it difficult and cost-prohibited to bring their entire team to one location.
- Quarterly training is available on a Teams call or provided by in-person training to restaurant teams as much as possible.
- Restaurant Operations and field support teams are kept abreast on all important information and updates through numerous daily email and text communications concerning upcoming severe weather, heat preparedness, hurricane preparedness, personal severe weather preparedness, and other issues that could impact the business or employees.
- A mass communication program is used daily, making it much easier to send multiple messages rapidly to the same group through templates.

Identify

Most threats to company restaurants across the 14-state layout come from mother nature. Torrential spring rains and tornados, severe winter storms, active tropical seasons, and other weather phenomena keep the Command Center team busy year-round. To help identify severe weather threats, the Command Center team uses two weather vendors – one for severe weather on land and one for tropical weather during hurricane season. Extreme weather impacts one or more restaurants across its 14-state enterprise every day, so getting that information out expeditiously to restaurants and field leaders is imperative.

Receiving severe weather reports from weather vendors through texts, emails, and vendor applications, the Command Center verifies the information before sending on to restaurants and field personnel. In the case of tornado warnings, restaurants go through a specific process, closing and securing the building for at least 30 minutes or until the threat no longer impacts the facility. If the threat is winter weather, the Command Center will send this information to restaurants as soon as possible so they can begin staff planning and product needs if roads are closed. Many lessons were learned from Winter Storm Uri in February 2021, but the most notable was to get information out early and often.

The Command Center also uses a tropical system weather vendor for threats from the Atlantic Ocean, Caribbean, and Gulf of Mexico during hurricane season. This vendor assists in identifying, analyzing, responding to, and recovering from tropical events that potentially impact coastal restaurants and employees. The tropical weather vendor provides the Command Center with daily assessments and forecasts of storms moving through the Atlantic, Caribbean, and Gulf. When it is evident a storm is going to make landfall near a Whataburger restaurant, the vendor provides the team with tropical meteorologists on all conference calls to give all engaged departments and franchisees the latest information and forecast so preparations and proper closures can take place. This information is used to make the best company and restaurant safety decisions.

Weather is not the only potential threat or activity the Command Center monitors and assesses. Other activities include power and water outages, boil water advisories, technology outages, fires, protests, demonstrations, social media, employee health, vehicle strikes, drive-thru issues, robberies, employee safety/injuries, fights, food safety, and new restaurant openings. The company is also currently opening an average of one new restaurant per week. There is an enormous amount of time taken each day identifying and assessing each of these events to see how it will impact the safety of employees and customers and potentially impact the company's brand reputation. Identifying threats across a wide area takes extraordinary threat intelligence.

The Command Center uses two threat intelligence vendors to receive clear vision and analysis of what occurs in and around restaurants, offices, learning centers, and Tier-1 suppliers. A quarter-mile circle is drawn around each of these locations. If any of these threats emerge in one of these circles, a notification is sent to the Command Center by email, text, app notification, and dashboard post. The information provided includes a brief description of the threat, the distance from the monitored location, the severity of the danger, when it occurred, and the ability to speak to an analyst to garner additional information about the incident. The team can then make decisions based on playbooks on who to engage, by what means, and how urgent this incident is to the business. It is imperative to be able to send the right information to the right people by the right means at the right time.

Respond

Strong leadership, clear and concise communication, and the ability to adapt to rapidly changing circumstances when responding to escalated incidents is what the Command Center provides on a daily basis. This concept depends most on trust and understanding from the restaurants and field support departments. These field teams know when they receive direction from the Command Center, it is the "Voice of Truth," and they feel comfortable following the directions.

The Command Center has 24 incident playbooks, which are step-by-step plans that outline the tasks and procedures each department will perform when responding to a specific incident. The tasks and procedures are updated annually and after each incident. Along with the playbooks is a communications matrix that outlines who the team communicates with, by what means, and how often. Response teams also use lists, checklists, and logs. Most major responses, such as hurricanes, are divided into phases, and procedures performed by each team depend on which phase of the incident.

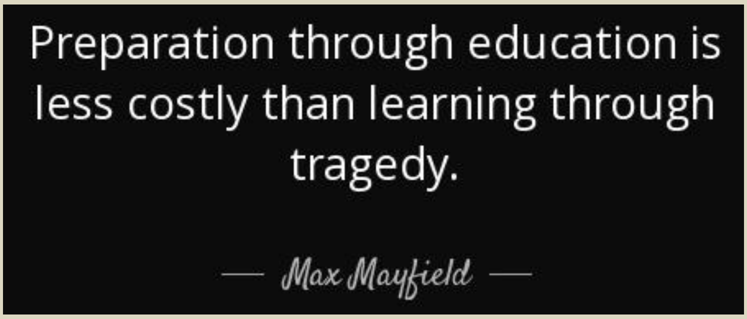
Recover

The priority once the incident has concluded is employee and customer safety. Whataburger goes to great lengths to ensure all employees have time to recover personally. Once the Command Center team knows the staff is ready, they use the recovery process to restore restaurants and the business to normal operations and hours, address residual restaurant or field team issues and unmet needs, and ensure all employees are recovering. The Whataburger Family Foundation addresses any employees' needs. The quicker the restaurant can recover, the sooner the company and its resources can assist the community in recovery.

Through it all, Whataburger remains committed to investing in the communities they serve. Its marketing and public relations teams will infiltrate the impacted area to assess how the company can fill voids or feed recovery teams and first responders after a critical event and meet the community's needs. Whataburger uses its food truck and volunteers to help communities in need by raising money for the community or feeding families in their time of need.

As the final recovery process, after all employees, customers, and communities fully recover, the Command Center will facilitate an after-action review, including lessons learned, best practices, and opportunities for improvement. These ideas and concepts are used to update all playbooks and task lists each department uses when responding to an escalated incident. This learned information is sent out again months later to ensure each team has addressed all issues.

Ron Derrick serves as the senior emergency manager at the Whataburger Command Center and oversees the daily operation of the Command Center and its staff. Ron spent over 30 years in fire and emergency medical services (EMS) and has been in emergency management since 1993. He has a bachelor's degree in emergency management from Jacksonville State University. Ron spent more than 20 years in the Kerrville Fire Department and Fredericksburg Fire and EMS and another six years as the operations manager for South-Central Texas for Acadian Ambulance Service. After a long fire and EMS career, he spent five years as the regional director of safety and emergency management for the Baptist Health System in San Antonio and six years as a senior controller in the USAA Command Center before taking his current position at Whataburger over five years ago. Ron is a Certified Business Continuity Professional and a certified State of Texas Pyrotechnic Operator. He has been a speaker at numerous conferences, including the TEEX Leadership Development Symposium and the Texas Division of Emergency Management Conference.



Preparation through education is less costly than learning through tragedy.

— Max Mayfield —

ICI
International
CBRNE INSTITUTE

A common roof for international CBRNE First Responders

☢ ☣ ☠

Join us!

Rue des Vignes, 2
B5060 SAMBREVILLE (Tamines)
BELGIUM

info@ici-belgium.be
www.ici-belgium.be