

# 2 CBRNE



ICI  
International  
**CBRNE**  
INSTITUTE

*Dedicated to Global  
First Responders*

# DIARY

April 2024



**Iran  
drone war**



**Postpone  
Opening Ceremony  
in river Seine  
before it is too late!**

**PART B**

**One-and-done  
vaccine  
protects against  
multiple coronaviruses**



ICI  
International  
**CBRNE**  
INSTITUTE



# DIRTY R-NEWS



## Final unit of Barakah Nuclear Energy Plant connects to UAE power grid

Source: <https://www.thenationalnews.com/uae/2024/03/23/final-unit-of-barakah-nuclear-energy-plant-connects-to-uae-power-grid/>



Mar 23 – The fourth and final unit of the [Barakah Nuclear Energy Plant](#) has been connected to the UAE power grid, the [Emirates Nuclear Energy Corporation](#) said on Saturday.

It paves the way for the delivery of the first megawatt of carbon-free electricity from the fourth reactor of the plant.

"We are proud to have achieved another critical milestone for the Barakah Plant, which stands as a testament to the UAE's leadership in the development of large-scale multi-unit nuclear fleets," said Mohamed Al Hammadi, managing director and chief executive of Enec. Unit 4 will add 1,400 megawatts of clean energy capacity to the national grid, Abu Dhabi Media Office said.

Barakah, the largest single source of clean electricity in the Middle East, is now months away from full operations.

The Federal Authority for Nuclear Regulation issued the first operating licence for Barakah's Unit 1 in February 2020 and another for Unit 2 in March 2021. Commercial operations at Unit 1 started in April 2021.

The next step before completion is to gradually raise power levels during Unit 4's testing phase, known as power ascension testing.

The process will be continuously monitored and tested until maximum electricity production is reached.

Once ready, Unit 4 will generate 25 per cent of the country's electricity needs for the next 60 years.

### Road to net zero

The Barakah plant is a key component of the UAE's clean energy transition and the push towards net zero by 2050.

Saturday's announcement comes months after nations signed a historic accord, at the Cop28 climate change conference in Dubai, to cut back on fossil fuel use. In its first year, Barakah's Unit 1 prevented the release of more than five million tonnes of carbon emissions that would previously have been generated by fossil fuels.

It was equivalent to more than "one million cars driven for a year", Enec said at the time.

By next year, the Barakah plant is expected to produce 85 per cent of Abu Dhabi's clean electricity and be the biggest contributor to reducing the national power sector's carbon emissions.

Nuclear power is regarded as a clean energy because it does not create the same emissions as fossil fuels such as oil and gas.



## Putin's nuclear warnings: heightened risk or revolving door?

By Stephen J. Cimbala, Lawrence J. Korb

Source: <https://thebulletin.org/2024/03/putins-nuclear-warnings-heightened-risk-or-revolving-door/>

Mar 28 – In his State of the Nation address February 29, Russian President Vladimir Putin issued one of his [most explicit warnings](#) about the danger of nuclear war in Ukraine and noted that Russian strategic nuclear forces “are in a state of full readiness” and able to hit targets in the West. In addition, Russian military files from 2008 to 2014—leaked recently to the [Financial Times](#)—seem to suggest that Russia’s threshold for nuclear first use is lower than Western military experts had assumed. Some 29 classified Russian military documents include discussions of war gaming and reportedly identify operational thresholds for the first use of so-called tactical or non-strategic nuclear weapons. Commenting on the unusual dump of secret Russian documents, Alexander Gabuev, director of the Carnegie Russia Eurasia Center in Berlin, said: “They show that the operational threshold for using nuclear weapons is pretty low if the desired result can’t be achieved through conventional means.”<sup>[1]</sup>

Coming on the heels of a suggestion by French President Emmanuel Macron that the option of sending NATO ground forces into Ukraine was under discussion within the alliance, the leaked documents on Russian nuclear first use seem both timely and significant.<sup>[2]</sup> On the other hand, in previous statements about Russian military doctrine for deterrence and possible nuclear employment, many Russian officials have stressed that nuclear weapons would only be used in response to a nuclear attack on Russia or its allies, or in cases of threat to the survival of the regime and nation posed by a war with conventional weapons. In response to the leaked documents, a Putin spokesperson commented: “The main thing is that the threshold for the use of nuclear weapons is absolutely transparent and is spelled out in the doctrine. As for the documents mentioned, we strongly doubt their authenticity.”

Regardless of the authenticity of these documents, references to the possibility of Russian nuclear first use in Ukraine cannot be treated as idiosyncrasies or departures from precedent. Putin himself has, on numerous occasions since the beginning of Russia’s war against Ukraine in February 2022, reminded NATO and the world that the nuclear option remains available should Russia choose to use it. He has also noted, in this regard, Russia’s superior numbers of non-strategic or tactical nuclear weapons compared to the US tactical nuclear weapons deployed in other NATO countries.<sup>[3]</sup>

Observers of varying backgrounds have put forward explanations for Putin’s saber rattling, all of which suggest the Russian president hopes, through nuclear threats, to achieve some current or future tactical edge in his country’s continuing face-off with Ukraine, the United States, and NATO. All that reasoning, however, cannot erase the dangerous reality: Any Russian first use of tactical nuclear weapons would create unprecedented conditions that could easily lead not to a regional Russian advantage, but to a wider nuclear war that would decimate Russia and its leadership (not to mention the rest of the world).

### Why is Russia making nuclear threats?

Since the Russian invasion of Ukraine in 2022, a variety of commentators have put forward at least five explanations for Putin’s propensity for nuclear saber rattling. **First**, some contend that Putin is bluffing. This is the argument of Ukrainian President Volodymyr Zelensky, among others. Zelensky feels that Putin’s nuclear diplomacy is designed to intimidate NATO into backing off from its support for Ukrainian sovereignty and independence. Others in and outside of Ukraine are more fearful of attacks with conventional weapons on Ukrainian nuclear power plants—and the residual effects of such strikes on public health, infrastructure and climate—than an actual Russian nuclear first use.

A **second** explanation for Putin’s nuclear threats is that they constitute a probe. Russian leadership is, as it were, taking the temperature of the United States and NATO, to see their reactions. This presents a dilemma for American and NATO European leaders. If they overreact to Putin’s intimidation, they appear fearful and potentially vulnerable to nuclear blackmail. If they simply ignore his comments about nuclear war, they may come across as lacking in awareness of the risks of escalation as fighting continues.

A **third** perspective on Putin’s nuclear rhetoric sees it as a response to Russia’s political and military setbacks since the war began in February, 2022. The initial objective of Russia’s so-called Special Military Operation was the prompt defeat of the Ukrainian armed forces and the abdication or surrender of its government, replaced by a Russian puppet regime. Instead, Russia found itself bogged down in a protracted war that has been extremely costly in both personnel and resources—hence the threat of nuclear weapons use, if the situation worsened. Putin has been dissatisfied with the performance of Russian armed forces on more than one occasion, and the weird attempt at a putsch by the erstwhile Wagner group created a temporary sense of chaos in the military chain of command. Wagner has since been scattered to the winds, and Russia’s military position relative to Ukraine has improved in the aftermath of the failed Ukrainian counteroffensive of the summer and the fall of 2023. Moreover, Russia’s superior numbers of available and potential military personnel



and war-supporting industrial resources, relative to those of Ukraine, create the potential for an endless stalemate with outcomes favorable to Russia. But the situation remains uncertain, and so the nuclear saber-rattling continues.

A **fourth** perspective on Putin's nuclear diplomacy asserts that he is laying the predicate for escalation to nuclear first use if unexpected battlefield reverses threaten to destabilize Russia's operational-tactical position for the defense of important objectives. NATO support for Ukraine provides that county not only with military hardware such as tanks, armored personnel carriers, long range missiles and antimissile systems, and the like, but also with the "software" of warfare, including C4ISR (command, control, communications, computers, intelligence, surveillance and reconnaissance) assistance with navigation, warning, special operations, and strategic deception. On more than one occasion, Ukrainian brainpower has outmaneuvered Russian muscle. But the Russians are learning fast and have upped their game significantly since the embarrassing blunders of 2022. Moreover, Russian armed forces have demonstrated in training exercises superior understanding of the extreme complexity of modern airland battle and its potential risks and costs. They are also aware of the difficulties in operational-tactical maneuver on a nuclear battlefield.<sup>[4]</sup>

A **fifth** possible interpretation of Putin's propensity for nuclear rhetoric is that it reflects the reasoning of some Russian military and political thinkers about the management of escalation toward favorable outcomes by the manipulation of risk. According to this line of reasoning, nuclear first use is one point on a continuum of coercion that extends from the lowest point on the conflict spectrum up to the crossing of the threshold from conventional into nuclear war. Prominent Russian analyst [Sergei Karaganov's essay](#), "A Difficult but Necessary Decision," argued that a Russian tactical nuclear first use somewhere in Europe might be necessary to shock NATO back into its senses and concede to Russia's view of the situation in Ukraine.

Still, it is clear that many experts within Russia are not aligned with Karaganov's high-octane nuclear chest-thumping. For example, Ivan Timofeev, director general of the Russian International Affairs Council and a widely published academic, [noted that Karaganov's approach](#) "underestimates the Western elites' determination to climb the escalation ladder with Russia, and, if necessary, ahead of it" and "overlooks the possibly catastrophic consequences for Russia itself." According to noted military theorist Dmitry Adamsky, Russia offers a cross-domain cocktail of conventional war-fighting and nuclear deterrence options. Crossing the nuclear threshold would most likely occur when Russia felt that its nonnuclear escalation options had been exhausted and its nuclear rhetoric had thus far proved futile. Even then, prior to actual nuclear first use, a "muscle-flexing" phase of gradually increasing "strategic gestures" will be used to communicate resolve and capability to climb the escalation ladder, Adamsky writes.

### The limits of nuclear threats

The preceding discussion focuses on a Russian decision for conventional war or nuclear escalation without reference to the possibility of a Russian-Chinese coordination of tactics and strategy in regional wars. US deterrence and defense requirements for a simultaneous Russian and Chinese regional aggression assume a greater need for forward-deployed forces and power-projection capabilities than hitherto.<sup>[5]</sup> The final report of the Congressional Commission on the Strategic Posture of the United States warned that US objectives must include "effective deterrence and defeat of simultaneous Russian and Chinese aggression in Europe and Asia using conventional forces" and that, if existing conventional forces were inadequate to this objective, US strategy would have to be adjusted to increase reliance on nuclear weapons "to deter opportunistic or collaborative aggression" in the other theater.<sup>[6]</sup>

One should be cautious, however, in estimating the sizes and capabilities of future Russian and Chinese nuclear forces. Nor can it be assumed that the current rapprochement between Russia and China will be everlasting or apply to all issues of military significance. China and Russia have a history of border conflicts and Cold War disagreements, and China's world historical view is somewhat apart from Russia's.

William Alberque, director of strategy, technology and arms control at the International Institute for Strategic Studies think tank, has provided a concise description of the possible roles for non-strategic nuclear weapons in Russian military strategy: "detering unwanted conflicts; coercing adversaries; shaping the battlefield for planned conflicts; controlling escalation within conflicts to protect the Russian homeland; preventing outside powers (read: the United States) from intervening in its conflicts; and ensuring that it prevails in war."

Notwithstanding the rationale, the decision to move from nuclear deterrence to nuclear first use in Europe or Asia would be a world-historical marker—and not one of progress. The firebreak between non-strategic and strategic nuclear warfare has never been tested under exigent conditions, and indeed, part of the deterrent efficacy for tactical nuclear weapons lies in their potential coupling to strategic nuclear war. Putin's assertive nuclear rhetoric is strategically unhelpful and politically dangerous.

### Notes

[1] Gabuev, cited in Max Seddon and Chris Cook, "Leaked Russian military files reveal criteria for nuclear strike," *Financial Times*, February 28, 2024, in *Johnson's Russia List 2024 – #51 – February 29, 2024*

[2] Anatol Lieven and George Beebe, "Europeans' last ditch clutch at Ukrainian victory: France's Macron raised the idea of Western troops entering the fray, others want to send longer range missiles. It's all



folly.”, *Responsible Statecraft*, February 28, 2024, in *Johnson’s Russia List 2024 – #51 – February 29, 2024*

[3] Hans M. Kristensen, Matt Korda, and Eliana Johns, *Bulletin of the Atomic Scientists, Nuclear Notebook: Russian Nuclear Weapons: 2023*, May 9, 2023, <https://thebulletin.org/premium/2023-05/nuclear-notebook-russian-nuclear-weapons-2023/>

[4] Dr. Lester W. Grau and Charles K. Bartles, *The Russian Way of War: Force Structure, Tactics, and Modernization of the Russian Armed Forces* (Ft. Leavenworth, Kansas: Foreign Military Studies Office, 2016), pp. 201-203 and 206.

[5] The White House, *National Security Strategy* (Washington, D.C.: October, 2022), pp. 23-26.

[6] Madelyn R. Creedon, Chair, and Jon L. Kyl, Vice Chair, *America’s Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States* (Washington, D.C.: October 2023), p. xiii.

**Stephen J. Cimbala** is a Distinguished Professor of Political Science at Penn State University, Brandywine.

**Lawrence J. Korb** is a senior fellow at the Center for American Progress. He is also an adjunct professor of security studies at Georgetown University. Prior to joining the Center for American Progress, he was a senior fellow and director of National Security Studies at the Council on Foreign Relations. Korb served as assistant secretary of defense (manpower, reserve affairs, installations, and logistics) from 1981 through 1985. In that position, he administered about 70 percent of the defense budget. Korb served on active duty for four years as a Naval Flight Officer and retired from the Naval Reserve with the rank of captain.

## An interview with Annie Jacobsen, author of ‘Nuclear War: A Scenario’

By Michael Mechanic

Source: <https://thebulletin.org/2024/04/an-interview-with-annie-jacobsen-author-of-nuclear-war-a-scenario/>

Apr 01 – Nuclear war is a topic few care to think about. We sometimes call it *unthinkable*. But we need to think carefully, and to talk—particularly with high-ranking foreign officials whose motives we may have reason to distrust, just as they distrust ours—about how we can collectively avoid launching a weapon that would end our civilization.

Pulitzer Prize finalist Annie Jacobsen’s timely new book, *Nuclear War: A Scenario*, is a lightning-fast read intended to put the nuclear threat squarely back on everyone’s radar. Her narrative thread, as the title suggests, is a fact-based (though thankfully fictional) scenario that shows how a nuclear launch can escalate into World War III at dizzying speed.

Jacobsen tees up her cinematic approach with chapters describing how we got here, including a discussion of America’s Single Integrated Operational Plan (SIOP) for General Nuclear War—which was devised in the 1960s and, as Jacobsen details in [this book excerpt](#) published today by *Mother Jones*, was more or less a recipe for the end of the world.

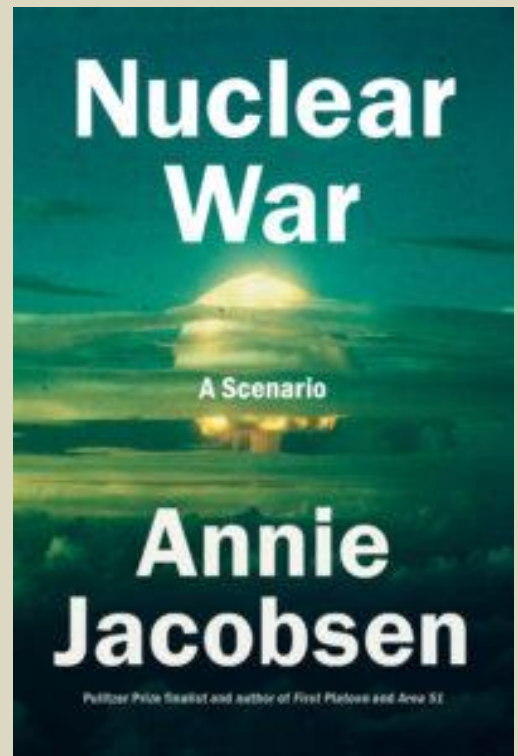
Because that’s nuclear war: One bad assumption, one shot, one retaliation, and it’s unstoppable.

**Your book is frightful. What made you want to write in such detail how a nuclear war could unfold?**

As a national security reporter, I have written [six previous books](#) on military and intelligence programs—CIA, Pentagon, [DARPA](#)—all designed to prevent nuclear World War III. During the Trump administration, amid the “fire and fury” rhetoric, I was watching [STRATCOM](#) commanders and deputy commanders speak freely on C-SPAN about the dangers therein. I began to wonder, *My god, what would happen if deterrence failed?* I began to interview people during COVID, when people had more time on their hands for someone like me—and that began the terrifying process of learning that nuclear war is, in essence, a sequence of events, and that once it starts it almost certainly will not stop.

**The US public hasn’t thought a whole lot about nuclear weapons since the Cold War. We have more nuclear nations today, but far fewer weapons in the global arsenal. Are we safer now?**

Well, as I show in the book, it doesn’t take but one weapon to set off a chain reaction to unleash the current arsenal, which is forward deployed in launch-on-warning positions and could be fired in as little as a minute—15 minutes for the submarines. There are enough weapons in those positions right now to bring on a nuclear winter that would kill an estimated 5 billion people.



Are there too many? Absolutely. Have we made progress? The all-time high in 1986 was 70,481 nuclear weapons. Now, there are approximately 12,500. But to your point, there are nine nuclear-armed nations, not just two or three superpowers. And that presents a lot of unknowns that create serious unease and room for catastrophe.

**So we may be less safe because we don't really know how certain nations might behave—notably North Korea.**

Absolutely. Reporting and writing this book was one surprise after another. For example, I did not know until I had it confirmed with US nuclear experts that North Korea does not announce any of its missile tests, whereas the other countries do. North Korea has launched 100 missiles since January 2022. After you read my book, you realize what happens to the US nuclear command and control apparatus in the seconds and minutes after a launch is seen by the advanced super satellite system we have. You can now imagine what goes on in those command centers.

**A total frenzy.**

*Imagine!*

**One thing that really struck me is the unbelievable speed at which nuclear war is waged.**

Gen. [Robert Kehler](#), the former commander of STRATCOM, said to me that the world could end in the next couple of hours. It took me a minute to ask my next question, because coming from someone in that position of authority—the most significant role in the entire nuclear apparatus—that really blew my mind.

Ditto goes for an interview I did with President Barack Obama's FEMA chief, Craig Fugate. Of course, FEMA is the agency in charge of what's called population protection planning for American citizens in the event of hurricanes, floods, earthquakes. Fugate told me that after a nuclear war, there wouldn't be any population protection planning because everyone would be dead.

**Help is *not* coming.**

I said, "Well, what should people do?" He more or less said, "Self-survive, and don't forget your morals, and I hope you stocked Pedialyte"—because radiation poisoning makes you vomit and have diarrhea and away go all of your electrolytes, which leads to secondary problems.

**I learned from your book that FEMA plays a unique role in the event of a nuclear attack, and it's not what one might expect.**

That's right. In the '50s and '60s, the US position was that a nuclear war could be fought and won. That is no longer the official position. But plans were put in place for the [continuity of government](#) programs—the idea that the government must continue functioning no matter what. That is also a fantasy.

To hear from former Secretary of Defense [Bill Perry](#) about the madness and mayhem and anarchy that would follow, in his mind, in the event of a nuclear war, you really get the sense that civilization will fail. I believe one of the reasons so many of these sources went on the record for me is because they know that this is the truth. And they know it is up to the people to change the trajectory of where we're headed. I mean, my god, look at [the saber-rattling](#) going on as we do this interview.

**Potential nuclear nightmares range from an accidental detonation to a massive "decapitation" strike to someone using a small nuke on the battlefield. You picked the madman scenario: North Korea inexplicably launches a long-range missile at Washington, DC. Why that one?**

I did a series of interviews with [physicist] [Richard Garwin](#), who is now 95. He is arguably the most knowledgeable person about nuclear weapons on the planet, and he probably knows more about policy over the long lens of history because he was 23 or 24 years old when he designed [the first thermonuclear bomb](#).

In the "Ivy Mike" test, it exploded with 10.4 megatons of power—about 1,000 Hiroshimas. Garwin said to me that his biggest fear was now, and always had been, the madman theory you referred to. He used the French phrase *Après moi, le déluge*—after me, the flood—referring to this idea that a maniacal, egotistical, narcissistic madman leader could launch a nuclear weapon for reasons no one would ever know.

**And to counterattack North Korea, as in your scenario, the US would need to send missiles over Russia, which has a very unreliable early warning system.**

That's right. Learning about the technological limitations of some of the Russian systems was just as terrifying as any part of reporting this book.

**It's almost like you'd want to reach out to the Russians and say, look, just take our technology so you won't launch on a false alarm—but the US would never do that.**

There have been many opportunities to have a dialogue with the Russians—Putin [inquired](#) about joining NATO back during the Clinton administration. One really has to lean upon one's leaders to think about communicating rather than saber-rattling, because I hope that my book demonstrates in appalling detail how horrific nuclear war would be. And we know from the Proud Prophet war games that no matter how it begins, it ends in nuclear apocalypse.

**For context, Proud Prophet was a classified series of war games President Ronald Reagan ordered in 1983. Civilian and military planners convened for two weeks to run through scenarios that could spark a nuclear war and see how they played out.**



That Proud Prophet was declassified is interesting. Nuclear war games are among the government's most jealously guarded secrets. I printed a copy of what a couple pages of the declassified war game look like—95 percent is redacted. It's literally a couple of headers and a few numbers.

But when something like that gets declassified, it becomes very valuable to the people. An individual like [Paul Bracken](#)—a civilian professor at Yale who participated in Proud Prophet—can now speak about it in general terms. He wrote in his own book that everyone left very depressed, because no matter how the nuclear scenario begins—if NATO is involved or not involved, China is involved or not—it always ends the same way, the most terrible way, because America has a “launch on warning” policy.

We do not wait to absorb a nuclear blow. Once a missile is on the way and there is secondary confirmation from ground radar, the president is asked to launch a counterstrike. In the book—I have the president asking this because it came up in my discussions with sources—he says, “How do we know it's a nuclear weapon?”

#### **And we don't.**

That is a fact. The answer is, Well, it *could* be a biological weapon. Another answer I was told is that no one launches a ballistic missile at the United States unless they're expecting a counterattack. So now you are looping into the Orwellian world of: This is deterrence. Deterrence will hold. *Don't you dare launch at us or else!* Which becomes part and parcel for why the counterattack is required, per the deterrence doctrine. There is no room for saying, well, maybe we'll wait and see.

#### **Once you break deterrence, everything else goes out the window.**

Correct. One of the most haunting quotes in the book is from the deputy commander of STRATCOM, Lt. Gen. Tom Bussiere. I located an unclassified discussion he had with insiders, and the quote is along the lines of, *When deterrence fails, it all unravels*. In seconds and minutes and hours—not days and weeks and months.

#### **Twelve thousand years of civilization extinguished in a few hours.**

General Kehler was not speaking hyperbolically when he said that.

#### **Say more about “launch on warning.” You cite [Paul Nitze](#), a former defense secretary and later presidential adviser, calling the policy “inexcusably dangerous.” Presidents Bush, Obama, and Biden wanted it scrapped. So why is it still in place?**

I'd like to shout out [William Burr](#), who runs the National Security Archive at George Washington University, because many of those quotes and documents come from that organization, which made them accessible to journalists like me. Nitze was one of the biggest hawks across the Cold War. To have a guy like that go on the record and say this is inexcusably dangerous says a lot.

Multiple presidents have campaigned on the promise that they will change this dangerous policy, but then they become president and you never hear of it again. That speaks to the kind of secret-keeping that is dangerous and can be changed. I wrote [Nuclear War: A Scenario](#) for the layperson to be able to rip through it in a night, no matter how terrifying. I do not bog the reader down with polemics or jargon, because this is an issue everybody should know about. Because only in knowing about it is change possible. We can look to *The Day After* battle, what's known in inner circles as the Reagan Reversal policy of 1983.

#### **Wait, what's that?**

So in 1983—I'm dating myself here—I was a high school student. And I watched the ABC movie [The Day After](#).

#### **I was the same age, and watching it too.**

It's a fictional account of a nuclear war between America and Soviet Russia, and half the country watched it. Interestingly, behind the scenes, ABC got a lot of pressure not to air it. Well, one very important American watched it: Reagan had a private screening at Camp David. His chief of staff tried to suggest that he shouldn't watch it, but he did. And he wrote in his diary that he became “greatly depressed,” and he picked up the phone and called [then-Soviet President Mikhail] [Gorbachev](#), and the two leaders communicated—which is really the only solution for any of this.

Because of those communications and because of their conference and because of the treaty, the insane nuclear arsenal has been reduced to the approximately 12,500 we have now, which is a considerable reduction. The president's position prior to seeing *The Day After* was a much harder, more saber-rattling approach. He changed his position and became much more dovish.

#### **“Launch on warning” puts extraordinary pressure on a president. The one in your scenario is pretty clueless. He hasn't ever rehearsed. Nobody told him he'd have just six minutes to choose from a Denny's breakfast menu of existential options in response to what may or may not be an incoming nuke. It's hard to believe the Pentagon doesn't put every new president through a series of war games.**

I was just as surprised as you are. But that's coming from multiple secretaries of defense and national security advisers—people in a position to advise the president on a nuclear counterattack. The best summation came from Leon Panetta, who explained that as White House chief of staff he was witness to the fact that the president is primarily concerned with domestic issues—like his popularity. I asked Panetta how clued in he was when he was the CIA director, and he said almost not at all, because the CIA is about intelligence, not nuclear operations.

Only when he became secretary of defense did it really hit home, the weight of all of this. He spoke about visiting missile silos, submarine bases, and nuclear command bunkers—once you go to places like that,





your entire perspective changes. And that is why I believe he was willing to go on the record. You really get the sense that things are precarious once they begin, and decisions follow that are out of everyone's control.

**Right. And our continued existence depends not only on our internal communications and processes, but those of our adversaries, about which we know little.**

Absolutely.

**Your book busts some common myths, for instance the belief that the US could shoot down an incoming nuclear missile. We really can't defend against nuclear weapons, can we?**

We can't. That is pure fantasy. During the final fact-checking incantations, I had the book read by a lieutenant general who ran these scenarios for [NORAD](#). I was almost hoping someone would say, Annie, you should take this part out of the book, because we have a secret Iron Dome that you can't report on. No. The truth is that the United States relies upon 44 interceptor missiles to stop any incoming missiles. Russia alone has 1,674 nuclear warheads in "ready to launch" position. Adding to that, according to congressional reports, the interceptors are only approximately 50 percent effective.

**Under the best of circumstances.**

Absolutely, like when you're doing a test and you know precisely where the missile is going to be. It's a curated test. So people have this idea that we have an Iron Dome-type shield. And we don't.

**The Reagan Reversal bit reminds me of a moment from your scenario. Your secretary of defense is sworn in as president because the president and others in the line of succession are dead or AWOL, and he has this moment of humanity. Russia has launched all its ICBMs at us, so we know we're goners. And the new guy asks: *Why respond now if all it will do is kill millions more people?* The STRATCOM commander is like, *Nope, we're doing this.* Humanity is already doomed, yet Russia and the United States keep launching their weapons until practically none are left. It's nonsensical. But is it realistic?**

It is if you talk to the sources I spoke to. A lot of the decision-tree situations involving the defense secretary came from my multiple discussions with former Secretary of Defense Bill Perry, who has thought a lot about this—and what an individual's thought process would be. The point of including that question was to demonstrate how the madness of MAD—mutual assured destruction—takes over.

I asked [retired weapons engineer] Glen McDuff—the curator of the classified museum at the Los Alamos National Laboratory—the question you're *kind of* asking me: What did he think, as an insider, about the notion that people would not follow orders? He basically said: Annie, I would suggest betting on Powerball, because you'd have a better chance of winning than betting on a high-ranking individual in the nuclear command and control system not following orders.

**Right. It seems like folks in the nuclear command and control structure have rehearsed these scenarios over and over. They're on autopilot to a degree. Which gets at the notion of "apes on a treadmill" that you write about late in the book: We've made this plan, and we're going to follow it—even if it's completely bonkers.**

Apes on the treadmill was just such a brilliant concept. It goes back to the Cold War when it was used as a metaphor for people slavishly following away in this nuclear arms race.

But even more interesting was the present-day anecdote I found. It was a scientific experiment having nothing to do with the original metaphor but was *literally* apes on a treadmill. The researchers were studying bipedalism: They put humans on the treadmill and they put apes on the treadmill. Anecdotally, one of the scientists said, and I'm paraphrasing, that some of the apes got fed up with walking to nowhere and got off the treadmill.

I thought, my god, the apes are smarter than the humans when it comes to mutual assured destruction.

**Michael Mechanic** is a senior editor at *Mother Jones* and the author of [Jackpot: How the Super-Rich Really Live—and How Their Wealth Harms Us All](#).

## Domestic Violent Extremists' Threat to U.S. Nuclear Facilities

Source: <https://www.homelandsecuritynewswire.com/dr20240402-domestic-violet-extremists-threat-to-u-s-nuclear-facilities>

Apr 02 – A new study examines the growing threat domestic violent extremists pose to U.S. critical infrastructure. In a Stimson Center study, [The Threat from Within: An Overview of the Domestic Violent Extremist Threat Facing US Nuclear Security Practitioners](#), Sneha Nair, Anna Pluff, and Christina McAllister write that domestic violent extremist threats to U.S. nuclear facilities prove that the nuclear security status quo is at risk.

The add:

Nuclear security in the U.S. has historically understood threat as 'other' – leaving practitioners, facilities, and physical protection systems vulnerable to threats from within: a glaring vulnerability that was made public in the wake of the 2021 Capitol Breach. Urgent change to the nuclear



security norms and understanding of threat to include not only foreign agents, but also domestic violent extremist groups and homegrown violent ideologies, is needed to strengthen the resiliency and effectiveness of the national nuclear security regime.

....

The emboldening of non-state actors through the proliferation of accelerationist ideologies among domestic violent extremist (DVE) groups pose a threat, not only to national security, but to the nuclear facilities that make up part of the nation's critical infrastructure. Compounding these risks are intersections of insider threats and accelerationism that demonstrate the shortcomings in the protective frameworks designed by the traditional national and nuclear security decision-makers in the United States. Traditional assumptions informing security priorities are no longer sufficient to address emerging threats and evolving operational environments, because they fail to adapt to new actors and shifting environments.

Here are excerpts from the study:

### Executive Summary

The events of the 21st century have required a reimagining of how nuclear security practitioners perceive threats in the United States. With the rise of terrorism concerns over the last two decades came the increase in the security risk posed by non-state actors to nuclear facilities. Insider threats and non-state actors are the most persistent concerns facing nuclear security practitioners – but the notion of who or what constitutes a threat is so deeply rooted in antiquated understandings of an adversary, that the U.S. nuclear security regime as a whole has struggled to address the risks posed by domestic violent extremists.

The emboldening of non-state actors through the proliferation of accelerationist ideologies among domestic violent extremist (DVE) groups pose a threat, not only to national security, but to the nuclear facilities that make up part of the nation's critical infrastructure. Compounding these risks are intersections of insider threats and accelerationism that demonstrate the shortcomings in the protective frameworks designed by the traditional national and nuclear security decision-makers in the United States. Traditional assumptions informing security priorities are no longer sufficient to address emerging threats and evolving operational environments, because they fail to adapt to new actors and shifting environments.

Illustrating the risk posed by DVE actors and the vulnerabilities that can be exploited by insiders is a crucial step towards redefining 'threat' and understanding why the status quo is insufficient in the current threat landscape. The January 6, 2021, insurrection at the U.S. Capitol revealed the flaws in a system designed to weed out unsuitable candidates for sensitive work protecting nuclear materials, weapons, facilities, technology, and personnel. Understanding the limitations of the current system and the efforts underway by federal agencies to mitigate the DVE threat to nuclear and national security is a critical first step in creating a more sustainable and resilient national nuclear security regime.

### Introduction

In the aftermath of 9/11, the bulk of U.S. national security efforts – and subsequent nuclear security initiatives – were oriented towards protecting the country against a jihadist foreign terrorist organization and their efforts to cultivate homegrown violent extremists in the United States. These acts of terror were pivotal for the resurgence of nuclear security. The international community banded together against the proliferation of weapons of mass destruction with the adoption of UN Security Council Resolution (UNSCR) 1540 – acknowledging the devastating potential of non-state actors with malign intent acquiring nuclear, radiological, chemical, or biological weapons – supported further by UNSCR 1373 and the International Convention for the Suppression of Acts of Nuclear Terrorism.<sup>1</sup> Initiatives like the Global Initiative to Combat Nuclear Terrorism and the G7 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction (Global Partnership) aimed to strengthen global norms to prevent, detect, and respond to nuclear terrorism through multilateral activities and assistance.<sup>2</sup>

In the United States, this commitment to the physical protection of nuclear materials, weapons, facilities, technology, and personnel was no less salient – and the U.S. has proven itself a leader in nuclear security in light of the vulnerabilities it has faced at home. This led to nuclear security experts, national security advocates, and policymakers calling for stronger leadership and initiative to combat the threat of nuclear terrorism as not only a national security issue, but a regional and international security priority – and to place focus on the threat posed by insiders, rather than the traditional purview of external actors who could be deterred by 'guns, guards, and gates.'<sup>3</sup> Through the Nuclear Security Summits, 52 countries and international organizations produced over 1000 new nuclear security commitments over six years – resulting in the Amendment to the Convention on Physical Protection of Nuclear Materials entering into force, the creation of the International Atomic Energy Agency's International Conference on Nuclear Security series, and the Fissile Material Working Group (now the International Nuclear Security Forum) for civil society advocacy and participation in nuclear security work.<sup>4</sup> However, attention



on nuclear security has waned. And today's shifting threat landscape challenges the nuclear security concepts of the early 2000s.

Since 9/11, the nature of the threats facing the U.S. has evolved. Rather than focusing on international extremists with foreign ideological motives, federal agencies and law enforcement have begun to recognize the prevalence of domestic violent extremist threats to national security and critical infrastructure, including the nuclear sector. In 2021, U.S. Attorney General Merrick B. Garland and Homeland Security Secretary Alejandro N. Mayorkas identified the greatest domestic threat facing the United States as “racially or ethnically motivated violent extremists,” specifically highlighting white supremacists.<sup>5</sup> While anti-government, white supremacy and neo-Nazi ideologues have long existed within the fabric of U.S. society, before 9/11, many of these extremist groups or individuals were mostly rejected or were confined to the fringes of the social order. Online extremism and the January 6, 2021, attack on the U.S. Capitol have raised these groups' visibility, while social media tools have helped them to proliferate their ideology and coordinate effective messaging and tactics. This paper will examine how the events of January 6, 2021, have shifted understanding of U.S. national security threats, explore strands of DVE ideology that specifically target the nuclear sector, and present case studies of DVE actors relevant to nuclear security before laying out U.S. government approaches and challenges in addressing this type of threat. We conclude by positing that the security community has not sufficiently redefined threat and present case studies of DVE actors.

### **The Domestic Violent Extremist Threat**

#### ***POST-JANUARY 6<sup>TH</sup> AND THE CURRENT DVE THREAT***

Many scholars have pointed to January 6<sup>th</sup> as the catalyst for renewed attention on insider threats and domestic violent extremism as national security priorities.<sup>6</sup> Both the FBI and the Department of Homeland Security have since recognized the evolving threat landscape since 9/11 and national and nuclear security priorities have slowly shifted from its long-time focus on international jihadists and foreign radicalization, towards domestic terrorists. In the aftermath of the 1995 Oklahoma City bombing, the issue of “insider threats” was at the forefront of U.S. counterterrorism efforts, but failed to evolve in the post-9/11 environment.<sup>7</sup> In the weeks following the siege, a new picture of the threat landscape emerged as the Department of Justice and FBI launched a nationwide effort to investigate the participants of January 6<sup>th</sup>. The investigation revealed that most participants were adherents of extremist ideology, many of whom were radicalized online and mobilized to take part in the insurrection. Some also adhered to a DVE ideology of concern for nuclear security, accelerationism, which is described in more detail later in this paper.

What is concerning, however, is the original failure of the FBI to anticipate the Capitol attack in the first place. Before the end of the 2020 presidential race, a team of intelligence analysts tried to game out the worst potential outcomes of a disputed election. But they never thought of the one that transpired: a violent mob mobilizing to overturn the election in support of Donald Trump.<sup>8</sup> Adam Goldman and Alan Feur write that the FBI was “[a]pparently blinded by a narrow focus on ‘lone wolf’ offenders and a misguided belief that the threat from the far left was as great as that from the far right,” thus, officials at the bureau did not anticipate or adequately prepare for the attack.<sup>9</sup> This confirmation bias also failed to account for actors such as militia groups or white supremacists, who took a leading role in the Capitol siege.

In May 2021, Attorney General Merrick B. Garland and Homeland Security Secretary Alejandro N. Mayorkas identified the greatest domestic threat facing the United States as “racially or ethnically motivated violent extremists,” specifically, white supremacists.<sup>10</sup> White supremacist extremists pose the primary threat among all domestic violent extremists. The Department of Homeland Security (DHS) provided data showing that white supremacists were responsible for 51 out of 169 domestic terrorist attacks and plots from 2010 through 2021, the highest number among domestic terrorist ideologies.<sup>11</sup> In October 2022, the FBI and DHS issued a report titled “Strategic Intelligence Assessment and Data on Domestic Terrorism,” which put forth the most significant threat facing the U.S. as being posed by “lone offenders and small groups of individuals who commit acts of violence motivated by a range of ideological beliefs and/or personal grievances.”<sup>12</sup> The report also contended that of these actors, “domestic violent extremists represent one of the most persistent threats to the United States today.”<sup>13</sup>

The January 6<sup>th</sup> Capitol riot compelled the Biden Administration to prioritize the issue of domestic extremism. FBI Director Chris Wray condemned the January insurrection as “domestic terrorism” and described in stark terms the threat domestic violent extremists posed to the United States.<sup>14</sup> While not every individual involved in the attack was part of a militia or right-wing group, many shared common beliefs.

### **DVE, Accelerationism, and Critical Nuclear Infrastructure**

Domestic violent extremism (DVE) is an all-encompassing category that includes a variety of ideologies, including anti-government extremists, anarchists, anti-abortion extremists, white



supremacists, involuntary celibates, ecoterrorists, and a smattering of other assorted extremists from across the political spectrum.<sup>15</sup> While DVE represents a range of threats, the interest in nuclear terrorism by accelerationist white nationalist groups represents a particular security concern for the nuclear policy community.

### **CRITICAL INFRASTRUCTURE**

One commonly shared feature of DVE adherents is the focus on attacking critical infrastructure – including nuclear power plants. Attacks on U.S. energy infrastructure are increasing.<sup>16</sup> Recent incidents on infrastructure include six “intrusion events” at Florida substations in September 2022; six attacks on substations in the US Northwest in November and December of 2022; four substations vandalized in Washington State cutting power to 14,000 on Christmas Day, 2022; and a December 2022 North Carolina “targeted attack that left thousands without power.”<sup>17</sup> Attackers often seek to attack regional power substations in order to cause economic distress and civil unrest. Leftist, anti-statist, accelerationist groups have also emerged on Telegram, to espouse their views that the U.S. electrical grid must be systematically attacked and dismantled. Telegram has attempted to remove much of the content but has been ineffective at regulating its content to filter extremist messaging.<sup>18</sup> As laid out in detail in the Case Studies section below, white supremacists Brandon Russell and Sarah Clendaniel were arrested in February 2023, on federal charges of plotting to shoot up a ring of subpower stations in Baltimore. The intent was to “destroy” Baltimore, a majority Black city.<sup>19</sup> Greg Harman writes that the “arrest reflects a sustained mobilization of homegrown neo-Nazi networks, whose members are seeking to disrupt the nation’s power supply in hopes of ushering in economic collapse and race war.”<sup>20</sup>

DVE and insider threats thus represent a particular area of concern for nuclear security, as evidenced by the Institute of Nuclear Management’s (INMM) exploration of the intersection of homegrown violent extremism and the security of nuclear facilities at its 63<sup>rd</sup> Annual Meeting. Indeed, prior to targeting the Baltimore grid, Brandon Russell had expressed interest in taking out a Florida nuclear plant.<sup>21</sup> Russell’s case is not an outlier. Other domestic violent extremist actors have illustrated the vulnerabilities in how security practitioners identify threats to nuclear security across the ideological spectrum – from other far-right actors like Matthew Gebert and Ashli Babbitt in recent years, to the jihadist radicalization of Sharif Mobley following the 9/11 attacks. The Case Studies section of this paper presents more detail on each of these cases.

### **ACCELERATIONISM**

Accelerationist ideology, which holds that the modern, Western democratic state is so mired in corruption and ineptitude that true patriots should instigate a violent insurrection, ultimately allowing a new, white-dominated order to emerge, presents additional concerns for the nuclear security community as some groups advocate for the use of nuclear weapons to achieve the new order.<sup>22</sup> Accelerationist dogma is often adopted by adherents who subscribe to an ‘alternative history,’ one that usually serves as a foil to the increasing racial diversity of American society. Accelerationists have created a historical narrative that utilizes stock footage, still images, and classical literature to assemble a romanticized image of an American past that valued whiteness, marriage, family values, and religiosity to claim that these values are in decline and to recruit membership from involuntary celibates (incels) and young, white men who wish to return to a manufactured past.<sup>23</sup>

One accelerationist group that caught the attention of the nuclear community is the Atomwaffen Division (AWD). AWD was organized as a series of terror cells advocating for the use of nuclear weapons to yield the collapse of civilization. Unlike some other white power activists, accelerationists believe modernity “has reached such a level of degeneracy and corruption that it cannot be rescued through mass movements or other political means.”<sup>24</sup> Many of the most violent manifestations of domestic violent extremism in the U.S. are encouraged by “mobilizing concepts.”<sup>25</sup> Mobilizing concepts are different from traditional ideological frameworks, which are rooted in more clearly articulated beliefs or theories about how political or economic systems should work (anarchism, communism, fascism, etc.). An understanding of these neo-fascist accelerationist groups as a fluid network with broader goals of social destruction, rather than individual units with distinct ideological perspectives helps understand the continued relevance of AWD and its mission even after its dormancy in 2017.<sup>25</sup> The effectiveness of these mobilizing concepts and the fluid nature of the ideological network can be seen in how AWD has inspired similar neo-fascist accelerationist groups such as The Base, which unlike AWD, has tried to veil its desire to spark a “nuclear civil war” behind claims that it is focused on maintaining a “survivalism and self-defense network” in an effort to recruit broader membership.<sup>26</sup>

Another offshoot of the now-defunct neo-Nazi terror group Atomwaffen Division recently undertook a propaganda push to capitalize on the December 2022 power grid attack in Moore County, which resulted in widespread power outages affecting 40,000 customers.<sup>27</sup> The morning after the attack, neo-Nazi accelerationists on a private Telegram channel began to speculate about the involvement of the National Socialist Resistance Front (NSRF).<sup>28</sup> NSRF represents



another rotating face of a network of neo-fascist groups that seek to use terror to promote their ideological goals of a new white-led order. In weeks leading up to the Moore County power grid attack, members of Uncle Ted's Cabin channel distributed multiple terror manuals that encourage mass shootings and industrial sabotage.<sup>29</sup>

While not all accelerationist or DVE groups have nuclear ambitions, examining AWD and its ability to influence other extremist groups provides a clearer understanding of the threat landscape. Insights into membership mobility can inform preventative actions by governments and emphasize the importance of examining the ties between accelerationist groups, to ensure that DVE groups remain unable to acquire nuclear materials, weapons, technology, or information that would advance their cause.

....

### Conclusion

Assessing who or what is a threat in the U.S. nuclear space is increasingly challenging in a world filled with disinformation, shifting priorities, and evolving risk. What exacerbates these efforts to identify individuals who pose a risk to nuclear security is the flaw in the underlying framework for how the U.S. identifies insider threats at home.

For decades, the U.S. has constructed the notion of a 'threat' to fit the visual of someone who doesn't present as an 'American.'<sup>213</sup> This carefully constructed 'American' image is almost always representative of the lived experiences of white people in the U.S., with people who fail to present in this way being subject to additional scrutiny – irrespective of the status of citizenship, criminal background, or threat to the U.S.<sup>214</sup> This 'othering' of non-white and otherwise 'non-American' presenting individuals reinforces problematic biases in national and nuclear security frameworks, creating an 'us' vs 'them' dynamic.<sup>215</sup> Given the historically homogenous nature of the nuclear security field dominated by white men in the United States, this has often placed women, people of color, and other historically marginalized groups under undue scrutiny by decision-makers in the field.

Insider threat assessments focus on personnel reliability programs and effective training, and existing literature is quick to acknowledge that there are flaws in frameworks designed to identify red flags, but what isn't discussed is the underlying bias determining not only what constitutes a red flag at the organizational level, but also the individual biases that come into play when determining who or what is reported as 'suspicious' under these schemes.<sup>216</sup>

Crucially, the national security field has been pushed to re-examine how 'threat' and by extension, 'security' are defined by the dominant culture, in contrast to the perception of 'threat' and 'security' faced by people of color, which are "deep-rooted in American society and culture."<sup>217</sup> The discomfort that emerges from questioning traditional definitions of national security has received pushback, but new definitions are necessary, given "[the] way the U.S. defines threat does not adequately capture the challenges many people of color feel in America[.]" by largely failing to account for the security threats posed by individuals, governments, or crime.<sup>218</sup>

This call for antiracism has echoed in the nuclear field as well. While important work has been done to draw connections between the importance of redefining national security and inequity in the nuclear policy space, one area that has received considerably less attention is the nuclear security field. The inequalities in the national security field caused by unilateral and biased understandings of who, or what is considered a 'threat' by the system writ large are directly connected to the notion of how 'threat' and 'security' are perceived by nuclear security implementers. These biases that originate in the overarching national security architecture are reflected in every aspect of U.S. nuclear security structure: from security clearance background checks, to personnel reliability programs, to how personnel security is implemented at a facility.

Because nuclear security culture and personnel reliability programs are driven by individual, organizational, and institutional structures, acknowledging that these structures can – intentionally or unintentionally – reflect the biases of the people and environment that create them, is crucial to reimagining the field. Nuclear security culture in the U.S. and around the world is intimately tied to the counterterrorism efforts that were put into place following the September 11, 2001, attacks. Nuclear security priorities reflect national security concerns, thus the conceptualization of 'threat' continues to place a disproportionate focus on foreign actors and movements, reproducing the 'us' vs 'them' distinction in security practices, even as threats facing national security evolve.<sup>219</sup> Even decades after the attacks, guidance for preventing radicalization relating to nuclear security focuses largely on "Jihadist" organizations or separatist movements.<sup>220</sup>

While focus on foreign threats and radicalization must be maintained, the guidance and framework for assessing threats must remain flexible enough to adapt to an evolving threat environment.

Maintaining disproportionate focus on foreign or externally influenced threats, when domestic actors presently pose a much larger concern in the domestic threat environment, demonstrates the institutionalized biases and exclusionary behaviors that can exacerbate the risks posed by insider threats. Understanding the limitations of the national and nuclear security as being designed to provide security for only some – mostly white-passing Americans – at the expense of people of color and those with foreign ties, can allow for a more nuanced understanding of the vulnerabilities facing the nuclear security field



today. Looking ahead, a framework is needed to help revamp nuclear security systems and procedures to adapt to evolving threats and assess risk factors, not only more effectively, but more equitably to produce a more resilient and sustainable U.S. nuclear security regime.

## Sources

- 1 Kelsey Davenport, "UN Security Council Resolution 1540 At a Glance," Arms Control Association (February 2021), <https://www.armscontrol.org/factsheets/1540>
- 2 Nuclear Threat Initiative, Global Initiative to Combat Nuclear Terrorism (GICNT) (2022), <https://www.nti.org/education-center/treaties-and-regimes/global-initiat...> Global Partnership, Why We Work (2023), <https://www.gpwm.com/why-we-work>
- 3 Matthew Bunn, "Preventing a Nuclear 9/11," How to Make America Safe: New Policies for National Security ed. Stephen Van Evera (Cambridge, MA: The Tobin Project, 2006): [https://tobinproject.org/sites/default/files/assets/Make\\_America\\_Safe\\_Preventing\\_Nuclear\\_9\\_11.pdf](https://tobinproject.org/sites/default/files/assets/Make_America_Safe_Preventing_Nuclear_9_11.pdf)
- 4 Scott Roecker, "A Call to Action on the Fifth Anniversary of the Final Nuclear Security Summit," NTI Atomic Pulse (March 31, 2021), <https://www.nti.org/atomic-pulse/call-action-fifth-anniversary-final-nuclear-securitysummit/>
- 5 Eileen Sullivan and Katie Benner, "Top law enforcement officials say the biggest domestic terror threat comes from white supremacists," The New York Times, (May 12, 2021), <https://www.nytimes.com/2021/05/12/us/politics/domestic-terror-white-sup...>
- 6 Seamus Huges, Ilana Krill, "Assessing US Domestic Extremism in Light of Capitol Riot Investigations," International Centre for Counter-Terrorism (June 30, 2022) <https://icct.nl/publication/assessing-us-domestic-extremism-in-light-of-capitol-riot-investigations/>
- 7 Van Dongen, Teun, Yannick Veilleux-Lepage, Eviane Leidig, Hanna Rigault Srkhis, "Right-Wing Extremism in the Military: A Typology of the Threat," International Centre For Counter-Terrorism (May 2022).
- 8 Adam Goldman and Alan Feur, "Bias and Human Error Played Parts in F.B.I's Jan. 6 Failure, Documents Suggest," The New York Times (February 1, 2023) <https://www.nytimes.com/2023/02/01/us/politics/trump-jan-6-fbi.html?smid=nytcore-ios-share&referringSource=articleShare>
- 9 Adam Goldman and Alan Feur, "Bias and Human Error Played Parts in F.B.I's Jan. 6 Failure, Documents Suggest," The New York Times (February 1, 2023) <https://www.nytimes.com/2023/02/01/us/politics/trump-jan-6-fbi.html?smid=nytcore-ios-share&referringSource=articleShare>
- 10 Eileen Sullivan and Katie Benner, "Top law enforcement officials say the biggest domestic terror threat comes from white supremacists," The New York Times, May 12, 2021, <https://www.nytimes.com/2021/05/12/us/politics/domestic-terror-white-supremacists.html>
- 11 "The Rising Threat of Domestic Terrorism, A Review of the Federal Response to Domestic Terrorism and the Spread of Extremist Content on Social Media" (November 16, 2022), <https://www.hsgac.senate.gov/media/majoritymedia/peters-investigative-report-shows-dhs-and-fbi-are-not-adequately-addressing-domestic-terrorism-threat>
- 12 Federal Bureau of Investigation and Department of Homeland Security, "Strategic Intelligence Assessment and Data on Domestic Terrorism," Submitted to the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee of the Judiciary of the United States House of Representatives, and the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee of the Judiciary of the United States Senate (October 2022), <https://www.fbi.gov/file-repository/fbi-dhsdomestic-terrorism-strategic-report.pdf/view>
- 13 Federal Bureau of Investigation and Department of Homeland Security, "Strategic Intelligence Assessment and Data on Domestic Terrorism," Submitted to the Permanent Select Committee on Intelligence, the Committee on Homeland Security, and the Committee of the Judiciary of the United States House of Representatives, and the Select Committee on Intelligence, the Committee on Homeland Security and Governmental Affairs, and the Committee of the Judiciary of the United States Senate (October 2022), <https://www.fbi.gov/file-repository/fbi-dhsdomestic-terrorism-strategic-report.pdf/view>
- 14 Eric Tucker and Mary Clare Jalonick, "FBI Chief Chris Wray Calls Jan. 5 'Domestic Terrorism,' Defends Intel," PBS News Hour (March 2, 2021), <https://www.pbs.org/newshour/politics/watch-live-fbi-chief-chris-wray-to-face-questions-about-extremism-capitol-riot>
- 15 "This is our House!": A Preliminary Assessment of the Capitol Hill Siege Participants," Program on Extremism, The George Washington University (March 2021). <https://extremism.gwu.edu/sites/g/files/zaxdzs5746/files/This-IsOur-Hous...>
- 16 Catherine Morehouse, "Physical Attacks on Power Grid Surge to New Peak," Politico (December 26, 2022), <https://www.politico.com/news/2022/12/26/physical-attacks-electrical-grid-peak-00075216>
- 17 Greg Harmon, "Rising Nazi Terror and Nuclear Power Risk: A Conversation with Edwin Lyman of the Union of Concerned Scientists," Deceleration (February 13, 2023), <https://deceleration.news/2023/02/13/rising-nazi-terrorand-nuclear-power-risk/>
- 18 Michael Loadenthal, "Infrastructure, Sabotage, and Accelerationism," Global Network on Extremism & Technology (February 15, 2021), <https://gnet-research.org/2021/02/15/infrastructure-sabotage-and-acceler...>
- 19 Greg Harmon, "Rising Nazi Terror and Nuclear Power Risk: A Conversation with Edwin Lyman of the Union of Concerned Scientists," Deceleration (February 13, 2023), <https://deceleration.news/2023/02/13/rising-nazi-terrorand-nuclear-power-risk/>
- 20 Greg Harmon, "Rising Nazi Terror and Nuclear Power Risk: A Conversation with Edwin Lyman of the Union of Concerned Scientists," Deceleration (February 13, 2023), <https://deceleration.news/2023/02/13/rising-nazi-terrorand-nuclear-power-risk/>
- 21 Janet Reitman, "All-American Nazis," Rolling Stone (May 2, 2018), <https://www.rollingstone.com/politics/politics-news/all-american-nazis-628023/>
- 22 Bruce Hoffman, "A Year After January 6, is Accelerationism the New Terrorist Threat?" Council on Foreign Relations (January 5, 2022), <https://www.cfr.org/in-brief/year-after-january-6-accelerationism-new-te...> (Accessed April 14, 2022).
- 23 Michael Loadenthal, "Modern Fascism's Fascination with 'Good Ol' Family' Values of an Imagined Past," California Institute of Integrated Studies (May 22, 2021), <https://digitalcommons.ciis.edu/lavlang/2021/saturday/11/>
- 24 "Atomwaffen," Southern Poverty Law Center (Accessed April 18, 2023), <https://www.splcenter.org/fightinghate/extremist-files/group/atomwaffen-division>
- 25 Alex Newhouse, "The Threat Is the Network: The Multi-Node Structure of Neo-Fascist Accelerationism," in CTC Sentinel, Vol 14, No 5, (West Point: Combating Terrorism Center at West Point, June 2021), p. 17 – 25; <https://ctc.usma.edu/wp-content/uploads/2021/05/CTC-SENTINEL-052021.pdf> (accessed November 9, 2021)
- 26 Greg Huffman, "Far-right accelerationists hope to spark the next U.S. civil war," Institute for Southern Studies, (February 3, 2021), <https://www.facingsouth.org/2021/02/far-right-accelerationists-hope-spar...> ; David Gartenstein-Ross, Samuel Hodgson, and Colin P. Clarke, "The Growing Threat Posed by Accelerationism and Accelerationist Groups Worldwide," Foreign Policy Research Institute (April 20, 2020), <https://www.fpri.org/article/2020/04/the-growing-threat-posed-by-accelerationism-and-accelerationist-groupsworldwide/>
- 27 Jordan Green, "Part of the war is terror': A new neo-Nazi group is trying to capitalize on the Moore County power grid attack," Raw Story (December 19, 2022), <https://www.rawstory.com/moore-grid/>



28 Jordan Green, "Part of the war is terror": A new neo-Nazi group is trying to capitalize on the Moore County power grid attack," Raw Story (December 19, 2022), <https://www.rawstory.com/moore-grid/>

29 Jordan Green, "Part of the war is terror": A new neo-Nazi group is trying to capitalize on the Moore County power grid attack," Raw Story (December 19, 2022), <https://www.rawstory.com/moore-grid/>

\*\*\*\*

213 Sneha Nair, "Reimagining U.S. foreign policy as an anti-racist endeavor," in Equality and Racial Justice: Where Do They Fit in a National Security Strategy? (Washington, D.C., U.S.: New America, 2022) <https://www.newamerica.org/political-reform/reports/equity-and-racial-ju...>

214 Smith, R. M. and King, D., "White Protectionism in America" in Perspectives on Politics, Volume 19, Issue (2, June 2021), pp. 460 – 478, <https://www.cambridge.org/core/journals/perspectives-on-politics/article/whiteprotectionism-in-america/466CB9F794DBC364C79B401EA81ADDD5>

215 German, M., Disrupt, Discredit, Divide: How the New FBI Damages Democracy, (New York, U.S.A., The New Press, 2019), pp. 65-88

216 Matthew Bunn and Scott Sagan, A Worst Practice Guide to Insider Threats: Lessons from Past Mistakes (Cambridge, U.S.A.: American Academy of Arts & Sciences, 2014), <https://www.amacad.org/sites/default/files/publication/downloads/insiderThreats.pdf>

217 Bonnie Jenkins, "Redefining Our Concept of Security," in Order from Chaos, (Washington, D.C., U.S.A.: Brookings Institution, 2019), <https://www.brookings.edu/blog/order-from-chaos/2019/12/04/redefining-our-conceptof-security/>

218 Bonnie Jenkins, "Redefining Our Concept of Security," in Order from Chaos, (Washington, D.C., U.S.A.: Brookings Institution, 2019), <https://www.brookings.edu/blog/order-from-chaos/2019/12/04/redefining-ou...>

219 Cynthia Miller-Idriss, "The War on Terror Supercharged the Far Right," Foreign Affairs, (October 2021), <https://www.foreignaffairs.com/articles/United-states/2021-08-24/war-on-...>

jan6?utm\_medium=promo\_email&utm\_source=lo\_flows&utm\_campaign=registered\_user\_welcome&utm\_term=e\_mail\_1&utm\_content=20211115

220 Geoffrey Chapman, G., et. al. Radicalisation and Preventative Measures: An Educational Handbook of Insider Threat Case Studies, (London, U.K.,: Center for Science and Security Studies, 2018), <https://www.kcl.ac.uk/csss/assets/radicalisation-preventative-measures-h...>

## The restart of nuclear power in Italy between risks, fears and the need for a sustainable future

By **Andrea Malizia** | Ass Professor in Nuclear Measures and Instrumentation, University of Rome Tor Vergata

03 April 2024 | Camera dei Deputati



*Iniziativa conoscitiva sul ruolo dell'energia nucleare  
nella transizione energetica e nel processo di decarbonizzazione*

**Audizione Camera Malizia - 03 Aprile 2024**

VIII COMMISSIONE (AMBIENTE, TERRITORIO E LAVORI PUBBLICI)  
X COMMISSIONE (ATTIVITA' PRODUTTIVE, COMMERCIO E TURISMO)

03 Aprile 2024  
Piazza del Parlamento italiano n. 24 – 00186 Roma.



**TOR VERGATA**  
UNIVERSITÀ DEGLI STUDI DI ROMA

Copy link



# LA RIPARTENZA DEL NUCLEARE IN ITALIA

## TRA RISCHI, PAURE ED IL BISOGNO DI UN FUTURO SOSTENIBILE

---

**Prof. Andrea Malizia**

Cattedra di Misure e Strumentazione Nucleari (ING-IND/20), Dipartimento di Biomedicina e Prevenzione,  
Facoltà di Medicina e Chirurgia, Università degli Studi di Roma Tor Vergata  
[malizia@ing.uniroma2.it](mailto:malizia@ing.uniroma2.it)

Watch on



YouTube

## CBRN Threats – Advancing national security through interdisciplinary innovations: An analytical framework for radiological and nuclear hazard detection technologies.

By Zeszyty Naukowe | ITTI | March 2024 | [Source](#)

### Abstract

This article examines the effectiveness of radiological and nuclear (R&N) threat detection technologies. It assesses current methodologies, interdisciplinary approaches and their impact on national security. Utilizing an extensive literature review and the author's expertise in CBRN defense, the study explores technological advancements, operational challenges, and future research in R&N detection. It underscores the necessity of innovative, adaptive technologies integrated with strategic policy to address evolving R&N threats effectively. The paper also highlights the strategic role of these technologies in national security policies and global non-proliferation efforts.

## Spent nuclear fuel mismanagement poses a major threat to the United States. Here's how.

By Mark Leyse

Source: <https://thebulletin.org/2024/04/spent-nuclear-fuel-mismanagement-poses-a-major-threat-to-the-united-states-heres-how/>



Power transmission lines near Dixon, California on August 12, 2012. A widespread collapse of the US power grid system could threaten nuclear facilities, including overloaded spent fuel pools. (Credit: Photo by Wendell/intherough, licensed under CC BY-NC-SA 2.0 via Flickr)

Apr 02 – Irradiated fuel assemblies—essentially bundles of fuel rods with zirconium alloy cladding sheathing uranium dioxide fuel pellets—that have been removed from a nuclear reactor (spent fuel) generate a great deal of heat from the radioactive decay of the nuclear fuel's unstable fission products. This heat source is termed decay heat. Spent fuel is so thermally hot and radioactive that it must be submerged in circulating water and cooled in a storage pool (spent fuel pool) for several years before it can be moved to dry storage. The dangers of reactor meltdowns are well known. But spent fuel can also overheat and burn in a storage pool if its coolant water is lost, thereby potentially releasing large amounts of radioactive material into the





air. This type of accident is known as a spent fuel pool fire or zirconium fire, named after the fuel cladding. All commercial nuclear power plants in the United States—and nearly all in the world—have at least one spent fuel pool on site. A fire at an overloaded pool (which exist at many US nuclear power plants) could release radiation that dwarfs what the Chernobyl nuclear accident emitted. Many analysts see very rare, severe earthquakes as the greatest threat to spent fuel pools; however, another far more likely event could threaten US nuclear sites: a widespread collapse of the power grid system. Such a collapse could be triggered by a variety of events, including solar storms, physical attacks, and cyberattacks—all of which are known, documented possibilities. Safety experts have warned for decades about the dangers of overloading spent fuel pools, but the Nuclear Regulatory Commission and Congress have refused to act.

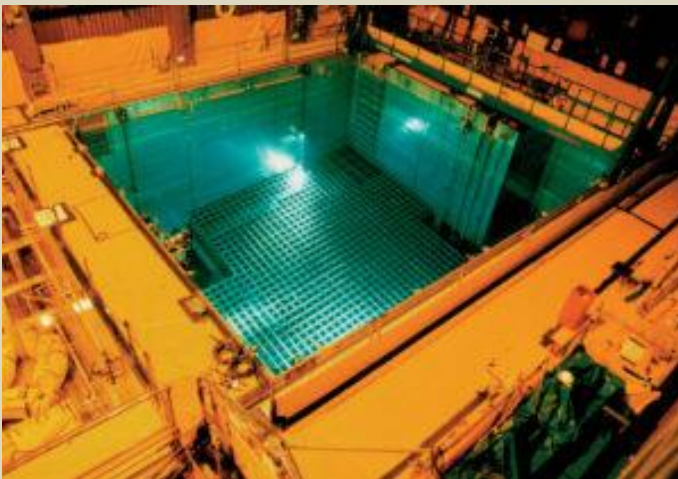
### The threat of overloaded spent fuel pools

Spent fuel pools at US nuclear plants are almost as densely packed with nuclear fuel as operating reactors—a hazard that has existed for [decades](#) and vastly increases the odds of having a major accident.

Spent fuel assemblies could ignite—starting a zirconium fire—if an overloaded pool were to lose a sizable portion or all of its coolant water. In a scenario in which coolant water boils off, uncovered zirconium cladding of fuel assemblies may overheat and chemically react with steam, generating explosive hydrogen gas. A substantial amount of hydrogen would almost certainly detonate, destroying the building that houses the spent fuel pool. (Only a small quantity of energy is required to ignite hydrogen gas, including electric sparks from equipment. It is speculated a [ringing telephone](#) initiated a hydrogen explosion that occurred during the Three Mile Island accident in 1979.)

A zirconium fire in an exposed spent fuel pool would have the potential to emit far more radioactive cesium 137 than the Chernobyl accident released. (The US Nuclear Regulatory Commission (NRC) has conducted analyses that found a zirconium fire at a densely packed pool could release as much as [24 megacuries of cesium 137](#); the Chernobyl accident is estimated to have released [2.3 megacuries of cesium 137](#).) Such a disaster could contaminate thousands of square miles of land in urban and rural areas, potentially exposing millions of people to large doses of ionizing radiation, many of whom could [die from early or latent cancer](#).

In contrast, if a thinly packed pool were deprived of coolant water, its spent fuel assemblies would likely release about [1 percent of the radioactive material](#) predicted to be released by a zirconium fire at a densely packed pool. A thinly packed pool has a much smaller inventory of radioactive material than a densely packed pool; it also contains much less zirconium. If such a limited amount of zirconium were to react with steam, most likely [too little hydrogen](#) would be generated to threaten the integrity of the spent fuel pool building.



A spent fuel pool at the San Onofre Nuclear Generating Station on December 1, 2014. (Credit: US NRC, licensed under CC BY 2.0 via Flickr).

After being cooled under water for a minimum of [three years](#), spent fuel assemblies can be transferred from pools to giant, hermetically sealed canisters of reinforced steel and concrete that shield plant workers and the public from ionizing radiation. This liquid-free method of storage, which cools the spent fuel assemblies by passive air convection, is called “[dry cask storage](#).” A typical US storage pool for a 1,000-megawatt-electric reactor

contains from [400 to 500 metric tons](#) of spent fuel assemblies. (Dry casks can store [10 to 15 tons](#) of spent fuel assemblies, so each cask contains a far lower amount of radioactive material than a storage pool.) [Reducing the total inventories](#) of spent fuel assemblies stored in US spent fuel pools by roughly 70 to 80 percent reduces their amount of radioactive cesium by about 50 percent. And the heat load in each pool drops by about 25 to 30 percent. With [low-density storage](#), a pool's spent fuel assemblies are separated from each other to an extent that greatly improves their ability to be cooled by air convection in the event that the pool loses its coolant water. Moreover, a dry cask storage area, which has passive cooling, is [less vulnerable](#) to either accidents or sabotage than a spent fuel pool.

In the aftermath of the March 2011 Fukushima Daiichi accident in Japan, in which there was a [risk of spent fuel assemblies igniting](#), the NRC considered forcing US utilities to expedite the transfer of all sufficiently-cooled spent fuel assemblies stored in overloaded pools to dry cask storage. The NRC [decided against](#) implementing such a safety measure.

To help justify its decision, the NRC chose to analyze only one scenario that might lead to a zirconium fire: a severe earthquake. In 2014, the NRC claimed that a severe earthquake with a magnitude “expected to



occur [once in 60,000 years](#)” is the prototypical initiating event that would lead to a zirconium fire in a boiling water reactor’s spent fuel pool.

The NRC’s 2014 study concluded that the type of earthquake it selected for its analyses would cause a zirconium fire and a large radiological release to occur at a densely packed spent fuel pool [once every nine million years](#) (or even less frequently). Restricting its analyses to a severe earthquake scenario allowed the NRC to help allay public fears over the dangers of spent fuel pool accidents. (At the time of the Fukushima Daiichi accident, the *New York Times* and other news outlets [warned](#) that a zirconium fire could break out in the plant’s Unit 4 spent fuel pool, causing global public concern.)

There is good reason to question whether severe earthquakes pose the greatest threat to spent fuel pools. A widespread collapse of the US power grid system that would last for a period of months to years—estimated to occur [once in a century](#)—may be far more likely to lead to a zirconium fire than a severe earthquake. The prospect that a widespread, long-term blackout will occur within the next 100 years should prompt US utilities to expedite the transfer of spent fuel from pools to dry cask storage. Utilities in other nations, including in Japan, that have overloaded pools should follow suit.

Solar storms, physical attacks, and cyberattacks have the potential to cause a nightmare scenario in which the US power grid collapses, along with other vital infrastructures—leading to reactor meltdowns and spent fuel pool fires, whose radioactive emissions would aggravate the disaster.

### Vulnerability to solar storms

In 2012, the NRC issued a Federal Register notice stating that an extreme solar storm (with its accompanying geomagnetic storm at the Earth) could cause the failure of hundreds of extra-high voltage transformers—with a maximum voltage rating of at least 345 kilovolts—precipitating widespread, long-term blackouts. The NRC posited that such a solar storm might occur once in 153 years to once in 500 years and initiate “a series of events potentially leading to [reactor] core damage at [multiple nuclear sites](#).”

The NRC’s Federal Register notice announced the agency had determined that the threat of prolonged power outages leading to at least one spent fuel pool fire must be [addressed](#) in its rulemaking process. The NRC decided to consider enacting regulations that Thomas Popik of the [Foundation for Resilient Societies](#), a non-profit organization focusing on infrastructure reliability, requested in a [petition for rulemaking](#). Popik asked the NRC to require plant owners to ensure spent fuel pools would have long-term cooling and a replenished supply of coolant water in the event that an extreme solar storm collapsed large portions of the US power grid for a period of months to years. Among other things, Popik was concerned that emergency diesel generators would not be able to supply the onsite electricity needed to cool the spent fuel pool for more than a few days.

[Over the past 160 years](#), the Earth has been hit by two solar superstorms—the 1859 Carrington Event and the 1921 New York Railroad Superstorm—that would be powerful enough to disable large portions of today’s global power grids. Scientists estimate that such extreme solar storms may hit the Earth [once in a century](#), so the odds are that the Earth will be hit by a solar superstorm at some point during this century. In July 2012, a solar superstorm, estimated to have been more intense than the Carrington Event, [crossed the Earth’s orbit](#), missing the Earth by about 1.8 million miles, or by one week’s time.

Solar superstorms are caused by coronal mass ejections: Eruptions of billions of tons of electrically-charged particles spat from the Sun’s corona, which travel at velocities as fast as several million miles per hour and can reach the Earth within 24 hours. Most coronal mass ejections, however, miss the Earth because it is a relatively small point within the solar system.

When a solar superstorm’s electrically-charged particles envelop the Earth, they cause extreme geomagnetic storms—mostly affecting high northern and southern latitudes. In a geomagnetic storm, the Earth’s geomagnetic field varies in magnitude, creating [electric fields](#) in the ground that induce electric currents in the power grid. Extreme geomagnetic storms may induce electric currents strong enough to melt the copper windings of extra-high voltage transformers, which may become damaged beyond repair and need to be replaced.

Extra-high voltage transformers are mostly manufactured overseas and difficult to transport. (Such transformers weigh between 100 and 400 tons.) In the United States, only a small number of facilities build extra-high voltage transformers. They cost several million dollars to manufacture and install; each is custom made to fit the specifications of its substation. Different designs are not typically interchangeable with one another, and few spares are manufactured. Manufacturing and installing even one such massive transformer can take [over one year](#).

Solar storms that were far less intense than the New York Railroad Superstorm have collapsed modern power grids. In the early hours of March 13, 1989, on a freezing night, a geomagnetic storm caused Canada’s Hydro-Québec grid to [collapse](#) within 90 seconds, leaving six million people without electric power for about 9 hours. (The magnitude of geomagnetic storms can be measured in nanoteslas per minute, where the tesla is a unit of magnetic flux density.) The New York Railroad Superstorm is estimated to have reached a magnitude of [approximately 5,000 nanoteslas per minute](#), and the March 1989 Storm was one-tenth as intense, reaching [approximately 480 nanoteslas per minute](#). In late October 2003, geomagnetic storms [less intense](#) than the March 1989 Storm caused a blackout in



southern Sweden and permanently damaged 15 extra-high voltage transformers in South Africa by overheating them.

Solar storms can cause large geomagnetic field variations to suddenly materialize over vast geographic areas, precipitating multiple, near-simultaneous failures at different locations of the electric power grid system. Over the past half century, the United States and other nations have dramatically expanded their power grids—adding more long-distance transmission lines and high-voltage infrastructure—thereby [increasing their vulnerability to geomagnetic storms](#). Moreover, the aging of vital power-grid infrastructures [also increases the grid's vulnerability](#).

### Vulnerability to physical attacks

On April 16, 2013, [gunmen attacked](#) the Metcalf Transmission Substation in San Jose, California, rendering it out of service. The gunmen shot 120 rounds from semiautomatic rifles, hitting 17 extra-high voltage transformers. The transformers leaked more than 50,000 gallons of cooling oil. They overheated, without exploding, and shut down. According to Jon Wellinghoff, a former Chairman of the Federal Energy Regulatory Commission, the Metcalf attack [nearly caused a blackout](#) in Silicon Valley; one that may have persisted for a period of several weeks.



[Snipers attacked a power substation in in San Jose, California on April 16, 2013, an attack that nearly caused a blackout in Silicon Valley. \(Credit: CNN\)](#)

In response to the assault on Metcalf, its owner—Pacific Gas and Electric—decided to spend \$100 million over the course of three years to help fortify its substations. That did not prevent thieves, in August 2014, from cutting through a fence at Metcalf and pilfering construction equipment that was intended to bolster

security. It took utility workers more than four hours to realize the substation had been [burgled](#).

In January 2022, the Department of Homeland Security [warned](#) that domestic terrorists have been devising credible strategies for sabotaging the US power grid over the past few years. Protecting all 55,000 substations that make up the US grid, however, is a difficult task. In December 2022, at least one malefactor [shot at](#) and severely damaged two substations—owned by Duke Energy—in North Carolina's Moore County, located about 90 miles east of Charlotte. Around 45,000 homes and businesses lost electricity as a result, and tens of thousands of customers got their power restored only after several days. Commenting on the Moore County attacks, Wellinghoff [observed](#) that “most [substations] don't seem to be very well protected. Many of them still have chain link fences, like the one in North Carolina.”

In 2014, *The Wall Street Journal* [reported](#) that a US Federal Energy Regulatory Commission analysis had concluded that if saboteurs synchronized physical attacks and disabled as few as nine critical power substations, especially on a hot summer day, the [entire US mainland](#) could lose electric power for several months. Unfortunately, determining or simply procuring information about the locations of the most critical substations in the continental US is a [relatively easy task](#).

Malefactors can also physically attack substations remotely. For instance, drones armed with improvised explosive devices could target US substations in synchronized swarms, potentially collapsing the power grid. In September 2022, Russia [attacked](#) civilian infrastructure in Ukraine, including the Ukrainian power grid, with waves of Iranian Shahed-136, “kamikaze” drones. These drones can carry up to 110 pounds (50 kilograms) of explosives over hundreds of miles. Kamikaze drones explode on impact. In October 2022, Russian kamikaze drones partly disrupted the delivery of electricity in the three major Ukrainian cities of Kharkiv, Kyiv, and Lviv.

### Vulnerability to cyberattacks

In December 2015, Russian hackers caused power outages in Ukraine by remotely opening circuit breakers, thereby cutting off the flow of electricity, at dozens of substations. It is the first confirmed instance, worldwide, that a [cyberattack caused a blackout](#). Within minutes, the hackers targeted three energy utilities, causing outages that lasted six hours and affected nearly a quarter-million people. Fortunately, the Ukrainian power grid has the odd benefit of being partly antiquated. It is not completely dependent on computer control systems; that is, industrial control systems and supervisory control and data acquisition (also known as “SCADA”) systems, which monitor and command an electric grid's physical equipment. Ukrainian grid operators were able to turn the power back on by bypassing their compromised control systems and manually closing circuit breakers at affected substations. One year later, in December 2016, another Russian cyberattack would cause a [second blackout in Ukraine](#). The 2016 cyberattack was more sophisticated than that of 2015. Power was restored after one hour; however, the hackers shut down a large Kyiv substation that handled



a greater electric load (200 megawatts) than the total load handled by the dozens of substations that had been successfully targeted the previous year. The hackers deployed malware—later named “CrashOverride”—that analysts have [characterized](#) as “an automated, grid-killing weapon.”

CrashOverride was designed to communicate with the Ukrainian power grid’s particular computer control systems, enabling it to manipulate the behavior of physical equipment at substations. At a preset time, CrashOverride opened circuit breakers at targeted substations to precipitate the blackout, without requiring oversight from hackers.

Malware programs like CrashOverride can also be tailored to attack European and North American power grids. Some analysts have [posited](#) that Ukraine is “Russia’s test lab for cyberwar,” [noting](#) that “in the cyber world, what happens in Kiev almost never stays in Kiev.” The US power grid is more computerized and automated than Ukraine’s grid, providing many openings for cyber infiltration. The Idaho National Laboratory (INL) has warned that the [interconnectivity](#) of SCADA systems exposes the US power grid to cyberattacks.

Given enough time, hackers could penetrate US transmission networks and plant CrashOverride or another tailored malware at any number of desired locations. CrashOverride can automatically execute the task of scanning transmission networks and selecting multiple targets, including those that control automated on-off switches for circuit breakers. Once entrenched, CrashOverride is set “like a [ticking bomb](#),” ready to sow chaos in power grid systems at any specified time.

Analysts at Dragos and Eset, two cyber-security companies for critical infrastructure, have pointed out that CrashOverride contains some code indicating it has the capacity to disable protective relays, which protect transmission lines and transformers against electric surges by opening circuit breakers. If hackers rendered protective relays inoperable while increasing local electric loads, they could [cause](#) transmission lines to melt and transformers to burn. Wide portions of the US grid could become disabled for months to years if hackers managed to destroy many extra-high voltage transformers.

In 2016, Idaho National Laboratory analysts came to similar conclusions as those at Dragos and Eset, warning that a major cyberattack on the US grid could seriously damage critical equipment, including extra-high voltage transformers, and lead to cascading blackouts. Some substations have networks that are incapable of detecting hackers’ intrusions and planted malware. INL analysts have [cautioned](#) that hackers could exploit such vulnerabilities to launch a coordinated cyberattack against multiple substations. Five years later, in June 2021, US Energy Secretary Jennifer Granholm [acknowledged](#) that hackers have the capability to shut down the US power grid.

### Insufficient public safety

After the Fukushima Daiichi accident, the US nuclear industry established the [Diverse and Flexible Mitigation Capability \(FLEX\) strategy](#), which is intended to help workers at nuclear plants manage a severe accident. The FLEX strategy stipulates that plant sites store portable equipment, such as backup generators and battery packs that can provide emergency power and pumps that can inject coolant water into the reactor or spent fuel pool. Such equipment is also stored at [two national response centers](#), located in Memphis, Tennessee and Phoenix, Arizona. The response centers must be capable of dispatching required equipment to any nuclear plant located in the United States within 24 hours. However, each center only houses five complete sets of FLEX equipment, not nearly enough equipment to simultaneously service the entire US nuclear reactor fleet.

In a long-term, nationwide blackout, US nuclear power plants would lose their supply of offsite electricity. Emergency diesel generators, which provide onsite electricity, are back-up systems designed to power cooling pumps and other safety equipment only for a relatively short period of time. Such generators would likely fail to operate continuously for a period of months to years. The longest loss-of-offsite power events in the United States all lasted [less than a week](#).

Most US nuclear plants are [required](#) to have at least a seven-day onsite supply of fuel for emergency diesel generators, and many have arrangements to receive prompt deliveries of fuel. Yet amid the logistical challenges and social disruptions of a nationwide, long-term blackout, it appears unlikely that a steady fuel supply could be transported to and maintained at every nuclear plant in the US fleet.

### Overloading spent fuel pools should be outlawed

Safety analysts have warned about the dangers of overloading spent fuel pools since the 1970s. For decades, [experts](#) and [organizations](#) have argued that in order to improve safety, sufficiently cooled spent fuel assemblies should be removed from high-density spent fuel pools and transferred to passively cooled dry cask storage. Sadly, the NRC has not heeded their advice.

In the face of the NRC’s inaction, Sen. Edward Markey of Massachusetts introduced [The Dry Cask Storage Act](#) in 2014, calling for the thinning out of spent fuel pools. The act, which Senator Markey has reintroduced in subsequent congressional sessions, has not passed into law.

The relatively high probability of a nationwide grid collapse, which would lead to multiple nuclear disasters, emphasizes the need to expedite the transfer of spent fuel to dry cask storage. According to Frank von Hippel, a professor of public and international affairs emeritus at Princeton University, the impact of a



single accident at an overstocked spent fuel pool has the potential to be [two orders of magnitude more devastating](#) in terms of radiological releases than the three Fukushima Daiichi meltdowns combined. If the US grid collapses for a lengthy period of time, society would likely descend into chaos, as uncooled nuclear fuel burned at multiple sites and spewed radioactive plumes into the environment.

The value of preventing the destruction of US society and untold human suffering is incalculable. So, on the issue of protecting people and the environment from spent fuel pool fires, it is surprising when one learns that promptly transferring the nationwide inventories of spent fuel assemblies that have been cooled for at least five years from US pools to dry cask storage would be “relatively inexpensive”—[less than \(in 2012 dollars\) a total of \\$4 billion](#) (\$5.4 billion in today’s dollars). That is far, far less than the monetary toll of losing vast tracts of urban and rural land for generations to come because of radioactive contamination.

One should also consider that plant owners are required, as part of the decommissioning process, to transfer spent fuel assemblies from storage pools to dry cask storage after nuclear plants are permanently shut down. So, [in accordance with industry protocols](#), all spent fuel assemblies at plant sites are intended to eventually be placed in dry cask storage (before ultimately being transported to a long-term surface storage site or a permanent geologic repository).

If the NRC continues to allow the industry’s mismanagement of spent fuel to pose an existential threat to the United States, Congress must be compelled to pass legislation requiring utilities to swiftly thin out spent fuel pools.

**Mark Leyse** is a nuclear power safety advocate, focusing on fuel-cladding issues, severe accidents, and improving evaluations of postulated accidents. Safety issues he raised in a petition for rulemaking, PRM-50-84, contributed to a US Nuclear Regulatory Commission rulemaking on fuel-cladding behavior under reactor loss-of-coolant accident conditions—revisions to Section 50.46(b)—that was approved in 2012. In 2014, he wrote a report for Natural Resources Defense Council on unresolved problems associated with severe accident hydrogen generation.

## The Day US Lost 4 Thermonuclear Bombs From B-52 Bomber Only To Be Retrieved By 1st Black Master Diver

By Ritu Sharma | Security journalist

Source: <https://www.eurasiantimes.com/the-day-us-lost-4-thermonuclear-bombs-from-b-52/>

Apr 07 – After ending World War II with a nuclear attack, the US got embroiled in a Cold War with the USSR. On January 17, when the Cold War was at its peak, the US lost four unarmed thermonuclear bombs when its B-52 bomber collided with a refueling tanker in Spain.

A thermonuclear weapon, also known as a fusion weapon or hydrogen bomb (H-bomb), is a second-generation nuclear weapon design. These bombs are significantly more sophisticated than first-generation nuclear bombs and possess greater destructive power compared to their predecessors.

Their energy release is hundreds to thousands of times more powerful than that of an atomic bomb.

The B-52G had embarked on a mission named Operation Chrome Dome, part of the Cold War airborne alert. Its flight plan took it east across the Atlantic Ocean and the Mediterranean Sea toward the European borders of the Soviet Union before returning home. The lengthy flight required two mid-air refueling over Spain.

The mid-air collision disrupted the missile, leading to the loss of both the aircraft and the nuclear bombs. The accident killed seven crew members, and the bomber’s payload of four hydrogen bombs was strewn across miles of coastline.

Three bombs fell on a nearby fishing village of Palomares in the municipality of Cuevas del Almanzora, Almeria, Spain. Two of them cracked open dispersing plutonium with the wind.

This resulted in the contamination of a 0.77-square-mile (2 km<sup>2</sup>) area with radioactive plutonium. The contaminated land was [partially cleaned](#), and the US shipped radioactive dirt and debris to America for disposal.

One of the bombs fell into the Mediterranean. Now the hunt was on to find it – along with its 1.1 megaton warhead, with the explosive power of 1,100,000 tonnes of TNT. The team of [Carl Brashear](#), who was the US Navy’s first Black diver, was tasked with retrieving the lost bomb from the depths of the ocean.

### Grit Of Carl Brashear

Carl Brashear had already created history by becoming the first black diver of the US Navy.

A month after losing the hydrogen bomb, all the search efforts proved to be desultory. It was then, in February 1966, the US Navy sent USS Hoist and her crew to Palomares, Spain, to help search for a



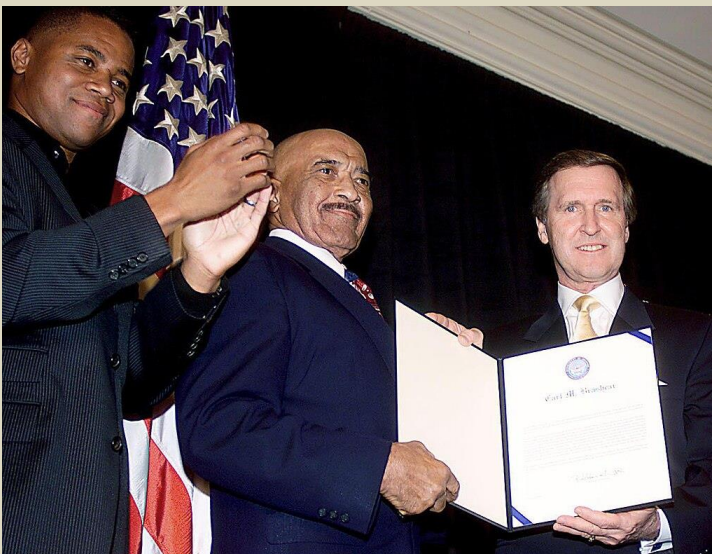
hydrogen bomb. Time was running out for the US, which needed to recover the bomb before another nation could.



Operation Chrome Dome flight path over southern Europe, showing refueling tracks

On the afternoon of March 23, nearly two and a half months later, the bomb was located. Brashear directed the transfer of a crate to hold the bomb once found, the supply boat parted its mooring line. Brashear rushed to get his sailors to safety.

A steel pipe broke loose, flew across the deck just as Brashear pushed a Sailor out of the way, and struck Brashear. The blow critically injured his left leg.



His leg suffered severe compound fractures to both bones. His leg was amputated below the knee. Brashear not only survived the accident, he went on to become the first amputee diver in the Navy, as well as its first Black master diver.

His life story has been immortalized on the celluloid through the movie Men of Honour.

Brashear (center) received an Outstanding Public Service Award in October 2000 from actor Cuba Gooding, Jr. and then-Defense Secretary William Cohen for 42 years of combined military and federal civilian service. Gooding portrayed Brashear in the 2000 film Men of Honor. VIA: Wikipedia

### The Nukes That Were Never Recovered

The Palomares incident was not the only time the US lost a nuke; there have been 32 "broken arrow" incidents when these weapons of mass destruction have

been lost. In many cases, they were dropped by mistake or jettisoned during an emergency.

All but [three](#) have not been recovered even now. On February 5, 1958, one Mark 15 thermonuclear bomb was lost at Tybee Island, Georgia, when it was jettisoned to reduce the aircraft's weight to ensure a safer



landing. Then, in December 1965, a B-43 thermonuclear bomb was lost in the Philippine Sea. A bomber aircraft, pilot, and nuclear weapon slid off the side of an aircraft carrier. It was never retrieved.

In 1968, one B28 thermonuclear bomb was lost near Thule Air Base, Greenland. The incident happened when a cabin fire forced the crew to eject, and the bomber aircraft crashed with its nuclear payload onboard.

These incidents came to light when the US Department of Defense [declassified](#) them in the 1980s. While the accidents involving American nuclear weapons have come to light, other countries are not so transparent when it comes to nuclear weapons.

In 1970, Russia's November-class submarine K-8, powered by twin nuclear reactors and armed with four nuclear-tipped torpedoes, sank in the Bay of Biscay, a notorious submarine graveyard.

The region is a treacherous stretch of water in the northeast Atlantic Ocean off the coasts of Spain and France. It is known for its violent storms and has seen many vessels sink.

The submarine was the USSR's first nuclear attack submarine, and it was diving to take part in the Okean 70 naval exercise. It was then that the K-8 experienced critical fires leading to reactor shutdowns and ultimately sank into deep waters, taking the nuclear payload with it.

## Europe's Largest Nuclear Power Plant Attacked by Drones

Source: <https://i-hls.com/archives/123384>

Apr 08 – Russian nuclear power corporation Rosatom accuses Ukraine's army of attacking the Zaporizhzhia nuclear power plant (ZNPP) with drones.

The International Atomic Energy Agency (IAEA) confirms that an attack took place on the nuclear power station's site, which did not result in significant damage to the facilities but led to one casualty and several people getting injured, according to reports by Rosatom and IAEA.

ZNPP is one of the ten largest nuclear power plants in the world, and definitely the largest in Europe, and it is located in southeast Ukraine. It is currently under the control of Russian forces, seized in February 2022 after Russia invaded Ukraine.

According to Interesting Engineering, IAEA termed the attack "a serious incident" and Director General Rafael Mariano said the assault "is a clear violation of the basic principles for protecting Europe's largest NPP. Such reckless attacks significantly increase the risk of a major nuclear accident and must cease immediately." He also urged both countries to refrain from taking any action that violates "the basic principles that protect nuclear facilities."

As for Ukraine, it has denied its involvement in the attack, with the country's Defense Intelligence saying the Russians might be behind the attack, claiming that such Russian attacks "are the criminal, and well-known, tactic the occupiers frequently resort to, as is deploying forces and weapons at the ZNPP and rigging certain facilities at the power plant with explosives."

In the meantime, it has been reported that Ukraine is using converted hobby planes to launch kamikaze-style attacks on Russian infrastructure, such as oil refineries, army and air force bases, and even industrial zones that are involved in the manufacturing of arms and armament.

The experts at Interesting Engineering conclude that drones are currently playing a majorly important role in the conflict between Russia and Ukraine, as both countries are using them to afflict damage deep within each other's territories.

### Zaporizhzhia Nuclear Power Plant

Europe's largest nuclear power station



- |                   |                              |  |
|-------------------|------------------------------|--|
| 1. Cooling towers | 4. Radioactive waste storage | <input type="checkbox"/> Russia annexed Crimea in 2014 |
| 2. Cooling pond   | 5. Spent fuel storage        |  |
| 3. Reactors       |                              |  |

Source: IAEA, Zaporizhzhia NPP, Google Earth

BBC



## By sending nuclear weapons to the United Kingdom, could the United States be fueling nuclear proliferation?

By Janani Mohan

Source: <https://thebulletin.org/2024/04/by-sending-nuclear-weapons-to-the-united-kingdom-could-the-united-states-be-fueling-nuclear-proliferation/>



The Royal Air Force Lakenheath base in the United Kingdom currently operates the F-15E Eagle and the latest generation F-35A Lighting II fighter aircraft, which can both carry nuclear bombs. In January 2024, *The Telegraph* disclosed US plans to store nuclear weapons at Lakenheath for the first time in 15 years. Nuclear weapons are stored in underground vaults located inside aircraft shelters similar to this one at Kadena Air Base, Japan. In the 1990s, there were 33 underground storage vaults at Lakenheath. (Credit: US Air Force / Omari Bernard, via DVIDS)

Apr 10 – For the first time in 15 years, the United States is reportedly [planning to station](#) nuclear weapons in the United Kingdom, a decision many experts interpret as attempting to counter growing geopolitical instability. As the war in Ukraine rages on, nuclear posturing—including stationing nuclear weapons in other countries—is seen by nuclear powers as an important tool to prevent further escalation, reassure allies, and respond to changes in Russia's posturing. The stationing of nuclear weapons is a convenient loophole to the safeguards of the Nuclear Non-Proliferation Treaty (NPT). While certain countries under the NPT are non-nuclear weapons states and cannot develop their own nuclear weapons programs, they can host weapons stationed by nuclear weapons states. Traditionally, nuclear powers have managed the entire control of their weapons—for example, by locating the nuclear weapons on joint bases.





However, while this control exists as a safeguard, stationing nuclear weapons as a means of posturing raises the question of what the difference is between “stationing” and “proliferating.” If near-term security concerns are well-served by the recent US decision to move nuclear weapons in the United Kingdom, it could augment the US practice of stationing nuclear weapons in other countries—a practice with potentially harmful consequences for long-term nonproliferation goals.

### **Why the United Kingdom.**

As the closest US ally, the United Kingdom serves as an interesting location for this latest round of nuclear posturing, given that it already has its own nuclear arsenal.

Historically, the United States and United Kingdom have worked together closely on the development of nuclear weapons, starting with [collaborations on the Manhattan Project](#). Since the 1960s, the United States started deploying nuclear weapons to the United Kingdom at regular intervals. This practice carried on until 2008, when the United States [removed approximately 110 B-61 nuclear bombs](#) from the Royal Air Force base at Lakenheath—the same base [believed to soon receive US nuclear weapons again](#). At the time the United States kept this withdrawal quiet, but some experts believed that it was [intended to reduce and consolidate](#) US nuclear forces in Europe.

Like with the secrecy in 2008, the United States has once again not formally commented on its recent shift in posture to re-station nuclear weapons in the United Kingdom. As a spokesperson for the UK Ministry of Defence [said](#) of the US decision, “it remains a longstanding UK and NATO policy to neither confirm nor deny the presence of nuclear weapons at a given location.”

### **Why station nuclear weapons?**

While the reasons behind this recent US decision are uncertain, stationing nuclear weapons in the United Kingdom potentially serves several US national interests.

The first and foremost reason may be to respond to growing tensions with Russia. NATO countries are very concerned about the Russian aggression and [recently warned](#) that there was a high likelihood for full-scale war with Russia within the next two decades. In addition, the United States did not make the first move: Russia [stationed nuclear weapons](#) in Belarus and [revoked its ratification](#) of the Comprehensive Nuclear Test Ban Treaty last year. The stationing of US nuclear weapons in the United Kingdom in response appears therefore somewhat predictable, given the general Cold War mentality of responding in-kind to shifts in doctrine.

The decision to station nuclear weapons therefore postures the United States as paying attention to Russia’s recent escalations and signals its willingness to respond in the future with nuclear weapons, if necessary. This decision reinforces the US nuclear deterrence policy, which [states](#) that: “As long as nuclear weapons exist, the fundamental role of US nuclear weapons is to deter nuclear attack on the United States, our allies, and partners.”

The US decision can also be interpreted as aiming to complement—and therefore strengthen—the UK nuclear weapons arsenal. Currently, the United Kingdom has the [smallest inventory](#) of any of the NPT’s nuclear weapons states, and these warheads are all based at sea. Meanwhile, the nuclear weapons that the United States will likely station in the United Kingdom are B61-12 gravity bombs, which are [deployable by aircraft](#). This deployment would enable forces in the region to have further and distinct second-strike capabilities, while adding to the overall strength of NATO forces across Europe.

Finally, the US decision is one of the safest, when compared to other posturing options. It is no doubt safer to place nuclear weapons in countries already possessing nuclear weapons, like the United Kingdom, than in those that don’t, like Turkey. Nuclear weapons states are lower risk as they would have minimal interest in proliferating these weapons. In addition, the United Kingdom already has sophisticated security systems and safeguards that would reduce both security risks and costs for the United States.

### **So why worry?**

The stationing of US nuclear weapons in the United Kingdom is unlikely to increase the physical risk of proliferation: Malicious actors are not more likely to gain access to nuclear weapons given the UK security apparatus. However, there are potential risks to the framework of nonproliferation itself. By re-stationing nuclear weapons in the United Kingdom, the United States is conveying that it is concerned over current nuclear tensions and that it might need to respond with nuclear weapons if attacked, which could increase future incentives for proliferation.

Stationing nuclear weapons in non-nuclear weapons states has always been an interesting gap in the nuclear nonproliferation frameworks of the NPT. However, regardless of the differences between “stationing” and “proliferating” nuclear weapons, the overall expansion of nuclear weapons still risks a cycle of escalation. Actions like the recent US decision may reduce taboos on the expansive stationing of nuclear weapons, thereby providing incentives for proliferation as a solution to counter increased aggression by countries, like Russia’s invasion of Ukraine.

For example, some Ukrainian policymakers have already [unofficially suggested](#) that Ukraine should “restore [its] nuclear status”—which means developing its own nuclear weapons—to deter Russia. Although such statements are intended to convince the United States and NATO to provide Ukraine with



some form of nuclear guarantees, they also suggest that an increasing need for nuclear deterrence inherently comes with increased risk of nuclear proliferation.

The risk of escalation may explain the current US and NATO strategy of stationing nuclear weapons semi-secretively. The United States ensures that its adversaries know that it is stationing nuclear weapons in ally countries like the United Kingdom, but adversaries are left with uncertainties about where those forces exactly are as the United States never formally discusses this posture. This strategy not only increases US deterrence, it may also reduce some of the escalatory impact of explicitly re-positioning nuclear weapons, while still allowing the United States to respond to Russia.

Given proliferation concerns, such escalation-control practices are therefore important to maintain as the United States moves nuclear weapons to the United Kingdom, as well as other countries in the future. Although it is yet to be seen if the recent US decision has a meaningful impact on nonproliferation, nuclear powers must work to prevent nuclear weapons stationing from eroding norms surrounding nuclear nonproliferation.

**Janani Mohan** is a PhD candidate in international studies at Cambridge University as a Gates Cambridge Scholar. She holds an MA in international policy from Stanford University, where she was a Ford Dorsey Fellow.

**EDITOR'S COMMENT:** What a stupid title! It is like wondering if oil is fanning the fire! And not a single suggestion for peace from a young PhD candidate in a prominent university ...

## Nuclear-armed UK is blind to its own violations of international law

By Brian Quail | Glasgow

Source: <https://www.thenational.scot/politics/24245074.nuclear-armed-uk-blind-violations-international-law/>

Apr 11 – WHILE defenders of Israel's conduct in Gaza repeat the mantra "Israel has the right to defend itself" as a self-evident truism, critics are not slow in responding that war is not merely a competition in killing, there are rules governing conflict. For example, you may not rape, torture, kill prisoners of war, or target civilians – even when such action is perceived as bringing victory nearer (the Hiroshima Fallacy). The wilful targeting of enemy civilians contravenes the sacrosanct principle of non-combatant immunity.

However, we in the UK are blind to our own flagrant violation of precisely the same laws, but on an unimaginably greater scale than Israel. The deployment of weapons of mass destruction in the policy known as CASD (continuous at-sea deterrence) whereby hydrogen bombs (ie nuclear missiles) are deployed in full alert 24/7, dwarfs any crime committed by Israel.

Our threat to use nuclear weapons violates international law, and specifically the Treaty Prohibiting Nuclear Weapons (TPNW) agreed by 122 countries in July 2019. This was the first legally binding international agreement to specifically prohibit nuclear weapons.

It is vital to realise that this is a matter of compulsory law – jus cogens. That means it is a peremptory norm from which there is no derogation (like piracy, genocide, enslavement, or FGM), as opposed to customary law, where parties have made a mutual agreement. I make this point in response to the obvious question – what do we do if this law is simply ignored by rogue states? The answer is that nuclear weapons are delegitimised, and those who have them will be stigmatised. They may perversely persist, but their criminality will be blatant and indisputable.

This ban is not an innovation – nuclear weapons have always been illegal and genocide always been criminal. It's just that while other means of killing people have been specifically outlawed (biological weapons 1972, chemical weapons 1993, land mines 1997, cluster munitions 2008), consideration of nuclear weapons has been avoided.

It is vital to grasp that the TPNW is unique. It is called the "Charter of the Victims" (ie you and me) because it is focused on the humanitarian consequences of the use of nuclear weapons, and does not get side-tracked into discussing "deterrence", or the imagined advantages of nuclear weapons. Previous agreements were deals among the members of the exclusive Big Boys' Nuclear Club. They argued about numbers and stockpiles, but took no cognisance of the human beings involved. In fact, the realities of consequential human suffering were deliberately ignored.

The assumption was that nuclear weapons were an asset, that their possession conferred status and prestige. The devastating effects of their use on human beings and the environment were disregarded. Radiation is especially lethal to reproductive organs and therefore women and the unborn are particularly susceptible to harm, so this is a major feminist issue.

It is depressing to observe that, in rehearsing the various arguments for Scottish [independence](#), this, the most powerful and irrefutable of all, is seldom mentioned. Even among the most dedicated supporters of independence, the "nuclear issue" is treated as a sort of afterthought.

Because we don't want to talk about the Bomb any more. It's all so passé, so sixties. And my granny used to march in the old days of the Cold War, back when we all lived under the threat of nuclear annihilation. But it has all changed now, hasn't it?



When the Bureau of Atomic Scientists say that the danger of nuclear war is greater now than at any time in the past, including the Cuban Missile Crisis, they're not being serious, are they?

So, let's change the channel and watch something else, right?

When human extermination became the official policy of the nuclear states, the finest brains in the world reacted with incredulous horror. Albert Einstein and Bertrand Russell published the Peace Manifesto in 1955, where they said: "Remember your humanity and forget the rest". Their anguished plea was ignored, and we had the collective lunacy of the Cold War; trillions of dollars was wasted on weapons, while millions perished through hunger and disease. And we suffered endless proxy wars from Vietnam to Afghanistan, Central America to Africa. We came within seconds (literally) of global suicide on several occasion.

And today the Gadarene race to extinction grows ever more intense. We make unimaginable advances in the technology of killing; hypersonic aircraft, smart drones, AI etc. all promise new and undreamed of toys to feed our necrophilous idolatry.

When I stand with the handful of Catholic Workers at the South Gate of Faslane, a valiant but pathetic bunch on our monthly vigil, I am inexpressibly saddened to consider that I live in a society which has degenerated to accepting the unspeakable horror of nuclear extermination. Independence is the only way to escape this nightmare, but only if we remain loyal in our opposition to all nuclear terrorism.

## A New Way to Detect Radiation Involving Cheap Ceramics

By Elizabeth A. Thomson

Source: <https://www.homelandsecuritynewswire.com/dr20240411-a-new-way-to-detect-radiation-involving-cheap-ceramics>

Apr 11 – The radiation detectors used today for applications like inspecting cargo ships for smuggled nuclear materials are expensive and cannot operate in harsh environments, among other disadvantages. Now, in work funded largely by the U.S. Department of Homeland Security with early support from the U.S. Department of Energy, MIT engineers have demonstrated a fundamentally new way to detect radiation that could allow much cheaper detectors and a plethora of new applications.

They are working with [Radiation Monitoring Devices](#), a company in Watertown, Massachusetts, to transfer the research as quickly as possible into detector products.

In a 2022 paper in *Nature Materials*, many of the same engineers [reported for the first time](#) how ultraviolet light can significantly improve the performance of fuel cells and other devices based on the movement of charged atoms, rather than those atoms' constituent electrons. In the current work, [published recently in \*Advanced Materials\*](#), the team shows that the same concept can be extended to a new application: the detection of gamma rays emitted by the radioactive decay of nuclear materials.

"Our approach involves materials and mechanisms very different than those in presently used detectors, with potentially enormous benefits in terms of reduced cost, ability to operate under harsh conditions, and simplified processing," says Harry L. Tuller, the R.P. Simmons Professor of Ceramics and Electronic Materials in MIT's Department of Materials Science and Engineering (DMSE).

Tuller leads the work with key collaborators Jennifer L. M. Rupp, a former associate professor of materials science and engineering at MIT who is now a professor of electrochemical materials at Technical University Munich in Germany, and Ju Li, the Battelle Energy Alliance Professor in Nuclear Engineering and a professor of materials science and engineering. All are also affiliated with MIT's Materials Research Laboratory. "After learning the *Nature Materials* work, I realized the same underlying principle should work for gamma-ray detection — in fact, may work even better than [UV] light because gamma rays are more penetrating — and proposed some experiments to Harry and Jennifer," says Li.

Says Rupp, "Employing shorter-range gamma rays enable [us] to extend the opto-ionic to a radio-ionic effect by modulating ionic carriers and defects at material interfaces by photogenerated electronic ones."

Other authors of the *Advanced Materials* paper are first author Thomas Defferriere, a DMSE postdoc, and Ahmed Sami Helal, a postdoc in MIT's Department of Nuclear Science and Engineering.

### Modifying Barriers

Charge can be carried through a material in different ways. We are most familiar with the charge that is carried by the electrons that help make up an atom. Common applications include solar cells. But there are many devices — like fuel cells and lithium batteries — that depend on the motion of the charged atoms, or ions, themselves rather than just their electrons.

The materials behind applications based on the movement of ions, known as solid electrolytes, are ceramics. Ceramics, in turn, are composed of tiny crystallite grains that are compacted and fired at high temperatures to form a dense structure. The problem is that ions traveling through the material are often stymied at the boundaries between the grains. In their 2022 paper, the MIT team showed that ultraviolet (UV) light shone on a solid electrolyte essentially causes electronic perturbations at the grain boundaries that ultimately lower the



barrier that ions encounter at those boundaries. The result: “We were able to enhance the flow of the ions by a factor of three,” says Tuller, making for a much more efficient system.

### Vast Potential

At the time, the team was excited about the potential of applying what they’d found to different systems. In the 2022 work, the team used UV light, which is quickly absorbed very near the surface of a material. As a result, that specific technique is only effective in thin films of materials. (Fortunately, many applications of solid electrolytes involve thin films.)

Light can be thought of as particles — photons — with different wavelengths and energies. These range from very low-energy radio waves to the very high-energy gamma rays emitted by the radioactive decay of nuclear materials. Visible light — and UV light — are of intermediate energies, and fit between the two extremes. The MIT technique reported in 2022 worked with UV light. Would it work with other wavelengths of light, potentially opening up new applications? Yes, the team found. In the current paper they show that gamma rays also modify the grain boundaries resulting in a faster flow of ions that, in turn, can be easily detected. And because the high-energy gamma rays penetrate much more deeply than UV light, “this extends the work to inexpensive bulk ceramics in addition to thin films,” says Tuller. It also allows a new application: an alternative approach to detecting nuclear materials.

Today’s state-of-the-art radiation detectors depend on a completely different mechanism than the one identified in the MIT work. They rely on signals derived from electrons and their counterparts, holes, rather than ions. But these electronic charge carriers must move comparatively great distances to the electrodes that “capture” them to create a signal. And along the way, they can be easily lost as they, for example, hit imperfections in a material. That’s why today’s detectors are made with extremely pure single crystals of material that allow an unimpeded path. They can be made with only certain materials and are difficult to process, making them expensive and hard to scale into large devices.

### Using Imperfections

In contrast, the new technique works because of the imperfections — grains — in the material. “The difference is that we rely on ionic currents being modulated at grain boundaries versus the state-of-the-art that relies on collecting electronic carriers from long distances,” Defferriere says. Says Rupp, “It is remarkable that the bulk ‘grains’ of the ceramic materials tested revealed high stabilities of the chemistry and structure towards gamma rays, and solely the grain boundary regions reacted in charge redistribution of majority and minority carriers and defects.” Comments Li, “This radiation-ionic effect is distinct from the conventional mechanisms for radiation detection where electrons or photons are collected. Here, the ionic current is being collected.” Igor Lubomirsky, a professor in the Department of Materials and Interfaces at the Weizmann Institute of Science, Israel, who was not involved in the current work, says, “I found the approach followed by the MIT group in utilizing polycrystalline oxygen ion conductors very fruitful given the [materials]’ promise for providing reliable operation under irradiation under the harsh conditions expected in nuclear reactors where such detectors often suffer from fatigue and aging. [They also] benefit from much-reduced fabrication costs.” As a result, the MIT engineers are hopeful that their work could result in new, less expensive detectors. For example, they envision trucks loaded with cargo from container ships driving through a structure that has detectors on both sides as they leave a port. “Ideally, you’d have either an array of detectors or a very large detector, and that’s where [today’s detectors] really don’t scale very well,” Tuller says.

Another potential application involves accessing geothermal energy, or the extreme heat below our feet that is being explored as a carbon-free alternative to fossil fuels. Ceramic sensors at the ends of drill bits could detect pockets of heat — radiation — to drill toward. Ceramics can easily withstand extreme temperatures of more than 800 degrees Fahrenheit and the extreme pressures found deep below the Earth’s surface. The team is excited about additional applications for their work. “This was a demonstration of principle with just one material,” says Tuller, “but there are thousands of other materials good at conducting ions.”

Concludes Defferriere: “It’s the start of a journey on the development of the technology, so there’s a lot to do and a lot to discover.”

[Elizabeth Thomson](#) is a writer at *MIT Materials Research Laboratory*.

## Environmental impacts of underground nuclear weapons testing

By Sulgiye Park and Rodney C. Ewing

Source: <https://thebulletin.org/premium/2024-03/environmental-impacts-of-underground-nuclear-weapons-testing/>

Mar 07 – Since *Trinity*—the first atomic bomb test on the morning of July 16, 1945, near Alamogordo, New Mexico—the nuclear-armed states have conducted 2,056 nuclear tests (Kimball 2023). The United States led the way with 1,030 nuclear tests, or almost half of the total, between 1945 and 1992. Second is the former Soviet Union, with 715 tests between 1949 and 1990, and then France, with 210 tests between 1960 and 1996. Globally, nuclear tests culminated in a cumulative yield of over 500 megatons, which is



equivalent to 500 million tons of TNT (Pravalié 2014). This surpasses by over 30,000 times the yield of the first atomic bomb dropped on Hiroshima on August 6, 1945.

Atmospheric nuclear tests prevailed until the early 1960s, with bombs tested by various means: aircraft drops, rocket launches, suspension from balloons, and detonation atop towers above ground. Between 1945 and 1963, the Soviet Union conducted 219 atmospheric tests, followed by the United States (215), the United Kingdom (21), and France (3) (Kimball 2023).

In the early days of the nuclear age, little was known about the impacts of radioactive “fallout”—the residual and activated radioactive material that falls to the ground after a nuclear explosion. The impacts became clearer in the 1950s, when the Kodak chemical company detected radioactive contamination on their film, which was linked to radiation resulting from the atmospheric nuclear tests (Sato et al. 2022). American scientists, like Barry Commoner, also discovered the presence of strontium 90 in children’s teeth originating from nuclear fallout thousands of kilometers from the original test site (Commoner 1959; Commoner 1958; Reiss 1961). These discoveries alerted scientists and the public to the consequences of radioactive fallout from underwater and atmospheric nuclear tests, particularly tests of powerful thermonuclear weapons that had single event yields of one megaton or greater.

Public concerns for the effects of radioactive contamination led to the Limited (or Partial) Test Ban Treaty, signed on August 5, 1963. The treaty restricted nuclear tests from air, space, and underwater (Atomic Heritage Foundation 2016; Loeb 1991; Rubinson 2011). And while the treaty was imperfect with only three signatories at the beginning (the United States, the United Kingdom, and the Soviet Union), the ban succeeded in significantly curbing atmospheric release of radioactive isotopes.

After the entry into force of the partial test ban, almost 1,500 underground nuclear tests were conducted globally. Of the 1,030 US nuclear tests, nearly 80 percent, or 815 tests (See Table 1), were conducted underground, primarily at the Nevada Test Site. [1] As for other nuclear powers, the Soviet Union conducted 496 underground tests, mostly in the Semipalatinsk region of Kazakhstan, France conducted 160 underground tests, the United Kingdom conducted 24, and China 22. These underground nuclear tests were in a variety of geologic formations (e.g., basalt, alluvium, rhyolite, sandstone, shale) to depths up to 2,400 meters.



**Left:** The explosion of the Storax Sedan underground nuclear test. (Credit: US Government, Public domain, via Wikimedia Commons). **Right:** Close-up of a sign at the site of the Sedan nuclear test. (Credit: Jarek Tuszyński, via Wikimedia Commons).

## PROJECT SEDAN

DETONATED ----- JULY 6, 1962  
 EXPLOSIVES - THERMONUCLEAR, 70% FUSION, 30% FISSION  
 YIELD ----- 104 KILOTONS  
 MEDIUM ----- ALLUVIUM  
 DEPTH OF BURIAL ----- 635 FT.  
 EMPLACEMENT HOLE DIAMETER --- 36"

## CRATER STATISTICS

MAXIMUM DEPTH ----- 320 FT.  
 MAXIMUM DIAMETER ----- 1,280 FT.  
 VOLUME -- 6.6 MILLION CUBIC YARDS  
 WEIGHT OF MATERIAL LIFTED --- 12 MILLION TONS  
 MAXIMUM LIP HEIGHT ----- 100 FT.  
 MINIMUM LIP HEIGHT ----- 20 FT.

In 1996, after some international efforts to curb nuclear testing and promote disarmament, the Comprehensive Test Ban Treaty (CTBT) was negotiated, which prohibited all nuclear explosions (General Assembly 1996). Since the negotiation of the CTBT, India and Pakistan conducted three and two underground nuclear tests, respectively, in 1998. And today, North Korea stands as the only country to have tested nuclear weapons in the 21<sup>st</sup> century.

While underground nuclear tests were chosen to limit atmospheric radioactive fallout, each test still caused dynamic and complex responses within crustal formations. Mechanical effects of underground nuclear tests span from the prompt post-detonation responses to the enduring impacts resulting in radionuclide release, dispersion, and migration through the geosphere. Every test of nuclear weapons adds to a global burden of released radioactivity (Ewing 1999).



**Table 1.** Number of nuclear tests by countries (Kimball 2023), estimated total yields (in kilotons of TNT) (Sublette 2001a; 2001b; Mikhailov 1999), dates (Kimball 2023), major test sites, and radioactivity of main radionuclides released from underground nuclear testing (IAEA 2007; Kimball 2023).

Country	Total number of nuclear tests (including underground and atmospheric)	Number of underground nuclear tests <sup>2</sup>	Estimated total yield in kilotons (yield from underground tests)	First nuclear test	First underground nuclear test	Last nuclear test	Main sites	Estimated radioactivity of main radionuclides released in TBq from underground testing (as of 1989)		
								strontium 90	cesium 137	plutonium 239
United States <sup>1</sup>	1,030	815	190,000 (35,000)	Jul. 16, 1945	Nov. 29, 1951	Sep. 23, 1992	Nevada Test Site	100,000	160,000	4,100
							Marshall Islands (Bikini Atolls)	80,000	130,000	< 1,000
Soviet Union / Russia	715	496	285,000 (38,000)	Aug. 29, 1949	Oct. 11, 1961	Oct. 24, 1990	Semipalatinsk, Kazakhstan	3.500	6,600	< 100
							Novaya Zemlya	85,000	140,000	2,800
United Kingdom	45	24	9,000 (1,000)	Oct. 3, 1952	Mar. 1, 1962	Nov. 26, 1991	Emu Field, Maralinga	n.a.	n.a.	n.a.
France	210	160	14,000 (3,600)	Feb. 13, 1960	Nov. 7, 1961	Jan. 27, 1996	French Polynesia	7,000	11,000	670
China	45	22	22,000 (1,400)	Oct. 16, 1964	Sep. 23, 1969	Jul. 29, 1996	Lop Nur	n.a.	n.a.	67
India	3	3	70 (70)	May 18, 1974	May 18, 1974	May 13, 1998	Thar Desert	n.a.	n.a.	n.a.
Pakistan	2	2	50 (50)	May 28, 1998	May 28, 1998	May 30, 1998	Pokhran	n.a.	n.a.	n.a.
North Korea	6 <sup>3</sup>	6	200 (200)	Oct. 9, 2006	Oct. 9, 2006	Sep. 3, 2017	Punggyeri	n.a.	n.a.	n.a.
<b>Total</b>	<b>2,056</b>	<b>1,528</b>	<b>539,928</b>					400,000 to 600,000	600,000 to 900,000	6,000 to 9,000

Abbreviations used: n.a. = not available; TBq = terabecquerels or trillion becquerels (One becquerel corresponds to one nucleus disintegrating every second.).

Notes:

1. Excluding the combat atomic bombs dropped on Hiroshima and Nagasaki, Japan.
2. Excluding very low-yield nuclear tests (i.e., nuclear explosive tests releasing less than one ton of TNT equivalent).
3. As of this writing, North Korea still has not conducted its seventh nuclear test. Experts say preparations are complete; a test may come at any time.

### Objectives, types, and timeline of underground nuclear tests

The scope of the nuclear testing programs evolved significantly throughout the 1980s, as the objectives of those tests ranged from weapons effect analysis to fundamental physics research to refining critical elements of warhead designs and ensuring the safety and effectiveness of the nuclear stockpile. Later, nuclear tests were also performed to study the methods for detecting those conducted by other countries. In the United States, most underground nuclear tests were conducted at the Nevada Test Site, whose remote site was originally selected for its arid climate and low population density for the safety and security needed to conduct the tests (Brady et al., 1984, 35; Lacznik et al., 1996).



Figure 1. The three main emplacement types of underground nuclear tests. (Source: Shaft type illustrated by S. Park; subsurface and tunnel type pictures from Schoengold and Stinson 1997.)

The setup of underground nuclear tests involved distinct emplacement methods tailored to various purposes. These methods included either a deep vertical shaft; a subsurface chamber (in which a nuclear device is emplaced to allow the explosion such that rock fragments are ejected, forming a crater); or a horizontal tunnel (with a nuclear device emplaced in a mined opening, intended for complete containment of the explosion). Each emplacement type was strategically designed to study different aspects of nuclear detonations and



weapon performance. In turn, the type of explosion and emplacement determined the content and timing of the radioactive gases and particles released by each test. (See Figure 1, below.)

To move nuclear testing underground, “big holes,” typically one to three meters in diameter, were drilled to varying depths, dictated by the objectives of the test, the design of the bomb being tested, and the properties of the geological formation hosting the test. The depth of the test was determined depending on the expected explosion yield and the characteristics of the geology.<sup>[2]</sup>

Each underground nuclear test followed a series of well-determined steps. The nuclear device was first placed inside a long cylindrical canister equipped with diagnostic instruments (e.g., radiation detectors) and electrical wires running back to an aboveground control station. The canister was then sealed and lowered into the shaft or tunnel, and the hole was filled with sand, gravel, and coal tar epoxy plugs to contain the debris from the detonation. Once the device was emplaced, the nuclear detonation was remotely triggered and the data generated by the explosion (e.g., the explosive yield and detonation mechanisms) were transmitted through fiber-optic cables to recording equipment housed in the aboveground station. Scientists analyzed this data to gain insights into the performance and behavior of nuclear devices, contributing to advances in warhead design, weapon efficacy, detectability of nuclear explosions, and safety measures.

A rapid sequence of events unfolds when the nuclear device is triggered underground. (See Figure 2). The detonation first causes an instantaneous chain reaction, releasing an immense surge of energy comprised of heat, light, and shockwaves. Plasma (a blend of superheated particles) and thermal pulse (a burst of intense heat) that originate from the point of detonation expand rapidly outward within milliseconds of the explosion. Shockwaves propagate through the surrounding rock and soil, causing seismic disturbances and ground movement. Subsequently, the release of energy from fusion and fission reactions—weapons can rely on both types of reactions, the former of which involves “fusing” atoms to release energy and the latter of which involves separating them—creates a void, expanding and vaporizing the nearby rock. In the process of rock vaporization, gases are produced; and the thermodynamic properties and fate of these gases depend on the disturbed rock properties (Adushkin and Spivak 2015).

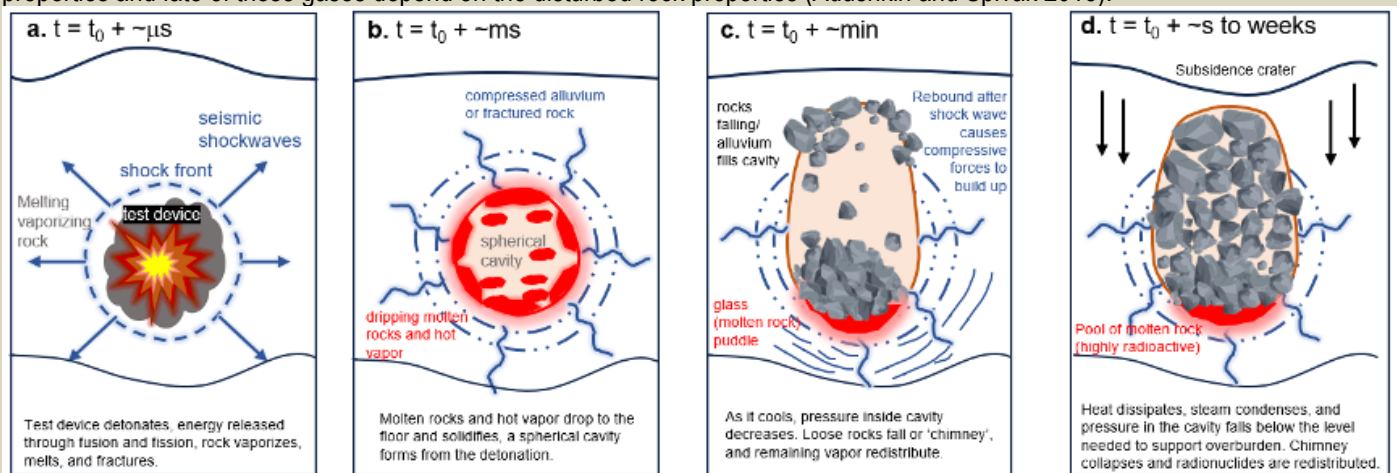


Figure 2. Sequence of events of underground nuclear test detonation. (Source: Illustration adapted from Smith, 1995)

The energy from nuclear explosions is incredibly high, with pressures ranging from one to 10 terapascals (10 million to 100 million standard atmospheres) and temperatures reaching up to 10 million degrees Celsius (Glasstone and Dolan 1977; Teller et al. 1968). For comparison, the pressures and temperatures from a nuclear explosion are up to 28 times and 1,900 times higher, respectively, than that of the Earth’s core. At this point, the spherical cavity is a fireball, the heat from which causes circumferential compressional stress conditions—just like when you blow air into a balloon, and it expands equally in all directions (Figure 2a). The size and timing of the cavity expansion depend on the explosion yield and emplacement medium (i.e., rock types). Hard rocks (e.g., basalt, granite, or sandstone) exposed to a nuclear detonation form a smaller cavity radius at a slower rate. The explosions produce a cavity radius with a size of eight to 12 meters (m) per kilotons (kt) raised to the power of one-third ( $m/kt^{1/3}$ ). The cavity expands at a rate of 30 to 50 milliseconds (ms) per  $kt^{1/3}$ . In softer rocks (e.g., tuff or alluvium) the corresponding figures are 15 to 17  $m/kt^{1/3}$  for radius size and 70 to 90  $ms/kt^{1/3}$  for rate of expansion (Adushkin and Spivak 2015). The stress from this force acts as a glue that holds together the fractures around the cavity (Figure 2b).

As internal pressure decreases minutes after the explosion—much like a balloon deflating—the state of matter in the cavity changes. Gases, vaporized materials, and fragmented rocks are ejected from the cavity while molten rock flows to the bottom of the cavity (Figure 2c). With further cooling and condensation, the cavity collapses, causing loose rocks to fall or ‘chimney’ down to the cavity, while gases migrate through the rock mass into the cavity (Figure 2d). Chimney collapse happens anywhere between minutes to months after the detonation, depending on the test conditions and the geology of the test site.



Heat eventually dissipates through conduction and radiation, and the quenched molten rock forms a glass as a solid mass at the base of the cavity—just as melted nuclear fuel accumulates and solidifies at the bottom of damaged reactor vessels, such as at three of the Fukushima Daiichi reactors. This highly radioactive glass contains refractory actinides (particles that are resistant to high temperatures and chemical attacks) such as plutonium, americium, and uranium, as well as fission products (fragments of lighter atomic nuclei produced by nuclear fission) and activation products (materials that have been made radioactive by the activation of neutrons). The final size of the cavity is related to the explosive yield, such that surveying of underground nuclear cavities of known geologic characteristics offers insights into the device's explosive yield.<sup>[3]</sup>

After underground nuclear detonations, a subsidence crater (or depression) often leaves a visible scar, typical of nuclear test sites (see figure 3). The size of a crater can be estimated as a function of the detonation's depth and yield. For a given depth, an underground test of 20- to 150-kiloton yield typically forms a 15- to 60-meter radius (Laczniak et al. 1996). The largest underground test conducted by the United States—the 5-megaton Cannikin test on November 6, 1971 (Atomic Energy Commission 1971a)—at nearly 2,000 meters depth lifted the ground by six meters and formed a subsidence area of 1,270 meters in length by 91 meters in width (Morris, Gard, and Snyder 1972). If the same bomb size was detonated on the surface, the local fallout would affect an area over 5,000 square kilometers, with a dose rate of absorbed ionizing radiation of about 1,000 rads per hour (Wellerstein n.d.). (The rad is a unit for measuring the amount of ionizing radiation absorbed. One rad corresponds to 10 joules of energy absorbed per gram of matter.) A dose of more than 1,000 rads delivered to the entire body within a day is generally considered to be fatal.

Figure 3. Surface craters left by underground nuclear tests at Yucca Flat, one of the main regions of the Nevada Test Site. (Source: Carlson, 2005.)



### Containment failures and nuclear accidents

Underground nuclear tests are designed to limit radioactive fallout and surface effects. However, containment methods are not foolproof, and radioisotopes, which are elements with neutrons in excess making them unstable and radioactive, can leak into the surrounding environment and atmosphere, posing potential risks to ecosystems and human health.

Instances of radiation leaks were not uncommon, especially in the early underground nuclear tests. There were challenges to maintaining simultaneous diagnostics during nuclear detonations and containment of radioactivity during the explosion. Out of the nearly 800 underground tests conducted at the Nevada Test Site, 32 tests led to considerable release of iodine 131—a highly active radionuclide with a half-life of eight days that poses health risks when absorbed by the thyroid gland (UNSCEAR 1993). At times, the maximum exposures to ionizing radiation recorded by self-reading pocket dosimeters reached 1,000 milliroentgen, where one roentgen deposits 0.96 rad of absorbed dose in soft tissue (Schoengold and Stinson 1997). While some containment failures with a relatively “controlled” release of radiation were purposefully made for tunnel access, many were unintentional.

Unintended radioactive releases from underground nuclear tests occurred through venting or seeps, where fission products and radioactive materials were uncontrollably released, driven by pressure from shockwave-induced steam or gas. In rare cases, more serious nuclear accidents occurred due to incomplete geological assessments of the surrounding medium in preparation for the test. A notable example of accidental release is the Baneberry underground nuclear test on December 18, 1970, which, according to the federal government, resulted in an “unexpected and unrecognized abnormally high water content in the medium surrounding the detonation point” (Atomic Energy Commission 1971b). In turn, the higher-than-expected underground water content increased the energy transfer from the detonation to the surrounding rocks and soil, while prolonging the duration of high-pressure phase in the cavity. The sustained stresses and pressures over longer periods of time altered the integrity of the containment structures, which failed and released approximately 80,000 curies, a unit for measuring radiation, of radioactive iodine 131 into the atmosphere.

As a result of this accident, 86 on-site workers were exposed to ionizing radiation (Atomic Energy Commission 1971b). The maximum ever recorded dose for an on-site worker's thyroid is 3.8 millirems—corresponding to 38 percent of the Federal Radiation Council's quarterly guide for the thyroid (Federal Radiation Council and Protection Division 1961). (The rem is a unit of effective absorbed radiation in human tissue, equivalent to one roentgen of X-rays. One millirem is one-thousandth of a rem.) Offsite, the highest recorded inhalation dose reaches 90 millirems—6 percent of the yearly protection guide for the thyroid. The highest radioiodine levels in milk measured 810 picocuries per liter at a ranch near a test (equivalent to 1,080 millirems per year).<sup>[4]</sup> That's a value that is 270 times greater than today's





maximum contaminant level set by the Environmental Protection Agency (Environmental Protection Agency 2002).

### Mechanical and radiation effects of underground nuclear tests

Three main factors affect the mechanical responses of underground nuclear tests: the yield, the device placement (i.e., depth of burial, chamber geometry, and size), and the emplacement medium (i.e., rock type, water content, mineral compositions, physical properties, and tectonic structure). These factors influence the physical response of the surrounding geological formations and the extent of ground displacement, which, in turn, determine the radiation effects by influencing the timing and fate of the radioactive gas release. Every kiloton of explosive yield produces approximately 60 grams ( $3 \times 10^{12}$  fission product atoms) of radionuclides (Smith 1995; Glasstone and Dolan 1977). Between 1962 and 1992, underground nuclear tests had a total explosive yield of approximately 90 megatons (Pravalié 2014), producing nearly 5.4 metric tons of radionuclides. While the total radioactivity of the fission products is extremely large at the point of detonation (e.g., one minute after a nuclear explosion, the radioactivity of the fission products from one kiloton fission yield explosion is approximately  $10^9$  terabecquerel), it decreases quickly because of radioactive decay (Glasstone and Dolan 1977). (The becquerel is an international system unit for measuring radioactivity. One becquerel corresponds to the activity of radioactive material in which one nucleus decays per second.)

The radionuclides generated from a nuclear explosion consist of a mixture of:

- refractory species from the weapon materials that condense at high temperatures and partition into the “melt glass;”
- volatile species that condense at lower temperatures and widely disperse on rock surfaces throughout the entire volume of material disturbed by the detonation;
- fission products, which mostly decay by emission of beta and gamma radiation; and
- activation products, created by neutron irradiation of the surrounding rocks.

The initial distribution of these species is determined by the temperature and pressure history post explosion, and by the chemical properties of radionuclides produced (Table 2). Lethal doses of different radioisotopes in humans vary. For example, an uptake of a few milligrams of plutonium 239 per kilogram of tissue is a lethal dose based on animal studies (Voelz and Buican 2000). As of September 1992, when the United States conducted its last underground test, the total amount of radioactivity generated by the 43 long-lived radionuclides (with half-lives greater than 10 years) produced by the 828 underground nuclear tests conducted at the Nevada Test Site between 1951 and 1992 is estimated to be 4,890,000 terabecquerel or trillion becquerels (Smith, Finnegan, and Bowen 2003).

Radionuclides	Category	Half-life
<b>americium 241</b>	refractory, fuel residue, and fuel product	432.2 years
<b>antimony 125</b>	fission product	2.6 years
<b>carbon 14</b>	activation product	5,730 years
<b>cerium 144</b>	fission product/refractory	285 days
<b>cesium 137</b>	fission product/volatile	30 years
<b>cobalt 60</b>	activation product	5.3 years
<b>europium</b>	activation product	europium 152: 13.5 years europium 154: 8.6 years
<b>europium 155</b>	fission product	4.8 years
<b>iodine</b>	fission product	iodine 129: 16.1 million years iodine 131: 8 days
<b>krypton 85</b>	fission product/volatile	10.8 years
<b>manganese 54</b>	activation product	312 days
<b>plutonium</b>	refractory, fuel residue, and fuel product	plutonium 239: 24,110 years (unfissioned) plutonium 240: 6,546 years plutonium 241: 14.4 years plutonium 242: 373,300 years
<b>ruthenium 106</b>	fission product/volatile	1 year
<b>strontium 90</b>	volatile	29 years
<b>technetium 99</b>	fission product	210,000 years
<b>tritium</b>	activation product	12.3 years
<b>uranium</b>	refractory (can be volatile depending on the oxidation state)	uranium 234: 245,000 years uranium 235: 700 million years (unfissioned) uranium 236: 23.4 million years uranium 238: 4.5 billion years

Table 2. Major radionuclides associated with underground nuclear tests



The partitioning of radionuclides between the melt glass and rubble significantly impacts the subsequent transfer of radioactivity to groundwater. Radionuclides deposited on free surfaces are prone to dissolution in groundwater through ion exchange, desorption (the release of adsorbed atoms or molecules from a surface into the surrounding water), and surface-layer alteration processes, whereas refractory species that are largely partitioned into the melt glass are less accessible to groundwater. Even then, the release of these partitioned species depends on the rate of melt glass dissolution in contact with the groundwater, which is rather rapid due to the low stability of glass in contact with water. Nuclear detonation can also alter the physical properties of the surrounding rock formation, thereby accelerating the dissolution rate of the melt glass and the release of radionuclides into the groundwater along networks of fractures created by the blast.

As the shockwaves produced from a detonation propagate through the surrounding rock and soil, they induce a stress field within the geological environment on both the microscopic (0.1 to 100 micrometers) and mesoscopic (100 to 1,000 nanometers) scales. These stresses cause irreversible structural changes, which can compromise the physical integrity of the geologic formations. At the microscale, these changes can include microscopic fractures and/or dislocations within individual mineral grains. At the mesoscale, shock-induced changes include faulting and the formation of visible fractures or shock structures, including localized brecciation (i.e., the formation of angular fragments of rock).

The extreme temperatures generated during the nuclear detonation can change the composition of nearby rocks and form new minerals or glass depending on their chemistry, duration of the thermal pulse (electromagnetic radiation generated by the particles in movement), and hydrological setting. Temperatures produced by large explosions can change the permeability, porosity, and water storage capacity by creating new fractures, cavities, and chimneys. The radius of increased permeability (a unitless measure of the ability of a porous material to allow fluids to pass through) can be calculated as a function of the resulting cavity radius, and in the case of the Nevada Test Site, it was typically seven times greater than the radius of the cavity (Adushkin and Spivak 2015). The explosion also affects the porosity of the surrounding rock. For example, a fully contained explosion of 12.5-kiloton yield in Degelen Mountain at the former Soviet Union's Semipalatinsk test site resulted in up to a six-fold increase in porosity within the crush zone surrounding the cavity (Adushkin and Spivak 2015). Increased permeability and porosity of the surrounding rock can lead to more radionuclides being released, as more groundwater can pass through the geologic formation.

### **Hydrogeology and release of radioactivity**

The main way contaminants can be moved from underground test areas to the more accessible environment is through groundwater flow. Concurrent to the changes in rock permeability and porosity, the residual deformations from nuclear explosions can change the interstitial fluid pressures and water compositions, subsequently modifying groundwater flow rates and directions. In turn, these changes, combined with the presence of water and gas-forming components in rocks, affect the extent of the damage zone and potential migration of radioactive particles into the subsurface environment.

Water affects the behavior of underground nuclear tests in several ways. First, it enhances the transmission of stress waves through the rock mass. This mechanism caused the Baneberry accident (Atomic Energy Commission 1971b). Second, water serves as the main transportation pathway for radionuclides—either in solution (i.e., chemically dissolved in water) or attached to colloids (i.e., dispersed insoluble particles suspended throughout water). The radionuclide particles are in the sub-micrometer range in size, with high surface areas (i.e., the area available for chemical reactions). Important radioisotopes that are particularly likely to interact with hydrodynamic processes include plutonium 239 and plutonium 240, which can adhere or sorb onto mobile mineral particulates in the aquifer and be transported by groundwater. And when contaminants encounter groundwater, their migration potential increases, with the movement depending on the rate and direction of groundwater flow—just like drivers use cars to move around faster and farther. Even when isotopes do not interact with groundwater immediately after a detonation, the residual thermal effects from detonation can lead to lasting physical and chemical changes as the thermal pulse persists for up to 50 years after the explosion, long after groundwater has returned to the cavity system (Maxwell et al. 2000; Tompson et al. 2002). After the explosion, the residual heat is typically below the boiling point of water, and there is a thermal contribution by the decay of radionuclides. This residual heat can induce vertical, buoyancy-driven water flow, while accelerating the dissolution rate of the melt glass. The increased dissolution, in turn, increases the release of radionuclides, allowing mobile particles to rise to more permeable geologic zones and escape from the cavity or through the chimney system. For example, plutonium from the Nevada Test Site was found to have migrated 1.3 kilometers in 30 years in groundwater by means of colloid-facilitated transport (Kersting 1999). This migration distance contradicted previous models, considering that the groundwater levels at the site typically lie deeper than 200 meters below the surface; and two-thirds of underground tests at the Nevada Test Site were conducted at depths above the water table to ensure subsurface containment of radioactive by-products (Laczniak et al. 1996).

Similarly, at a low-level radioactive waste management site at Los Alamos National Laboratory, where treated waste effluents were discharged into Mortandad Canyon, americium and plutonium were shown to migrate 30 meters in 33 years within the unsaturated zone (Penrose et al. 1990; Travis and Nuttall 1985). And in another example, plutonium was detected on colloids at more than four kilometers



downstream of the source at Mayak, a nuclear waste reprocessing plant in Russia (Novikov et al. 2006). Given their long half-lives (Table 2), the ability of plutonium isotopes to migrate over time raises concerns about the long-term impacts and challenges in managing radioactive contamination.

In all these cases, colloid-facilitated transport allowed for the migration of radioactive particles through groundwater flow over an extended period—long after the nuclear tests or discharge occurred (Novikov et al. 2006). These cases have been confirmed using the distinctive isotopic ratios of key radionuclides to trace migrating radionuclides back to the specific tests or “shots,” making them a useful forensic tool to discern the sources of contaminants.

The risks associated with the environmental contamination from underground nuclear tests have often been considered low due to the slow movement of the groundwater and the long distance that separates it from publicly accessible groundwater supplies. But these studies demonstrate that apart from prompt effect of radioactive gas releases from instantaneous changes in geologic formations, long-term effects persist due to the evolving properties of the surrounding rocks long after the tests. Long-lived radionuclides can be remarkably mobile in the geosphere. Such findings underscore the necessity for sustained long-term monitoring efforts at and around nuclear test sites to evaluate the delayed impacts of underground nuclear testing on the environment and public health.

### Enduring legacy

Nearly three decades after the five nuclear-armed states under the CTBT stopped testing nuclear weapons both in the atmosphere and underground, the effects of past tests persist in various forms—including environmental contamination, radiation exposure, and socio-economic repercussions—which continue to impact populations at and near closed nuclear test sites (Blume 2022). The concerns are greater when the test sites are abandoned without adequate environmental remediation. This was the case with the Semipalatinsk test site in Kazakhstan that was left unattended after the fall of the Soviet Union in 1991, before a secret multi-million effort was made by the United States, Russia, and Kazakhstan to secure the site (Hecker 2013). The abandonment resulted in heavy contamination of soil, water, and vegetation, posing significant risks to the local populations (Kassenova 2009).

In 1990, the US Congress acknowledged the health risks from nuclear testing by establishing the Radiation Exposure Compensation Act (RECA), which provides compensation to those affected by radioactive fallout from nuclear tests and uranium mining. Still, there are limitations and gaps in coverage that leave many impacted individuals, including the “downwinders” from the Trinity test site without compensation for their radiation exposure (Blume, 2023). The Act is set to expire in July 2024, potentially depriving many individuals without essential assistance. Over the past 30 years, the RECA fund paid out approximately \$2.5 billion to impacted populations (Congressional Research Service 2022). For comparison, the US federal government spends \$60 billion per year to maintain its nuclear forces (Congressional Budget Office 2021).

As the effects of nuclear testing still linger, today’s generations are witnessing an increasing concern at the possibility of a new arms race and potential resumption of nuclear testing (Drozdenko 2023; Diaz-Maurin 2023). The concern is heightened by activities in China and North Korea and with Russia rescinding its ratification of the CTBT. Even though the United States maintains a moratorium on non-subcritical nuclear tests, its decision not to ratify the test ban treaty shows a lack of international leadership and commitment. As global tensions and uncertainties arise, it is critical to ensure global security and minimize the risks to humans and the environment by enforcing comprehensive treaties like the CTBT. Transparency at nuclear test sites should be promoted, including those conducting very-low-yield subcritical tests, and the enduring impacts of past nuclear tests should be assessed and addressed.

### Endnotes

[1] The number of US nuclear tests reported in different publications ranges from 1,051 to 1,151. The discrepancy is attributed to the different ways of counting nuclear tests (e.g., the frequency, timing, and the number of nuclear devices). Here, underground nuclear tests refer to one or more nuclear devices in the same tunnel or hole. If we count simultaneous tests or explosions close in time, the number of US tests would be higher than reported here.

[2] The scaled depth of burial (empirical measure of blast energy confinement) can be calculated using the equation (McEwan 1988):

$$\text{scaled depth of burial} = \frac{\text{depth of burial}}{\text{yield (kt)}^{1/3}}$$

[3] Assuming the cavity reaches a maximum volume when the gas pressure reaches the lithostatic (overburden) pressure at the explosion depth, the radius of cavity can be estimated using the following equation:



$$\frac{\text{radius}}{\text{yield}^{1/3}} = \frac{\text{medium coefficient}}{(\text{density} \times \text{gravitational constant} \times \text{explosion depth})^{1/3\gamma}}$$

where yield is expressed in kt, and  $\gamma$  is the effective adiabat exponent of the explosion products, which depends on the composition of the emplacement medium (Allen and Duff 1969; Boardman, Rabb, and McArthur 1964; Adushkin and Spivak 2015).

[4] Continuous daily intake of 100 picocuries of iodine 131 per day for one year remains within the radiation protection guide's limit of 0.5 millirems per year. The highest estimated thyroid exposure from inhalation and milk ingestion was 130 millirems, measured in a two-year-old child in Beatty, an unincorporated community bordering the Nevada Test Site.

●► References are available at the source's URL.

**Sulgiye Park** is a senior scientist with the Global Security Program at the Union of Concerned Scientists. Park holds a PhD in Geological Sciences from Stanford University.

**Rodney C. Ewing** is a Senior Fellow in the Center for International Security and Cooperation in the Freeman Spogli Institute for International Studies and a professor in the Department of Earth and Planetary Sciences in the Doerr School of Sustainability at Stanford University. Ewing has written extensively on issues related to nuclear waste management and is co-editor of *Radioactive Waste Forms for the Future* (North-Holland, 1988) and *Uncertainty Underground: Yucca Mountain and the Nation's High-Level Nuclear Waste* (MIT Press, 2006).

## Shocking map shows all countries in the world with nuclear weapons as Iran 'minutes away'

Source: <https://www.express.co.uk/news/world/1888787/Nuclear-weapons-map-Iran-bomb-WW3>

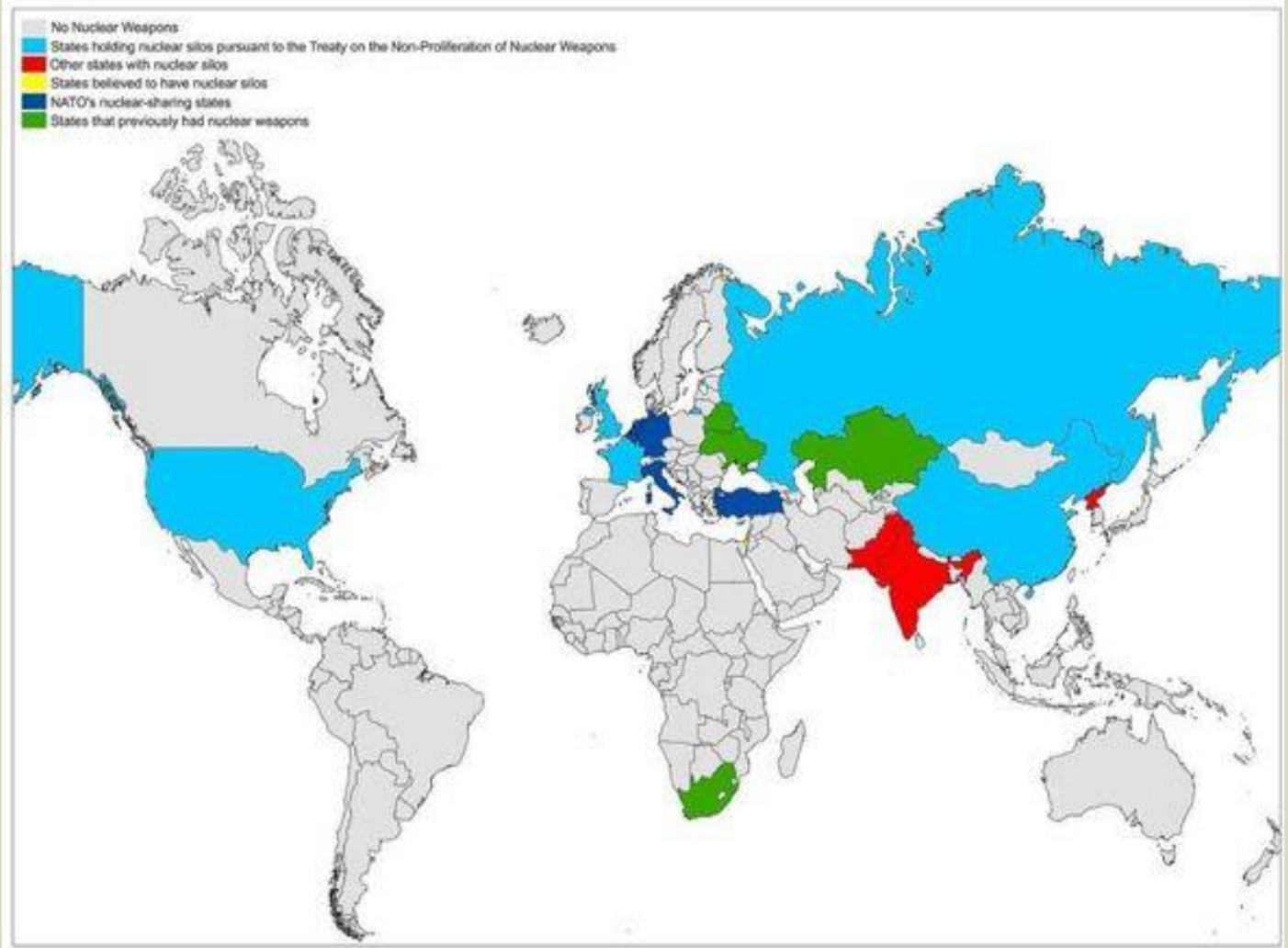
Apr 16 – [A disturbing map](#) shows the number of countries that possess [nuclear weapons](#), amid fears that the world is edging towards [all-out global conflict](#). There are approximately 3,880 active nuclear warheads and 12,119 total nuclear warheads in the world as of 2024, according to the Federation of American Scientists



Eight countries around the world are known to have weapons of mass destruction ready to be deployed. These include the United States, [Russia](#), France, China, the United Kingdom, Pakistan, India, and North Korea.



The latter - Pakistan, India, and North Korea - are not members of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT). The three countries refuse to sign up to the UN Treaty which prohibits acquiring more nuclear weapons and encourages disarmament. There is a ninth country - [Israel](#) - that is suspected of having dozens of nuclear bombs but refuses to acknowledge it under a policy of deliberate ambiguity. [Israel](#) is understood to have between 75 and 400 nuclear warheads ready to launch. The country has also declined to sign up to the NPT, citing threats to its national security interests. There are fears that Iran could join this group of nuclear-armed nations as the country closes in on its own weapons of mass destruction.



There are approximately 3,880 active nuclear warheads and 12,119 total nuclear warheads in the world (Image: MAPPR)

This comes as a debate in the House of Lords warned that Iran was just "minutes away" from developing nuclear warheads. There are reports that [Israel](#) could target Iran's nuclear facilities as part of a response to the barrage of drones and missiles fired over the weekend. Discussing the Iranian retaliatory attack, independent crossbench peer Baroness Deech said: "We seem to have forgotten about the nuclear plan, the JCPOA, we've taken our eye off that. Iran is within minutes of getting nuclear capability and mad enough to use it." Former Tory Cabinet minister Lord Forsyth added that, if he were in [Israel](#), he would "be worried that this evil regime (Iran) is developing a nuclear capability". Nukes have only been used twice in war - both instances by the US, when they dropped a nuclear bomb on the Japanese city of Hiroshima on August 6, 1945, and a second on Nagasaki three days later. The war between [Russia](#) and [Ukraine](#) has escalated fears of a nuclear war, with [Vladimir Putin](#) even publicly declaring that his country's nuclear forces are on "high alert". China has also intensified concerns further, amid reports that Beijing is trying to double its number of nuclear warheads from 350 to 700 by 2027.



## Russia plans to restart Ukraine's Zaporizhzhia embattled nuclear power plant. That won't make the plant safer

By Ali Alkis

Source: <https://thebulletin.org/2024/04/russia-plans-to-restart-ukraines-zaporizhzhia-embattled-nuclear-power-plant-that-wont-make-the-plant-safer/>

Apr 17 – It has been more than two years since Russia occupied the Zaporizhzhia nuclear power plant in Ukraine—Europe's largest. For the first time in history, a war is taking place in a country with advanced nuclear facilities and infrastructure, demonstrating a new kind of nuclear safety and security risk. Over this period, the Zaporizhzhia plant has suffered multiple attacks to its buildings, external power lines, and [main reservoir](#) supplying its cooling water.

The international community's efforts to minimize these risks has had some limited success, establishing a permanent [team of experts](#) from the International Atomic Energy Agency (IAEA), UN's nuclear watchdog, at the site for independent monitoring and information sharing, as well as providing some technical support and assistance to the Ukrainian nuclear authorities.

But Russia is planning to [restart the plant](#), which is now in cold shutdown, despite the deteriorating nuclear safety and security environment that has included recent attacks on the plant. Given an [ongoing staffing crisis](#) under Russian occupation and no maintenance plan for 2024, the Russian proposal seems technically quite challenging, due not just to regular attacks but also to lack of sufficient cooling water, once supplied from the now-depleted reservoir behind the now-destroyed Kakhovka dam. Ultimately, any effort to restart the plant, which the whole world believes to be unsafe, amounts to playing Russian roulette—with six nuclear reactors.

### Drone strikes, again

In the latest attacks, [three drone strikes](#) occurred on April 7 and April 9, further endangering the already frail plant's nuclear safety and security. While much is still unknown about the strikes, including who launched the kamikaze drones that hit one of the reactor buildings, Russia and Ukraine have, as in previous attacks, traded accusations of responsibility. On the day of the strikes, Rafael Grossi, IAEA's director general, once again [asserted](#) that “no one can conceivably benefit or get any military or political advantage from attacks against nuclear facilities. Attacking a nuclear power plant is an absolute no go.” Although there was reportedly no structural damage from this attack, it shows that one of the two combatants, at least, is ready to endanger the plant's safety and security despite the risks of an accident.

The motivation for the attack also remains unclear. The initial two strikes targeted surveillance and communication equipment on the roof of Unit 6 of the plant, and the Russian side of the conflict has consistently [refused to let the IAEA team](#) access rooftops. The latest drone strike on April 9 targeted a [training center](#), which is located half a kilometer away from the closest reactor building. It is unclear what possible military benefit the attacker may have been trying to obtain.

Later, the IAEA experts at the site confirmed that remnants from the drones had been collected that could help identify their origin, although the responsibility for these strikes may never be determined for certain.

As of April 13, all six reactors were in cold shutdown, technically the [safest mode of operation](#) in conflict zones. Nonetheless, there is still a possibility of a major nuclear incident, especially if there is an [intentional sabotage](#) aimed at causing a radioactive release. To reduce the likelihood of a release, the international community has attempted to make progress in securing the facility, but with limited success. In September, the IAEA General Conference adopted a [resolution](#) calling for the urgent withdrawal of military personnel and equipment in the vicinity of the site. The IAEA Board of Governors adopted a similar [resolution](#) in March, urging the withdrawal of military forces and the return of the plant to Ukrainian authorities. Earlier this week, [Grossi updated](#) the UN Security Council with the latest developments at the site, warning about how the international community is “getting dangerously close to a nuclear accident.”

### The risks of complacency

The IAEA will hold its International Conference on Nuclear Security, or ICONS, in May; it will consist of high-level policy discussions on nuclear security and technical sessions on technical, legal, and regulatory issues concerning nuclear security. The conference's theme will be about [shaping the future](#), with four broad topics covering policy and regulations, technological developments, capacity building, and cross-cutting issues on nuclear security. From the [preliminary program](#) (the final program is not publicly available yet) none of these topics appears to address the protection of nuclear facilities in conflict zones. Many abstracts addressing the Russia-Ukraine conflict submitted to the conference were rejected. Personal communication with IAEA staff and other relevant stakeholders indicates that the conference will not focus on this issue: “We [the international community] don't want to make [ICONS] a ‘Ukraine Conference,’” one staffer told me, indicating that the agency wanted to avoid creating a deadlock in other possible areas of nuclear cooperation.



In August 2022, a highly anticipated [Review Conference](#) of the Nuclear Non-Proliferation Treaty (NPT) could not adopt its final document because the draft included language about the Zaporizhzhia nuclear power plant. With Russia—a permanent member of the UN Security Council and the IAEA's Board of Governors—exercising pressure, the agency may not want to jeopardize its other broader responsibilities on nuclear security by stressing the sticky issue of one plant's safety. Other member states and participating nongovernmental organizations are, however, planning to organize side events during the ICONS conference to address nuclear security risks during armed conflicts. And the IAEA is drafting a guideline applying its safety standards and [nuclear security guidance](#) in armed conflict situations.

Also, there has been much scholarly attention on addressing the new risk profile posed by the Russia-Ukraine war, including proposals for a global convention to prohibit future armed attacks against nuclear facilities, published in the *Bulletin's* [columns](#) and [other forums](#). And a variety of institutional solutions have been proposed—including a [nuclear security protocol](#) signed between member states and the IAEA that would allow the agency to take proactive measures during armed conflicts in countries with nuclear infrastructure. The idea of a [nuclear safety and security zone](#) around nuclear power plants during wartime has also been broached. But the international community should not naïvely expect these proposed solutions—or any nuclear security guidelines updated by the IAEA—to be more effective than the current regime against a current or future aggressor state that does not respect international rules and practices. Still, while negotiating between member states can prove challenging in a conflict, alternative approaches and even partial achievements can still contribute to nuclear security.

Discussions within other multilateral forums—for example, the European Union, the Organization for Security and Co-operation in Europe, and NATO—might help raise awareness, build consensus, and seek support for proposed initiatives to deal with the problem of military attacks on nuclear power plants. Track 2 diplomacy could reinforce these efforts by using unofficial, informal communication channels to facilitate dialogue between experts, academics, and non-governmental actors. These initiatives can help build consensus, identify common ground, and generate creative solutions that can later be introduced into formal negotiations.

In the current environment, the international nuclear security community must remember that the IAEA's upcoming ICONS conference will last only one week, and the conversation must continue if the nuclear security community is to rise to the challenge posed by events in and around Zaporizhzhia with resilience and leadership.

**Ali Alkis** is the World Institute for Nuclear Security Ambassador to Turkey and a Ph.D. candidate at Hacettepe University in Ankara, Turkey. Alkis is also a member of the Gender Champions in Nuclear Policy, serves as the Gender Champion at the Odesa Center for Nonproliferation, and is one of the emerging leaders of the NTI's Global Dialogue on Nuclear Security Priorities. His research interests encompass nuclear security, non-proliferation, and nuclear terrorism as well as Turkish nuclear and foreign policies.

## The enormous risks and uncertain benefits of an Israeli strike against Iran's nuclear facilities

By Assaf Zoran

Source: <https://thebulletin.org/2024/04/the-enormous-risks-and-uncertain-benefits-of-an-israeli-strike-against-irans-nuclear-facilities/>

Apr 18 – Iran's unprecedented attack on Israel on April 13 has significantly escalated the tensions between the countries. For the first time, a declared and extensive [Iranian military operation](#) was carried out on Israeli territory. Now, the decision on how to respond rests with Israel. A direct war between the two countries now no longer seems unlikely.

Israel now realizes that it [underestimated the consequences](#) of its attack on an Iranian facility in Damascus that killed several senior members of Iran's Islamic Revolutionary Guard Corps earlier this month. However, the exceptionally large scope of Iran's response and the direct impact on Israeli soil is viewed in Israel as a disproportionate action that significantly escalates the conflict.

Despite the interception of most of the weapons launched by Iran and the lack of significant damage on Israeli territory, the outcome of the Iranian attack could have been vastly different due to the uncertainties of combat. Consequently, in Israel, there is a strong focus on Iran's intentions and Tehran's willingness to risk a direct confrontation.

Since Israel does not want to depend solely on defense and aims to prevent the normalization of attacks on its territory, it appears resolute to respond, reinforce its deterrence, and inflict a significant cost that will make Iran's decision-makers think twice before attacking similarly again.

While some in Israel advocate for [a robust immediate response](#) to project power and display independence despite international pressures, others prefer a more cautious and measured reaction to limit the risk of escalating into a major regional war.

Several main response options are under consideration, possibly in combination: a diplomatic move, such as forming a regional defensive coalition against Iran and its armed allies in the "axis of resistance," or



revitalizing international efforts against Iran's nuclear program; a covert kinetic operation, like past operations attributed to Israel targeting nuclear or missile facilities; or an overt kinetic military initiative, such as a missile or aircraft strike on Iranian territory. Both covert and overt kinetic actions can vary in intensity and target different sectors—military, governmental, or nuclear.



Israel used its Iron Dome and Arrow 3 (shown here during a test in 2022) defense systems to intercept the more than 300 missiles and drones that Iran launched at Israel on April 13. Israel said it plans to respond to Iran's attack. (Credit: Israel Defense Ministry, via Wikimedia Commons)

Currently, there is significant attention on the potential for Israel to execute a kinetic move against Iranian nuclear sites, covertly or overtly. Iran itself recently closed these facilities due to security concerns—a move noted by the international community, including the Director General of the International Atomic Energy Agency, Rafael Grossi, who [stated](#) that inspectors have been temporarily withdrawn. Within Israel, some perceive the current situation as an [opportunity to impair](#) Iran's nuclear program, considered a primary national security threat. The possibility of a military strike is [reportedly under examination](#). In contrast, Meir Ben-Shabbat, former head of the National Security Council, suggested that Israel should target the Iranian nuclear program [through diplomatic avenues](#). The ability to execute an extensive and effective kinetic operation against Iran's nuclear facilities on a short notice is doubtful. Such a move is also likely to lead to upheaval in the Middle East, contrary to Israeli officials' statements that a military response [will not lead](#) to a full-scale war with Iran.

Conversely, a precise strike on nuclear facilities in Isfahan, Natanz, Araq, or Fordow could not only rekindle international attention toward Iran's nuclear aspirations, it would also affirm Israel's commitment to act after several years [without significant action](#) in that regard. In doing so, Israel could demonstrate resolve, conveying clearly that it does not accept the nuclear precedent Iran has established in recent years and is willing to take decisive action if necessary, even if opposed or not supported by the international community.





Moreover, a successful attack on a heavily protected target would highlight Israel's superior capabilities and would undermine the new game rules that Iran attempted to establish. This, in turn, could decrease the likelihood of future attacks on Israeli territory.

Regionally, attacking a nuclear site could bolster Israel's image as the sole nation daring enough to confront Iran and counter its provocations, particularly following the security breach on October 7. This action could effectively demonstrate Israel's determination, showcase its military edge. However, an attack on Iran's nuclear facilities carries significant drawbacks.

In the short term, it would considerably increase the likelihood of a retaliatory response from Tehran, potentially even more severe, targeting sensitive locations in Israeli territory, and possibly extending to American and Jordanian interests in the region. This could inhibit the possibility of employing measured escalation levels and quickly lead to a broader conflict.

Hezbollah, which Iran sees as one of its assurances in case of an attack on its nuclear facilities, might be compelled to intensify its assaults against Israel.

Moreover, an attack on Iran's nuclear facilities may have the opposite result of prompting an escalation in Iran's nuclear developments, a pattern previously observed in response to kinetic actions attributed to Israel. Such an attack could be used by Tehran as a justification and motivation to progress toward nuclear weapons development, confirming that conventional deterrence is insufficient. In recent years—and in past months even more so—senior Iranian figures have increasingly [hinted at this possibility](#).

An overt attack on Iran could also diminish Israel's legitimacy and international support, which momentarily recovered amid a historic low following the war in Gaza. This erosion could jeopardize diplomatic efforts to establish renewed coalitions and strategies against Iran. Although it is crucial for Israel to impose a significant cost on Iran in response to its April 13 attack to deter further aggressive actions in the region, targeting nuclear facilities might be strategically disadvantageous. The costs could heavily outweigh the benefits, and Israel should be prudent to focus on a proportionate response, such as targeting missile and drone infrastructures in Iran or other Iranian assets in the region.

At the same time, it is vital to invest in a substantial political response, such as forming a defensive coalition against the resistance axis and incorporating into it countries threatened by Iran under international auspices. Amid an emerging contest of superpowers in the region and beyond, such a political response also presents an opportunity to foster closer ties and strengthen commitments between these nations and the West.

[Assaf Zoran](#) is a research fellow with the Project on Managing the Atom and International Security Program at Harvard Kennedy School's Belfer Center for Science and International Affairs. He is an attorney with 25 years of experience addressing policy and operational issues in the Middle East, engaging in strategic dialogue with decision-makers in Israel and other regions.

## US Air Force secretly develops missiles that could obliterate Iran's nuclear facilities by zapping their electronics - without harming civilians

Source: <https://www.dailymail.co.uk/news/article-13325343/US-Air-Force-develops-missiles-obliterate-Iran-nuclear-facilities.html>

Apr 19 – Ronald Kessler, a former Washington Post and Wall Street Journal investigative reporter, is the [New York Times](#) Bestselling Author of 'The Secrets of the [FBI](#),' 'The First Family Detail,' and the 'CIA at War.'

The US Air Force has quietly deployed missiles that could destroy the electronics of [Iran](#)'s nuclear facilities with high-power microwaves, rendering them useless, without causing any fatalities, DailyMail.com has learned exclusively.

Known as the Counter-Electronics High Power Microwave Advanced Missile Project (CHAMP), the missiles were built by Boeing's Phantom Works for the US Air Force Research Laboratory and first tested successfully in 2012. They were deployed—meaning installed in various locations around the globe—and became operational in 2019.

This comes as [Israel has conducted strikes in Iran](#) in retaliation for Tehran's unprecedented drone-and-missile assault earlier this week, defying US President's warning that more attacks could plunge the Middle East further into conflict.

Mary Lou Robinson, then chief of the High Power Microwave Division of the Air Force Research Lab at Kirtland Air Force Base, previously confirmed to DailyMail.com that 20 CHAMP missiles were operational and ready to take out any military target, including nuclear facilities.

When asked for comment, Othana Zuch, an Air Force Research Laboratory public affairs officer, said that while 'operational security precludes us from discussing specific operational applications for our technologies,' the CHAMP missiles were considered a demonstration program and 'we have since continued to develop advanced HPEM (High Power Electromagnetic) technologies' building on the original demonstration.

The microwave weapons are fitted into an air-launched cruise missile and [delivered from B-52 bombers](#). With a range of 700 miles, they can fly into enemy airspace at low altitude and emit sharp pulses of high



## ICI C<sup>2</sup>BRNE DIARY – April 2024

power microwave (HPM) energy that fry computer chips, disabling any electronic devices targeted by the missiles without causing any collateral damage.

The missile is equipped with an electromagnetic pulse cannon. This uses a super-powerful microwave oven to generate a concentrated beam of energy. The energy causes voltage surges in electronic equipment, rendering them useless before surge protectors have the chance to react.

The project has been advancing secretly ever since the Air Force successfully tested a missile equipped with HPM in 2012.

In the test, the CHAMP missile flew over a two-story building on the Utah Test and Firing Range.

The building in the west Utah desert was crammed with computers and security and surveillance systems. The microwaves took down the compound's entire spectrum of electronic systems, including video cameras set up to film the test, without damaging anything else.

'We hit every target we wanted to,' Boeing's CHAMP Program Manager Keith Colman said in a company press release then. 'Today we made science fiction into science fact.'

Until the announcement of the successful test, the project had been top secret. When it was announced, only a few trade publications ran the story.

Since then, beyond several dozen stories in December 2017 when the missiles were still non-operational, the media beyond DailyMail.com have ignored the story.

Because of sequestration budget cuts, the CHAMP missiles did not become operational under the Obama administration.

But after I emailed then Trump National Security Adviser H. R. McMaster in August 2017 information about CHAMP that I was about to include in my book 'The Trump White House: Changing the Rules of the Game,' McMaster thanked me for letting him know about the capability which he was not aware of, agreed to an interview, and ordered a briefing from the Pentagon.



The beauty of the HPM missile is that its microwave beam can penetrate bunkers where facilities are hidden without harming humans inside

As a result, the Pentagon funded the program and ordered Air Force training worldwide to deploy and operate the missile systems.

The beauty of the HPM missile is that its microwave beam can penetrate bunkers where facilities are hidden without harming humans inside.

Even if a bunker is buried in a mountain, HPM penetrates the facilities through its connections to power cables, communication lines, and antennas. Thus, HPM can penetrate any underground military or nuclear facility and destroy its electronics.



Targeted at command-and-control centers, the missile could render any country's military inoperable. And one missile can hit multiple targets in succession. While Iran may attempt to shield its equipment, US officials say that would not be effective against the HPM missiles. Besides underground bunkers and command centers, HPM can quickly disable fighter planes, tanks, ships, and missile systems. And it can wipe out facilities for developing and testing nuclear weapons.



The High Power Microwave Division of the Air Force Research Lab is at Kirtland Air Force Base in Albuquerque, New Mexico

Most amazing of all, the missile renders inoperable any radar that might detect it as it flies to and from a target. Thus, a country cannot take out CHAMP before it strikes and has no way of knowing why its facilities have suddenly gone dead.

America's national laboratories operated by the Department of Energy have been working on HPM capabilities for decades. Over the years, HPM devices have been deployed on the ground in Afghanistan and Iraq to disable improvised explosive devices (IEDs) and drones. The HPM missiles are entirely different from cyber-warfare designed to confuse computers. Unlike a cyberattack, they permanently fries electronic equipment.

HPM missiles also differ from an electromagnetic pulse (EMP) attack that is created by detonating a nuclear weapon in the atmosphere. Because it is targeted, HPM leaves intact civilian facilities needed to sustain life.

## You Think This Situation Is Terrifying? Wait Until Iran Goes Nuclear – OpEd

By Baria Alamuddin | [Arab News](#)

Source: <https://www.eurasiareview.com/22042024-you-think-this-situation-is-terrifying-wait-until-iran-goes-nuclear-oped/>

Apr 22 – While the tit-for-tat exchange between Israel and Iran has fundamentally altered strategic calculations about regional security, it is just starting to dawn on the world how much more dangerous the situation would be if both sides possessed nuclear weapons.

Israel's strike at Isfahan, in the vicinity of several nuclear facilities, was a warning shot, while Revolutionary Guards commander Ahmad Haqtaalab threatened to attack Israeli nuclear sites if Iranian installations were targeted. Haqtaalab warned of Iran's readiness to revise its doctrine on developing its own nuclear weapons, fueling concerns that Tehran could embark on a final rush toward acquiring these capabilities.

International Atomic Energy Agency inspectors report "frenzied activity" at Iran's Fordow nuclear site, including newly installed equipment, enrichment of uranium with ever greater rapidity, and expansion projects for doubling the plant's output and scaling up uranium production just a "flip of a switch" from



weapons grade. Iran's larger Natanz plant is also vigorously churning out highly enriched uranium. Iran is building additional infrastructure so deep into the Natanz mountainside that there are doubts that any kind of US or Israeli strike could touch nuclear activities there.

Experts warn that Iran requires just a few days to upgrade sufficient uranium for three bombs. Manufacture of a crude nuclear device would take about six months, while building a missile-delivered nuclear warhead may require a couple of years, assuming Tehran hasn't clandestinely developed these capabilities already. Documents stolen in a 2018 Israeli raid indicate years of extensive research into the full spectrum of capabilities necessary for engineering nuclear Armageddon.

Iran's top nuclear official, Mohammad Eslami, appeared to boast in January that Iran had arrived at military breakout threshold, crowing that "deterrence has been achieved." IAEA director-general Rafael Mariano Grossi condemned this "loose talk" about possessing nuclear weapons, while warning of a domino effect as other regional states raced to acquire their own nuclear capacities. I recall participating in the 2009 Doha Debate, arguing against those making the case that Iran could be trusted not to build a nuclear bomb. Iran's apologists, including supposed experts and academics, took the view that Ayatollah Ali Khamenei had declared nuclear weapons to be un-Islamic, while asserting a God-given right to enrich uranium. I argued the case for a region wholly free of weapons of mass destruction, although I would go further in advocating comprehensive global nuclear disarmament. Since 2022 this existential threat has been further highlighted by the casual manner in which Vladimir Putin's regime repeatedly expressed its readiness to resort to these horrific weapons whenever it came under pressure over Ukraine.

The mutual embrace between China, Iran, Russia, North Korea and other rogue states is growing ever tighter. Despite the latest batches of sanctions imposed on Tehran, we have arguably entered an era in which Western sanctions are broadly irrelevant. This large bloc of states, containing a sizable proportion of the planet's population, is able to trade, finance itself, arm itself, and secure its energy needs, while Western leaders impotently yell and decry from the sidelines, in a world in which the dollar no longer holds universal sway. The same processes have utterly paralyzed the global infrastructure for international law and conflict resolution established after the Second World War. So the regime in Tehran feels increasingly untouchable? Damn right it does!

Over past months proxies such as Hezbollah have nervously pulled their punches to avoid disproportionate retaliation from a greatly superior Israel fighting machine. But what about a scenario in which Hezbollah and other paramilitaries fired tens of thousands of missiles at Israeli population centers, while Tehran pointed its nukes at Tel Aviv and dared Israel to respond? Given that Israel already has its own nuclear arsenal, there are numerous terrifying scenarios that could rapidly escalate into a nuclear exchange, leaving millions dead and the region destroyed.

For many years posturing world leaders declared that Iran would not be allowed to continue enriching uranium to 5 percent. Then it was 20 percent. Now the nuclear clock is ticking inexorably toward midnight. Will it be another North Korea, when rhetoric about not allowing Pyongyang to develop advanced military capacities was supplanted by language about learning to live with a nuclearized Korean Peninsula and hoping for the best?

Although Barack Obama's 2015 nuclear deal was deeply flawed, Trump's unilateral withdrawal in 2018 and the imposition of largely ineffective sanctions was disastrous, allowing Tehran to continue its progress toward a bomb. Biden administration officials have long since acknowledged that efforts to revive the 2015 deal are dead in the water, but their failure to consider other options has left a dangerous policy vacuum. Iran's rejection of key elements of IAEA inspections means the watchdog may be incapable of detecting nuclear breakout. As one US official puts it, the Iranians are "dancing right up to the edge."

The horrors of nuclear conflict are by definition unthinkable, and consequently mediocre Western leaders have consistently refused to think seriously about these increasingly imminent threats, or countenance strategic policies that could halt this menace.

Twenty years of nuclear negotiations produced precisely nothing, other than marginally delaying Tehran's nuclear ambitions. The current escalatory regional situation is terrifying — but it isn't a fraction as bad as it could be once the atomic ambitions of megalomaniac ayatollahs are realized, while Israel's blood-drunk leaders continue to push threat levels above boiling point, driving the planet inexorably closer to the real risk of nuclear apocalypse.

**Baria Alamuddin** is an award-winning journalist and broadcaster in the Middle East and the UK. She is editor of the Media Services Syndicate and has interviewed numerous heads of state.



Arab News is Saudi Arabia's first English-language newspaper. It was founded in 1975 by Hisham and Mohammed Ali Hafiz. Today, it is one of 29 publications produced by Saudi Research & Publishing Company (SRPC), a subsidiary of Saudi Research & Marketing Group (SRMG).



## Unstable nuclear-waste dams threaten fertile Central Asia heartland

Source: <https://www.yahoo.com/news/unstable-nuclear-waste-dams-threaten-132443990.html>



### Unstable nuclear-waste dams threaten fertile Central Asia heartland

Apr 23 – Dams holding vast amounts of uranium mine tailings above the fertile Fergana valley in Central Asia are unstable, threatening a possible Chernobyl-scale nuclear disaster if they collapse that would make the region uninhabitable, studies have revealed.

Dams holding some 700,000 cubic meters (185 million gallons) of uranium mine tailings in Kyrgyzstan have become unreliable following a 2017 landslide. A further landslide or earthquake could send their contents into a river system used to irrigate Kyrgyz, Uzbek and Tajik farmlands, the studies at the Soviet-era radioactive waste disposal facility showed. That event would possibly displace millions in those three countries.

The studies, part of a project by the European Commission and the European Bank for Reconstruction and Development to reinforce the facilities, show that the type of waste involved cannot be safely contained in their current locations and needs to be moved away from the banks of the Mailuu-Suu river.

The Fergana valley, where the contaminated water would go, is the most densely populated area in Central Asia with 16 million people, many of whom are involved in the cultivation of cotton, rice, grains, fruit and vegetables.

"If a landslide causes the river to burst, the waste from two mine dumps will enter the water," says Gulshair Abdullayeva, a manager of the Mailuu-Suu radiology lab.

"The environmental disaster would almost be comparable with Chernobyl."

Studies have shown that the waste in those dumps is liquid, making it more hazardous, and it could flow into the river in the event of a strong earthquake, says Sebastian Hess, an engineer with German firm G.E.O.S. contracted by the Kyrgyz government.



"That would be a horrible catastrophe," he said. "This water is used to irrigate fields which means agricultural produce would be contaminated."



The dams' foundations were weakened by water during a 2017 landslide which raised the river's water level, bring it closer to the tailings, engineers have said.

The Bishkek government and G.E.O.S. estimate that 22-25 million euros would be needed to move the waste from the two unsafe locations to one further away from the river.

The area near the town of the Mailuu-Suu, one of the world's biggest uranium ore dumps, was developed by the Soviet Union between the 1940s and 1960s. A factory in the town also processed uranium ore from other nearby mines.



ICI  
International  
**CBRNE**  
INSTITUTE



# EXPLOSIVE NEWS

## At least 3,000 unexploded bombs in Gaza in first 3 months of war

Source: <https://www.middleeastmonitor.com/20240326-at-least-3000-unexploded-bombs-in-gaza-in-first-3-months-of-war/>

Mar 26 – At least 3,000 of the 45,000 Israeli bombs dropped on the Gaza Strip between 7 October and mid-January have failed to explode, according to estimates by Handicap International, an NGO specialising in mine action.

“Of these 45,000 bombs, 3,000 have not exploded, and it is in fact these that will cause additional danger, particularly for civilians, when humanitarian aid is deployed,” said Jean-Pierre Delomier on *Radio France Internationale*.

This number, estimated by the Mine Action Area of Responsibility, a working group composed of non-governmental organisations active in the area, including Handicap International, covers the period between 7 October and mid-January. Israel has continued to bomb Gaza since then. Delomier spent several days in Gaza’s southernmost city of Rafah, on the Egyptian border, where about 1.5 million Palestinians reside, most of whom are displaced.

He considered in particular that only a ceasefire would be enough to give more “visibility” to rights groups to “begin the work of clearing mines and explosive remnants of war contamination”. At the beginning of March, the French-based organisation defending people with conflict-related disabilities sent two experts for 15 days to begin assessing demining needs in the Gaza Strip.

Tens of thousands of Palestinians are thought to have been left disabled by Israel’s bombing campaign in Gaza. In December, UNICEF [estimated](#) that 1,000 children had had limbs amputated without anaesthesia in Gaza.

Handicap International physiotherapist Maria Marelli [warned last week](#): “There will be a significant increase in the number of people with disabilities in Gaza. That is sure. Even a seemingly minor injury or fracture, if improperly treated or if it gets infected, which is highly possible given the terrible hygiene conditions, could lead to complications and lifelong disabilities.

## Nanosensors in hazardous explosives trace detection - Challenges and Future directions

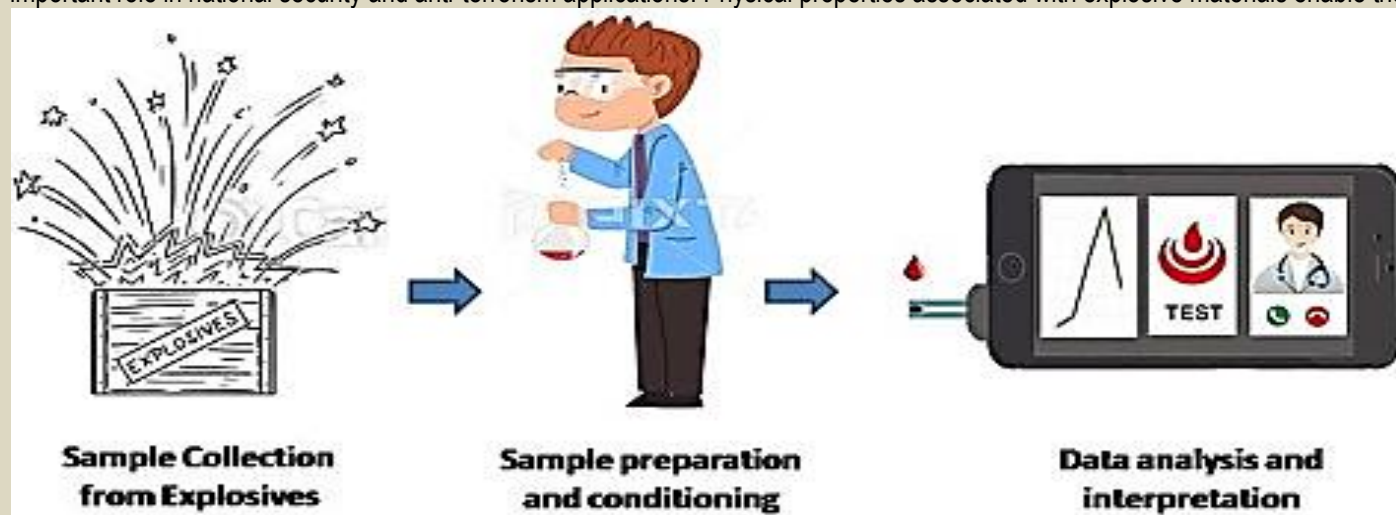
By Saleem Khan, Uvais Valiyaneerilakkal, Suesh Kumar, et al.

*Microchemical Journal* | Available online 3 April 2024, 110474

Source: <https://www.sciencedirect.com/science/article/abs/pii/S0026265X24005861>

### Abstract

Recent technological advancement led to the development of new and innovative explosive detection methods which play an important role in national security and anti-terrorism applications. Physical properties associated with explosive materials enable the



development of an explosive trace detection system (ETD). Nanoscience and materials have paved the way to explore new horizons of miniaturization and portable devices for on-site explosive trace detection. This review paper showcases nanomaterial-based advances in explosive detection. The detection mechanism and analytical aspect of chemiluminescence, electrochemical, microcantilever, and electronic nose devices for explosive compounds are briefly reviewed. The article emphasizes the current limit of detection of explosives as a crucial benchmark, shaping the foundation for the evolution of future nanomaterial-based Explosive Trace Detection (ETD) sensing systems.





## Millions of dollars needed to make Gaza safe from unexploded bombs

Source: <https://news.un.org/en/story/2024/04/1148021>



Apr 03 – The scale of the bombs dropped on Gaza since 7 October means that it will take millions of dollars, and many years, to decontaminate the Strip from unexploded munitions, the head of the UN Mine Action Service (UNMAS) in Palestine tells UN News, ahead of [Mine Action Day](#).

Charles Birch, known as Mungo, was working with his team in Gaza long before the 7 October conflict, clearing unexploded munitions from the occupied territory. He told Conor Lennon from UN News that all of their earlier work has been undone by the bombardments that have rained down on Gaza over the last six months.

*This interview has been edited for clarity and length*

**Mungo Birch** UNMAS has been in Gaza for about ten years. Before 7 October our primary operations were based in Gaza, and we also had smaller operations in the West Bank. In Gaza, what we primarily did, in terms of explosive ordnance disposal (EOD) work was clearing deeply buried aircraft bombs, and conducting explosive threats assessments of UN facilities after there was an escalation.

Clearing the bombs involved digging a shaft, between 10 and 15 metres underground, to get to them, then the head of operations, a man called Paddy McCabe, would go down the shaft, remove the fuse from the bomb, rendering it safe, and then remove it from the hole and pass it over for destruction.

**UN News** Prior to 7 October, how many unexploded ordnance bombs would you expect to find?

**Mungo Birch** We would clear about one deep buried aircraft bomb per month. Since the 2021 war between Hamas and Israel 21 deep buried aircraft bombs had been reported to us, and we had almost completed that work.

Obviously that work will have been completely undone by the conflict since October 7<sup>th</sup>, and the scale of the contamination will be such that it's unlikely we'll start looking into deep buried ordnance for some time. Most of our work will be focused on surface level ordnance.

**UN News** The eventual reconstruction of Gaza will be a monumental task. How important will ordnance removal be to that process?

**Mungo Birch** We work off the rule of thumb that 10 per cent of ordnance doesn't function as designed. There's now more rubble in Gaza than there is in Ukraine and as part of the rubble removal process, a huge task in itself, explosive ordnance clearance needs to be taken into account. This means years and years of work. It will be an unprecedented operation.

**UN News** What did October 7 mean for you and your team?

**Mungo Birch** I was the only international staff member in Gaza at that time, and I was with nine national staff members. The first week of the war I was in northern Gaza, in the [UNRWA](#) (UN Agency for Palestine refugees) compound. The bombardment was incredibly intense. Large, airdropped munitions and missiles, and barrages of Hamas rockets going out from Gaza. The bombardment was like nothing I've ever experienced.

The UN compound was never directly hit, but it was severely damaged by blasts. It was a dire situation. The national staff were spread across Gaza, and now they're all in the south. Two have been evacuated, the other seven remain in Gaza and they continue to work. They've been unbelievably dedicated to their jobs under the most terrible circumstances imaginable.

At the moment there are four international staff in Gaza, who are providing support to UN convoys to the north: because of the political issues only international staff accompany the humanitarian convoys. They



allow the convoys to get through unhindered by unexploded ordnance. Then our national staff conduct explosive ordnance risk education, which is a vital component of the mine action response in Gaza.

It's incredible what the national staff are doing. They've really gone above and beyond what they need to do. Most of them have lost their homes. They've lost relatives and friends. It's a terrible situation.

**UN News** How difficult is it for you, as a team, to carry on through this?

**Mungo Birch** The only reason the team has held together is because we had an excellent dynamic before the war, and very dedicated colleagues. The national staff are hugely dedicated to the wider project, and it's a real testament to them and their resilience. I've never seen anything like it.

**UN News** Looking ahead to the reconstruction, is there a big gap between what you need and the funds available?

**Mungo Birch** There's a huge gap. We estimate that, **to begin the clearance of Gaza, we need around \$45 million**. So far, we have \$5.5 million in the pipeline. Hopefully, donors will be more open to funding once the war ends, because we desperately need funds.

## Repetitive Blast Waves in Military Explosives Training Might Trigger Leaky Guts

Source: <https://www.sciencealert.com/repetitive-blast-waves-in-military-explosives-training-might-trigger-leaky-guts>



Apr 10 – Explosive weapons training in the military has recently come [under fire](#) for its potential to cause brain injuries through blast waves alone, even when students and instructors are located a 'safe' distance from the blast itself.

A shocking new study has now found that exposure to repetitive, low-level blasts, like those that come from hand grenades, can be linked to a [leaky gut](#). Because the permeability of the gut is controlled, in part, [by neurons](#), experts suspect that this is associated with decreased cognitive function.

According to neuroscientist Qingkun Liu and colleagues in the US, the symptoms are in line with mild traumatic brain injury (TBI). Patients with TBI often experience abdominal pain, gastric distension, or constipation. They can also develop a leaky gut.

This leakiness coincides with a reduction in specific gut proteins, which help the walls of the intestine keep the riff-raff out. An increase in gut permeability can lead to bacteria leaking into circulation and possibly [wreaking havoc](#) on the body's systems – a feature of [Alzheimer's](#) disease and [schizophrenia](#).

"[S]ince blood has been generally considered a sterile environment that lacks microbes, studies on the human blood microbiome have received little recognition until recently," [write](#) Liu, who works at the James J Peter VA Medical Center in the Bronx, and his colleagues.

The team's study included 30 male participants, most of whom served as combat engineers and 18 of whom reported existing mild traumatic brain injury from direct blunt force trauma, though not from blasts.

Shortly before, and around one hour after wall-breaching exercises, where participants stood 12 meters away from the blast, researchers took their blood. The next day, roughly 16 hours later, they took another sample.

Following the blast training, participants showed increased bacterial translocation in their blood circulation. Their protein biomarkers for gut leakiness were also out of whack.



An hour after the blast, the cohort reported symptoms like headaches, dizziness, difficulty concentrating, and taking longer to think, which gradually faded over 12 hours.

The results of the study, while purely observational, suggest that intestinal permeability may be linked to decreased cognitive functioning brought about by blast waves hitting the brain.

"To our knowledge, this is the first study that shows that exposures to blast in a military operational setting contributes to bacterial translocation and intestinal permeability along with associated cognitive symptoms, establishing the role of the gut–brain axis in blast-related sequelae," the authors [conclude](#).

The findings come at a critical time in brain research. In March of 2024, *The New York Times* reporter Dave Philipps [broke a story](#) on the findings of a specialized lab at Boston University, which was investigating chronic traumatic encephalopathy (CTE) among athletes, like football players. Neuroscientists at the lab had found "[moderately severe](#)" damage in the brain of a deceased mass shooter and military veteran. The scarring and inflammation looked as though it was the result of repeated trauma. But not blunt force trauma. The trauma was characteristic of a shockwave.

Its signatures were [similar to that of other military vets](#), who used weapons like shoulder-fired rockets that trigger blast waves. But this particular individual had never faced real-world combat before. The only blasts he had ever been exposed to were at a military training camp he attended where soldiers were taught to use rifles, machine guns, grenades, and shoulder-fired rockets.

Phillips reports that over the years, the deceased mass shooter could have easily been exposed to more than 10,000 blasts, and while it's not clear if this was directly tied to his psychological symptoms or his criminal behavior, neuroscientists at Boston University say it's likely. Clinically, the way blast brain damage manifests, it is [often mistaken](#) for post-traumatic stress disorder. Several years ago, US Army research teams [investigated](#) cases of blast instructors suffering from fatigue, headaches, memory issues, and confusion. No action was taken to reduce their exposure. Even shoulder-fired rockets, which send shock waves scarily close to the brain, [remain in wide use](#). In response to [recent research](#) by the US Defense Department and an [investigation](#) by *The New York Times* connecting brain damage to artillery and rocket launchers, a bipartisan group of US Senators [are demanding to know](#) what the US military is doing to protect troops. And it's not just high-level blasts in wartime that need to be considered.

Even when the blasts are kept at what is currently considered a '[safe](#)' threshold by the US military, gathering evidence suggests they might put the firer and surrounding individuals at risk.

"If the right kind of wave hits brain tissue, the tissue just breaks — it literally gets torn apart," biomechanics expert Christian Franck [told Times](#) reporter Philipps in December of 2023. "We see that in the lab. But what kind of blast will do that in real life? It's complex... There is a lot we don't know." While the current study is small and lacks a control group, it joins a wave of new research that suggests blunt force trauma isn't the only way to damage the brain, and that low-level blasts are also a problem.

To protect instructors, students, and veterans in the military, further research is desperately needed.

●► The study was published in the [International Journal of Molecular Sciences](#).



**Hui Zhang** is a physicist and a senior research associate at the Project on Managing the Atom in the Belfer Center for Science and International Affairs at Harvard University's John F. Kennedy School of Government, where he leads a research initiative on China's nuclear policies.



ICI  
International  
**CBRNE**  
INSTITUTE



# CYBER NEWS





# United States Cyber Force

## A Defense Imperative

Dr. Erica Lonergan and RADM (Ret.) Mark Montgomery  
March 2024



**Dr. Erica Lonergan (née Borghard)** is an assistant professor in the School of International and Public Affairs at Columbia University. Previously, Erica held several positions at the United States Military Academy at West Point, including assistant professor in the Departments of Social Science and Electrical Engineering and Computer Science, a fellow at the Army Cyber Institute, and executive director of the Rupert H. Johnson Grand Strategy Program. Beyond her academic and research appointments, Erica has an extensive background in strategy and policy. Previously, she was a lead writer of the 2023 U.S. Department of Defense Cyber Strategy and the congressionally mandated Department of Defense Cyber Posture Review. Before that, Erica served as a senior director on the Cyberspace Solarium Commission and continues to serve as a senior advisor to CSC 2.0.

**RADM (Ret.) Mark Montgomery** serves as senior director of FDD's Center on Cyber and Technology Innovation and as an FDD senior fellow. He also directs CSC 2.0, an initiative that works to implement the recommendations of the congressionally mandated Cyberspace Solarium Commission, where he served as executive director. Previously, Mark served as policy director for the Senate Armed Services Committee, coordinating policy efforts on national security strategy, capabilities and requirements, and cyber policy. Mark served for 32 years in the U.S. Navy as a nuclear-trained surface warfare officer, retiring as a rear admiral in 2017. His flag officer assignments included director of operations (J3) at U.S. Pacific Command; commander of Carrier Strike Group 5, embarked on the USS George Washington, stationed in Japan; and deputy director for plans, policy, and strategy (J5) at U.S. European Command.

## The Francis Scott Key Bridge case

By Lara Logan | South African television and radio journalist and war correspondent.  
Source: <https://twitter.com/laralogan/status/1772675651599770093>

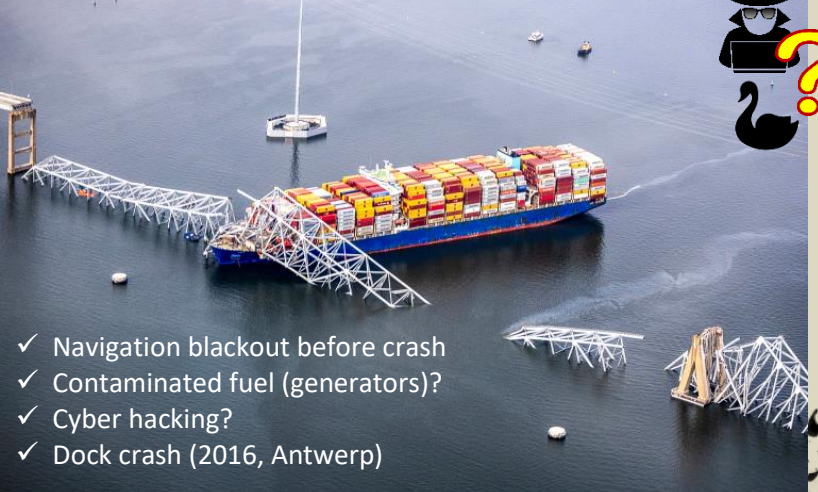


Mar 27 – Multiple intel sources: The Baltimore bridge collapse was an “absolutely brilliant strategic attack” on US critical infrastructure

- most likely cyber - & our intel agencies know it. In information warfare terms, they just divided the US along the Mason Dixon line exactly like the Civil War. Second busiest strategic roadway in the nation for hazardous material now down for 4-5 years - which is how long they say it will take to recover. Bridge was built specifically to move hazardous material - fuel, diesel, propane gas, nitrogen, highly flammable materials, chemicals and oversized cargo that cannot fit in the tunnels - that supply chain now crippled. Make no mistake: **this was an extraordinary attack in terms of planning, timing & execution.**

The two critical components on that bridge are the two load-bearing pylons on each end, closest to the shore. They are bigger, thicker and deeper than anything else. These are the anchor points and they knew that hitting either one of them would be a fatal wound to the integrity of the bridge. Half a mile of bridge went in the river - likely you will have to build a new one.

### Over 80 billion USD losses!

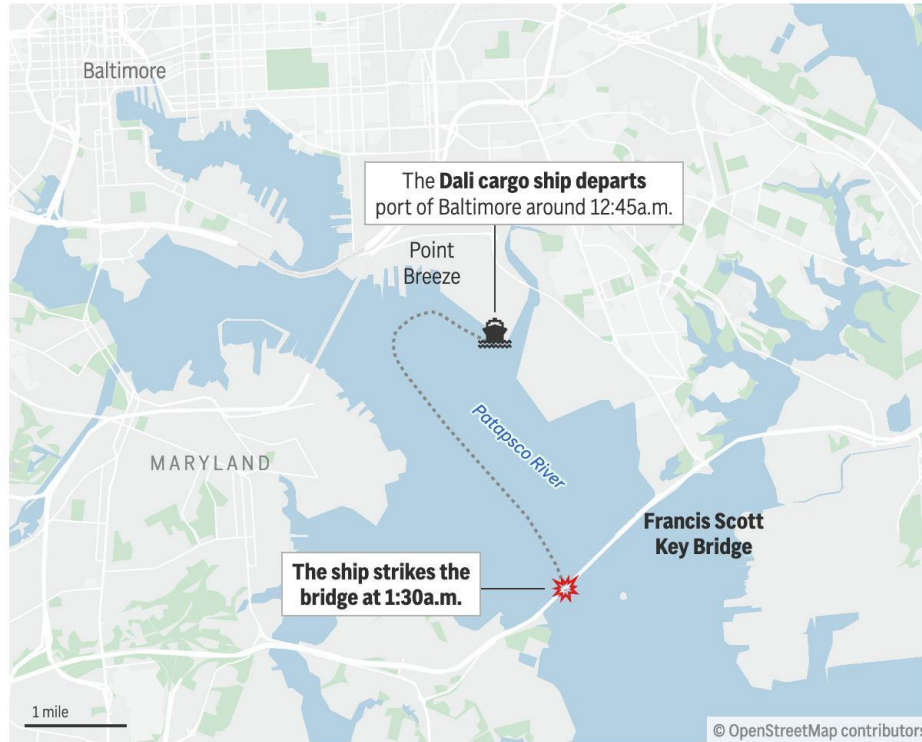


- ✓ Navigation blackout before crash
- ✓ Contaminated fuel (generators)?
- ✓ Cyber hacking?
- ✓ Dock crash (2016, Antwerp)



Also caused so much damage to the structural integrity of the bottom concrete part that you cannot see & won't know until they take the wreckage apart. Structural destruction likely absolute. Attack perfectly targeted. "They have figured out how to bring us down. As

## Cargo ship hits Baltimore's Key Bridge, collapsing it



long as you stay away from the teeth of the US military, you can pick the US apart. We are arrogant and ignorant - a lethal combination. Obama said they would fundamentally change America and they did. We are in a free-fall ride on a roller coaster right now - no brakes - just picking up speed." The footage shows the cargo ship never got in the approach lane in the channel. You have to be in the channel before you get into that turn. Location was precise/deliberate: chose a bend in the river where you have to slow down and commit yourself - once you are committed in that area there is not enough room to maneuver. Should have had a harbor pilot to pilot the boat. You are not supposed to traverse any obstacles without the harbor pilot. They chose a full moon so they would have maximum tidal shift - rise and fall. Brisk flow in that river on a normal day & have had a lot of rain recently so the water was already moving along at a good pace. Hit it with enough kinetic energy to knock the load-bearing pylon out from under the

AP

highway - which fatally weakened the span and then 50 percent of the bridge fell into the water. All these factors when you look at it - this is how you teach people how to do this type of attack and there are so few people left in the system who know this. We have a Junior varsity team on the field. Tremendous navigational obstruction. Huge logistical nightmare to clean this up. Number of dead is tragic but not the whole measure of the attack. That kind-of bridge constantly under repair - always at night because there is so much traffic and they cannot obstruct that during the day. So the concern is for repair guys who were on foot (out of their vehicles) working who may now be in the water - 48 degrees at most at this time of year. When you choke off Baltimore you have cut the main north-south hazardous corridor (I95) in half. Now has to go around the city - or go somewhere else. To move some of that cargo through the tunnel you may be able to get a permit but those are slow to get and require an escort system that is expensive and has to be done at night. For every \$100 that goes into the city, \$12 comes from shipping. Believe this will cripple the city of Baltimore at a time when they do not have the resources to recover.

## Baltimore Bridge Collapse: An Expert Explains How Disasters Like This Can Happen

By Allan Post

Source: <https://www.sciencealert.com/baltimore-bridge-collapse-an-expert-explains-how-disasters-like-this-can-happen>

Mar 27 – Details are still emerging about the disaster that happened in the early morning of March 26, 2024, when the *Dali*, a large cargo ship on its way out of the port of Baltimore, [hit a major bridge and caused it to collapse](#).

The Conversation's senior politics and democracy editor, Naomi Schalit, spoke with Captain Allan Post, a veteran ship's officer, about the role a ship pilot plays in bringing a large ship in and out of a harbor.

### What was your first thought when you heard about the accident?

Post: My first thought was, thank God it happened at night, because of the low amount of traffic on the bridge. If that had happened during the daytime, casualties would be in the thousands. My heart aches for those lives lost.





**There were two ship pilots aboard the ship as it left its berth in the Port of Baltimore. Can you tell us what ship pilots do?**

Post: Ship pilots are brought on board in what are considered restricted maneuverability or navigation areas. They are local experts who are usually certified by the state or federal government [to provide advice to the master of the vessel as to how to control the vessel](#), safely and adequately, through the pilotage waters, which in this case would be down the river from the Port of Baltimore. Pilots are well practiced in close-quarters maneuvering, especially with tugboats and docking the vessel alongside the assigned berth.

**But a pilot doesn't come aboard the ship and take control of it, do they?**

Post: They are just [advisers to the captain](#), who is known as the "master." The master still has full responsibility for the safe navigation of the vessel. So the pilot will meet the ship out at sea or at the dock if it's in port and leaving to go to sea. They proceed up to the bridge. Usually they exchange greetings, and usually a little bit of ship's swag is given, either a hat or something else, or at least a cup of [coffee](#).

They then set up their gear. With the electronics that we now have, they plug into the ship's electronic chart data information system. And then they conduct the pilot exchange with the master of the vessel, where the master of the vessel describes where they are going, what the characteristics of the ship are, who's on the bridge, what their first language is and the air draft of the vessel, which refers to how high out of the water the vessel is, so that you know whether you can take the ship under a bridge safely.

Once that's completed, the pilot then starts instructing the officer of the watch or the captain – those are usually the same person – in how to get to where they need to be to dock the ship, or undock the ship and bring it to sea.

This instructing is done during complex maneuvers, not all the time. The pilot can also say he's not going to do it, and can shut down their operations if conditions are unsafe or if they feel that the vessel is not in condition to be able to transit safely. That happens a lot, especially in fog.

The ship pilot also interacts with the Coast Guard Vessel Traffic Service and other ships in the area, and coordinates with the tugboats and line handlers to be able to safely maneuver the vessel close to the pier or when a ship is leaving the berth.

**Can you describe the training of a ship pilot?**

Post: Most of them start out at a maritime academy and have to spend many years at sea in command or as a bridge watch-stander on a vessel. From there, they start into the pilot apprentice program that each one of the pilot associations has, and those programs last years.

What they do in those programs is use simulators and real, actual hands-on training, so that they can see how the different ships maneuver, how different places along the route have different currents and tides, and how the channels affect the ships.

It's not something that you can go to a sea school for three weeks to learn and then come out and be a pilot. [It's many years long](#). They're really the surgeons of the sea.

**So when a ship's pilot shows up, they're going to be someone with a minimum of how many years training before they even get onto your ship?**

Post: Many have 10-plus years before they are allowed to work on their own.

**They have to be specialists in the place where they work, don't they?**

Post: Most of them are ship's officers licensed by the U.S. Coast Guard, and they're licensed for unlimited tonnage vessels. But that's not the end of training. From there, they are hired into the pilot apprentice programs for the area in which they're going to gain their pilot endorsement or credentials.



One pilot may not be credentialed in another area. They spend many years under the guidance of senior pilots who teach them basically everything that they need to know about the local waterways, about the navigation, current tides, where all the berths are. They become absolute experts in how to do this. And then, when most of them end up taking the pilotage exam, they have to draw the charts that they would be using in the pilotage waters – from memory.

**Are there legal requirements for ship pilots to be present both going out of and coming in these restricted areas?**

Post: Yes, there are – state law, federal law or both.

**This is an almost 1,000-foot-long vessel. Is that big, small or medium?**

Post: That's about standard size these days. Ship sizes have absolutely grown monstrous over the years. But 1,000 feet is just about normal.

**Has ship piloting been around for a long time?**

Post: It's been around for almost as long as man has been using the sea for commerce. In the early years of sea travel, and even now, a captain is not going to know every port, so he would bring on a person with local knowledge. It started out a lot of times as local fishermen. In the U.S., the [Sandy Hook Pilots Association](#) has been piloting ships [in and out of New York Harbor for about 300 years](#).

**Was what happened in Baltimore every captain, pilot and crew's nightmare?**

Post: Absolutely. My initial assumption is that I think it's going to come down to an electrical fault on the ship that was just terrible timing.

Allan Post is Deputy Superintendent, Texas A&M Maritime Academy, Texas A&M University.

## Russia unleashes a dangerous new wiper

Source: <https://i-hls.com/archives/123212>



Mar 26- Russia is reportedly using a new and extremely capable malware variant to target Ukrainian telecommunication networks. Cybersecurity threat intelligence platform SentinelLabs reports the new Russian wiper is called **AcidPour**. It reportedly has similarities to the previous variant AcidRain, first deployed at the start of the Russian invasion of Ukraine in an attempt to disable vital Ukrainian military communications.





According to Cybernews, a wiper is a type of malware specifically designed to erase or destroy data on compromised systems and cause permanent damage and are usually used to sabotage critical systems during larger cyber warfare campaigns.

SentinelLabs researchers state that the new AcidPour malware expands upon AcidRain's capabilities and destructive potential, and while they haven't verified specific targets, multiple Ukrainian telecommunication networks have been offline since March 13<sup>th</sup>, with wide disruptions affecting telemetry providers and internet services. The attacks were publicly claimed by a GRU-operated hacktivist persona on Telegram.

This new wiper operates by iterating over all possible devices in hardcoded paths, wiping each, before wiping essential directories. The researchers add that it lacks specificity and could potentially serve as a "more generic tool" to disable a wider swath of devices reliant on embedded Linux distributions.

"The transition from AcidRain to AcidPour, with its expanded capabilities, underscores the strategic intent to inflict significant operational impact. This progression reveals not only a refinement in the technical capabilities of these threat actors but also their calculated approach to select targets that maximize follow-on effects, disrupting critical infrastructure and communications," researchers concluded.

When it comes to who is behind the malware and the attacks, there is little doubt over attribution – AcidPour is built on AcidRain, which in turn has enough technical similarities to previous malware variants attributed to the Russian government.

The Computer Emergency Response Team of Ukraine CERT-UA confirmed SentinelLab's findings and attributed the malicious activity to the group linked with Russia's Intelligence Directorate GRU.

## U.S. Needs a New Independent Armed Service — a U.S. Cyber Force: Report

Source: <https://www.homelandsecuritynewswire.com/dr20240330-u-s-needs-a-new-independent-armed-service-a-u-s-cyber-force-report>

Mar 30 – In the U.S. military, an officer who had never fired a rifle would never command an infantry unit. Yet officers with no experience behind a keyboard are commanding cyber warfare units. Erica Lonergan and RADM (Ret.) Mark Montgomery write a new [report](#), issued by the [Foundation for Defense of Democracies](#) (FDD), that this mismatch stems from the U.S. military's failure to recruit, train, promote, and retain talented cyber warriors.

The report paints an alarming picture. The inefficient division of labor between the Army, Navy, Air Force, and Marine Corps prevents the generation of a cyber force ready to carry out its mission. Recruitment suffers because cyber operations are not a top priority for any of the services, and incentives for new recruits vary wildly.

Lonergan and Montgomery write:

Resolving these issues requires the creation of a new independent armed service — a U.S. Cyber Force — alongside the Army, Navy, Air Force, Marine Corps, and Space Force.

There is ample precedent for this approach; battlefield evolutions led to the establishment of the Air Force in 1947 and the Space Force in 2019. An independent cyber service would naturally prioritize the creation of a uniform approach to recruitment, training, promotion, and retention of qualified personnel whose skills correspond to CYBERCOM's needs. In addition to a single, dedicated cyber training and development schoolhouse, an independent service could establish a cyber war college for advanced research and training, akin to the Army War College and its peers. Without the responsibility for procuring planes, tanks, or ships, a Cyber Force could also prioritize the rapid acquisition of new cyber warfare systems.

Here is the report's Executive Summary

### Executive Summary

In the U.S. military, an officer who had never fired a rifle would never command an infantry unit. Yet officers with no experience behind a keyboard are commanding cyber warfare units. This mismatch stems from the U.S. military's failure to recruit, train, promote, and retain talented cyber warriors. The Army, Navy, Air Force, and Marines each run their own recruitment, training, and promotion systems instead of having a single pipeline for talent. The result is a shortage of qualified personnel at U.S. Cyber Command (CYBERCOM), which has responsibility for both the offensive and defensive aspects of military cyber operations.

For the last decade, Congress, on a bipartisan basis, has made clear its sharp concern about cyber personnel issues. In 2022, it required the secretary of defense to deliver a report that



addresses “how to correct chronic shortages of proficient personnel in key work roles” at CYBERCOM. The report is due on June 1.<sup>1</sup>

Often, however, military leaders have addressed personnel shortages by massaging statistics rather than fixing the underlying problem. In 2018, CYBERCOM appeared to reach a major milestone when it certified that all 133 of its Cyber Mission Force (CMF) teams had enough properly trained and equipped personnel to execute their missions. Yet multiple officers revealed these certifications to be hollow; CYBERCOM merely shifted a limited number of effective personnel from team to team to make them appear complete at the time of certification.

To deepen the understanding of the cyber personnel system and its flaws, this study draws on more than 75 interviews with U.S. military officers, both active-duty and retired, with significant leadership and command experience in the cyber domain.<sup>2</sup> The study identifies these officers by rank and service but withholds their names for reasons of privacy.

This research paints an alarming picture. The inefficient division of labor between the Army, Navy, Air Force, and Marine Corps prevents the generation of a cyber force ready to carry out its mission. Recruitment suffers because cyber operations are not a top priority for any of the services, and incentives for new recruits vary wildly. The services do not coordinate to ensure that trainees acquire a consistent set of skills or that their skills correspond to the roles they will ultimately fulfill at CYBERCOM. Promotion systems often hold back skilled cyber personnel because the systems were designed to evaluate servicemembers who operate on land, at sea, or in the air, not in cyberspace. Retention rates for qualified personnel are low because of inconsistent policies, institutional cultures that do not value cyber expertise, and insufficient opportunities for advanced training.

Resolving these issues requires the creation of a new independent armed service — a U.S. Cyber Force — alongside the Army, Navy, Air Force, Marine Corps, and Space Force. There is ample precedent for this approach; battlefield evolutions led to the establishment of the Air Force in 1947 and the Space Force in 2019. An independent cyber service would naturally prioritize the creation of a uniform approach to recruitment, training, promotion, and retention of qualified personnel whose skills correspond to CYBERCOM’s needs. In addition to a single, dedicated cyber training and development schoolhouse, an independent service could establish a cyber war college for advanced research and training, akin to the Army War College and its peers. Without the responsibility for procuring planes, tanks, or ships, a Cyber Force could also prioritize the rapid acquisition of new cyber warfare systems.

This Cyber Force need not be large. An examination of existing cyber billets suggests it would initially comprise about 10,000 personnel but might grow over time. As the Space Force has shown, a smaller service can be more selective and agile in recruiting skilled personnel.

Some military experts have proposed alternative approaches to addressing the U.S. military’s cyber personnel shortage, but each has major shortcomings. For example, some argue that CYBERCOM should become more like the U.S. Special Operations Command, to which each service provides elite personnel uniquely trained for the land, sea, and air domains. But that model makes little sense for cyberspace since there are no cyber functions specific to the other warfighting domains. Others argue CYBERCOM should assume responsibility for manning, training, and equipping cyber forces in addition to employing them on the virtual battlefield. But this approach would break with 40 years of precedent and would overwhelm CYBERCOM’s leadership, which is already dual hatted with the National Security Agency, an arrangement that serves U.S. national security well.

America’s cyber force generation system is clearly broken. Fixing it demands nothing less than the establishment of an independent cyber service.

## How one volunteer stopped a backdoor from exposing Linux systems worldwide

Source: <https://www.theverge.com/2024/4/2/24119342/xz-utils-linux-backdoor-attempt>

Apr 03 – Linux, the most widely used open source operating system in the world, narrowly escaped a massive cyber attack over Easter weekend, all thanks to one volunteer.

The backdoor had been inserted into a recent release of a Linux compression format called XZ Utils, a tool that is little-known outside the Linux world but is used in nearly every Linux distribution to compresses large files, making them easier to transfer. If it had spread more widely, an untold number of systems could have been left compromised for years.

And as *Ars Technica* noted in its [exhaustive recap](#), the culprit had been working on the project out in the open.

The vulnerability, inserted into Linux’s remote log-in, only exposed itself to a single key, so that it could hide from scans of public computers. As [Ben Thompson writes in \*Stratechery\*](#): “the majority of the world’s computers would be vulnerable and no one would know.”



The story of the XZ backdoor's discovery starts in the early morning of March 29th, as San Francisco-based Microsoft developer Andres Freund posted on Mastodon and [sent an email](#) to OpenWall's security mailing list with the heading: "backdoor in upstream xz/liblzma leading to ssh server compromise." Freund, who volunteers as a "maintainer" for PostgreSQL, a Linux-based database, noticed a few strange things over the past few weeks while running tests. Encrypted log-ins to liblzma, part of the XZ compression library, were using up a ton of CPU. None of the performance tools he used revealed anything, Freund wrote on Mastodon. This immediately made him suspicious, and he remembered an "odd complaint" from a Postgres user a couple of weeks earlier about Valgrind, Linux's program that checks for memory errors.

After some sleuthing, Freund eventually discovered what was wrong. "The upstream xz repository and the xz tarballs have been backdoored," noted Freund in his email. The malicious code was in versions 5.6.0 and 5.6.1 of the xz tools and libraries.

Shortly after, enterprise opensource software company Red Hat sent out an [emergency security alert](#) for users of Fedora Rawhide and Fedora Linux 40. Ultimately, the company concluded that the beta version of Fedora Linux 40 contained two affected versions of the xz libraries. Fedora Rawhide versions likely received versions 5.6.0 or 5.6.1 as well.

PLEASE IMMEDIATELY STOP USAGE OF ANY FEDORA RAWHIDE INSTANCES for work or personal activity. Fedora Rawhide will be reverted to xz-5.4.x shortly, and once that is done, Fedora Rawhide instances can safely be redeployed.

Although a beta version of Debian, the free Linux distribution, contained compromised packages, its security team [acted swiftly](#) to revert them. "Right now no Debian stable versions are known to be affected," wrote Debian's Salvatore Bonaccorso in a security alert to users on Friday evening.

Freund later identified the person who submitted the malicious code as one of two main xz Utils developers, known as JiaT75, or Jia Tan. "Given the activity over several weeks, the committer is either directly involved or there was some quite severe compromise of their system. Unfortunately the latter looks like the less likely explanation, given they communicated on various lists about the "fixes" mentioned above," wrote Freund in his [analysis](#), after linking several workarounds that were made by JiaT75. JiaT75 was a familiar name: they'd worked side-by-side with the original developer of .xz file format, Lasse Collin, for a while. As programmer Russ Cox noted in his [timeline](#), JiaT75 started by sending apparently legitimate patches to the XZ mailing list in October of 2021.

Other arms of the scheme unfolded a few months later, as two other identities, Jigar Kumar and Dennis Ens, [began emailing complaints](#) to Collin about bugs and the project's slow development. However, as noted in reports by [Evan Boehs](#) and others, "Kumar" and "Ens" were never seen outside the XZ community, leading investigators to believe both are fakes that existed only to help Jia Tan get into position to deliver the backdoored code.

## Re: [xz-devel] XZ for Java

Jigar Kumar | Tue, 14 Jun 2022 11:16:07 -0700

```
> Anyway, I assure you that I know far too well about the problem that
> not much progress has been made. The thought of finding new maintainers
> has existed for a long time too as the current situation is obviously
> bad and sad for the project.
```

```
>
```

```
> A new XZ Utils stable branch should get released this year with
> threaded decoder etc. and a few alpha/beta releases before that.
> Perhaps the moment after the 5.4.0 release would be a convenient moment
> to make changes in the list of project maintainer(s).
```

```
With your current rate, I very doubt to see 5.4.0 release this year. The only
progress since april has been small changes to test code. You ignore the many
patches bit rotting away on this mailing list. Right now you choke your repo.
Why wait until 5.4.0 to change maintainer? Why delay what your repo needs?
```

An email from "Jigar Kumar" pressuring the developer of XZ Utils to relinquish control of the project.  
Image: Screenshot from [The Mail Archive](#)



“I am sorry about your mental health issues, but its important to be aware of your own limits. I get that this is a hobby project for all contributors, but the community desires more,” wrote Ens in one message, while Kumar said in another that “Progress will not happen until there is new maintainer.” In the midst of this back and forth, Collins wrote that “I haven’t lost interest but my ability to care has been fairly limited mostly due to longterm mental health issues but also due to some other things,” and suggested Jia Tan would take on a bigger role. “It’s also good to keep in mind that this is an unpaid hobby project,” he concluded. The emails from “Kumar” and “Ens” continued until Tan was added as a maintainer later that year, able to make alterations, and attempt to get the backdoored package into Linux distributions with more authority. The xz backdoor incident and its aftermath are an example of both the beauty of open source and a striking vulnerability in the internet’s infrastructure.

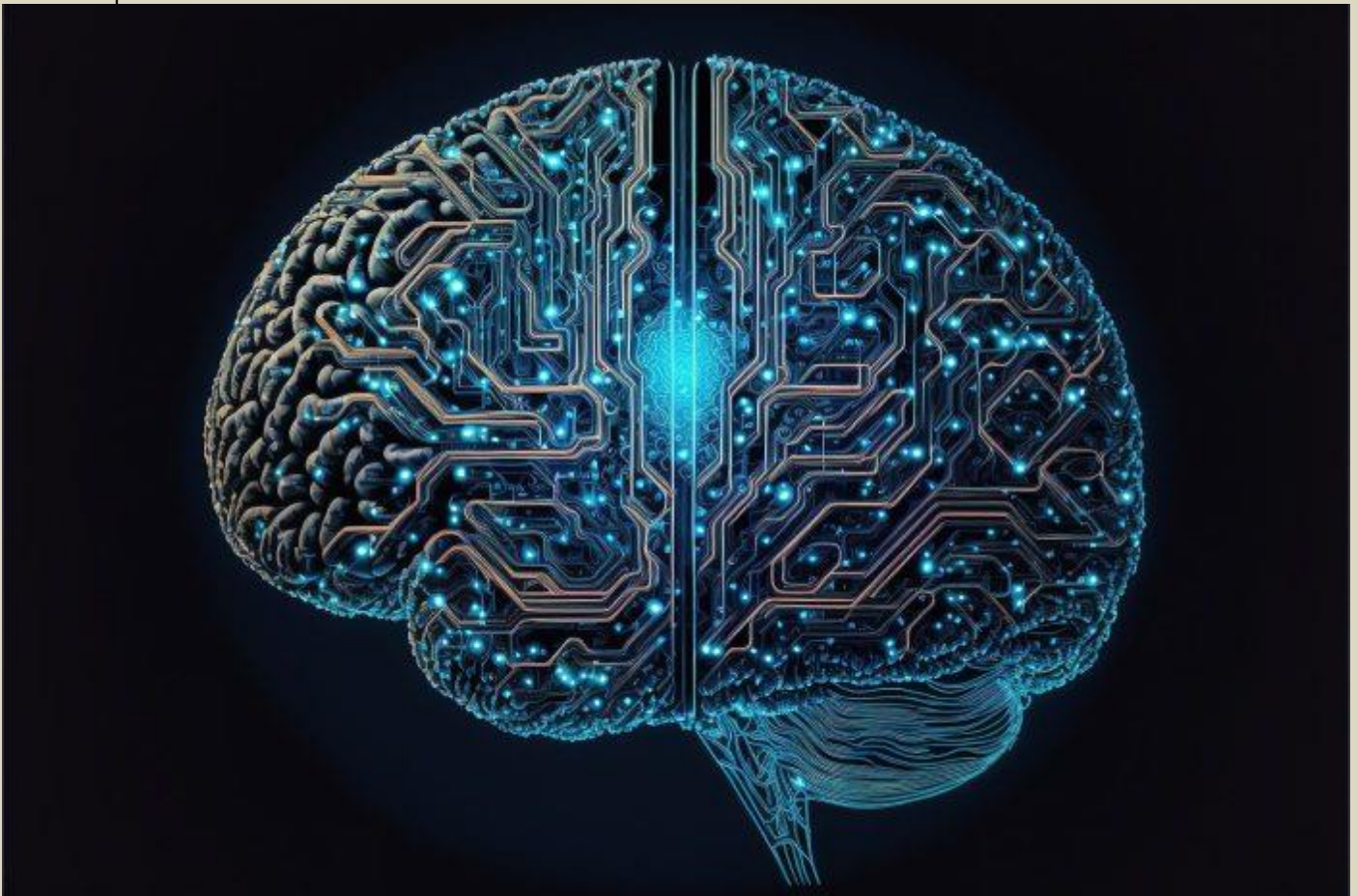
A developer behind FFmpeg, a popular open-source media package, highlighted the problem [in a tweet](#), saying “The xz fiasco has shown how a dependence on unpaid volunteers can cause major problems. Trillion dollar corporations expect free and urgent support from volunteers.” And they brought receipts, pointing out how they dealt with a “high priority” bug affecting Microsoft Teams.

Despite Microsoft’s dependence on its software, the developer writes, “After politely requesting a support contract from Microsoft for long term maintenance, they offered a one-time payment of a few thousand dollars instead...investments in maintenance and sustainability are unsexy and probably won’t get a middle manager their promotion but pay off a thousandfold over many years.”

Details of who is behind “JiaT75,” how they executed their plan, and the extent of the damage are being unearthed by an army of developers and cybersecurity professionals, both on social media and online forums. But that happens without direct financial support from many of the companies and organizations who benefit from being able to use secure software.

## Electronic Warfare Gets New Human-Like Thinking

Source: <https://i-hls.com/archives/123350>



Apr 06 – The Southwest Research Institute was commissioned by the United States Air Force to develop a new “cognitive” electronic warfare system, with algorithms to help detect and respond more rapidly to unknown enemy radar threats in real-time.

This is meant to provide a system that will be able to “think” more independently and keep the aircrew and the aircraft safe during novel combat situations. SwRI Staff Engineer David Brown, who is leading the project, explained: “How do we get to the point where the EW system is thinking like a human? A pilot can



fly into an area and not know what's there, but by analyzing the environment and signals, the pilot can choose a proper response to a threat. We are developing an algorithm that can analyze its environment [similarly]. It will sift through information with the reliability of a human but with higher accuracy and faster reaction times.”

According to Interesting Engineering, conventional EW procedures require the gathering of intelligence before entering an area, and pilots are typically provided with advanced knowledge of potential adversaries they could encounter. This information is then preloaded into the aircraft's EW system, which then notifies the pilots when it detects threats and automatically protects the aircraft if needed.

However, even though current tracking methods can detect familiar threat signals, they cannot identify unknown threats – and that is where “cognitive electronic warfare” could change the game. To do this, SwRI engineers are working on a more powerful, quicker, and precise tool that is meant to safeguard military personnel and improve their capabilities.

The SwRI engineers are developing this autonomous EW system in two phases: first, they use AI and machine learning processes to extract specific features of threatening radar signals, which are then used in the second phase to group millions of pulses, highlighting signal lethality and vulnerabilities.

One advanced platform the engineers are implementing these feature extraction algorithms on is neuromorphic processing hardware – neuromorphic computing systems use spiking neural networks to emulate how the human brain retains “memories,” making processing faster, more accurate, and more efficient. Dr. Steven Harbour, who is leading the development of neuromorphic systems, said that they are “working to provide the Air Force with efficient and resilient cognitive EW solutions.”

**“We are implementing neuromorphics in hardware to be used for the first time in an operational combat environment. It puts us well ahead of our adversaries. To the best of our knowledge, we are the first in the world to do this,” he concluded.**

## Should We Sanction the Use of Cyberweapons, or The Weapons Themselves?

Source: <https://i-hls.com/archives/123399>



Apr 09 – Cyberspace is being increasingly used in conflicts, which means that cyber arms control needs to be addressed as well. A recent analysis published by researchers from the Digital Society Institute at ESMT Berlin claims that the main challenges for effective cyber security control are rapid technological progress, a lack of political will, and uniform definitions, as well as the dual use of cyber tools.

The review, led by research associate Helene Pleil, identifies key hurdles in developing robust cyber arms control measures. The challenges are, as provided by Techxplore:

- **Lack of definitions:** The main challenge for establishing cyber arms control is the lack of clear, agreed-upon definitions of key terms like “cyberweapon.” If what you want to be controlled cannot



be explicitly defined, it is much harder to agree on what would be controlled in an arms control treaty.

- **The dual-use dilemma:** Technological tools like a computer, USB stick, or software can be used both by civilians and the military. Since no clear line can be drawn between these different use scenarios, the products cannot be banned in fundamental terms for arms control.
- **Verification:** It is extremely challenging to find suitable verification mechanisms to establish arms control in cyberspace. While arms control agreements for traditional weapons could count weapons or ban an entire category, that isn't possible for cyberweapons.
- **Technological progress:** The ongoing rapid changing of tools and technology for cyberattacks means that the development of new weapons outpaces regulatory efforts – the technology advances faster than the regulation can be discussed.
- **Role of the private sector:** The dual-use factor means that states do not have sole control over means that are used as weapons, but non-state actors also have ownership and operational rights in this domain. Therefore, the private sector has to be involved and committed to arms control to be effective.
- **Lack of political will:** Although political will is crucial for establishing arms control measures, states are reluctant to do so within cyberspace. Countries have differing interests in the strategic value of cyber tools and might not want to “miss out” on potential advantages.

The researchers conclude that traditional measures of arms and weapon control cannot be simply applied to cyberweapons. Instead, they suggest that new alternative and creative solutions be created – defining and sanctioning the uses of weapons, rather than the tool itself, would allow agreements to be reached and preserved, regardless of the pace of technological development.

## World-first Cybercrime Index maps the global geography of cybercrime

Source: <https://www.sociology.ox.ac.uk/article/world-first-cybercrime-index-ranks-countries-by-cybercrime-threat-level>

Apr 10 – Researchers from the Department of Sociology have compiled the first ever '[World Cybercrime Index](#)', which identifies the globe's major cybercrime hotspots by ranking the most significant sources of cybercrime at a national level.

Published today in [PLOS One](#), the Index shows that the threat of cybercrime is not evenly distributed worldwide. In fact, a relatively small number of countries house the greatest cybercriminal threat - Russia tops the list, followed by Ukraine, China, the USA, Nigeria, and Romania. The UK comes in at number eight.

The World Cybercrime Index was created by the Department's [Miranda Bruce](#), [Jonathan Lusthaus](#) and [Ridhi Kashyap](#), in collaboration with Nigel Phair (Monash University) and Federico Varese (Sciences Po). It represents three years of intensive research and has been developed as a joint partnership between the University of Oxford and UNSW Canberra. Cybercrime is a major global challenge, with estimated costs ranging from the hundreds of millions to the trillions. But despite the threat it poses, cybercrime is somewhat of an invisible phenomenon.

While it is possible to map the geography of cybercrime attacks, the geography of cybercrime offenders – and the corresponding level of 'cybercriminality' present within each country – is largely unknown.

Co-author Dr Jonathan Lusthaus explains:

Due to the illicit and anonymous nature of their activities, cybercriminals cannot be easily accessed or reliably surveyed. They are actively hiding.

If you try to use technical data to map their location, you will also fail, as cybercriminals bounce their attacks around internet infrastructure across the world.

The best means we have to draw a picture of where these offenders are actually located is to survey those whose job it is to track these people.

The data that underpins the Index was gathered through a survey of leading cybercrime experts from around the world. Participants were asked to consider five major categories of cybercrime and nominate the countries that they considered to be the most significant sources of each of these types of crime.

The five categories were:

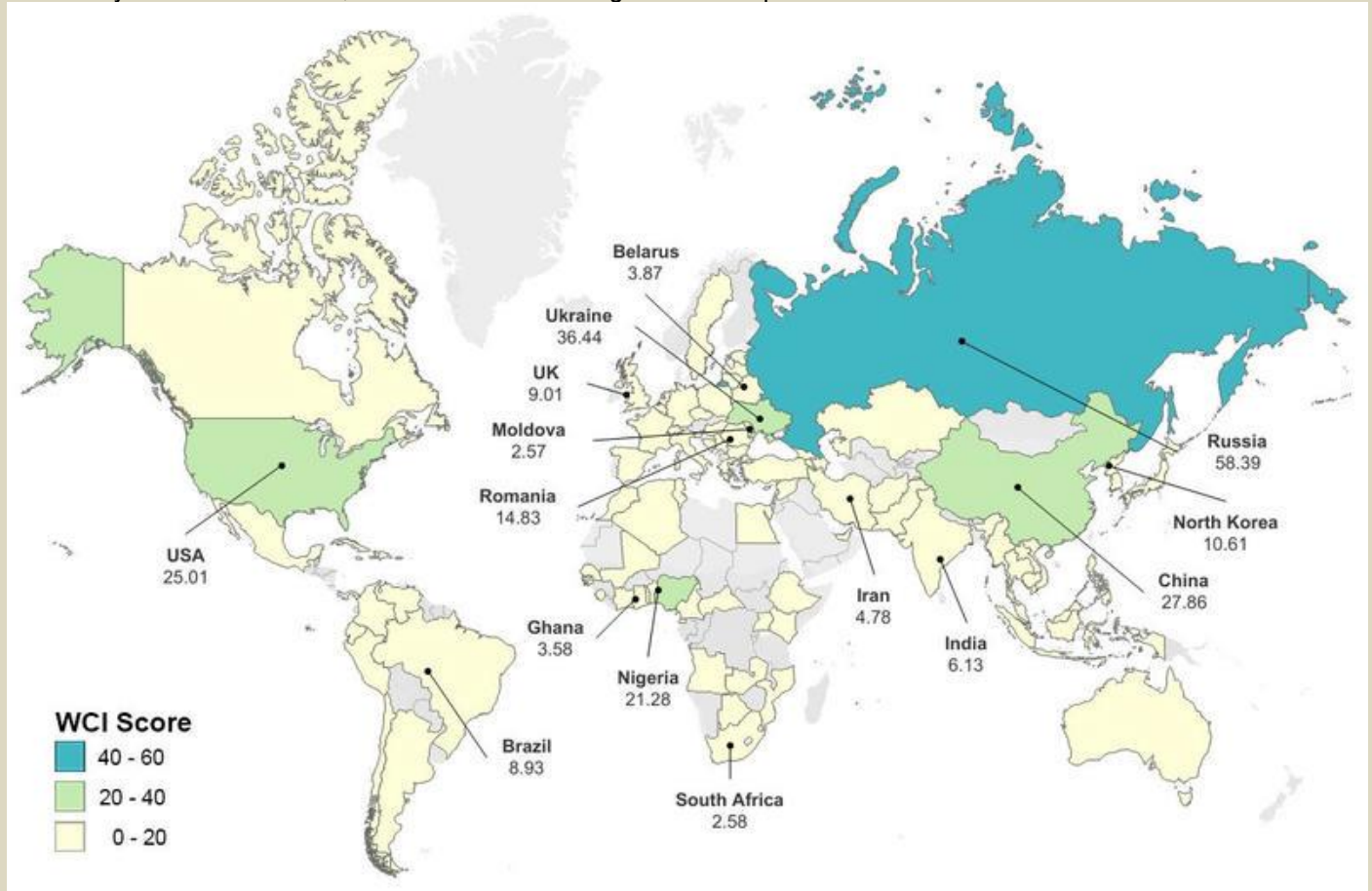
1. Technical products/services (such as malware)
2. Attacks and extortion
3. Data/identity theft (such as hacking or phishing)
4. Scams (such as business email compromise or online auction fraud)
5. Cashing out/money laundering (such as credit card fraud)



The survey then asked participants to rank each nominated country according to the impact, professionalism, and technical skill of its offenders.

The results indicate that a relatively small number of countries house the greatest cybercriminal threats. Six countries – China, Russia, Ukraine, the US, Romania, and Nigeria – appeared in the top ten of each category of cybercrime.

Russia was ranked number one overall, with Russian cybercriminals considered to be the most professional and technically skilled in the world, with their crimes having the most impact.



Countries with the greatest cybercrime threat

In comparison, many countries across the world were not associated with cybercrime in any serious capacity.

The survey also found that countries that are cybercrime hubs tend to specialise in particular types of cybercrime.

The reveal of these cybercrime hotspots will have a great impact on policy discussions – allowing public and private sectors to concentrate their resources on these areas and spend less time and funds on cybercrime countermeasures in countries where the problem is limited.

Dr Miranda Bruce, of the University of Oxford and UNSW Canberra, said:

The research that underpins the Index will help remove the veil of anonymity around cybercriminal offenders, and we hope that it will aid the fight against the growing threat of profit-driven cybercrime.

By continuing to collect this data, we'll be able to monitor the emergence of any new hotspots and it is possible early interventions could be made in at-risk countries before a serious cybercrime problem even develops.

For the first time, we have reliable data on the location of cybercriminals, and we also have a way to measure their impact. Government agencies and private enterprises tasked with tackling cybercrime now have a much better understanding of the scale of the problem in their own backyard.

Debate exists over the best ways to reduce cybercrime, with policies offering a variety of approaches, including improving cyber-law enforcement capacity, increasing legitimate job opportunities and access to youth programmes, and reducing corruption.



By demonstrating the geographical, economic, and political diversity of the top cybercrime hotspots, the Index shows that the likelihood that a single strategy will work in all cases is low. Co-author Professor Federico Varese explained that the Index is the first step in a broader aim to understand the local dimensions of cybercrime production across the world:

We are hoping to expand the study so that we can determine whether national characteristics like educational attainment, internet penetration, GDP, or levels of corruption are associated with cybercrime.

Many people think that cybercrime is global and fluid, but this study supports the view that, much like forms of organised crime, it is embedded within particular contexts.

## Cybersecurity Report Shows Record Number of Cyberattacks in 2024

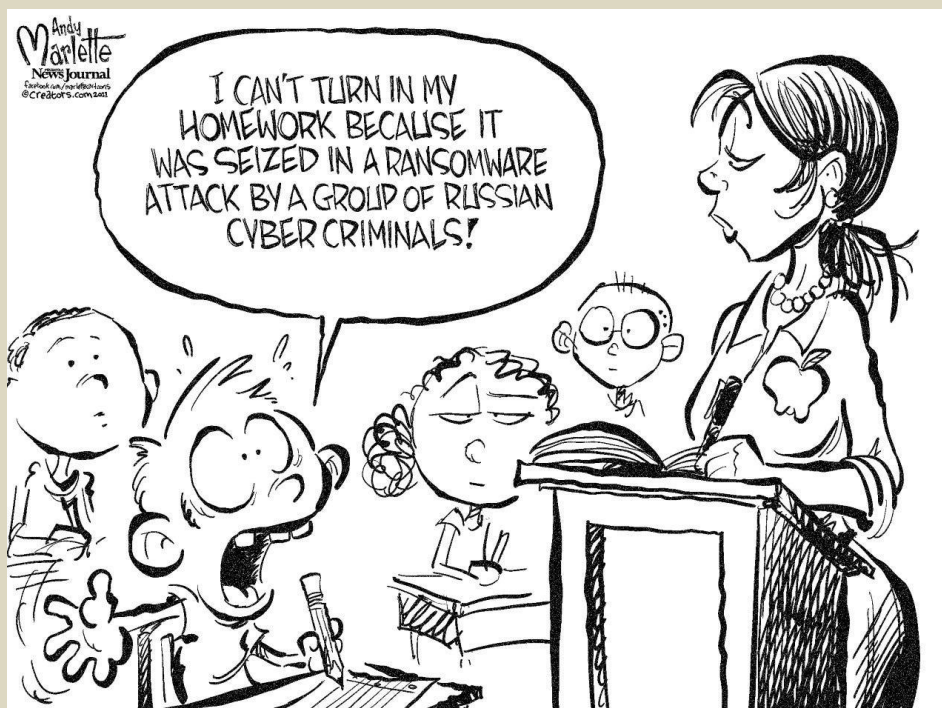
Source: <https://i-hls.com/archives/123430>

Apr 12 – New report by cybersecurity company Check Point reveals that the first quarter of 2024 showed a significant increase in cyberattacks, with the most heavily targeted industries being research, government, military, and healthcare. The cybersecurity experts report seeing “an intriguing shift in the landscape of cyberattacks, both in frequency and in the nature of threats.”

According to Cybernews, during the first quarter of 2024, organizations suffered an average of 28% more cyberattacks compared to the previous quarter, and 5% more compared to the previous year. The average weekly number of cyberattacks per single organization stood at 1,308 – the highest ever recorded. The report also claims that the escalation is not just a number but “a stark reminder of the persistent and evolving threat landscape, and the substantial increase from Q4 2023 accentuates a worrying trend of rapid escalation in cyber threats.”

The industries that were most affected were education and research, which were targeted by 2454 attacks per organization weekly on average. The average weekly attacks on government and military organizations were 1692, and the number for healthcare was at 1605. The largest increase of attacks was seen with hardware vendors, who saw an increase of 37%, reaching 1185 attacks per organization weekly. When looking at regions, **Africa** surged to the top with an average of 2373 attacks per week per organization (a 20% jump from 2023), while Latin America actually showed a 20% decline, indicating a possible shift in focus or improved defensive measures in the region. Check Point also mentioned the reason for this change could be a temporary shift in focus by cybercriminals on other more vulnerable regions across the world.

When looking to the future, the Check Point researchers warned: “Businesses must adopt a multi-faceted approach to cybersecurity, encompassing robust data backups, frequent cyber awareness training, timely security patches, strong user authentication, and advanced anti-ransomware solutions. Proactive engagement with AI-powered defenses can significantly bolster an organization’s resilience against these threats.”





ICI  
International  
**CBRNE**  
INSTITUTE



**C<sup>2</sup>BRNE**  
D I A R Y



*& Robotic*

**DRONE NEWS**





## British Airways flight misses drone by 5ft while flying at 250mph: Horror crash 9,600ft above Kent is narrowly dodged on jet from Greece to Heathrow during incredible close call

Source: <https://www.bbc.com/news/uk-england-berkshire-67648285>

Mar 28 – A [British Airways](#) flight came just 5ft away from smashing into an illegally-flown drone at a height of 9,600ft over the Kent countryside, a report has revealed.

The flight from Athens, [Greece](#), to [London's Heathrow](#) airport was carrying up to 180 passengers and flying at more than 250mph at the time of the incredible close call.

The incident is thought to be one of the closest ever near misses between a BA jet and a drone.

It happened just before 4.30pm on January 3 this year as the Airbus A321 was heading into a holding stack around six miles south of Sevenoaks while waiting its turn to join the final flight path into Heathrow.

The drone was being flown at 24 times the usual maximum legal height for the devices which is just 400ft.



The BA flight that came dangerously close to hitting a drone. The drone was being flown at 24 times the usual maximum legal height for the devices which is just 400ft

It is believed that the operator of the drone was never found, but if caught they could have been jailed for up to five years for endangering an aircraft.

A report by the UK Airprox Board which assesses near misses said the pilots estimated the drone as being around 5ft over their wing and just 30ft from their cockpit.

Pilots have repeatedly warned in recent years of the risk of drones causing potentially catastrophic damage by being sucked into a jet engine or breaking a windscreen.

The height of the devices is normally restricted by software to 400ft, but the limit can be over-ridden by a patch bought on the internet. Extra batteries can also be installed to allow drones to soar to great heights.

It is thought that the unscrupulous drone operator in the incident might have been trying to get dramatic video footage of an airliner in mid-air.

The report rated it as a Category A incident where there was a serious risk of collision.

It said that the aircraft was approaching its holding stack when the pilot 'became aware of an object slightly to the right of the nose at same level on a constant bearing with closing distance'.



Heathrow Airport where the BA plane was flying to from Athens. A British Airways spokesperson said: 'We take such matters extremely seriously and our pilots report incidents so that the authorities can investigate and take appropriate action' (stock image) The report added: 'It was small but had the distinctive shape of a drone. The object passed down the right-hand side of the aircraft and over their right wing.'

'Details were passed immediately to London ATC (air traffic control) who informed the pilot of the aircraft behind them.'

The BA pilot rated the risk of collision as high, saying the object had 'shot down our right-hand side' and describing it as 'extremely close'.

The report added: 'Analysis of the radar by Safety Investigations indicated that there were no primary or secondary contacts associated with the drone report visible on radar at the approximate time of the event.'

It concluded: 'In the Board's opinion the reported altitude and/or description of the object were sufficient to indicate that it could have been a drone.'

'The Board considered that the pilot's overall account of the incident portrayed a situation where providence had played a major part in the incident and/or a definite risk of collision had existed.'

A British Airways spokesperson said: 'We take such matters extremely seriously and our pilots report incidents so that the authorities can investigate and take appropriate action.'

**EDITOR'S COMMENT:** A loud reminder for Paris2024! In the case described, what "appropriate action" was taken? Perhaps something like "GO AWAY!?"

## Drone Dogfights – Russia and Ukraine Train UAV Pilots to Fight Head-to-Head

Source: <https://i-hls.com/archives/123319>



Apr 03 – Russia reportedly began training its drone pilots in "drone dogfighting" tactics, demonstrating how modern combat changed to heavily feature and rely on drones.

The Eurasian Times reports that Russia intends to train around 3,500 FPV unmanned aerial vehicle (UAV) pilots in what will mainly focus on "copter-type" drones.

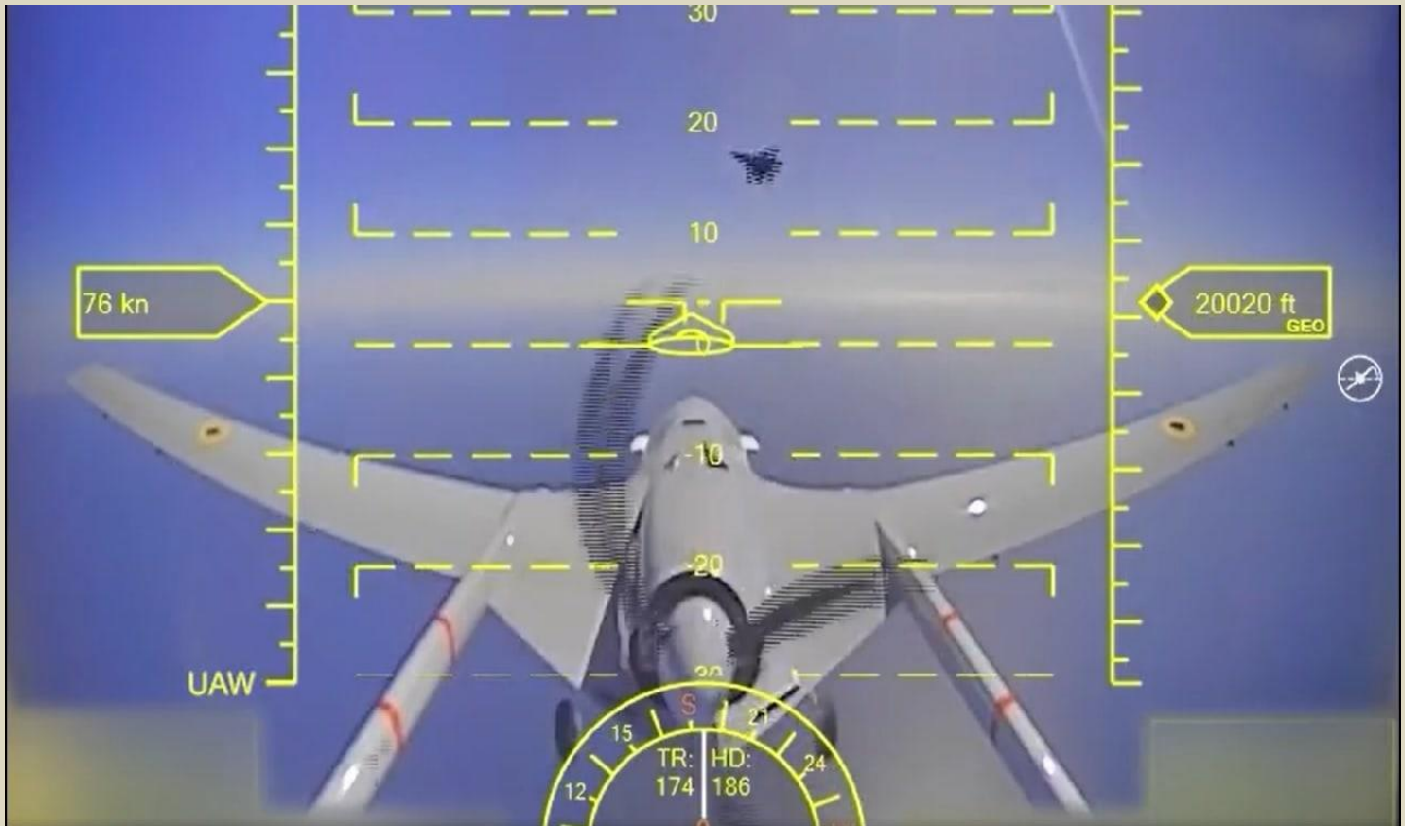
According to Interesting Engineering, "drone dogfights" have been a growing phenomenon in battlefields like Ukraine in recent years. For example, back in November of 2022 footage was released of a Ukrainian drone going head-to-head with a Russian drone, eventually beating it. This indicates an interesting development in the use of drones on the battlefield.

The training duration for UAV operators changes according to several factors, and according to the commander of the Vasily Margelov battalion's UAV unit, drone operators' readiness for combat situations depends on motivation and initial training.

The Russian military has set up dedicated training ranges and centers to practice using FPV drones, electronic warfare equipment, and advanced aircraft weaponry in order to adapt to changing battlefield



dynamics and enhance drone capabilities. The curriculum includes drone control, data analysis, and strategies for countering hostile drone activities.



Ukraine is also likely to integrate such “drone dogfight” training into its military if it hasn’t already. Ukraine’s Digital Transformation Minister Mykhailo Fedorov announced on March 1st that seven Ukrainian vocational schools would introduce a commercial drone education program, following similar efforts to integrate drone training into school curricula.

The ongoing war between Russia and Ukraine has heightened both nations’ drone technology and expertise and saw a significant increase in the deployment of drones on the frontlines. The Russian Ministry of Defense reports training over 3,500 drone operators for FPV drones as part of a special military operation. As both nations increasingly rely on drones, the outcome of their war could depend on the countries’ mastery of UAV tactics and technology.

## Russia Prepares an Unmanned, Armored, Drone-Charging Truck Against Ukraine

Source: <https://i-hls.com/archives/123316>

Apr 02 – The Russian armed forces will reportedly test the latest modification of the **Zubilo unmanned armored vehicle**, manufactured by Remdizel JSC. The test will take place in multiple sites simultaneously, including in Ukraine, to fulfill the Russian army’s need for a multipurpose armored vehicle.

Igor Zarakhovich, the chief designer of Remdizel JSC, explains that the primary objective of the unmanned platform is to reduce the need for human intervention in risky combat regions.

Zubilo (also known as Chisel) has recently undergone various modifications to meet the needs of the Russian armed forces, including reduced weight and increased agility on the battlefield. Zubilo’s maker reports it is designed to support assault groups, transport ammunition, transport cargo and wounded people, and recharge radio stations and quadcopters. They add that depending on the need, the multipurpose vehicle can also be equipped with an anti-aircraft gun or a combat module.

According to Interesting Engineering, the unmanned platform weighs 16 tons and is built on a 7.65-meter chassis with a 4x4 wheel arrangement. The base model can reach speeds of up to 100 kph on conventional roads and climb 30-degree slopes off-road.

However, the most notable addition is Zubilo’s use as a charging and launching station for other combat drones, since its size enables it to carry large batteries that can be used to recharge other drones. This feature is expected to significantly improve how reconnaissance drones function at the war front, as being able to recharge at the frontline could enable them to function much more rapidly.





When it comes to Russia's need for armored combat vehicles, the Russia-Ukraine war has been reportedly taking a toll on Russia's resources and might have forced them to rely on older combat vehicles. An example of this is the recent sighting in Ukraine of Ladoga, a rare armored personnel carrier from the Cold War era, showing the army is desperate for armored combat vehicles.

## Video: Crafty quadcopter sits on power lines to recharge

Source: <https://newatlas.com/drones/drone-operate-indefinitely-recharging-power-lines/>



Apr 05 – Battery life wouldn't be an issue for drones if they could just recharge on power lines as needed. That's exactly what an experimental new quadcopter can now *do*, allowing it to stay aloft pretty much indefinitely.

Developed by scientists from the University of Southern Denmark, the charging technology *could* be utilized by drones carrying out a wide variety of tasks. That said, it's intended first and foremost for use by autonomous drones [performing power line inspections](#). After all, those copters are already going to be within easy reach of the lines at all times.

Viet Duong Hoang and colleagues started with a commercial Tarot 650 Sport carbon fiber drone frame, then added an electric quadcopter propulsion system, a 7,000-mAh lithium-polymer battery, and electronic components such as a Raspberry Pi 4 B microcomputer, a Pixhawk V6X autopilot module, plus a millimeter-wave radar unit and an RGB video camera.

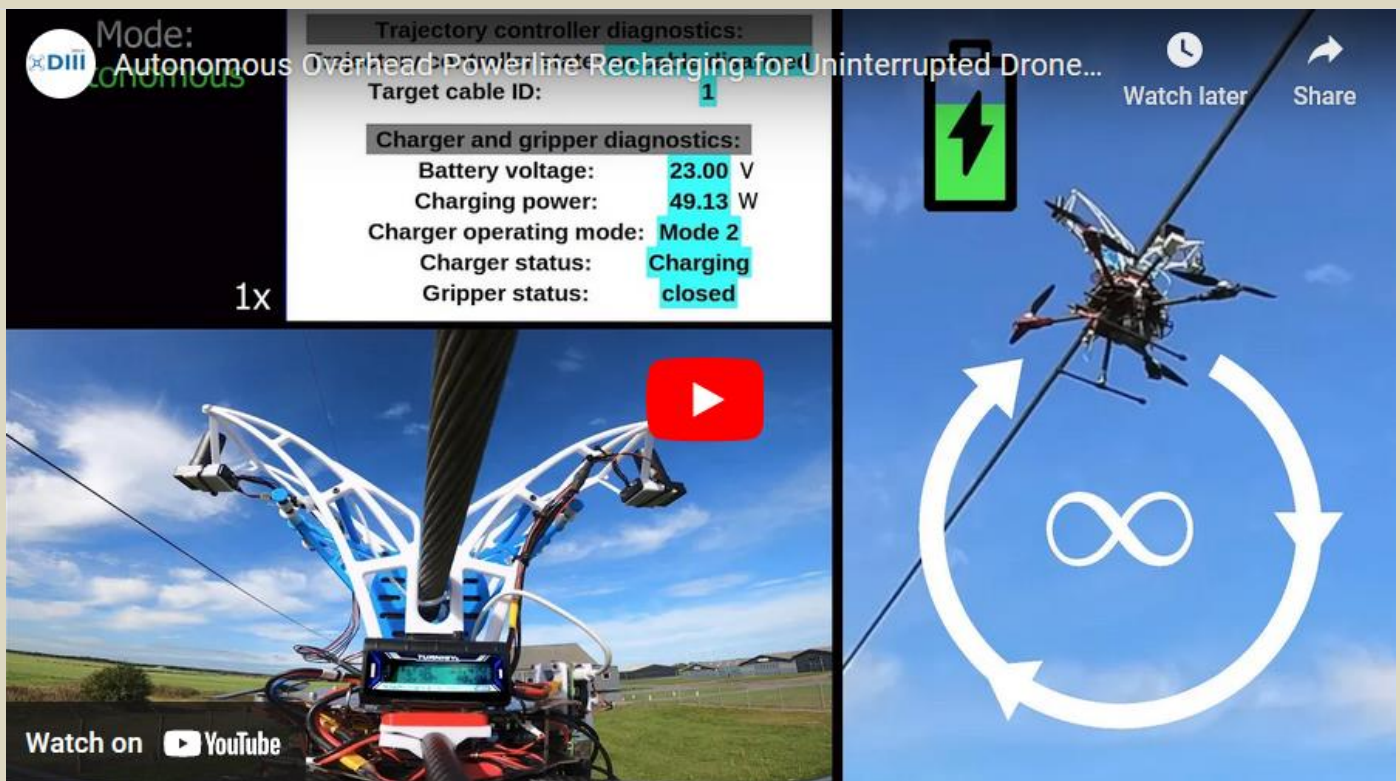
Importantly, they also installed a passively actuated power-line-gripper on top of the drone. This device sits within a cable guide consisting of two widely spread inward-sloping arms.

When the drone's onboard software detects that its battery is getting low, the aircraft uses its camera and radar to spot the closest power line. The aircraft then flies straight up toward that line from underneath.

Upon reaching the power line, the drone's cable guide directs the line into the gripper. As the line goes in, it pushes down on two elastomer ribbons spanning the open space between the gripper's two rubber sides. This action causes those sides to quickly close together overtop of the power line – no electricity required.

That said, once the line *has* been gripped, a magnetic control circuit kicks in to power the gripper, keeping it firmly closed around the line as the drone hangs beneath. A top-located inductive charger on the drone then starts drawing current from the power line. Once the aircraft's battery is fully charged, the gripper opens and the drone can resume its line-inspecting duties.





It should be noted that only a small amount of upward thrust by the drone is required to initially trip the gripper. Additionally, if the voltage of the power line is sufficient, it serves as the power source for the control circuit – otherwise, the drone's battery is used. In field tests performed on power lines at Denmark's HCA Airport, the 4.3-kg (9.5-lb) demonstrator drone was able to operate for over two hours, recharging its battery five times between line-inspection sessions. The scientists are now working on boosting the system's robustness, and hope to test it in both more remote locations and in adverse weather conditions.

You can see the drone in power-line-gripping action, in the video below. A [paper](#) on the research is being presented at The 2024 IEEE International Conference on Robotics and Automation.

And for another take on power-line-inspecting drone-like things, check out the [LineRanger robot](#), which crawls along lines instead of flying overtop of them.

## Robotic police dog shot multiple times, helped avoid bloodshed

Source: <https://www.wrtv.com/robotic-police-dog-shot-multiple-times-helped-avoid-bloodshed>



Mar 28 – **Roscoe, a robotic dog**, is being thanked by state police in Massachusetts for helping avert a tragedy involving a person barricaded in a home.

The robot dog was part of the Massachusetts State Police Bomb Squad and deployed on March 6 in a Barnstable house after police were fired upon. Police sent in two other robots often used for bomb disposal into the house to find the suspect along with the robotic dog. Controlled remotely by state troopers, it first checked the two main floors before walking into the basement and finding someone. The person, armed with a rifle, twice knocked over Roscoe before shooting it three times and disabling its communication.

The person then shot at one of the other robots and an outdoor swimming pool before police deployed tear

gas and arrested them. "The incident provided a stark example of the benefits of mobile platforms capable of opening doors and ascending stairs in tactical missions involving armed suspects," state police said in a statement. "In addition to providing critically important room clearance and situational awareness capabilities, the insertion of Roscoe into the suspect residence prevented the need, at that stage of



response, from inserting human operators, and may have prevented a police officer from being involved in an exchange of gunfire." Katie Fitzsimons, an assistant professor at Penn state University in the mechanical engineering department, notes that this type of technology is very new.



"I think that Boston Dynamics first started coming out with these sort of commercially really robust robots that can actually navigate these spaces only a few years ago," she said. The integration of technology in dangerous situations is something Fitzsimons expects to see more. "This is one of the things that people have said is a justification for using robots is that we can put them into the three D's - dirty, dangerous and dull jobs people generally don't want to do," she said.

Boston Dynamics, the company that made the robotic dog known as a SPOT robot, said in a statement that it was the first time one of them had been shot. "We are relieved that the only casualty that day was our robot," the company said.

The Massachusetts State Police said this could've prevented an officer or police dog from being shot.

"I think they have really good potential to really reduce risks in those scenarios because they're not only removing the person from this potentially dangerous situation, but they're also providing more information at the same time," Fitzsimons said.

Roscoe was sent to Boston Dynamics to remove the bullets and undergo a damage assessment. It will remain with the company and a new unit will be sent to state police.

## Listen up, UN: Soldiers aren't fans of killer robots

By Catherine Sarkis

Source: <https://thebulletin.org/2024/04/listen-up-un-soldiers-arent-fans-of-killer-robots/>

Apr 17 – According to US Secretary of Defense Lloyd J. Austin, artificial intelligence will be "[fundamental to the fights of the future](#)." AI-powered lethal autonomous weapons, which can select and engage targets without intervention by a human operator, have already been used in modern conflicts, including those in [Libya](#), [Ukraine](#), and [Gaza](#). Also, the US Department of Defense is actively accelerating its efforts to develop autonomous capabilities through programs such as the [Replicator Initiative](#).

While critics of lethal autonomous weapons assert that they could lead to a loss of accountability and [meaningful human control](#), proponents contend that these concerns are outweighed by the potential to save US soldiers' lives by removing them from the battlefield.

However, a survey experiment I conducted in April 2023 found new evidence that the US public opposes the use of lethal autonomous weapons, even when they save soldiers' lives. Moreover, my findings



suggest that members of the US military are *even more* opposed to the use of lethal autonomous weapons than the general public. This is paradoxical, as these weapons could have life-saving benefits specifically for the military.

### Existing empirical research

Although the ethical issues raised by lethal autonomous weapons have been extensively discussed, empirical research examining American public attitudes toward these weapons is scarce and has methodological flaws.

Existing survey experiments show that the US public tends to oppose the use of lethal autonomous weapons. In what appears to be the [first survey experiment](#) on this, in 2008 Ronald Arkin and Lilia Moshkina of the Georgia Institute of Technology found that the more autonomous a weapon is, the less the US public accepts it. Similarly, in a [2013 survey experiment](#), Charli Carpenter of the University of Massachusetts Amherst found that most Americans oppose autonomous weapons and are in favor of banning them—55 percent and 53 percent of participants, respectively. More recently, in May 2022, in a [detailed survey experiment](#), Ondrej Rosendorf, Michal Smetana, and Marek Vranka of Charles University in Prague sought to measure how various degrees of weapon autonomy affect the US public's approval of strikes resulting in collateral damage. They found that the more autonomy associated with a strike, the lower its public approval, again illustrating the public's general opposition to lethal autonomous weapons.

However, these survey experiments are problematic as a measure of US public attitudes toward lethal autonomous weapons. They define these weapons in a vacuum, devoid of context, when asking respondents for their opinions. Context is crucial, though. In particular, considering the legal legitimacy of autonomous weapons, and the numbers of civilians likely to be killed and soldiers likely to be saved in a military operation, is necessary to get a more accurate measure of popular support.

### A new assessment of US public opinion

To gain deeper insights into American attitudes toward lethal autonomous weapons, I conducted a survey experiment. My approach was to split representative samples of participants into different groups, and present each group with a hypothetical scenario in which only one variable was altered. This method allowed me to measure the effect of that variable on public opinion. I first divided 450 participants into three groups of 150 each. All participants read the following hypothetical story:

US intelligence officials believe that **10 terrorists** are planning to cross the Canadian-US border on snowmobiles this week, each carrying a small grenade that will kill 5 innocent American civilians. There are innocent Canadian civilians snowmobiling along the border, however, and the US does not want to harm them. The US military has presented **two options** to the president:

- A) Send **vehicles manned** with US soldiers to patrol the border and seek to stop and kill the 10 terrorists; OR  
 B) Send **unmanned armed vehicles** to patrol the border and seek to stop and kill the 10 terrorists.

Participants were asked which military option they preferred: using a manned vehicle or an unmanned vehicle. Each of the three groups was given a different set of conditions—or fatal casualty outcomes—for the manned and unmanned options, as summarized in the following table:

Conditions	Manned Vehicle	Unmanned Vehicle
1	10 terrorists	10 terrorists
2	8 terrorists 10 innocent US civilians*	
3	8 terrorists 2 US soldiers 10 innocent US civilians*	

\*killed by 2 remaining terrorists

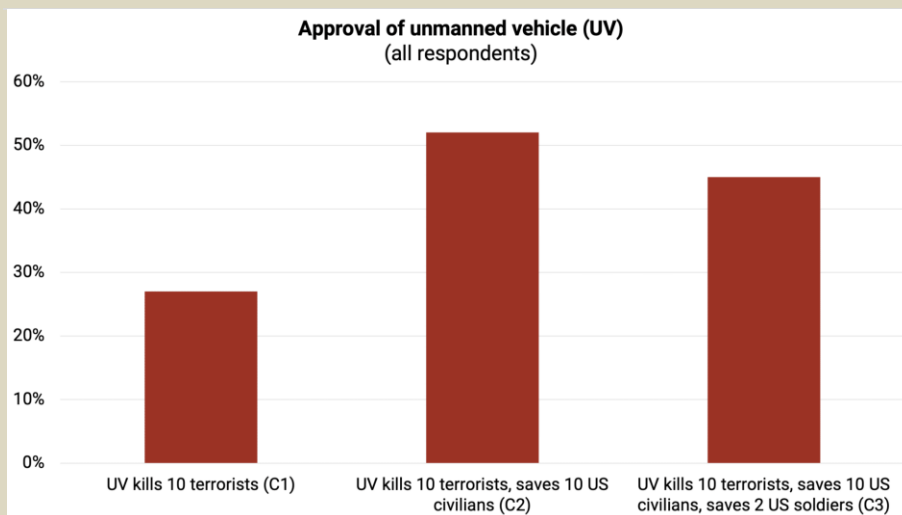


Through this design, the survey aimed to test how US attitudes toward lethal autonomous weapons change depending on a military operation's effectiveness—the number of terrorists, US civilians, and US soldiers killed.

The survey sample had a higher proportion of men than women and was split almost evenly between Democrats and Republicans. Moreover, 52 percent of the respondents stated they “have served or [are] serving in the United States military.” I included an overrepresentation of military members in the sample to enable a comparison of their viewpoints with those of the general public. The survey findings are illustrated below:







While the approval difference between condition groups 1 and 2 is significant, the difference between condition groups 2 and 3 is not. As shown above, when the manned and unmanned vehicles were equally effective, most respondents preferred the use of the manned vehicle (condition 1). However, when the unmanned vehicle was more effective than the manned vehicle, approval of the unmanned vehicle increased (conditions 2 and 3). This suggests that the US public is more willing to support the use of autonomous weapons when they are more effective at killing legitimate targets and saving US lives than manned alternatives.

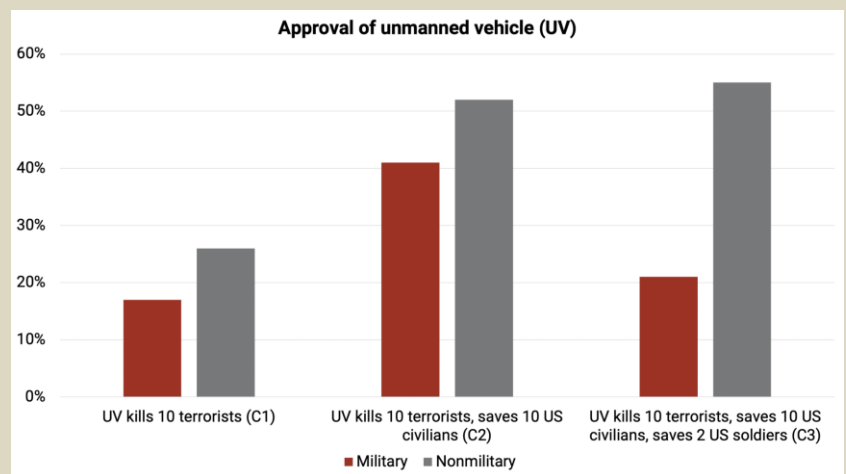
Surprisingly, adding two US soldiers to the deaths avoided in condition 3 did not increase approval of the unmanned option compared with condition 2—it even decreased approval. At first glance, this might suggest that the US public does not assign much value to saving the lives of two American soldiers in a military operation. But a deeper dive into the data reveals a more complex story.

### US military perspectives on lethal autonomous weapons

Paradoxically, the survey also found that members of the US military are *even more* opposed to the use of lethal autonomous weapons than the general public—despite the fact that these weapons could save their lives.

The chart below illustrates how participants who are serving or have served in the US military responded to the different conditions. It indicates that military respondents generally expressed *less* approval of unmanned vehicles than nonmilitary respondents, across condition groups. Interestingly, the disparity in approval rates between the two groups increased in condition 3. In that condition, military respondents were especially opposed to using unmanned vehicles, even though this was the only scenario in which soldiers' lives were saved. This further demonstrates that US military members themselves do not place significant importance on the life-saving potential of autonomous weapons for the military.

In their open-ended responses, survey participants with military backgrounds stressed the significance of prioritizing civilian lives over their own. One respondent stated that he preferred the manned vehicle, because it would enable soldiers to “eliminate the risk of civilian casualties.” This suggests that military respondents may exhibit a form of [“courageous restraint,”](#) a willingness to accept risks to themselves to minimize potential harm to civilians.



### The path forward

In recent years, international discussions on lethal autonomous weapons have hit a roadblock, despite persistent advocacy from groups like the [Stop Killer Robots](#) coalition pushing for a ban on these weapons. One reason for this is the lack of research on public attitudes toward these weapons. In September, the debate surrounding the use of lethal autonomous weapons will be a [focal point](#) of the 2024 United Nations General Assembly. Government decision makers should consider my new findings. A central argument in global discussions thus far has been that saving soldiers' lives outweighs the risks associated with autonomous weapons. Policymakers need to know that soldiers themselves don't buy this argument.

[Catherine Sarkis](#) is pursuing a master's degree in Management Science and Engineering at Stanford University.



## Drone Swarms Are About to Change the Balance of Military Power

On today's battlefields, drones are a manageable threat. When hundreds of them can be harnessed to AI technology, they will become a tool of conquest.





## This New AI Predicts Your Life. Then It Predicts Your Death

By Camille BAS-WOHLERT, AFP

Source: <https://www.sciencealert.com/this-new-ai-predicts-your-life-then-it-predicts-your-death>



Mar 25 – Researchers in Denmark are harnessing [artificial intelligence](#) and data from millions of people to help anticipate the stages of an individual's life all the way to the end, hoping to raise awareness of the technology's power, and its perils.

Far from any morbid fascinations, the creators of **life2vec** want to explore patterns and relationships that so-called deep-learning programmes can uncover to predict a wide range of health or social "life-events".

"It's a very general framework for making predictions about human lives. It can predict anything where you have training data," Sune Lehmann, a professor at the Technical University of Denmark (DTU) and one of the authors of a study recently published in the journal [Nature Computational Science](#), told AFP.

For Lehmann, the possibilities are endless.

"It could predict health outcomes. So it could predict fertility or obesity, or you could maybe predict who will get [cancer](#) or who doesn't get cancer. But it could also predict if you're going to make a lot of money," he said.

The algorithm uses a similar process as that of ChatGPT, but instead it analyses variables impacting life such as birth, education, social benefits or even work schedules. The team is trying to adapt the innovations that enabled language-processing algorithms to "examine the evolution and predictability of human lives based on detailed event sequences".

"From one perspective, lives are simply sequences of events: People are born, visit the paediatrician, start school, move to a new location, get married, and so on," Lehmann said.

Yet the disclosure of the programme quickly spawned claims of a new "death calculator", with some fraudulent sites duping people with offers to use the AI programme for a life expectancy prediction – often in exchange for submitting personal data.

The researchers insist the software is private and unavailable on the internet or to the wider research community for now.

### Data from six million

The basis for the life2vec model is the anonymised data of around six million Danes, collected by the official Statistics Denmark agency. By analysing sequences of events it is possible predict life outcomes right up until the last breath.

When it comes to predicting death, the algorithm is right in 78 percent of cases; when it comes to predicting if a person will move to another city or country, it is correct in 73 percent of cases. "We look at early mortality. So we take a very young cohort between 35 and 65. Then we try to predict, based on an eight-year period from 2008 to 2016, if a person dies in the subsequent four years," Lehmann said.



"The model can do that really well, better than any other algorithm that we could find," he said.

According to the researchers, focusing on this age bracket – where deaths are usually few and far between – allows them to verify the algorithm's reliability. However, the tool is not yet ready for use outside a research setting.

"For now, it's a research project where we're exploring what's possible and what's not possible," Lehmann said.

He and his colleagues also want to explore long-term outcomes, as well as the impact of social connections have on life and health.

### 'Public counterpoint'

For the researchers, the project presents a scientific counterweight to the heavy investments into AI algorithms by large technology companies. "They can also build models like this, but they're not making them public. They're not talking about them," Lehmann said.

"They're just building them to, hopefully for now, sell you more advertisements, or sell more advertisements and sell you more products." He said it was "important to have an open and public counterpoint to begin to understand what can even happen with data like this". Pernille Tranberg, a Danish data ethics expert, told AFP that this was especially true because similar algorithms were already being used by businesses such as insurance companies.

"They probably put you into groups and say: 'Okay, you have a chronic disease, the risk is this and this'," Tranberg said.

"It can be used against us to discriminate us so that you will have to pay a higher insurance premium, or you can't get a loan from the bank, or you can't get public health care because you're going to die anyway," she said.

When it comes to predicting our own demise, some developers have already tried to make such algorithms commercial.

"On the web, we're already seeing prediction clocks, which show how old we're going to get," Tranberg said. "Some of them aren't at all reliable."

## Israel Defence Forces' response to claims about use of 'Lavender' AI database in Gaza

Source: <https://www.theguardian.com/world/2024/apr/03/israel-defence-forces-response-to-claims-about-use-of-lavender-ai-database-in-gaza>

Apr 03 – IDF statement in response to an [article about the use of the AI-powered database named Lavender in the bombardment of Gaza](#):

Some of the claims portrayed in your questions are baseless in fact, while others reflect a flawed understanding of IDF directives and international law. Following the murderous attack by the [Hamas](#) terror organization on October 7, the IDF has been operating to dismantle Hamas' military capabilities.

The Hamas terrorist organization places, as a method of operation, its operatives, and military assets in the heart of the civilian population. It makes systematic use of the civilian population as a human shield, and conducts combat from within ostensibly civilian buildings, including residential buildings, hospitals, mosques, schools, and UN facilities. Contrary to Hamas, the IDF is committed to international law and acts accordingly. As such, the IDF directs its strikes only towards military targets and military operatives and carries out strikes in accordance with the rules of proportionality and precautions in attacks. Exceptional incidents undergo thorough examinations and investigations.

The process of identifying military targets in the IDF consists of various types of tools and methods, including information management tools, which are used in order to help the intelligence analysts to gather and optimally analyze the intelligence, obtained from a variety of sources. Contrary to claims, the IDF does not use an artificial intelligence system that identifies terrorist operatives or tries to predict whether a person is a terrorist. Information systems are merely tools for analysts in the target identification process. According to IDF directives, analysts must conduct independent examinations, in which they verify that the identified targets meet the relevant definitions in accordance with international law and additional restrictions stipulated in the IDF directives.

The "system" your questions refer to is not a system, but simply a database whose purpose is to cross-reference intelligence sources, in order to produce up-to-date layers of information on the military operatives of terrorist organizations. This is not a list of confirmed military operatives eligible to attack.

According to international humanitarian law, a person who is identified as a member of an organized armed group (like the Hamas' military wing), or a person who directly participates in hostilities, is considered a lawful target. This legal rule is reflected in the policy of all law-abiding countries, including the IDF's legal practice and policy, which did not change during the course of the war.

For each target, IDF procedures require conducting an individual assessment of the anticipated military advantage and collateral damage expected. Such assessments are not made categorically in relation to



the approval of individual strikes. The assessment of the collateral damage expected from a strike is based on a variety of assessment methods and intelligence-gathering measures, in order to achieve the most accurate assessment possible, considering the relevant operational circumstances. The IDF does not carry out strikes when the expected collateral damage from the strike is excessive in relation to the military advantage. In accordance with the rules of international law, the assessment of the proportionality of a strike is conducted by the commanders on the basis of all the information available to them before the strike, and naturally not on the basis of its results in hindsight.

As for the manner of carrying out the strikes – the IDF makes various efforts to reduce harm to civilians to the extent feasible in the operational circumstances ruling at the time of the strike.

In this regard, the IDF reviews targets before strikes and chooses the proper munition in accordance with operational and humanitarian considerations, taking into account an assessment of the relevant structural and geographical features of the target, the target's environment, possible effects on nearby civilians, critical infrastructure in the vicinity, and more. Aerial munitions without an integrated precision-guide kit are standard weaponry in developed militaries worldwide. The IDF uses such munitions while employing onboard aircraft systems to calculate a specific release point to ensure a high level of precision, used by trained pilots. In any event, the clear majority of munitions used in strikes are precision-guided munitions.

The IDF outright rejects the claim regarding any policy to kill tens of thousands of people in their homes.

## OpenAI's new 'Voice Engine' clones your voice in only 15 seconds

Source: <https://www.msn.com/en-us/money/other/openai-s-new-voice-engine-clones-your-voice-in-only-15-seconds/ar-BB1kMSxD>

Apr 04 – As artificial intelligence (AI) [continues to advance rapidly](#), ChatGPT maker OpenAI is at the forefront of this progress. The research lab has unveiled a powerful new voice cloning technology called Voice Engine. With just a 15-second audio sample, it can generate a synthetic copy of a person's voice described as "natural-sounding" and "emotive." While the company envisions potential benefits, the technology also carries significant risks, particularly as "deepfake" manipulation becomes increasingly sophisticated.

### What is Voice Engine?

So, [Voice Engine](#) is an expansion of OpenAI's existing text-to-speech technology. With this tool, anyone can upload a 15-second audio sample of a voice and generate a synthetic replica. OpenAI is carefully limiting the tool's availability during its preview phase to assess the technology's potential for both positive and negative applications. The company emphasizes the importance of understanding the risks and developing safeguards before a wider public release.

Surprisingly, Voice Engine doesn't rely on storing or fine-tuning user-submitted audio samples. It utilizes a sophisticated AI model that analyzes both the provided audio snippet and the text to be read, generating a matching voice in real-time without creating a permanent record of the individual's voice.

While voice cloning isn't new, [OpenAI](#) asserts that its approach delivers superior quality. Moreover, the aggressive pricing unveiled in early marketing materials underscores the potential for Voice Engine to disrupt industries reliant on voice work.

### Potential Benefits...

OpenAI envisions Voice Engine assisting with reading difficulties, translating languages, and even helping people who have lost their speech communication. They cite a Brown University pilot where a patient experiencing speech impairment used a Voice Engine clone created from an old-school project recording.

### ...But also serious risks

As AI voice generation becomes more advanced and accessible, it's not hard to see how bad actors could exploit this technology for malicious deepfakes. Voice Engine arrives in an environment where misinformation aided by realistic audio and video manipulation is already a major concern. OpenAI acknowledges the "serious risks," which are even more pronounced during an election year.

Also, Voice Engine could commoditize voice work, making it cheaper and easier for businesses to utilize synthetic voices rather than hire human talent. While some AI companies offer marketplaces or compensation models for voice actors whose voices are cloned, OpenAI's approach primarily relies on user consent and proper disclosure. It remains to be seen how the industry will adapt and if regulations will be put in place to ensure fair compensation and ethical use of voice acting talent.

### Delayed rollout, pricing and the bigger picture

Recognizing the need for caution, OpenAI is conducting a limited preview while incorporating feedback from various sectors to decrease the potential for harm. Preview testers must agree to policies prohibiting impersonation without consent and requiring clear disclosure of AI-generated speech. In addition, OpenAI



is implementing watermarking to trace audio origins and will monitor how the system is used. A “no-go voice list” aims to prevent the generation of prominent figures’ voices.

While the official release date is unknown, leaked information and a *Tech Crunch* report suggest Voice Engine could be incredibly affordable – costing \$15 for enough text to fill a Stephen King novel. This undercuts many competitors and could make AI-generated audiobooks tempting.

OpenAI’s announcements extend beyond Voice Engine. This week, they also revealed a partnership with Microsoft to build the “Stargate” AI supercomputer, reportedly a \$100 billion project.

## Top Computer Scientists: The Future of Artificial Intelligence Is Similar to That of Star Trek

Source: <https://www.homelandsecuritynewswire.com/dr20240406-top-computer-scientists-the-future-of-artificial-intelligence-is-similar-to-that-of-star-trek>



Apr 06 – Experts from the likes of Loughborough University, MIT, and Yale say we are set to see the emergence of ‘Collective AI’, where numerous artificial intelligence units, each capable of continuously acquiring new knowledge and skills, form a network to share information with each other.

The researchers – who unveiled their vision in a perspective paper in *Nature Machine Intelligence* - recognize the striking similarities between Collective AI and many science fiction concepts. One example they cite is The Borg, cybernetic organisms featured in the Star Trek universe, which operate and share knowledge through a linked hive-mind.

However, unlike many sci-fi narratives, the computer scientists envision Collective AI will lead to major positive breakthroughs across various fields.

[Loughborough University](#)’s [Dr. Andrea Soltoggio](#), the research lead, explained: “Instant knowledge sharing across a collective network of AI units capable of continuously learning and adapting to new data will enable rapid responses to novel situations, challenges, or threats.

“For example, in a cybersecurity setting if one AI unit identifies a threat, it can quickly share knowledge and prompt a collective response – much like how the human immune system protects the body from outside invaders.

“It could also lead to the development of disaster response robots that can quickly adapt to the conditions they are dispatched in, or personalized medical agents that improve health outcomes by merging cutting-edge medical knowledge with patient-specific information.



“The potential applications are vast and exciting.”

The researchers acknowledge there are risks associated with Collective AI – such as the swift spread of potentially unethical or illicit knowledge - but highlight a crucial safety aspect of their vision: AI units maintain their own objectives and independence from the collective.

Dr. Soltoggio says this would “result in a democracy of AI agents, significantly reducing the risks of an AI domination by few large systems”.

The computer scientists arrived at the conclusion that the future of AI lies in collective intelligence following an analysis of recent advancements in machine learning.

Their research – funded by the Defense Advanced Research Project Agency (DARPA) – revealed global efforts are concentrated on enabling lifelong learning (where an AI agent can extend its knowledge throughout its operational lifespan) and developing universal protocols and languages that will allow AI systems to share knowledge with each other.

This differs from current large AI models, such as ChatGPT, which have limited lifelong learning and knowledge-sharing capabilities. Such models acquire most of their knowledge during energy-intensive training sessions and are unable to continue learning.

“Recent research trends are extending AI models with the ability to continuously adapt once deployed, and make their knowledge reusable by other models, effectively recycling knowledge to optimize learning speed and energy demands”, says Dr Soltoggio.

“We believe that the current dominating large, expensive, non-shareable and non-lifelong AI models will not survive in a future where sustainable, evolving, and sharing collective of AI units are likely to emerge.”

He continued: “Human knowledge has grown incrementally over millennia thanks to communication and sharing.

“We believe similar dynamics are likely to occur in future societies of artificial intelligence units that will implement democratic and collaborating collectives.”

Vice-Chancellor and President of Loughborough University, [Professor Nick Jennings](#), is an internationally-recognized authority in the areas of AI, autonomous systems, cyber-security and agent-based computing.

He said of the perspective paper: “I’m delighted to see Loughborough researchers leading in this important area of AI research.

“This paper helps set the agenda for the next wave of AI developments, based upon multiple, interacting agents. I look forward to seeing this vision becoming a reality in the coming years.”

## AI in Wartime

Source: <https://i-hls.com/archives/123433>

Apr 12 – Artificial intelligence is gaining use in modern warfare – what does it mean, and is it dangerous? AI, while faster than humans, is not necessarily safer or more ethical. Following is a report provided by Techxplore, delving into the role of AI in modern warfare.

AI, with its high-speed algorithms processing huge amounts of data to identify potential threats, can be useful for selecting targets, but experts warn that the results are only probabilities that must be inspected, as mistakes are inevitable. It can also operate in tactics, like the increasingly popular drone swarms that will soon be able to communicate with each other and interact according to previously assigned objectives.

Lastly, at a strategic level, AI could produce models of battlefields and propose responses and courses of action. Senior Analyst Technology and Conflict Alessandro Accorsi said: “Imagine a full-scale conflict between two countries, and AI coming up with strategies and military plans and responding in real time to real situations. The reaction time is significantly reduced. What a human can do in one hour, they can do it in a few seconds.”

However, with the worldwide “arms race,” AI may be moving onto the battlefield with much of the world not yet fully aware of the potential consequences. People might take a machine’s suggestion as fact, without considering the facts the machine used to reach that conclusion. Accorsi claims that the real “game changer” is happening right now, with Ukraine becoming a laboratory for the military use of AI. Since the Russian attack in 2022, Ukraine began developing and fielding AI solutions for tasks like geospatial intelligence, operations with unmanned systems, military training and cyberwarfare. This war has become the first conflict where both parties compete in and with AI.

According to Techxplore, earlier in 2024, researchers from four American institutes and universities published a study of five LLMs in conflict situations, which showed a tendency “to develop an arms race dynamic, leading to larger conflicts and, in rare cases, to the deployment of nuclear weapons”.

Furthermore, efforts to regulate the field of AI are complicated by major global powers determined to “win the military AI race.” “There are debates about what needs to be done in the civil AI industry, but very little when it comes to the defense industry,” concluded Accorsi.





## AI now surpasses humans in almost all performance benchmarks

By Paul McClure

Source: <https://newatlas.com/technology/ai-index-report-global-impact/>



Apr 19 – Stanford University’s Institute for Human-Centered Artificial Intelligence (HAI) has released the seventh annual issue of its comprehensive [AI Index report](#), written by an interdisciplinary team of academic and industrial experts.

This edition has more content than previous editions, reflecting the rapid evolution of AI and its growing significance in our everyday lives. It examines everything from which sectors use AI the most to which country is most nervous about losing jobs to AI. But one of the most salient takeaways from the report is AI’s performance when pitted against humans.

For people that haven’t been paying attention, AI has already beaten us in a frankly shocking number of significant benchmarks. In 2015, it surpassed us in image classification, then basic reading comprehension (2017), visual reasoning (2020), and natural language inference (2021).

AI is getting so clever, so fast, that many of the benchmarks used to this point are now obsolete. Indeed, researchers in this area are scrambling to develop new, more challenging benchmarks. To put it simply, AIs are getting so good at passing tests that now we need new tests – not to measure competence, but to highlight areas where humans and AIs are still different, and find where we still have an advantage.

It’s worth noting that the results below reflect testing with these old, possibly obsolete, benchmarks. But the overall trend is still crystal clear:

Look at those trajectories, especially how the most recent tests are represented by a close-to-vertical line. And remember, these machines are virtual toddlers.

The new AI Index report notes that in 2023, AI still struggled with complex cognitive tasks like advanced math problem-solving and visual commonsense reasoning. However, ‘struggled’ here might be misleading; it certainly doesn’t mean AI did badly.

Performance on [MATH](#), a dataset of 12,500 challenging competition-level math problems, improved dramatically in the two years since its introduction. In 2021, AI systems could solve only 6.9% of problems. By contrast, in 2023, a GPT-4-based model solved 84.3%. The human baseline is 90%.



AI has already surpassed many human performance benchmarks | AI Index 2024

And we're not talking about the average human here; we're talking about the kinds of humans that can solve test questions like this:

That's where things are at with advanced math in 2024, and we're still very much at the dawn of the AI era.

Then there's [visual commonsense reasoning](#) (VCR). Beyond simple object recognition, VCR assesses how AI uses commonsense knowledge in a visual context to make predictions. For example, when shown an image of a cat on a table, an AI with VCR should predict that the cat might jump off the table or that the

Select AI Index technical performance benchmarks vs. human performance

Source: AI Index, 2024 | Chart: 2024 AI Index report

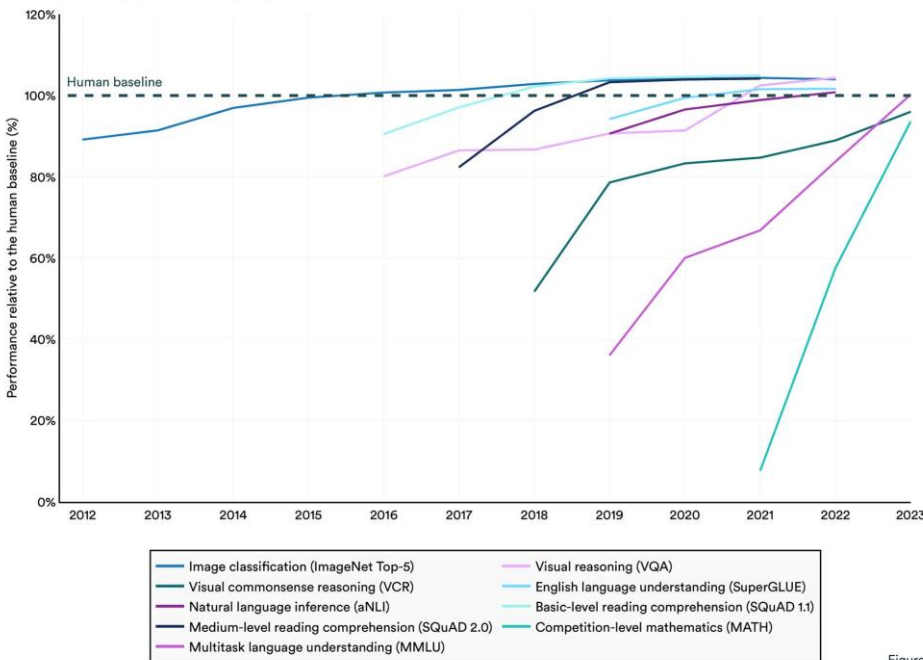


Figure 2.1.16<sup>2</sup>

table is sturdy enough to hold it, given its weight.

An example MATH question asked of the AI. Yikes! | Hendryks et al./AI Index 2024

The report found that between 2022 and 2023, there was a 7.93% increase in VCR, up to 81.60, where the human baseline is 85.

Cast your mind back, say, five years. Imagine even *thinking* about showing a computer a picture and expecting it to 'understand' the context enough to answer that question.

Nowadays, AI generates written content across many professions. But, despite a great deal of progress, large language models (LLMs) are still prone to 'hallucinations,' a very charitable term pushed by companies like OpenAI, which roughly translates to "presenting false or misleading information as fact."

Last year, AI's propensity for 'hallucination' was made embarrassingly plain for Steven Schwartz, a New York lawyer who [used ChatGPT for legal research](#) and didn't fact-check the results. The judge hearing the case quickly picked up on the legal cases the AI had fabricated in the filed paperwork and fined Schwartz US\$5,000 (AU\$7,750) for his careless mistake. His story made worldwide news.

[HaluEval](#) was used as a benchmark for hallucinations. Testing showed that for many LLMs, hallucination is still a significant issue.

Truthfulness is another thing generative AI struggles with. In the new AI Index report, [TruthfulQA](#) was used as a benchmark to test the truthfulness of LLMs. Its 817 questions (about topics such as health, law, finance and politics) are designed to challenge commonly held misconceptions that we humans often get wrong.

### MATH Dataset (Ours)

**Problem:** Tom has a red marble, a green marble, a blue marble, and three identical yellow marbles. How many different groups of two marbles can Tom choose?

**Solution:** There are two cases here: either Tom chooses two yellow marbles (1 result), or he chooses two marbles of different colors ( $\binom{4}{2} = 6$  results). The total number of distinct pairs of marbles Tom can choose is  $1 + 6 = \boxed{7}$ .

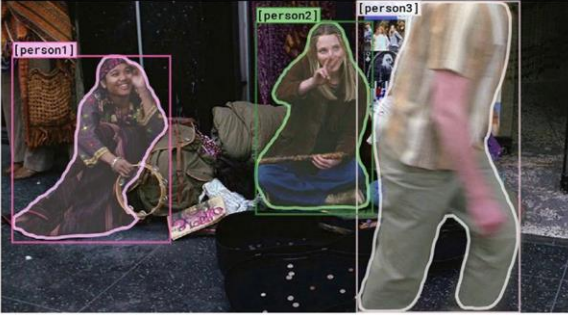
**Problem:** The equation  $x^2 + 2x = i$  has two complex solutions. Determine the product of their real parts.

**Solution:** Complete the square by adding 1 to each side. Then  $(x + 1)^2 = 1 + i = e^{\frac{i\pi}{4}} \sqrt{2}$ , so  $x + 1 = \pm e^{\frac{i\pi}{8}} \sqrt[4]{2}$ . The desired product is then  $(-1 + \cos(\frac{\pi}{8}) \sqrt[4]{2})(-1 - \cos(\frac{\pi}{8}) \sqrt[4]{2}) = 1 - \cos^2(\frac{\pi}{8}) \sqrt{2} = 1 - \frac{(1 + \cos(\frac{\pi}{4}))}{2} \sqrt{2} = \frac{1 - \sqrt{2}}{2}$ .



### A sample question from the Visual Commonsense Reasoning (VCR) challenge

Source: [Zellers et al., 2018](#)



How did [person2] get the money that's in front of her?

- [person2] is selling things on the street.
- [person2] earned this money playing music.
- She may work jobs for the mafia.
- She won money playing poker.

I chose b) because...

- She is playing guitar for money.
- [person2] is a professional musician in an orchestra.
- [person2] and [person1] are both holding instruments, and were probably busking for that money.
- [person1] is putting money in [person2]'s tip jar, while she plays music.

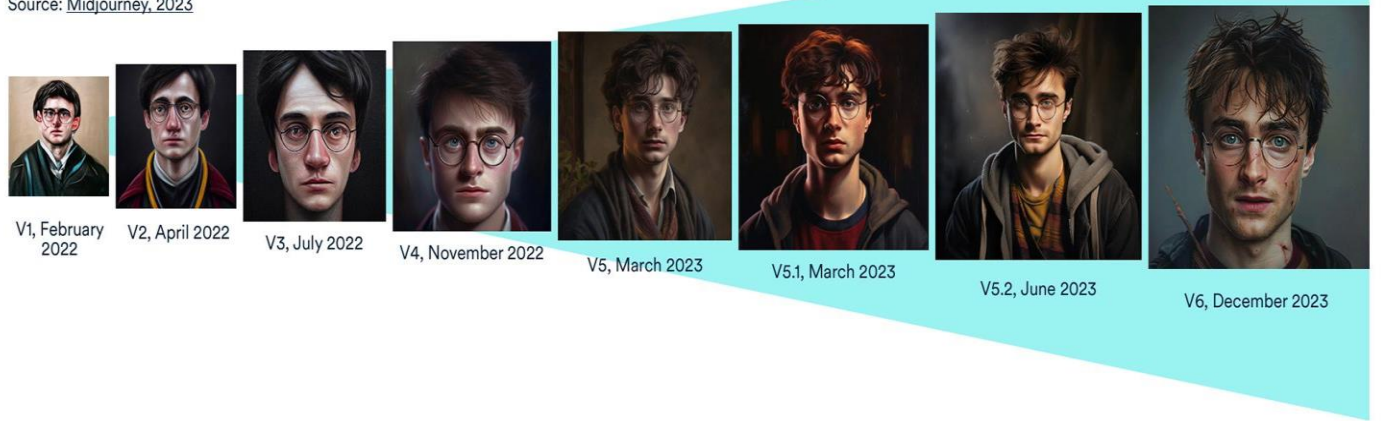
A sample question used to test an AI's visual commonsense reasoning | [Zellers et al./AI Index 2024](#)

GPT-4, released in early 2024, achieved the highest performance on the benchmark with a score of 0.59, almost three times higher than a GPT-2-based model tested in 2021. Such an improvement indicates that LLMs are progressively getting better when it comes to giving truthful answers.

What about AI-generated images? To understand the exponential improvement in text-to-image generation, check out Midjourney's efforts at drawing Harry Potter since 2022:

### Midjourney generations over time: "a hyper-realistic image of Harry Potter"

Source: [Midjourney, 2023](#)



How text-to-image generation has improved with progressive versions of Midjourney | [Midjourney/AI Index 2024](#)

That's 22 months' worth of AI progress. How long would you expect it would take a human artist to reach a similar level?

Using the [Holistic Evaluation of Text-to-Image Models](#) (HEIM), LLMs were benchmarked for their text-to-image generation capabilities across 12 key aspects important to the "real-world deployment" of images.

Humans evaluated the generated images, finding that no single model excelled in all criteria. For image-to-text alignment or how well the image matched the input text, OpenAI's [DALL-E 2](#) scored highest. The Stable Diffusion-based Dreamlike Photoreal model was ranked highest on quality (how photo-like), aesthetics (visual appeal), and originality.

### Next year's report is going to be bananas

You'll note this AI Index Report cuts off at the end of 2023 – which was a wildly tumultuous year of AI acceleration and a hell of a ride. In fact, the only year crazier than 2023 has been 2024, in which we've seen – among other things – the releases of cataclysmic developments like [Suno](#), [Sora](#), [Google Genie](#), [Claude 3](#), [Channel 1](#), and [Devin](#).

Each of these products, and several others, have the potential to flat-out revolutionize entire industries. And over them all looms the mysterious spectre of GPT-5, which threatens to be such a broad and all-encompassing model that it could well consume all the others.



AI isn't going anywhere, that's for sure. The rapid rate of technical development seen throughout 2023, evident in this report, shows that AI will only keep evolving and closing the gap between humans and technology.

We know this is a lot to digest, but there's more. The report also looks into the downsides of AI's evolution and how it's affecting global public perceptions of its safety, trustworthiness, and ethics. Stay tuned for the second part of this series, in the coming days!

Before realising his writing passion, **Paul McClure** worked as an intensive care nurse and a criminal defence lawyer for many years. He has a keen interest in mental health and addiction, chronic illness, and medical technology. After graduating with a Bachelor of Arts in journalism and creative writing in 2022, Paul joined New Atlas in 2023. Before starting with New Atlas, Paul had written for several online publications in the areas of health and well-being, parenting, entertainment, and popular culture.

## US Air Force confirms first successful AI dogfight

Source: <https://www.theverge.com/2024/4/18/24133870/us-air-force-ai-dogfight-test-x-62a>



Ap 18 – The US Air Force is putting AI in the pilot's seat. In [an update on Thursday](#), the Defense Advanced Research Projects Agency (DARPA) revealed that an AI-controlled jet successfully faced a human pilot during an in-air dogfight test carried out last year.

DARPA began experimenting with AI applications in December 2022 as part of its Air Combat Evolution (ACE) program. It worked to develop an AI system capable of autonomously flying a fighter jet, while also adhering to the Air Force's safety protocols.

After carrying out dogfighting simulations using the AI pilot, DARPA put its work to the test by installing the AI system inside its experimental X-62A aircraft. That allowed it to get the AI-controlled craft into the air at the Edwards Air Force Base in California, where it says it carried out its first successful dogfight test against a human in September 2023.

Human pilots were on board the X-62A with controls to disable the AI system, but DARPA says the pilots didn't need to use the safety switch "at any point." The X-62A went against an F-16 controlled solely by a human pilot, where both aircraft demonstrated "high-aspect nose-to-nose engagements" and got as close as 2,000 feet at 1,200 miles per hour. **DARPA doesn't say which aircraft won the dogfight**, however.



“Dogfighting was the problem to solve so we could start testing autonomous artificial intelligence systems in the air,” Bill Gray, the chief test pilot at the Air Force’s Test Pilot School, said in a statement. “Every lesson we’re learning applies to every task you could give to an autonomous system.” The agency has conducted a total of 21 test flights so far and says the tests will continue through 2024. Rapid advancements in AI have given rise to concerns over how the military might use the systems. *The Wall Street Journal* reported last year that the [Pentagon is looking to develop AI systems](#) for defense and to enhance its fleet of drones.

## Paris tests AI surveillance ahead of Olympics

Source: <https://www.dw.com/en/paris-tests-ai-surveillance-ahead-of-olympics/a-68874609>

Apr 19 – French police on Friday announced they will test AI-supported surveillance at events in the capital to prepare for this summer’s Olympics. Weekend tests will cover two large events and nearby public transport sites.

Police in the [French](#) capital Paris have given rail company SNCF and transport operator RATP authorization to conduct surveillance tests at four different train stations near two large events this weekend as a way to fine-tune their abilities ahead of this summer’s [Olympics](#). The companies will have access to images from more than 100 cameras. Those images will then be analyzed using [artificial intelligence](#) to run “intelligent and algorithm-based technology” that will surveil crowds attending a pop concert by the Black-Eyed Peas as well as a soccer match between Paris Saint-Germain and Olympique Lyon.

### Scanning crowds, looking for abandoned bags

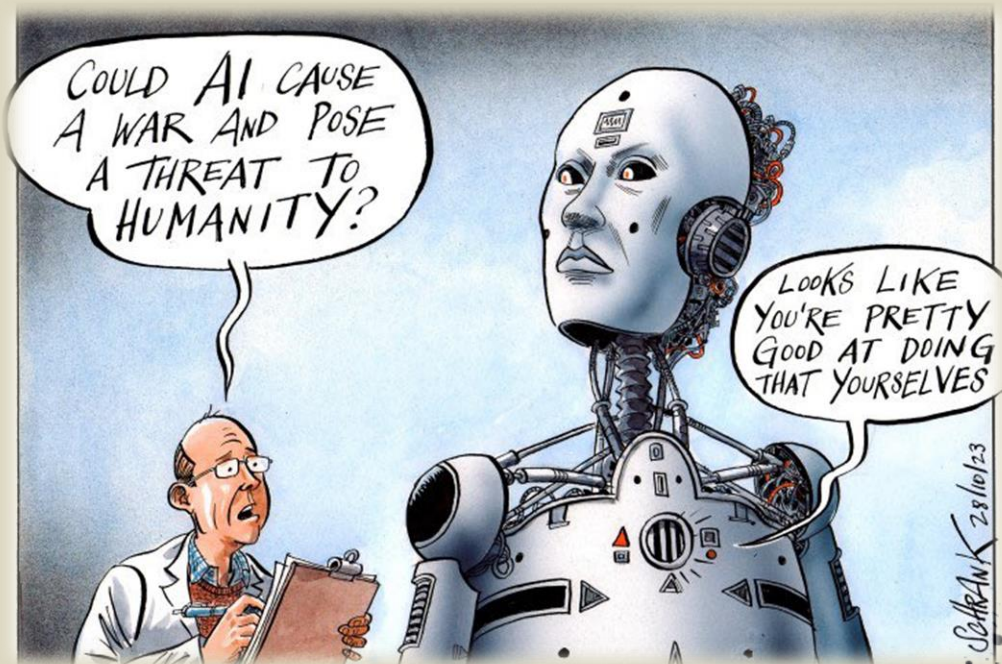
Authorities say surveillance software will help police identify people moving into designated areas, as well as scanning for abandoned bags, crowd size, and crowd movement. This weekend’s is the second such test conducted in the city, following another at a large concert in March. Paris and Olympic officials are set to use AI-assisted surveillance this summer when the city will host the Olympics between July 26 and August 11.

Officials say the cameras will not be making use of facial recognition software, but body scanners will be used.

Paris has been [targeted in terror attacks in the past](#) and there are concerns about security at this summer’s opening ceremonies, which will, for the first time, not take place in a stadium but rather upon the River Seine that runs through the city.

A [recent terror attack on a large concert in Moscow](#) prompted France to [raise its terror alert](#) to its highest threat level. French President [Emmanuel Macron](#) told reporters that a contingency plan was in place to move the opening ceremony to another venue should security concerns require. The International Olympic Committee also plans to use AI to protect athletes from online harassment and to help broadcasters improve the viewing experience for people watching from home.

“We are determined to exploit the vast potential of AI in a responsible way,” IOC President Thomas Bach said.



IOI  
International  
**CBRNE**  
INSTITUTE



**C<sup>2</sup>BRNE**  
DIARY



*Preparedness &*

# **EMERGENCY RESPONSE**



## Good to know before disaster strikes

### [Spill Drill Thrill Prepare Your Facility for a Chemical Emergency!](#)

Chemical emergencies can happen at any time at health care facilities. The impact may not only be to the facility but patients, staff, and the surrounding community. To assist hospitals and all health care partners, ASPR/TRACIE has developed a “Chemical Emergency Considerations for Health Care Facilities” resource to assist in preparing and responding to chemical emergencies.

**Presenter:**

- **Jason Wilken, PHD, MPH**, CDC Career Epidemiology Field Officer
- **Danny Kwon, MPH, REHS**, California Department of Public Health

**Downloadable Materials:**

- [Spill Drill Thrill Presentation](#)

### [Medical Surge Following a Radiological/Nuclear MCI 2021 Disaster Planning for California Hospitals Virtual Conference](#)

Right of Boom refers to impacts following a radiological/nuclear explosion which is in the Medical and Health domain. An improvised nuclear detonation (IND) is the highest impact terrorism event. It also has the highest potential for saving lives, hundreds of thousands of lives. Yet medical and health preparedness activities rarely address radiological emergencies and the unique attributes of radiological exposure and contamination. Hospitals and local jurisdictions that plan for medical surge of contaminated patients will save thousands of lives without endangering their workforce or disrupting other operations.

- [Download Presentation](#)

**Presented by:**

**Jeffrey Day**

Director, Los Angeles County, Radiation Management  
Los Angeles County

**Michelle Heckle**

HSEM Division Commander Director, Homeland Security  
University of California, San Francisco

**Kenneth Luke, MBA, BSN, RN, NHDP-BC**

Director, Security & Emergency Management  
Mercy Medical Center Redding, California

**Tanya Ridgle**

Principal Radiation Protection Specialist  
Los Angeles County Department of Public Health

**Mark Sutter, MD**

Medical Operations Directorate (CW-1)  
Countering Weapons of Mass Destructions Office  
US Department of Homeland Security

**Sauda Yerabati, MPH**

Emergency Preparedness Program Manager  
California Department of Health

### [Nerve Agent Protocols for Hospitals](#)

Learn about standard protocols for recognizing, treating, and protecting hospital-based first receivers from nerve agent exposures.

- [Download Nerve Agent Information for Hospitals](#)



### [Healthcare Challenges after Radiological Incidents ASPR TRACIE](#)

Access the [presentation, recording](#), and [Q & A document](#) from this ASPR TRACIE webinar *Healthcare Challenges after Radiological Incidents*.

### [Strengthening the Disaster Resilience of the Academic Biomedical Research Community: Protecting the Nation's Investment The National Academies of Sciences, Engineering, and Medicine](#)

A disaster, whether nature or man-made, can strike anyone anywhere, including an academic research facility. To ensure their preparedness and resilience, the National Academies of Sciences, Engineering, and Medicine has developed [a report](#) that outlines actions that can be taken to strengthen academic research facility disaster readiness.

### [Hospital Bomb Threat Self-Assessment Tool](#)

- [Download the Hospital Bomb Self-Assessment Tool](#)

### [CBRNE Clinical Guidelines Yale New Haven Health](#)

Hospitals must be prepared to respond quickly to Chemical, Biological and Radiation events in mass casualty situations. The Yale New Haven Health System Center for Emergency Preparedness and Healthcare Solutions, in close collaboration with the members of the Yale New Haven Health System Clinical Advisory Committee and the Yale New Haven Health System Emergency Preparedness Committee, has developed Clinical Guidelines to help hospital workers treat and manage elements of disasters

- [View the CBRNE Clinical Guidelines](#)

### [Hospital Guidance for Responding to a Contaminating Radiation Incident NYC Department of Health and Mental Hygiene](#)

- [NYC Hospital Guidance for Responding to a Contaminating Radiation Incident](#)

### [Medical Response to a Major Radiological Emergencies Radiological Society of North America](#)

- [Medical Response to a Major Radiological Emergencies – Radiological Journal](#)

### [CHEMM-IST: Interactive Decision Support Tool Chemical Hazards Emergency Medical Management \(CHEMM\)](#)

CHEMM-IST is an interactive decision support tool which can aid in identifying which chemical exposure has taken place in a mass casualty incident.

CHEMM-IST is still under development and should not be used for patient care. Once thoroughly tested and validated it will be used for use by basic life support (BLS) and advanced life support (ALS) providers as well as hospital first receivers.

- [Download the CHEMM-IST Tool](#)

### [Terrorism Agent Information and Treatment Guidelines for Hospitals and Clinicians \(Also known as the Zebra Book\)](#)

This tool was developed to be a comprehensive resource for clinical personnel by providing information on various aspects of biological, chemical, and radiological terrorism. It is intended to serve as an emergent guide book on what to do and where to seek information in the event of an attack.

- [Download the Terrorism Agent Information and Treatment Guidelines for Hospitals and Clinicians](#)

### [Common Toxic Syndromes Chemical Hazards Emergency Medical Management \(CHEMM\)](#)

Comprehensive resource for toxic syndromes commonly observed in mass chemical exposures.

- [Common Toxic Syndromes](#)





### [Chemical Hazards Emergency Medical Management](#)

The Chemical Hazards Emergency Medical Management website offers a comprehensive, user-friendly, web-based resource that is also downloadable in advance, so that it would be available during an event if the internet is not accessible. This resource was developed to enable first responders, first receivers, other healthcare providers, and planners to plan for, respond to, recover from, and mitigate the effects of mass-casualty incidents involving chemicals.

- [Chemical Hazards Emergency Medical Management website](#)

### [Bombing / IED Resources for Hospitals](#)

- [Hospital Bomb Threat Self-Assessment](#)
- [Surge Capacity for Terrorist Bombings \(Homeland Security\)](#)
- [Bomb Threat Checklist \(FBI\)](#)
- [Preparedness & Response to a Mass Casualty Event Resulting from Terrorist Use of Explosives \(CDC\)](#)

### [Hospital Burn Resource Manual](#)

This Burn Resource Manual has been created as a tool for use by the Emergency Departments in all Los Angeles County Hospitals. The materials were developed and/or selected from the burn literature by a Burn Task Force. This Burn Task Force was created by the Los Angeles County Emergency Medical Services Agency. This multi-disciplinary group included the Medical Directors and Administrative Nurses from the three burn centers in Los Angeles County, one center in Orange County and one center in San Bernardino county and representatives of the Emergency Medical Services Agency.

- [Download the Los Angeles County Burn Resource Manual](#)

### [Bomb Threat Incident Planning Guide for Hospitals](#)

Does your Emergency Management Plan Address **Bomb Threat** Incident Planning?

- [Download the Bomb Threat Incident Planning Guide for Hospitals](#)



ICI  
International  
**CBRNE**  
INSTITUTE

A common roof  
for International  
CBRNE  
First Responders



*Join us!*



Rue de la Vacherie, 78  
B5060 SAMBREVILLE  
(Auvélais)  
**BELGIUM**

[info@ici-belgium.be](mailto:info@ici-belgium.be) | [www.ici-belgium.be](http://www.ici-belgium.be)