

# IC<sup>2</sup> CBRNE DIARY

*Dedicated to Global First Responders*

December 2022



*Happy New Year*

**PART B**



ICI  
International  
**CBRNE**  
INSTITUTE



# DIRTY R-NEWS







## The Surprising Afterlife of Unwanted Atom Bombs

By William J. Broad

Source: <https://www.nytimes.com/2022/11/17/science/retired-nuclear-bombs-b83.html>Top of Form



Retired nuclear weapons being readied for disassembly at the government's Pantex plant near Amarillo, Texas, in 1996. Credit...Remi Benali/Liaison, via Getty Images

Nov 17 – What happens when old atomic bombs are retired? Last month, the Biden administration [announced](#) its intention to withdraw the nation's most powerful weapon from the U.S. nuclear arsenal.

The bomb is called the B83. It is a hydrogen bomb that debuted in 1983 — a time when President Reagan was [denouncing](#) Russia as “an evil empire.” The government made 660 of the deadly weapons, which were to be delivered by fast bombers. The B83 was 12 feet long, had fins and packed an explosive force roughly 80 times greater than that of the Hiroshima bomb. Its job was to obliterate hardened military sites and command bunkers, including Moscow's.

What now for the B83? How many still exist is a federal secret, but not the weapon's likely fate, which may surprise anyone who assumes that getting rid of a nuclear weapon means that it vanishes from the face of the earth.

Typically, nuclear arms retired from the U.S. arsenal are not melted down, pulverized, crushed, buried or otherwise destroyed. Instead, they are painstakingly disassembled, and their parts, including their deadly plutonium cores, are kept in a maze of bunkers and warehouses across the United States. Any individual facility within this gargantuan complex can act as a kind of used-parts superstore from which new weapons can — and do — emerge.

“It's like a giant Safeway,” said [Hans M. Kristensen](#), the director of the Nuclear Information Project at the Federation of American Scientists, a private research group in Washington. “You go in with a bar code and get what you need.”

One weapon that nuclear planners want to make from recycled parts and designs is the [W93](#) — [billed](#) as the first new warhead for the nation's nuclear arsenal since the Cold War. The Biden administration [announced](#) the weapon's birth in March and estimated it would cost up to \$15.5 billion. The finished warhead would sit atop submarine missiles starting in or around 2034. Despite its description as new, the official government plan [states](#) that the weapon will be “anchored on previously tested nuclear components,” not new explosive parts.





“It’s bizarre how these things cycle around,” Mr. Kristensen said. “It’s nuclear whack-a-mole. You hit one down, and another pops up.”

The recycling has no direct bearing on the overall size of the nation’s nuclear arsenal, as the reused explosive parts are often employed for making replacement weapons, not new ones. That’s the case with the W93s, which are to replace or supplement old submarine warheads.

for greater arms control livid. They’ve long argued that other nations view the storage of explosive weapon parts as a sign that the United States wants the option to make swarms of new warheads. That perception, they add, can fuel new arms races and nuclear proliferation.



Some components of the B83, which can explode with a force 80 times greater than the Hiroshima bomb. The nonnuclear parts are in the foreground; the nuclear warhead is the bullet-like cylinder at the back. It holds the plutonium pit and the hydrogen fuel, which gives the bomb its vast powers of destruction. Credit...Department of Defense

“Getting rid of them would be a good thing,” said [Frank N. von Hippel](#), a nuclear physicist who advised the Clinton White House and now teaches at Princeton University. “It would signal that we have no expectation of rebuilding our arsenal.”

But hawks see the stored parts as crucial for the hedging of nuclear bets. Of late, they [cite](#) China’s [growing nuclear arsenal](#) as a developing threat that may require atomic rearmament.

“It’s important to keep these parts around,” said [Franklin C. Miller](#), a nuclear expert who held federal posts for three decades before leaving government service in 2005. “If we had the manufacturing complex we once did, we wouldn’t have to rely on the old parts.” He added that other nuclear powers can and do make new atomic parts.

Beyond the weapon debate, critics of the atomic recycling warn that the nuclear storage complex is a disaster waiting to happen. It has a long history of [accidents](#), safety lapses and [security failures](#) that could lead to a nuclear catastrophe. “It’s dangerous,” said [Robert Alvarez](#), a nuclear expert who, from 1993 to 1999 during the Clinton administration was a policy adviser to the Department of Energy, which runs the







nation’s atomic weapons infrastructure. “And it’s getting more dangerous, as the quantities in storage have increased.” The plutonium cores of retired hydrogen bombs are of particular concern, Mr. Alvarez and others say. Roughly the size of a grapefruit, these cores are usually referred to as pits. The United States now [has](#) at least 20,000 pits in storage. They’re kept at [a sprawling plant](#) in the Texas panhandle known as Pantex. Plutonium is [deadly to humans](#) in tiny amounts, and that greatly complicates its safekeeping.

If recycled, pits from the B83 bombs would enter plutonium bunkers at Pantex that are already overcrowded and overtaxed. Mr. Alvarez [said](#) that torrential rains in 2010 and 2017 flooded a major plutonium storage area at the Pantex site. Repairs, he added, cost hundreds of millions of dollars.

The Clinton, Bush and Obama administrations all made plans — with costs in the billions of dollars — to get rid of excess plutonium stocks, which grew rapidly after the Cold War because of arms disassembly. But no strategy has so far succeeded.



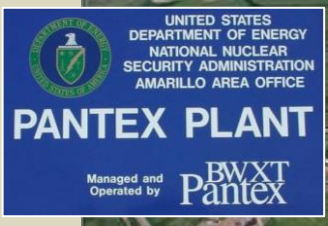
Workers packaging a plutonium pit from a nuclear weapon in a storage canister at the Pantex plant in 1996.Credit...Remi Benali/Liaison, via Getty Images

Plans to recycle parts of the B83 may come to naught if Republicans on Capitol Hill have their way. Early this year, they [criticized](#) the Biden administration’s emerging plan to retire the powerful bomb, which they said was needed for targeting hard and deep targets.

But Mr. Kristensen of the science federation said that the Republicans were unlikely to succeed in saving the B83 even after retaking the House, which gives them new clout in determining military budgets and priorities. He said that the weapon, four decades after entering the U.S. arsenal, was more likely to start its afterlife in the storage maze.

“They’ve tried to stuff it down the throat of the administration, but the military hasn’t expressed any need for it,” he said of Republican attempts to block the B83’s withdrawal. “I think it will probably be retired. I think this one’s dead.”



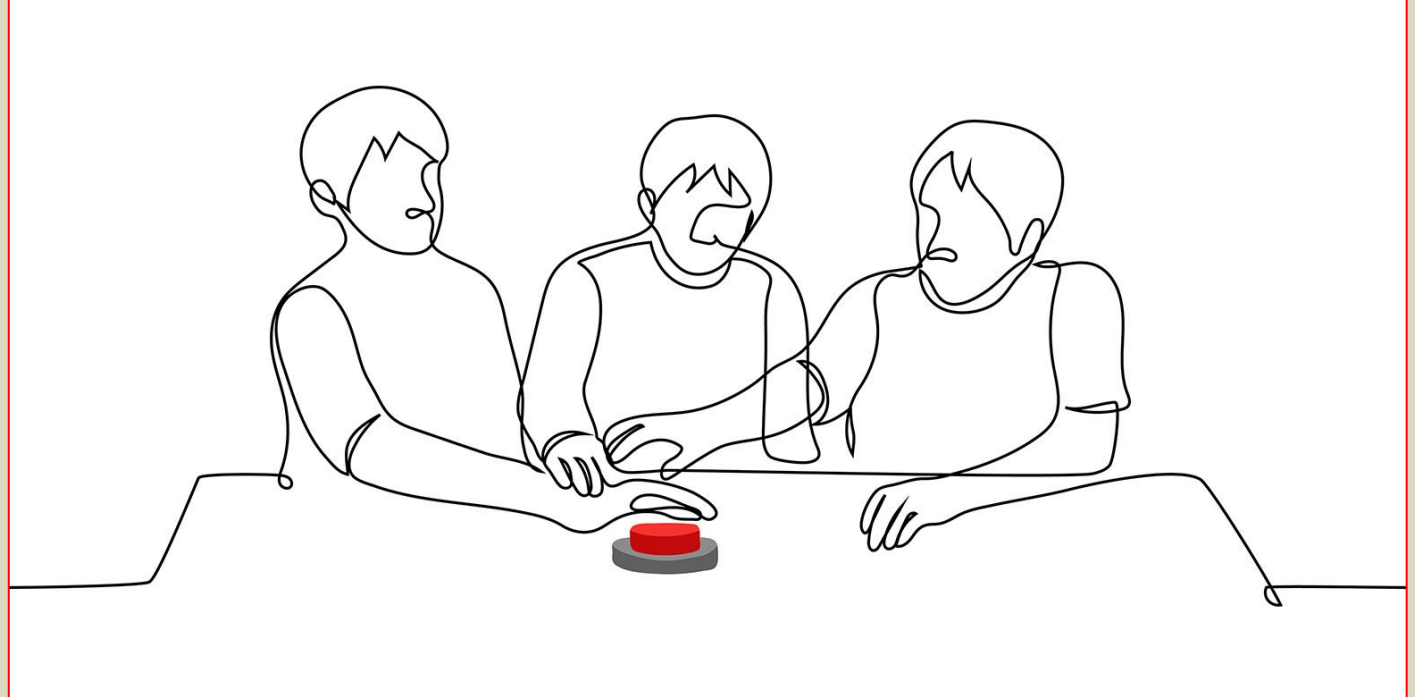


The Pentagon has given the old weapon [no public support](#). Officials say that an overhaul meant to extend the weapon's life would be costly and in any case would put bombers in jeopardy because they'd have to fly so close to targets. Newer arms use satellite guidance, so bombers can drop their weapons from afar. For instance, the B61 model 12 [has](#) a computer brain and four maneuverable fins that let it zero in on deeply buried targets. To be [deployed in Europe](#) late this year, it is a designated replacement for the B83. And yes, its explosive parts come from the atomic recycling bin.

[William J. Broad](#) is a science journalist and senior writer. He joined The Times in 1983, and has shared two Pulitzer Prizes with his colleagues, as well as an Emmy Award and a DuPont Award.

### The nuclear reality is unsettling

Source: <https://ethz.ch/en/news-and-events/eth-news/news/2022/11/blog-the-nuclear-reality-is-unsettling.html>



Nov 24 – Stephen Herzog is researching how nuclear weapons could be better controlled and eventually eliminated. For him, Putin's threats are a reason to fundamentally question the nuclear "balance of terror." "I research nuclear arms control." For years, this line produced blank stares in social settings as I tried to explain my job's importance. After all, nuclear weapons are quite distant from the lives of most people, particularly since the Cold War has been over for decades.







Then came the invasion of Ukraine on February 24. Russian President Vladimir Putin warned that the West risked nuclear retaliation with attempts to assist Ukraine in the conflict.<sup>1</sup> Suddenly, my Center for Security Studies colleagues and I found ourselves explaining the world's unpleasant nuclear realities to the media and public.

The nuclear dimensions of this war have created twin imperatives for researchers. First, experts must unpack facts in a way that avoids scaremongering. Second, scientists should contribute to making the future safer and free of nuclear fears. So ultimately the question is: How can we prevent leaders like Putin from suddenly being able to threaten the world with nuclear warheads?

### **Nuclear risks remain**

The U.S. bombings of Hiroshima and Nagasaki ushered in the atomic age. Soon the United States and Soviet Union pointed nuclear arms at each other's cities. Backed by game theory, the belief was that this "balance of terror" would prevent a third world war. Many researchers even declared the new world safer. Is the world really safer? Today, nine countries possess approximately 12,700 nuclear warheads.<sup>2</sup> Most cities in the United States, Russia, China, and European NATO states are under 30 minutes from destruction with ballistic missiles at all times. Neutral Switzerland has also built bunkers to protect its population from a nuclear war.<sup>3</sup> In a nuclear-armed world, confrontations carry immeasurable risks. Imagine if an AI simulated the Cold War and its numerous close calls like the Cuban Missile Crisis 10, 100, or maybe even 1,000 times. In how many cases would millions of people die because someone pressed the proverbial "red button"? The fact that luck probably played a big role in the absence of catastrophes should make us skeptical about the safety of our nuclear future.<sup>4</sup>

### **An uncomfortable responsibility**

Discussing global nuclear risks and vulnerability with the public is no easy task. These issues are complex and there are no simple or reassuring answers to most questions. I believe it is unethical to speculate with mathematical odds on how likely it is that nuclear weapons will be used in Ukraine. My response to queries is that nuclear use remains unlikely, but its dramatic consequences require our attention. Nuclear threats have been part of the fabric of international security for over 75 years. However, polling shows most people would prefer to live in a world without nuclear weapons. Ultimately, we have to decide whether to support leaders who embrace the status quo or those who seek nuclear disarmament.

### **Science's role**

Addressing long-term nuclear dangers necessitate changes in how publics and policymakers talk about nuclear arms. For this reason, in a recent *Science* magazine editorial, I advocated for research into the desirability and feasibility of nuclear disarmament.<sup>5</sup> Here are three important approaches to begin reframing discussions about nuclear weapons:

1. Scientists who view nuclear deterrence as "playing with fire" cannot assume governments and publics will learn this lesson until it is too late. Critics won't convince advocates without researching viable alternatives that can provide for states' security.
2. Likewise, innovative disarmament verification studies are necessary. I often hear that nuclear weapons can never be verifiably eliminated. Current monitoring technologies offer a good start for imagining how the international community could police a disarmed world. Yet, extensive further research and development is needed before the public and policymakers can fully trust disarmament verification technology.
3. Just as research fueled nuclear deterrence strategy at the height of the Cold War, science can help drive the transition away from that past. Researchers have a responsibility to contextualize the possible risks to publics concerned by reports of nuclear drills and images of mushroom clouds.

Nuclear deterrence is a theory. But Putin's threats should remind us that gray theory can carry implications for humanity's survival. Like all theories, the core tenets of nuclear deterrence deserve interrogation.

**Stephen Herzog is a Senior Researcher in Nuclear Arms Control at the Center for Security Studies (CSS) at ETH Zurich.**

## **War puts cleanup of Russia's radioactive wrecks on ice**

**By Charles Digges**

Source: <https://thebulletin.org/2022/11/war-puts-cleanup-of-russias-radioactive-wrecks-on-ice/>

Nov 28 – When Russia assumed the rotating chairmanship of the Arctic Council in 2021, Moscow brought the environmentally minded eight-nation body an ambitious proposal. Over the next 14 years, it would raise from the depths of the Arctic a toxic array of rusting nuclear garbage—including two entire nuclear submarines—that had been dumped during the Soviet era.





The Soviet submarine K-159 sank on August 30, 2003 while being towed to be dismantled, killing 9 people. (The Bellona Foundation)

The project was estimated to cost about \$394 million at current exchange rates and had the backing of Vladimir Putin. His Arctic development plan ordered the retrieval of the subs and the accompanying radioactive waste by 2035.

Russian gas, oil, and mineral conglomerates wanted the wrecks cleared away from nascent Arctic shipping routes. Fishermen from either side of Russia's border with Scandinavia, concerned that radioactive leakage from the submarines' reactors would contaminate fisheries, also celebrated the news. It was a rare alignment of the stars, pleasing environmentalists, business interests, the Kremlin, and European governments all at the same time.

By November 2021, discussions were underway with the powerful European Bank of Reconstruction and Development, which [promised](#) to help fund a preliminary review to establish how the subs should be lifted.

Then, in February, Russia invaded Ukraine.

Since then, the West has imposed a raft of sanctions against Moscow, and the intergovernmental buzz on the Arctic submarine and radioactive junk lift has gone silent.

Norway was among the first to step back, [ceasing](#) scientific exchanges with Moscow as soon as May and [pausing](#) funding to its decades-old bilateral nuclear safety commission with Russia in June. Days later, Moscow [retorted](#) tartly, saying it, too, was ceasing its work with the commission over the "unfriendly line" Norway had taken since the beginning of hostilities in Ukraine.

For an alliance that had weathered political tremors as turbulent as Moscow's 2014 annexation of Crimea, the rift was profound. Even when mutual distrust between East and West had been high, Norway and Russia had been able to reach above the politics to safely dispose of the most toxic elements of Cold War history. But the invasion of Ukraine proved to be a last straw.

Moscow insists that it will lift the submarines on its own. But does it stand any chance of doing so by itself? And if it can't, what is at stake?







### A history of cooperative cleanup

Throughout the Cold War, the Soviet Union and the United States built more than 400 nuclear submarines, assuring each superpower the ability to fire nuclear missiles even after their land-based silos had been decimated by a first strike. The fjords and coastlines around Murmansk adjacent to NATO member Norway became the hub of the Soviet Northern Fleet, and a dumping ground for radioactive waste and spent nuclear fuel.



Murmansk, Russia (aristidov/Wikipedia, CC BY 3.0)

After the Iron Curtain fell, the disturbing scale of this legacy came to light. [It was revealed that at Andreyeva Bay](#), a nuclear submarine refueling site just 60 kilometers from the Norwegian border, 600,000 metric tons of irradiated water leaked into the Barents Sea from a nuclear fuel storage pool in 1982. The site contained 22,000 spent nuclear fuel assemblies pulled from more than 100 subs, many kept in rusted containers stored in the open air.

Fearing contamination, Norway spearheaded a sweeping cleanup effort with other Western nations. Combined they spent more than \$1 billion to dismantle 197 decommissioned Soviet nuclear subs that rusted dockside, still loaded with spent nuclear fuel. One thousand Arctic navigation beacons powered by strontium batteries were replaced, many with solar powered units provided by the Norwegians.

### What is still in the sea?

Like numerous other countries, including the United States, the Soviet Union had a habit of dumping its radioactive problems at sea.

The 1993 White Book—a sort of confession to this dumping published by crusading ecologist Alexei Yablokov when serving as Boris Yeltsin’s environmental minister—outlined the scope of the problem, though for years its revelations continued to be viewed by many in the Russian government as state secrets.







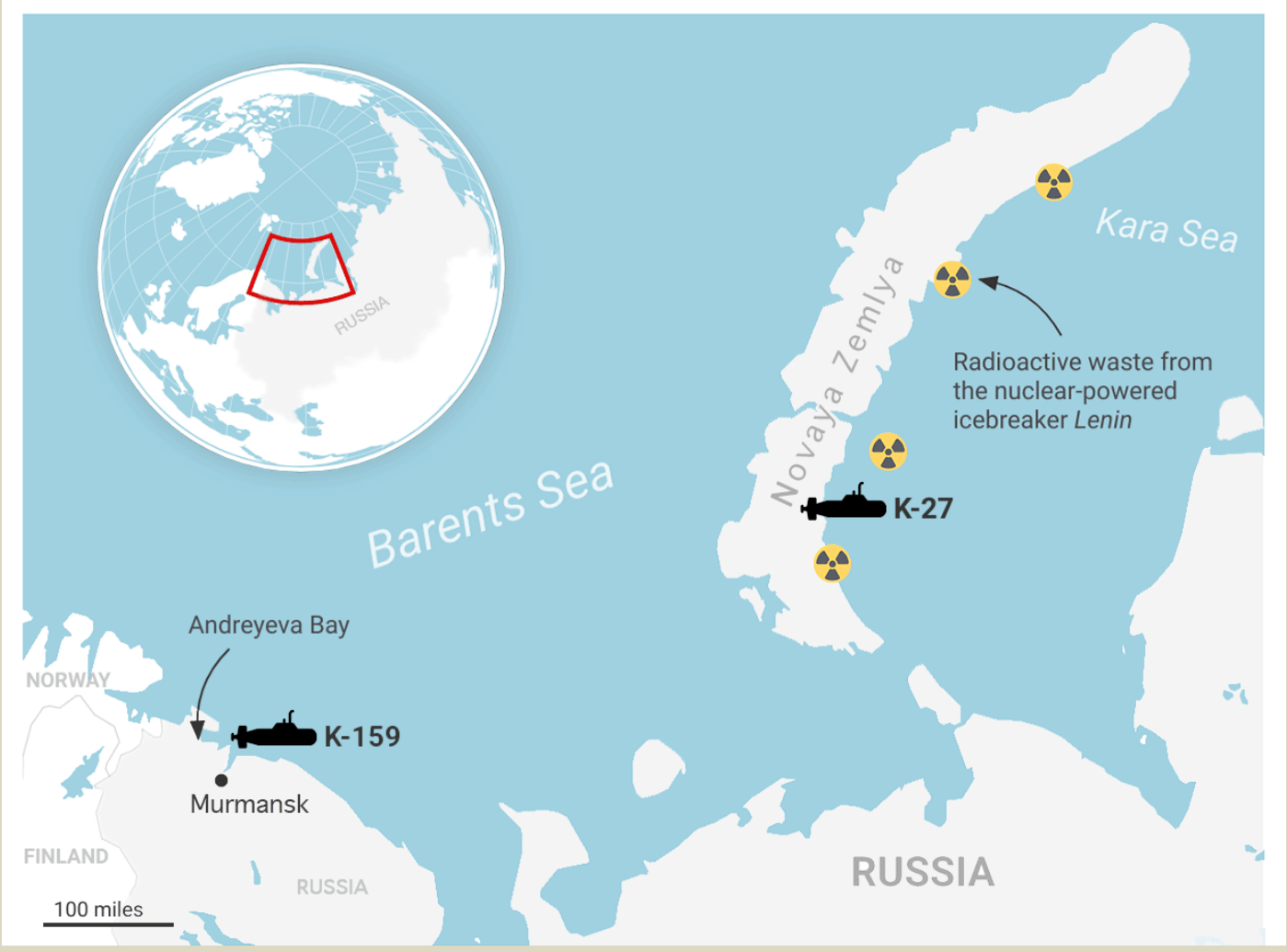
A 2019 feasibility study for the sub lifting project, drawn up by the Norwegian Radiation and Nuclear Safety Authority with the help of other European nuclear safety agencies, confirmed Yablokov's data and laid bare what the Soviets had intentionally sunk: 18,000 radioactive objects, including 19 vessels and 14 nuclear reactors.

While the radiation emitted by most of these cast offs has been smothered to near background levels thanks to decades of built-up undersea silt, a study by the Russian Academy of Sciences nonetheless identified 1,000 objects that still produce high levels of gamma radiation.

Ninety percent of that radiation is emitted by six objects that Rosatom, Russia's state nuclear firm, has deemed urgent and targeted for lifting: two nuclear submarines; the reactor compartments from three nuclear submarines; and the reactor from the legendary icebreaker Lenin.

## The Arctic's top priority nuclear waste cleanup sites

 Sunken submarine      Dump sites for reactors, components, and spent nuclear fuel containers



Of 1,000 underwater objects still emitting high-level gamma radiation, 90 percent is from just six objects. (Map by Thomas Gaulkin / Datawrapper / OpenStreetMap contributors)

“We consider even the extremely low probability of radioactive materials leaking from these objects as posing an unacceptable risk for the ecosystems of the Arctic,” Anatoly Grigoriev, Rosatom’s head of international technical assistance, said in July.

The two nuclear submarines—which together contain one million curies of radiation, or about a quarter of that released in the first month of the Fukushima disaster—pose the greatest challenge to lift and have received most of the press.







Bow of K-27



Stern of K-27



Tower (front view)



Tower (back view) and rails



Stern hatch



Bow anchor

Figure 4.4. The nuclear submarine K-27 in the outer part of the Stepovogo Fjord.

The first of these is the K-27. Launched in 1962, the 360-foot sub suffered a radiation leak in one of its experimental liquid-metal cooled reactors after just three days at sea. Over the next several years, the Soviet navy attempted to repair or replace the reactors, but in 1979, they gave up and decommissioned the vessel.

Too radioactive to be dismantled conventionally, the K-27 was towed to the Arctic Novaya Zemlya nuclear testing range in 1982 and scuttled in one of the archipelago's fjords at a depth of just 33 meters. The sinking took some effort. The sub was weighed down by asphalt to seal its fuel-filled reactor and a hole was punched in its aft ballast tank to swamp it.

But the fix won't last forever. The sealant around the reactor was only meant to stave off radiation leaks until 2032. More troubling still is that the K-27's highly enriched fuel could, in the right circumstances, generate an uncontrolled nuclear chain reaction leading to a significant local release of radiation.

The other submarine, the K-159, was in use from 1963 to 1989. It was added to the toxic subsea catalog in 2003, after the Cold War's end. But its position north of Murmansk, astride some of the Barents Sea's most fertile fishing grounds and busiest shipping lanes, has made it a source of special anxiety. Already a 305-foot

rust bucket from years of neglect, the K-159 sank while being towed to a Murmansk shipyard for dismantlement, killing nine sailors who were on board to bail out water in transit.

Unlike the K-27, however, no safeguards to secure the K-159's two reactors were put in place before it sank, meaning it went down loaded with 800 kilograms of spent uranium fuel.

**The danger the subs pose to the environment**

Expeditions to the subs in recent years haven't revealed serious upticks in contamination beyond background radiation levels. A [joint Norwegian-Russian mission](#) to the K-159 in 2018 discovered breakage along the sub's hull, but, as in years previous, reported no elevated radiation levels in sediment and seawater samples.

Similarly, [a Russian expedition](#) to measure radioactivity around the K-27 this past October, which charted contamination levels in glaciers surrounding Novaya Zemlya, found nothing amiss.

Photo: JOINT NORWEGIAN-RUSSIAN EXPERT GROUP for investigation of Radioactive Contamination in the Northern Areas





But experts from both sides of the Russian border say that such circumstances won't last. Officials at the Norwegian Radiation and Nuclear Safety Authority insist that leaks from the K-159 are only a matter of time—and that even rumors of increased contamination could damage the Arctic fishing industry.

Alexander Nikitin—a former Russian Navy submarine captain with Norway's Bellona Foundation who sat on Rosatom's public advisory council before it disbanded over the Ukraine war—agreed. In his accounting, the subs will continue to degrade and slowly release cesium 137 and strontium as water seeps into the reactors.

A [2013 study](#) by Norway's Institute of Marine Research used computer simulations to model what impact that might have on local populations of cod and capelin, Norway's Arctic cash crop. The study showed that if all the radioactive material from the K-159's reactors were to be released in a single "pulse discharge," it would increase the levels of slow-decaying cesium 137 in the muscles of cod in the eastern Barents Sea at least 100 times.

That would still be below limits set by the Norwegian government following the Chernobyl disaster in 1986. "Here the question is that some of the radionuclides leached out of the reactors can get into fish—and the fish onto someone's dinner table," Nikitin said. "It's difficult to estimate the impact."

Even low doses, he said, would be enough to scare consumers off Norwegian fish. As of 2021—a decade after the Fukushima accident — there were [still 15 countries](#) banning the import of seafood from Japan, despite numerous studies establishing acceptably low concentrations of radionuclides in fish caught in that area.

By one estimate, a ban on fish from the Kara and Barents Seas could cost the Norwegian and Russian economy a combined \$140 million a month—an economic hardship that some say would be worse than any direct environmental damage.

### Will Russia do it alone?

Moscow has stumbled in its first solo steps on this project. As [recounted](#) with unusual candor by Atomnya Energia, a Russian nuclear industry trade publication supported largely by Rosatom itself, the project can't even secure financing from Russia's Ministry of Finance, which called Rosatom's cost projections "insufficiently substantiated."

"But how can I substantiate the cost of work that has never been done before?" the publication quoted Rosatom's Grigoriev as lamenting. Russia also blew past a deadline to deliver an overarching road map outlining how the project would be undertaken due to bureaucratic confusion and squabbles.

One problem: Russia lacks the kind of special vessels that can lift a submarine. The last time the country attempted such an operation, the Kursk, a 17,000-metric ton vessel, sank during a military exercise in August 2000. That botched rescue attempt fueled indignation at Putin, who was then less than a year into his first presidential term.

After delaying the arrival of Norwegian rescue divers to the Kursk for nine days, during which time the surviving crew perished, the Kremlin was quick to invite the Dutch companies Mammoet and Smit International to coordinate the technically demanding raising of the wreck a little more than a year later.

With the Dutch, and anyone else, almost surely unwilling to help, Russia is alone with trying to build its own salvage vessels to lift the K-27 and K-159—ship construction that would inflate the estimate cost of the lifting operation by another several million dollars. Numerous designs for such a ship have been batted about—employing anything from balloons to giant pincers to lift the subs—but nothing has come of them. At the July conference, Oleg Vlasov, who heads Malakhit, Russia's federal marine engineering bureau, complained that he didn't have enough technical information about the wrecks from Rosatom, despite the numerous expeditions to them, to even begin designing such a vessel.

"We've been talking too much and for too long," Oleg Vlasov, who heads Russia's federal marine engineering bureau, warned Rosatom in July. If Russia doesn't act soon, he said, the vessels will become so enfeebled in their watery graves that it might be safest to leave them where they are. It is this scenario that Nikitin finds the most likely after the invasion of Ukraine.

"The issue of lifting these sunken objects will continue to be postponed and obscured, and the authorities will begin to explain that they don't pose a serious threat, and that over time they'll become safer, and so on," he said.

He added that none of the Rosatom meetings about the sub lift that he attended prior to the invasion of Ukraine had focused on Russia building its own vessels to lift the subs. Rather, they focused on which countries to ask to lift them.

But Nikitin and other members of Russian civil society who made up Rosatom's public council won't be attending more such meetings in the foreseeable future. And transparency on the Russian side—honed over many difficult years—might be one of the biggest environmental casualties of Moscow's invasion of Ukraine.

**Charles Digges** is the editor of [Bellona.org](#), the environmental news pages of the Bellona Foundation of Oslo, Norway, where he primarily covers issues related to the Russian civilian and military nuclear complex. Previously he lived and worked in Russia as a reporter and editor for *The St Petersburg Times* and *The Moscow Times*.







# China nuclear warhead stockpile to reach **1,500** by 2035 if it continues its build-up pace, US says

Source: <https://www.abc.net.au/news/2022-11-30/china-nuclear-warhead-stockpile-to-reach-1500-by-2035-pentagon/101714288>

Nov 30 – China will likely have a stockpile of 1,500 nuclear warheads by 2035 if it continues with its current nuclear build-up pace,

according to a report released by the Pentagon.

The figure underscores mounting US concerns about China's intentions for its expanding nuclear arsenal, even though the projections do not suggest China is accelerating the pace of its already-brisk warhead development.

"They've got a rapid build-up that is kind of too substantial to keep under wraps," a senior US defence official said during a news briefing on the Pentagon's annual report on China's military.

"It does raise questions about whether they're kind of shifting away from a strategy that was premised on what they referred to as a 'lean and effective deterrent'."

The report, which primarily covers activities in 2021, said China has a nuclear stockpile of more than 400 warheads.



And the Pentagon's projection for [China's nuclear arsenal of 1,000 warheads by 2030 remained unchanged](#), the official said, adding the projection for 2035 was based on an unchanged pace of expansion.

China says its arsenal is dwarfed by those of the United States and Russia, and that it is ready for dialogue, but only if Washington reduces its nuclear stockpile to China's level.

The United States has a stockpile of about 3,700 nuclear warheads, of which roughly 1,740 were deployed — or readied for use — according to the Stockholm International Peace Research Institute (SIPRI) think-tank. Chinese leader Xi Jinping signalled during a Communist Party Congress in October that China would strengthen its strategic deterrent, a term often used to describe nuclear weapons.



The report reiterated concern about increasing pressure by Beijing on self-ruled Taiwan, an island that China sees as a breakaway province. However, **the US official said Washington did not see an invasion of Taiwan as imminent.**

## Iran's Centrifuges: Models and Status

Source: <https://www.iranwatch.org/our-publications/weapon-program-background-report/irans-centrifuges-models-status>

Nov 30 – Iran possesses thousands of gas centrifuges that are the mainstay of its nuclear program. Gas centrifuges spin uranium hexafluoride gas (UF6) to separate uranium isotopes suitable for nuclear fuel, a process known as uranium enrichment.<sup>[1]</sup> The number and capacity of these machines determine Iran's "breakout" time: how long it would take Iran—if it decided to do so—to produce the fuel for a small nuclear arsenal. The machines are also key to Iran's ability to "sneakout" by producing nuclear weapon fuel at secret sites.



In recent years, Iran has developed and deployed centrifuge models that can enrich greater amounts of uranium with fewer machines relative to its original IR-1 design. Iran's increasing mastery of centrifuge design and manufacturing raises the risk of a "sneakout," and it reflects an acquisition of knowledge that cannot be reversed.





### ICI C<sup>2</sup>BRNE DIARY – December 2022

The table below sets out the capacity and primary materials of each of Iran’s currently-deployed centrifuge models, as well as the number of each model known from publicly-available IAEA reports<sup>[2]</sup> to be installed and/or enriching uranium at Iran’s three declared enrichment sites: the Fuel Enrichment Plant (FEP) and Pilot Fuel Enrichment Plant (PFEP) at Natanz and the Fordow Fuel Enrichment Plant (FFEP) at Fordow.

In addition to the models listed in the table, Iran has developed several other centrifuge designs that are not currently installed at any of its declared sites, including the IR-2, IR-3, IR-6m, IR-6sm, IR-6smo, IR-8s, and IR-9s.

The information in the table about the number of centrifuges installed or operating is based on IAEA reports. The information on centrifuge capacity and rotor material is based on a November 2021 Iran Watch report, [Beyond the IR-1: Iran’s Advanced Centrifuges and their Lasting Implications](#), which contains analysis of each centrifuge model.

MODEL	CAPACITY (SWU/yr) <sup>[3]</sup>	ROTOR ASSEMBLY MATERIAL <sup>[4]</sup>	FIRST TESTED <sup>[5]</sup>	# INSTALLED	# IN PRODUCTION MODE <sup>[6]</sup>
IR-1	~0.8 <sup>[7]</sup>	Aluminum + maraging steel	Late 1990s	Total: 7187 at FEP: <sup>[11]</sup> 6124 at PFEP: 18 at FFEP: 1045	Total: 6848 at FEP: <sup>[11]</sup> 5786 at PFEP: 18 at FFEP: 1044
IR-2m	~4-5 <sup>[8]</sup>	Maraging steel + carbon fiber	2009	Total: 2681 at FEP: <sup>[12]</sup> 2610 at PFEP: 71 at FFEP: 0	Total: 1110 at FEP: <sup>[12]</sup> 1044 at PFEP: 66 at FFEP: 0
IR-4	~4-5 <sup>[8]</sup>	Carbon fiber	2009	Total: 713 at FEP: <sup>[12]</sup> 522 at PFEP: 191 at FFEP: 0	Total: 537 at FEP: <sup>[12]</sup> 348 at PFEP: 189 at FFEP: 0
IR-5	6-10 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2013	Total: 38 at FEP: 0 at PFEP: <sup>[13]</sup> 38 at FFEP: 0	Total: 35 at FEP: 0 at PFEP: <sup>[13]</sup> 35 at FFEP: 0
IR-6	6-10 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2013	Total: 1048 at FEP: 522 at PFEP: 194 at FFEP: 332	Total: 1047 at FEP: 522 at PFEP: 193 at FFEP: 332
IR-6s	3-6 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2013	Total: 40 at FEP: 0 at PFEP: <sup>[13]</sup> 40 at FFEP: 0	Total: 39 at FEP: 0 at PFEP: <sup>[13]</sup> 39 at FFEP: 0
IR-7	11-20 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2019	Total: 1 at FEP: 0 at PFEP: 1 at FFEP: 0	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0
IR-8	16-24 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2017	Total: 1 at FEP: 0 at PFEP: 1 at FFEP: 0	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0
IR-8B	10-15 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2019	Total: 1	Total: 0







MODEL	CAPACITY (SWU/yr) <sup>[3]</sup>	ROTOR ASSEMBLY MATERIAL <sup>[4]</sup>	FIRST TESTED <sup>[5]</sup>	# INSTALLED	# IN PRODUCTION MODE <sup>[6]</sup>
				at FEP: 0 at PFEP: 1 at FFEP: 0	at FEP: 0 at PFEP: 0 at FFEP: 0
IR-s	8-12 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2019	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0
IR-9	34-50 <sup>[9]</sup>	Carbon fiber <sup>[10]</sup>	2021	Total: 1 at FEP: 0 at PFEP: 1 at FFEP: 0	Total: 0 at FEP: 0 at PFEP: 0 at FFEP: 0

Footnotes

- [1] Natural uranium contains about 0.7 percent of the fissionable isotope U-235. Uranium is considered enriched when the concentration of U-235 is increased. Uranium enriched up to 5 percent concentration of U-235 is suitable for nuclear reactors. Weapons-grade uranium is usually defined as 90 percent U-235.
- [2] As of November 10, 2022.
- [3] The capacity of a centrifuge is measured in “separative work units” (SWU) per year. SWU reflect the effort needed to separate the two uranium isotopes (U-235 and U-238) in the enrichment process. A centrifuge with a higher SWU per year can enrich greater quantities of uranium to higher levels in shorter periods of time than a less efficient centrifuge.
- [4] The rotor of a centrifuge is what spins the uranium hexafluoride (UF6) gas to separate uranium isotopes. Centrifuges use “bellows” between rotors to form a rotor assembly that allows for flexibility when spinning at higher speeds. The bellows and the rotors themselves must be made with strong, lightweight material. Carbon fiber is an ideal material for this purpose, but aluminum and specialty steels such as maraging steel can also be used.
- [5] Fed with UF6; excludes mechanical testing.
- [6] Accumulating enriched uranium
- [7] Calculated from output data contained in IAEA reports.
- [8] Based on the capacity of the Pakistani P2 centrifuge, the base model for the IR-2m and IR-4.
- [9] The low end of the range is based on estimates contained in "A Comprehensive Survey of Iran's Advanced Centrifuges" by David Albright, Sarah Burkhard, and Spencer Faragasso, published by The Institute for Science and International Security on December 2, 2021 and available at <https://isis-online.org/isis-reports/detail/a-comprehensive-survey-of-ir...> the high end of the range consists of nominal claims made by Iranian officials or Iranian media (possibly referring to kg UF6 SWU/yr, which has a value 1.47 times higher than the more standard kg U SWU/yr).
- [10] Due to technological progression, centrifuges developed after the IR-4 are assumed to have their rotor assembly made entirely from carbon fiber even when not explicitly confirmed as such.
- [11] The figure for installed IR-1 centrifuges is arrived at by adding the number of additional machines installed (40) as reported in [GOV/2022/62](#) Para. 21 to the total planned in the Iranian DIQ (6084) as reported in [GOV/INF/2021/27](#) Para. 3. The figure for IR-1 centrifuges in production mode assumes that the two cascades reported in [GOV/2022/62](#) Para. 21 to be installed but not being fed uranium are not among the newly-reconfigured 174-machine cascades. It applies an average of 169 machines per cascade (obtained by dividing the 6084 total planned machines in the DIQ by the 36 total planned cascades) and then adds 40 to account for the additional machines installed in the four newly-configured cascades.
- [12] The IR-2m and IR-4 figures for FEP are an estimate based on an average of 174 machines per cascade, obtained by dividing the total number of machines planned in the Iranian DIQ reported in [GOV/INF/2021/27](#) Para. 3 (1044) by the number of planned cascades (6). That average (174) is multiplied by the number of cascades reported in [GOV/2022/62](#) Para. 21 to be both installed and in production mode. Although Iran subsequently increased the number of planned IR-2m cascades in its updated DIQ as reported in [GOV/INF/2022/17](#) Para. 7 and [GOV/INF/2022/23](#) Para. 3, there is no indication that it altered the number of centrifuges contained in each cascade.
- [13] Figures for IR-5 and IR-6s centrifuges in R&D Line 5 at PFEP are calculated using the IAEA's most recent reporting on the number of centrifuges comprising the cascade in R&D Line 1, verified on August 15, 2021 (see [GOV/INF/2021/40](#) Para. 4). Iran informed the IAEA on August 2, 2022, that it had swapped





the numbering of R&D Lines 1 and 5 (see [GOV/2022/39](#) Para. 23). Therefore, R&D Line 5 after August 2, 2022, corresponds to R&D Line 1 before that date.

## Nuke Kiev

Source: <https://nuclearsecrecy.com/nukemap/>

Weapon: 100MT | Airburst

**NUKEMAP** 2.72 : FAQ [MISSILEMAP](#)

1. Drag the marker to wherever you'd like to target.  
Or you can select a preset...  
Or type in the name of a city:

2. Enter a yield (in kilotons):   
"Tsar Bomba" – largest USSR bomb designed (100 Mt)

3. Basic options: Height of burst:   Airburst  Surface  
Other effects:  Casualties  Radioactive fallout

Advanced options: ▶

4. Click the "Detonate" button below.

Note that you can drag the target marker after you have detonated the nuke.

Estimated fatalities: **2,055,070**  
Estimated injuries: **1,025,780**

In any given 24-hour period, there are on average 3,990,268 people in the light (1 psi) blast range of the simulated detonation.

Modeling casualties from a nuclear attack is difficult. These numbers should be seen as evocative, not definitive. Fallout effects are deliberately ignored, because they can depend on what actions people take after the detonation. For more information about the model, [click here](#).

Effect distances for a 100 megaton airburst: ▼

- Fireball radius: 6.1 km (117 km<sup>2</sup>)
- Maximum size of the nuclear fireball; relevance to damage on the ground depends on the height of detonation. If it touches the ground, the amount of radioactive fallout is significantly increased. Anything inside the fireball is effectively vaporized. Minimum burst height for negligible fallout: 5.49 km.
- Moderate blast damage radius (5 psi): 32.6 km (3,350 km<sup>2</sup>)
- At 5 psi overpressure, most residential buildings collapse, injuries are universal, fatalities are widespread. The chances of a fire starting in commercial and residential damage are high, and buildings so damaged are at high risk of spreading fire. Often used as a benchmark for **moderate** damage in cities. Optimal height of burst to maximize this effect is 14.5 km.
- Thermal radiation radius (3rd degree burns): 73.7 km (17,080 km<sup>2</sup>)
- Third degree burns extend throughout the layers of skin, and are often painless because they destroy the pain nerves. They can cause severe scarring or disablement, and can require amputation. 100% probability for 3rd degree burns at this yield is 13.9 cal/cm<sup>2</sup>.
- Light blast damage radius (1 psi): 91.8 km (26,450 km<sup>2</sup>)
- At a around 1 psi overpressure, glass windows can be expected to break. This can cause many injuries in a surrounding population who comes to a window after seeing the flash of a nuclear explosion (which travels faster than the pressure wave). Often used as a benchmark for **light** damage in cities. Optimal height of burst to maximize this effect is 21.7 km.

\*Detonation altitude: 14,490 m. (Chosen to maximize the 5-psi range.)

The following errors were encountered trying to implement these settings:

- The blast pressure equation for 20 psi failed to give a result for the given yield and height settings. The maximum detonation height for this effect to be felt on the ground is 13.1 km.
- The initial nuclear radiation equation for 500 rem failed to give a result for the given yield and height settings. The maximum detonation height for this effect to be felt on the ground is 6.99 km.

In any given 24-hour period, there are on average 3,990,268 people in the light (1 psi) blast range of the simulated detonation. Modeling casualties from a nuclear attack is difficult. These numbers should be seen as evocative, not definitive. Fallout effects are deliberately ignored, because they can depend on what actions people take after the detonation.

### Effect distances for a 100 megaton airburst\*:

**Fireball radius: 6.1 km (117 km<sup>2</sup>)**

Maximum size of the nuclear fireball; relevance to damage on the ground depends on the height of detonation. If it touches the ground, the amount of radioactive fallout is significantly increased. Anything inside the fireball is effectively vaporized. Minimum burst height for negligible fallout: 5.49 km.

**Moderate blast damage radius (5 psi): 32.6 km (3,350 km<sup>2</sup>)**

At 5 psi overpressure, most residential buildings collapse, injuries are universal, fatalities are widespread. The chances of a fire starting in commercial and residential damage are high, and buildings so damaged are at high risk of spreading fire. Often used as a benchmark for **moderate** damage in cities. Optimal height of burst to maximize this effect is 14.5 km.

**Thermal radiation radius (3rd degree burns): 73.7 km (17,080 km<sup>2</sup>)**

Third degree burns extend throughout the layers of skin, and are often painless because they destroy the pain nerves. They can cause severe scarring or disablement, and can require amputation. 100% probability for 3rd degree burns at this yield is 13.9 cal/cm<sup>2</sup>. **Light blast damage radius (1 psi): 91.8 km (26,450 km<sup>2</sup>)**

At a around 1 psi overpressure, glass windows can be expected to break. This can cause many injuries in a surrounding population who comes to a window after seeing the flash of a nuclear explosion (which travels faster than the pressure wave). Often used as a benchmark for **light** damage in cities. Optimal height of burst to maximize this effect is 21.7 km.

\*Detonation altitude: 14,490 m. (Chosen to maximize the 5-psi range.)

The following errors were encountered trying to implement these settings:

- The blast pressure equation for 20 psi failed to give a result for the given yield and height settings. The maximum detonation height for this effect to be felt on the ground is 13.1 km.
- The initial nuclear radiation equation for 500 rem failed to give a result for the given yield and height settings. The maximum detonation height for this effect to be felt on the ground is 6.99 km.







Note: Rounding accounts for any inconsistencies in the above numbers. Also, yields above 20 Mt are derived from a scaling of 20 Mt yields, and are not as validated as those under 20 Mt.

**Fallout:** Your choice of burst height is too high to produce significant local fallout. The minimum burst height to produce appreciable fallout for a yield of 100 megaton is 5.49 km.

●► Watch also: [Video](#)

## Broken promises: how nuclear armed states are failing on their commitments to disarm

Source: [https://www.icanw.org/nuclear\\_weapons\\_modernisation\\_russia\\_china\\_us\\_failing\\_commitments\\_to\\_disarm](https://www.icanw.org/nuclear_weapons_modernisation_russia_china_us_failing_commitments_to_disarm)



Dec 02 – As the US Air Force shows off its new B-21 stealth bomber and Russia and China are expanding and updating their own nuclear arsenals, we explore how these states are violating their commitments under international law and increasing the risk of nuclear catastrophe.

The United States Air Force today showed off its latest means of using weapons of mass destruction: the B-21 stealth bomber. This aircraft, developed by Northrop Grumman, [is designed to](#) drop two new types of nuclear weapons: the B61-12 nuclear gravity bomb and the LRSO nuclear-armed air-launched cruise missile, as well as various conventional weapons. The B61-12 nuclear bomb has an explosive yield of [up to 50 kilotons](#); in comparison, the bomb that destroyed Hiroshima in 1945, killing more than 140,000 people, had a yield of just 16 kilotons.

A single B61-12 bomb dropped by a Northrop Grumman B-21 would likely kill hundreds of thousands of civilians and injure many more, and cause massive damage to civilian infrastructure and the environment; radioactive fallout could contaminate large areas across multiple countries.

The development of the B-21 represents yet another step in the modernisation of the US nuclear arsenal. The B-21 bomber will [reportedly be deployed](#) at three bases in the US, resulting in an increase of the number of bomber bases with nuclear weapons from two bases today to five bases by the 2030s. The B-





21 will carry new and “improved” nuclear weapons, and is obviously intended to do so for decades to come.

Northrop Grumman, the manufacturer of the B-21, received \$5 billion in income from nuclear-weapon-related contracts in 2021, and spent \$11 million on lobbying elected officials, including those who approve such contracts. The company also contributed several million dollars to think tanks researching and writing about nuclear weapons. [Source](#).

But the US is certainly not alone: Russia and China are also expanding and updating their nuclear arsenals. Russia has developed and successfully tested its new [Sarmat ICBM](#); the missile was displayed in public in November. The [Sarmat](#) is intended to replace the SS-18 ICBM and will likely carry the same warheads: 10 warheads per missile, each with a yield of 500-800 kilotons. That means that one Sarmat missile could carry the same destructive force as at least 250 Nagasaki-size warheads, only one of which killed 74,000 people in 1945. According to a [US report](#), China has recently increased its nuclear arsenal beyond 400 warheads, and now has 300 ICBMs, an increase of 200 since 2021. Chinese nuclear submarines are reportedly now patrolling while armed with nuclear missiles. (Since both Russia and China are much less transparent than the US about their nuclear capabilities, it is possible that they are also modernizing and expanding their arsenals in other ways.)

All these steps by China, Russia and the US are directly contrary to their obligations under the [Nuclear Non-proliferation Treaty \(NPT\)](#). The NPT requires them to “pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament”. [Under the NPT](#), the three countries have made an “unequivocal undertaking ... to accomplish the total elimination of their nuclear arsenals” and have committed to “pursue policies that are fully compatible with the Treaty and the objective of achieving a world without nuclear weapons”.

In light of this, the Executive Director of ICAN, Beatrice Fihn, said: “These developments show once again that nuclear-armed states cannot be trusted to pursue nuclear disarmament in good faith. Modernising their arsenals is risking a new nuclear arms race and is incompatible with the objective of achieving a world without nuclear weapons. This is particularly disturbing and dangerous, given the sharply heightened risk of use of nuclear weapons.”

With Russia’s threats to use nuclear weapons against anyone intervening in the the Ukraine conflict, responses from other governments that imply possible retaliation with nuclear weapons, commentary and analysis examining scenarios in which nuclear weapons might be used, recent military exercises involving nuclear weapons, and testing by North Korea of nuclear-capable ballistic missiles, many observers agree that the idea of using nuclear weapons is being normalised, and the decades-old taboo against their use is being eroded. Governments, analysts and anti-nuclear campaigners have all been warning that the risk of nuclear conflict is now as high as it has ever been.

ICAN Executive Director, Beatrice Fihn, commented “This is why the [Treaty on the Prohibition of Nuclear Weapons \(TPNW\)](#) is so important. Now that the treaty is in force, nuclear weapons are comprehensively prohibited under international law. By joining the TPNW and participating actively in its implementation, countries can contribute to stigmatising and delegitimising nuclear weapons and building a robust global norm against them. The TPNW is clear: the actions of nuclear-armed states to retain, modernize and expand their nuclear arsenals are illegal, immoral and unacceptable,”

You can share an article by clicking on the share icons at the top right of it.

The total or partial reproduction of an article, without the prior written authorization of [Le Monde](#), is strictly forbidden.

For more information, see our [Terms and Conditions](#).

For all authorization requests, contact [droitsdauteur@lemonde.fr](mailto:droitsdauteur@lemonde.fr).

[https://www.lemonde.fr/en/energies/article/2022/12/04/iran-begins-construction-of-new-nuclear-power-plant\\_6006520\\_98.html](https://www.lemonde.fr/en/energies/article/2022/12/04/iran-begins-construction-of-new-nuclear-power-plant_6006520_98.html)

## Iran begins construction of **new** nuclear power plant

Source: [https://www.lemonde.fr/en/energies/article/2022/12/04/iran-begins-construction-of-new-nuclear-power-plant\\_6006520\\_98.html](https://www.lemonde.fr/en/energies/article/2022/12/04/iran-begins-construction-of-new-nuclear-power-plant_6006520_98.html)

Dec 04 – Iran on Saturday began construction on a new nuclear power plant in the country's southwest, Iranian state TV announced, amid tensions with the US over sweeping sanctions imposed after Washington pulled out of the Islamic Republic's nuclear deal with world powers.

The announcement comes as Iran has been rocked by nationwide protests challenging the theocratic government that began after the death of a young woman in police custody over an allegedly violation of the Islamic dress code. In a possibly related move, Iran's semi-official IRNA news agency late Saturday,







December 3, quoted a top prosecutor as saying officials had "closed" the morality police force responsible for enforcing the dress code. It gave no details.



The new 300-megawatt plant, **known as Karoon**, will take **eight years to build** and cost around \$2 billion, the country's state television and radio agency reported. The plant will be located in Iran's oil-rich **Khuzestan province**, near its western border with Iraq, it said. The construction site's inauguration ceremony was attended by Mohammed Eslami, head of Iran's civilian Atomic Energy Organization, who first unveiled construction plans for Karoon in April. Iran has one nuclear power plant at its southern port of Bushehr that went online in 2011 with help from Russia, but also several underground nuclear facilities.

**One step away**

The announcement of Karoon's construction came less than two weeks after Iran said it had begun producing enriched uranium at 60% purity at the country's underground Fordo nuclear facility. The move is seen as a significant addition to the country's nuclear program. Enrichment to 60% purity is one short,

technical step away from weapons-grade levels of 90%. Non-proliferation experts have warned in recent months that Iran now has enough 60%-enriched uranium to reprocess into fuel for at least one nuclear bomb.

The move was condemned by Germany, France and Britain, the three Western European nations that remain in the Iran nuclear deal. Recent attempts to revive Iran's 2015 nuclear deal, which eased sanctions on Iran in exchange for curbs on its nuclear program, have stalled.

**Amid nationwide protests**

Since September, Iran has been roiled by nationwide protests that have come to mark one of the greatest challenges to its theocracy since the chaotic years after its 1979 Islamic Revolution. In a statement issued by the state-run IRNA news agency Saturday, the country's national security council announced that some 200 people have been killed during the protests, the body's first official word on the casualties. Last week, Iranian General Amir Ali Hajizadeh tallied the death toll at more than 300 .

The contradictory tolls are lower than the toll reported by Human Rights Activists in Iran, a US-based organization that has been closely monitoring the protest since the outbreak. In its most recent update, the group says that 469 people have been killed and 18,210 others detained in the protests and the violent security force crackdown that followed.

**Nuclear deal**

We are interested in your experience using the site.

The United States unilaterally pulled out of the Iran nuclear deal – formally known as the Joint Comprehensive Plan of Action, or JCPOA – in 2018, under then-President Donald Trump. It reimposed sanctions on Iran, prompting Tehran to start backing away from the deal's terms. Iran has long denied ever seeking nuclear weapons, insisting its nuclear program is peaceful.

**EIDTOR'S COMMENT:** Karoon, Bushehr and Barakah (UAE) – the Arab Gulf is turning nuclear. Cross your fingers!

**Radiological risk assessment caused by RDD terrorism in an urban area**

By Hyojoon Jeong , Misun Park, Haesun Jeong, et al

*Appl Radiat Isot.* 2013 Sep; 79:1-4.

Source: <https://www.sciencedirect.com/science/article/abs/pii/S0969804313002030>

**Abstract**

This paper specifically discusses a radiological risk assessment due to RDDs (Radiological Dispersion Devices) containing Cs-137 in the metropolitan area of Seoul, South Korea. The comparison of an effective dose caused by airborne plume and deposited Cs-137 is performed with and without consideration of the wind direction. When the dose is computed conservatively, an effective dose is around twice that of a dose computed realistically. Monte Carlo simulations showed that the 95% confidence interval for morbidity was 2.40×10(-5) to 8.55×10(-5), and mortality was 3.53×10(-5) to 1.25×10(-4).





## A Game Theoretical Model of Radiological Terrorism Defense

By Shraddha Rane and Jason Timothy Harris

*IJNS, Vol. 7 (2020); No. 2*

Source: <https://trace.tennessee.edu/ijns/vol7/iss2/7/>

### Abstract

Radiological dispersal devices (RDD) pose a threat to the United States. Healthcare facilities housing high-risk radioactive materials and devices are potentially easy targets for unauthorized access and are vulnerable to malevolent acts of theft or sabotage. The three most attractive candidates for use in RDD considered in this study are: <sup>60</sup>Co (radiosurgery devices), <sup>137</sup>Cs (blood irradiators) and <sup>192</sup>Ir (brachytherapy high dose radiation device). The threat posed by RDDs has led to evaluating the security risk of radioactive materials and defending against attacks. The concepts of risk analysis used in conjunction with game theory lay the foundations of quantitative security risk management. This paper develops a two player non-cooperative one-shot simultaneous defender-attacker game. The defender (healthcare facility) chooses to defend one of the three high-risk radioactive material targets and the attacker (terrorists or adversaries) chooses to attack one of the three high-risk radioactive material targets. A risk-informed approach is used to model players' payoffs or expected utilities for each choice of strategies. A game-theoretic model (RDD game) captures the strategic interaction between competing players who act rationally to maximize their expected utility. The evaluation of the RDD game results in a von Neuman max-min strategy solution being preferable to a mixed strategy Nash equilibrium solution. The von Neumann max-min strategy solution of the defender defending cobalt and the attacker attacking cesium is found to be the most prescriptive result, thus favoring the current efforts of phasing out cesium blood irradiators and replacing them with alternative technologies. The RDD game not only gives the defender strategic options to budget scarce security resources but also helps healthcare facilities make optimal choices under severe uncertainty about the terrorist threat.

## Iran Building Nuclear Weapons

By David Albright

*December 05, 2022*

Source: <https://www.homelandsecuritynewswire.com/dr20221205-iran-building-nuclear-weapons>

### Background

- ❖ Rather than a traditional nuclear weapons program, Iran threatens the world with a program ready to produce nuclear weapons "on-demand." Its readiness program poses a difficult challenge to the international community and the International Atomic Energy Agency (IAEA).
- ❖ Due to its past, large-scale nuclear weapons program, called the Amad Plan, Iran has a readiness program with less need for secret nuclear weapon development activities. Iran has advanced its nuclear weapons readiness under civilian nuclear and military non-nuclear cover projects. Using a civilian cover, Iran has in recent years successfully produced highly enriched uranium (HEU) and near HEU metal.
- ❖ Understanding the pace of Iran building nuclear weapons matters, in particular, for designing strategies against Iran moving to construct them.

### Findings

- ❖ Iran is increasingly viewed as a nuclear power, yet it has so far not been subjected to harsh international and regional penalties.
- ❖ Iran has multiple pathways to build nuclear weapons: (1) Reviving and completing the Amad Plan with a capability of serially producing many warheads suitable for ballistic missiles (and possibly cruise missiles); (2) launching an accelerated effort to achieve a few crude nuclear weapons; or (3) a combination of both. Iran's likelier pathway to nuclear weapons is the pursuit of both an accelerated approach and a revival of the Amad Plan.
- ❖ The time needed to revive and complete the Amad Plan is estimated as two years, at which point Iran would have produced its first missile-delivered nuclear warhead and created the infrastructure for serial warhead production.
- ❖ An accelerated program, benefiting from earlier Amad work, could produce its first crude nuclear weapon in six months. Too often, the missile warhead pathway is overemphasized.
- ❖ A priority is ensuring that Iran is inhibited, or deterred, from deciding to build nuclear weapons.

### Introduction

A frequently propagated red herring is that if Iran's leadership has not decided to build nuclear weapons, it does not have a nuclear weapons program, as if only a directive to build them or the act of building them qualifies. However, for a country like Iran, a simplistic binary model does not suffice. Similarly, this type of







categorization did not apply to Taiwan in the 1980s, when it had a program of being ready to build nuclear weapons on short order, if requested by the regime's leadership. <sup>1</sup>

Taiwan had not made a decision to actually build nuclear weapons, nor had it shown any intention to build them, but it wanted to be ready to do so quickly in case a Chinese invasion was imminent. However, the United States feared that if the Chinese discovered the program, whether ready or not, it would invade. As a result, the United States took dramatic and secret steps to not only shut it down but insisted that Taiwan dismantle much of its associated infrastructure, including a research reactor, a secret plutonium separation plant, and an extensive secret nuclear weapons simulation and high explosive testing program. Taiwan had given the unfinished secret plutonium separation project a civilian cover story, and the research reactor was under International Atomic Energy (IAEA) inspections. Nonetheless, the U.S. government was determined to block Taiwan's pathway to a nuclear weapon once and for all.

Likewise, today, Iran does not appear to have a program focused on the actual building of nuclear weapons. But it does appear to have a program to be prepared to make nuclear weapons and to do so on short order based on covert and overt activities and facilities. Rather than a traditional nuclear weapons program, Iran threatens the region and the world with a program ready to produce nuclear weapons "on-demand."

This type of program serves the Iranian regime's interests. While Iran increasingly is viewed as a nuclear power, it has so far been able to avoid harsh international and regional penalties. All the while, it can act to bolster its nuclear weapons capabilities. Given its existing capabilities, this approach also permits Iran to minimize the need for secret nuclear weapon development activities, which if discovered could catalyze more dangerous threats against the regime.

Today, Iran is closer to being able to build nuclear weapons than it was in 2003 at the end of the Amad Plan, its large-scale nuclear weapons program in the early 2000s, aimed at building five nuclear weapons with cores of weapon-grade uranium. <sup>2</sup> While international efforts have complicated Iran's maintenance of a nuclear weaponization program, and even over time stymied some activities, no evidence has emerged that Iran stopped its nuclear weaponization efforts after 2003. Nonetheless, building an arsenal of nuclear weapons is a complex challenge, requiring a range of nuclear capabilities, and many that need to be kept ready under utmost secrecy.

Since the Amad Plan, Iran has focused on creating an uranium enrichment program able to make weapon-grade uranium, a capability that was years away in 2003 when the Amad Plan was halted. It now has established a vast uranium enrichment program, housed in multiple facilities, based on advanced centrifuges, and is well-practiced in producing up to 60 percent enriched uranium – a small step from weapon-grade uranium.

Meanwhile, Iran has resisted all efforts by the IAEA to cooperate and fully reveal its nuclear programs, providing what is known as both a correct and complete nuclear declaration, a necessary step in the IAEA process of determining that Iran's nuclear program is peaceful. Nonetheless, the IAEA has accumulated a large body of evidence that Iran is hiding nuclear materials and activities associated with its nuclear weapons program. In the last few years, the IAEA has discovered undeclared nuclear materials and activities at four sites in Iran: three called Marivan, Varamin, and Lavisan-Shian, are linked to facilities and activities of the Amad Plan and the fourth, Turquz-Abad, with current-day storage of Amad equipment and material. These discoveries are the tip of the iceberg of Iran's nuclear weaponization capabilities, many kept intact after Amad's halt. These capabilities collectively represent decades of accumulated equipment, knowledge, and experience, including the preservation of the extensive activities and accomplishments of the Amad Plan.

Under the current conditions, despite the buildup in tensions with Iran, it is not possible to predict when or if the Iranian regime might decide to build nuclear weapons. But the regime is rapidly advancing its uranium enrichment program and nuclear-weapons-capable ballistic missile programs, while threatening to reduce further inspections.

Iran may still, however, fear the negative consequences of building nuclear weapons in the near future, which could include far harsher sanctions, military strikes, and nuclear proliferation among its Middle East neighbors. It may want to return to the Joint Comprehensive Plan of Action (JCPOA), at least for a few years, to gain immediate sanctions relief, the end of the UN missile embargo in 2023, and the expiration of the UN Security Council snapback mechanism in 2025.

Yet, there are probable triggers that could cause the Iranian regime to implement its readiness effort and build nuclear weapons. One such could be the regime assessing its survival is at stake; another would be military strikes against Iran's nuclear sites that do not deter the regime from rebuilding those sites. Although not all of the triggers can be prevented, Iran acting on them to build nuclear weapons can be deterred.

In the absence of a major triggering event, the regime may be waiting for a time when the intersection of capabilities, i.e. speed to the bomb, and negative consequences is viewed as manageable. Although this balance point is difficult to predict, the former—Iran's potential course of building a nuclear arsenal—can be analyzed, and the latter—negative consequences—can be bolstered, inhibiting Iran from crossing that line in the first place. As Iran continues to get closer to being able to rapidly build nuclear weapons, additional risks may develop. The quicker Iran can make a nuclear weapon, the more tempted the leadership may be to give the go-





ahead and accept the price it will have to pay internationally. Simultaneously, the risk increases of the West mistakenly concluding that Iran is dashing to the bomb, leading to harsh and destabilizing countermeasures.

For all of these reasons, understanding the pace of Iran building nuclear weapons matters, in particular for designing strategies against Iran moving to construct them.

### **What Could an Iranian Move to Nuclear Weapon Status Look Like?**

The Iranian situation poses unusual challenges. Its nuclear program is rather unique in the annals of nuclear proliferation. It learned how to build nuclear weapons but stopped a full-fledged nuclear weapons program before building any. Yet, it did not fully stop its nuclear weapons effort and is resisting the type of denuclearization undertaken by Taiwan and South Africa, stonewalling IAEA efforts at further transparency.

The Iranian regime today has the choice between two basic strategies to achieve nuclear weapons status—a relatively quick path to revive and complete the Amad Plan with a capability of serially producing many warheads suitable for ballistic missiles (and possibly cruise missiles) as well as testing underground, and/or an accelerated, interrelated effort to achieve a few crude nuclear weapons. Either strategy could be invoked separately or in parallel.

The particular course would depend on the trigger causing Iran to decide to build nuclear weapons and Iran's perception of the world's reaction, including the feasibility of progressing without risking draconian responses that would disable the nuclear weapons effort. Detectability of the effort would likely be one main consideration, and relatedly, speed, as the transition time between a decision to build nuclear weapons and the possession of the first one poses enormous risks to the regime if the effort is discovered. Further consideration would be given to the desired military strike capabilities of the nuclear weapons and their deterrence effect. An accelerated program to its first and perhaps second nuclear weapon would have less chance of premature detection, but Iran would likely also want to create a formidable arsenal of nuclear-tipped ballistic missiles able to reach Israel and eventually Europe, if not the United States.

### ***Amad Plan Revival***

Iran could revive and complete the Amad Plan, creating an industrial-scale nuclear weapons production complex able to serially produce nuclear warheads for ballistic missiles and perhaps cruise missiles. The Amad Plan was well structured, with hundreds of well-defined tasks, each with a schedule, along with careful tracking of progress and shortcomings of each task. By late 2003, and the halt of the Amad Plan, most tasks associated with nuclear weaponization were completed or well on their way to completion, the organizational hierarchy was set, needed physical infrastructure mapped out, and large-scale facilities designed or under construction.

This revival is credible because unlike a country ending its nuclear weapons program, Iran did not disperse Amad personnel or order a halt to all nuclear weapons work. Amad's leaders were extremely upset at the regime leadership's decision to halt the program and were allowed to form successor organizations that conducted nuclear weapons-related projects, serving to solve some of Amad's bottlenecks and to keep many Amad personnel employed up to today. The IAEA has also alleged that Iran has maintained and hidden nuclear and nuclear-related equipment and materials left from the Amad Plan.

However, starting up and finishing the Amad Plan's initial goals of five nuclear weapons would take time. After the halt of the program, several facilities were abandoned or never finished, and some key development activities are still required.

Under a revival, Iran could produce weapon-grade uranium late in the process, using stocks of enriched uranium. It could also build a clandestine enrichment plant, where it could receive diverted stocks of safeguarded enriched uranium for further, secret enrichment to weapon-grade.

### ***Accelerated Program***

If speed and minimizing detection are emphasized, Iran could initiate an accelerated secret program, focused on finishing the most essential work on nuclear weaponization. Experience from Iran's Amad Plan efforts would be invaluable in planning and executing the accelerated nuclear weapons program to build simpler nuclear explosive devices on an expedited schedule. Late in this process, Iran could "breakout" and divert enriched uranium to the production of weapon-grade uranium, allowing for a relatively rapid completion of its first nuclear weapons. Iran would probably calculate that the time between diversion and actualization of its first nuclear weapons would not allow an effective international response.

Under an accelerated program, Iran's weapons would likely be non-missile deliverable but could be used for underground testing to demonstrate a capability, delivered by crude delivery systems, or hinted at while their existence would simultaneously be denied. The last option was used successfully by Pakistan in the 1980s, leaving the world to ponder how many nuclear weapons it had and what type. If Iran conducted an underground nuclear test, the political and strategic effect would likely be profound, even without any clear indication of Iran having deployed nuclear weapons. Given the extent of terrorism conducted by the Iranian regime and







its proxies, an unconventional delivery system should not be discounted, especially in the face of desperation. These weapons, despite their relative crudeness, would likely provide Iran with a nuclear weapon status, likely deterring enemies, while finishing its missile-deliverable warheads.

### **Iran's Nuclear Weapons Readiness Program<sup>3</sup>**

Iran's current nuclear status is both credible and threatening to other countries, because under the Amad Plan, Iran did have a nuclear weapons program like the one in Pakistan or in South Africa in the 1970s and 1980s. Adding to concerns, Iran has strategic and political reasons to build nuclear weapons and an authoritarian political system able to suppress domestic opposition to building them.

Iran is way beyond what is sometimes called a latent nuclear weapons program, a term often pinned on Japan because it has a large stock of separated plutonium. But despite Japan's latency status, the country has not performed any concrete work on weaponizing that plutonium or given any sign of being ready to build nuclear weapons. Iran's leadership is thinking about nuclear weapons, preserving nuclear weapons capabilities, including related information and equipment, advancing those capabilities, and fighting off exposure and demands for greater transparency. Iran has an active capability with key nuclear weaponization abilities in place, and—it is highly likely—a plan to exercise the option to make nuclear weapons, including a process or at least a strategy if the regime's leadership decides to do so.

Traditional definitions of a nuclear weapons program thus do not fit Iran's situation today, particularly when they are applied to assessments of whether specific aspects of nuclear weaponization are active from one year or another. In the context of Iran, as was the case for Taiwan, a more realistic and useful definition of a nuclear weapons program should include a program that is preparing itself to build nuclear weapons, if an order is given.<sup>4</sup>

A new, broader definition of a nuclear weapons program includes a set of related activities aimed at seeking and building nuclear weapons, but it allows for programs encompassing a collection of activities aimed at being ready, on command and in short order, to build nuclear weapons. In evaluating whether Iran's program qualifies under this broader definition, assessments should look at all measures taken to create the technological and organizational conditions for producing nuclear weapons, including the planning and construction of nuclear weapon research, development, and production facilities. Iran should also be assessed on whether it is developing or maintaining the various nuclear capabilities that better position it to produce nuclear weapons, should the leadership choose to build them. In such an assessment, sensitive safeguarded nuclear facilities matter; breakout timelines become an important measure of the threat; inspection deadlocks over access to personnel and sites become an indicator of possible or covert nuclear weapons-related activities; and discovery of the construction of secret nuclear sites or their razing is met with a presumption of guilt. Illicit procurements and procurement attempts related to nuclear weaponization are another indicator of undeclared nuclear weapons-related activities. An active management structure, as indicated in Iran's case by the maintenance of a secret nuclear weapons archive, would qualify as evidence indicative of an ongoing nuclear weapons effort. Overall, the entire nuclear program must be considered, both overt and covert components, as well as potential non-nuclear cover programs.

Under that definition, Iran has at a minimum an active nuclear weapons readiness program, a capability amplified since the Amad Plan. Its readiness program is centered at both secret and safeguarded facilities.

### ***Mohsen Fakhrizadeh and His Successors***

Iran's long-time leader of its nuclear weapons efforts was Mohsen Fakhrizadeh, with the support and guidance of Iran's most senior leadership. He led the Amad Plan and its predecessor organization, the Physics Research Center, known by its acronym PHRC. He continued leading Amad's successor organizations, the most recent known by its acronym, SPND, which included many former members of the Amad Plan, until his violent death in November 2020.

His death was a setback for Iran and has complicated maintaining a nuclear weapon readiness capability, given his enormous amount of institutional knowledge, his recognized managerial skills, and his political influence. However, Fakhrizadeh and his colleagues from the Amad Plan also mentored a new generation that appears to be sufficiently capable to carry on, despite Fakhrizadeh's death. In addition, the IRGC and Iran's military industries have a variety of experienced managers, two of which emerged as heads of SPND following Fakhrizadeh's death in late 2020, both well versed in Iran's missile and other military industries.

The first replacement was IRGC Brigadier General Mahdi Farahi, aka Seyyed Mahdi Farahi. He was formerly Deputy of Iran's Ministry of Defense for Armed Forces Logistics (MODAFL) and Managing Director of the Defence Industries Organisation (DIO), and head of the Aerospace Industries Organisation (AIO). He has been designated by both the United States and the European Union because of his nuclear proliferation and/or ballistic missile activities. He was also reportedly involved in the development of an 80-ton rocket booster being jointly developed by Iran and North Korea and travelled to Pyongyang, North Korea during contract negotiations.<sup>5</sup>

Farahi remained as head of SPND for less than a year, being replaced in September 2021 by Reza Mozaffarinia, aka Reza Mozaffarinia Hosein. Mozaffarinia is a former deputy defense minister of MODAFL





and Dean of Malek Ashtar University (MUT), a university controlled by MODAFL. Mozaffarinia has made significant contributions to Iran's missile program, according to his U.S. Treasury Department designation in 2013.

Based on interviews with knowledgeable sources, neither man was part of the Amad Plan or has significant nuclear background or expertise. A priority was stabilizing SPND after Fakhrizadeh's death, and they both accepted orders to continue with Fakhrizadeh's methods. As a result, the structure of SPND did not change after his death. The core Amad groups remain intact, in particular the explosive and radiation groups. <sup>6</sup> Former Amad personnel remain senior experts in these programs. The core of Iran's nuclear weaponization capabilities thus remain in SPND under new leadership. If the Iranian regime decided to build nuclear weapons, despite the loss of such a unique leader of its nuclear weapons program, it maintains the expertise and managers to do so.

After decades of almost exclusively non-military figures leading the Atomic Energy Organization of Iran (AEOI), it was recently placed under the leadership of a figure with an extensive background in Iran's military industries. In August 2021, the newly elected President Ebrahim Raisi appointed Mohammad Eslami as the new head of the AEOI. Eslami is a civil engineer who was formerly Deputy Defense Minister for Research and Industry and served as head of the Defence Industries Training and Research Institute, which earlier had contained the Amad Plan. He was also managing director of Iran Aircraft Manufacturing Industries (HESA), deputy director of Aerospace Industries Organization (AIO), deputy for engineering and development plans at Defense Industries Organization (DIO), and deputy for engineering and passive defense at the Ministry of Defense and Armed Forces Logistics (MODAFL). For his activities, Eslami was designated by the U.N. Security Council and the European Union.

Eslami may have had earlier connections to the nuclear program. In 2015, Eslami reportedly participated in negotiations with the IAEA about the IAEA's investigation into possible military dimensions of Iran's nuclear program. During this period, leading up to the JCPOA's implementation in early 2016, the Iranian regime's negotiating strategy was very successful, undermining the IAEA from obtaining a complete Iranian nuclear declaration and convincing the United States and its European allies that such a declaration was extraneous to implementing the JCPOA. <sup>7</sup>

With Eslami now in firm control of the AEOI, does his appointment, a person with extensive senior-level military industrial experience, signify an increasing militarization of the AEOI? It bears watching whether Eslami will create closer ties and cooperation between the AEOI and military industries.

### **The Pillars of a Nuclear Weapons Program**

Any successful nuclear weapons program must be built on three pillars: nuclear explosive material production, nuclear weaponization, and delivery systems. The most important aspect of a nuclear weapons readiness program is a commitment to be ready to make both nuclear test devices and deliverable nuclear weapons on an expedited schedule. Meeting such a schedule would require the preparation of many capabilities and require the involvement of several military institutions beyond the SPND, in particular those involved in nuclear-capable delivery systems, and the AEOI.

A challenge identified in the Taiwanese case was the need to ensure that nuclear weapons personnel would be ready to build nuclear weapons when ordered, all the while denying that there was a nuclear weapons program. This was a subterfuge harder for Taiwan to maintain given its more cordial working relationship with the IAEA and the regular presence of U.S. personnel at its nuclear sites. If a decision were made to build a nuclear weapon, Taiwan's government needed assurance that personnel were well-practiced and ready to act. There would not be time to start from scratch to develop needed skills or train new personnel. The role of civilian or non-nuclear military cover stories was critical in practicing preparation for or honing skills needed in a breakout to nuclear weapons. In Iran, the AEOI has taken the lead on developing civilian nuclear cover programs, while SPND and other military research organizations can provide non-nuclear military cover for maintaining nuclear weaponization skills, particularly given that it contains so many former Amad Plan persons. One important nuclear weapons-related practice under a civilian cover can be seen in AEOI's deployment of a capability under IAEA safeguards to make near 20 percent enriched uranium metal. The use of near 20 percent enriched uranium can stand in for the production of weapon-grade uranium metal. Within SPND and associated organizations, where cover stories are plentiful, many necessary, secret capabilities are enshrined, allowing the development and maintenance of a range of nuclear weaponization-related capabilities. Some capabilities may even involve personnel unaware of the underlying purpose of their work. These "dual-use" activities and projects can keep personnel ready to act to build nuclear weapons on short order, if a decision to proceed were made. A former senior member of Taiwan's nuclear weapons program called this state of readiness, "hot standby." <sup>8</sup>

Seen from this perspective, Iran's constant defiance and blocking of the IAEA is crucial to maintain its nuclear weapons readiness programs. It has to deny inspectors access to military sites and personnel and stonewall their requests for information about suspect undeclared materials and activities. This strategy helps prevent the IAEA from learning about secret nuclear weaponization-related activities and assets and prevents interpersonal relationships from developing, contradictions in officials' statements, and relationships that could increase the chance of leaks and unintentional disclosures. It would also help explain the regime's periodic, despicable efforts to portray IAEA inspectors as little more than spies for the West.







Maintaining the ability to produce weapon-grade uranium is far easier for Iran. The safeguarded uranium enrichment program serves as one of the most significant cover stories, developing the capability of producing weapon-grade uranium on short order and being able to build clandestine centrifuge plants involving advanced centrifuges. As of November 2022, utilizing its existing stocks of enriched uranium and centrifuge enrichment capability, Iran could produce enough weapon-grade uranium for four nuclear weapons in one month. By the end of the second month after starting breakout, it could have enough material for five weapons, the number of weapons set as the original Amad Plan target.

Iran's ballistic missile force and its accomplishments in increasing the precision of their missiles are impressive. Many of these missiles are capable of delivering nuclear warheads. Iran has the distinction of having the largest conventionally armed ballistic missile force in the world; others with comparable missile forces have put nuclear weapons on them. It possesses thousands of ballistic missiles of various ranges up to 2000 kilometers, with many precision-guided. During the last two decades, Iran prioritized achieving a high degree of precision and accuracy in its missiles, a goal it has demonstrated visibly in recent years – about 90 percent of current missile production is precision-guided missiles. Iran's ballistic missile program is being watched carefully by Western intelligence agencies for signs it is working on modifying its missiles' nose cones to carry nuclear warheads, surveillance which may be inhibiting Iran from modifying its missiles to carry nuclear weapons. In addition, Iran appears constrained in developing a reentry vehicle for an ICBM, despite developing rocket engines with sufficient thrust for an ICBM under the cover of a space launch program.

### **Nuclear Goals and Challenges**

As outlined in the Nuclear Archive, the goals of the post-Amad nuclear program were to build a secret enrichment plant at Fordow and produce an industrial prototype of the Saqib series of nuclear weapons. The Saqib-type nuclear weapons constituted a pivotal post-Amad project.

1. **Saqib-1<sup>9</sup>** was a system for static testing, where its technical specifications were finished in 2003. This type of device could be tested underground.
2. **Saqib-2** was a system for installation in the reentry vehicle, where the technical specifications of this system were, in late 2003, to be developed in such a way that it meets the flight parameters needed for integration into a ballistic missile.
3. **Saqib-3** was a Shahab 3 reentry vehicle equipped with Saqib-2, a missile deliverable nuclear weapon.

There is no reason to believe that Iran's basic goals have changed fundamentally. But there is evidence that the last 20 years further shaped the nuclear weapons program.

On one hand, Iran's nuclear weapons program has suffered numerous setbacks and delays, including the premature closure of the Amad Plan, the discovery of the Fordow enrichment plant, ongoing leaks about nuclear weapons efforts, at times tough IAEA inspections, killings of its key scientists, Stuxnet and other cyberattacks, sabotage of centrifuge manufacturing and enrichment plants, increased sanctions against its programs, threats of wide-scale military strikes, and international opprobrium. Arms control in the shape of nuclear freezes and the JCPOA temporarily limited Iran's activities and increased their monitoring. Iran's Amad personnel know they have been, and remain, under intensive surveillance by multiple intelligence agencies and have been targets of espionage, and worse. Moreover, the Amad workforce is aging, and some believe that Iran's nuclear weaponization skills are declining as this workforce ages, although Iran is also believed to be training and mentoring younger generations of scientists and engineers to replace this first generation of weaponeers. The nuclear weapons program's current state is bound to be complex and highly camouflaged. On the other hand, Iran has persisted in its efforts. Moreover, if a decision were taken, Iran can reverse any decline in weaponization skills. Its nuclear weapons capabilities appear far more formidable today, particularly when looking at the two more visible nuclear weapons pillars: production of weapon-grade uranium and nuclear-capable ballistic missiles.

One gain for Iran, but a failure for the rest of the world, is that by simply putting a secret nuclear site under IAEA safeguards, it preserved the site—even opened the door for improving it—if a civilian purpose could be concocted. This was made easier by the legitimization of Iran's uranium enrichment program under shifting European and U.S. policies and arms control deals. The world grew anesthetized to Iran's cheating. Almost the entire Amad Plan nuclear fuel cycle is now either shut down or under IAEA inspections, but it is impossible for the IAEA to guarantee a strictly peaceful use. The U.S. government certainly rejected this type of outcome in the case of Taiwan, where it demanded the dismantlement of an operating safeguarded research reactor and the destruction of a reprocessing plant under construction. <sup>10</sup>

It remains difficult to estimate the timeframe Iran has envisioned for implementing its readiness to build nuclear weapons, but any setbacks in weaponization have been made up by drastic improvements in missile delivery and weapon-grade uranium production and processing capabilities.

### **Characterizing the Nuclear Weaponization Status**

One starting point is to consider the progress made by the Amad Plan's nuclear weaponization project, a subproject of Project 110, codenamed the Operating System Project. This project included almost the entirety of Iran's efforts to build the nuclear weapon itself, absent efforts to integrate the warhead into a





ballistic missile. A snapshot of this project's work is seen in a Nuclear Archive electronic file, a Gantt diagram of all the Operating System Project's subprojects, including names, tasks, and schedules. <sup>11</sup> The diagram dates to about late 2001 or early 2002, about two years into the Amad Plan, which started in March 2000, and about 18 months before it was halted.

This Gantt diagram is useful in estimating timelines because it is a specialized form of spreadsheet template used by project managers worldwide to schedule and coordinate tasks, where each task is on one line, and its start and completion date can be represented graphically, along with its progress. Moreover, the spreadsheet allows sections to be expanded or contracted, allowing an examination of different parts or the whole. The Gantt diagram for the Operating System Project contains 650 lines, indicating a highly detailed plan.

At the time the diagram was updated in early 2002, the project's overall progress was 40 percent complete. The major subprojects, in the Gantt diagram, with percentage completed, are:

- Product System Engineering — 83 percent completed
- Neutron Source Design and Production — 33 percent completed
- Weapon-Grade Core Design and Production — 51 percent completed
- Multi-point hemi-spherical initiation systems — Shock Generator Design and Production — 45 percent completed
- Construction and Equipping of Nuclear Weapons Assembly Workshop — 0 percent Completed
- Product Engineering Prototype — 28 percent completed

The Amad Plan continued for another 18 months before halting, allowing the Operating System Project to make significantly more progress. For example, Nuclear Archive documents show that the Shock Generator project may likely have been completed by the end of 2003. <sup>12</sup> Unfortunately, however, a late 2003 Gantt diagram update is not available to reveal overall progress by that date.

The Amad Plan also included a Warhead Project, also known as Project 111, focused on integrating a nuclear warhead into a ballistic missile. This project was further from completion in 2003 than the Operating System Project.

The weaponization and integration projects, finished or incomplete by the end of 2003, can be derived from other Nuclear Archive information. Based on Figure 10.4 in *Iran's Perilous Pursuit of Nuclear Weapons*, several key weaponization activities that would still be needed today and were largely finished under the Amad Plan by 2004, include:

- 1) Maintaining the capability to use computer codes to simulate a nuclear weapons explosion. Greater use of simulations would make component testing less necessary.
- 2) Retaining a mastery of the shock wave generator, including possibly having conducted a successful cold test of a nuclear explosive with a surrogate nuclear core. (A cold test is the last step before building a nuclear weapon.)
- 3) Having the capability to make the neutron initiator.
- 4) Finishing a pilot plant to make weapon-grade uranium cores (sites subsequently abandoned or likely repurposed).

SPND inherited considerable expertise in these areas and appears fully able to maintain or even advance these capabilities, either by conducting activities under cover stories or carefully undertaking clandestine efforts. With advances in computer technologies, and the wider availability of supercomputers, one would expect that SPND's capabilities to simulate a fission nuclear explosive would be quite advanced today.

Another key aspect of making nuclear weapons concerns weapon-grade uranium metal, including:

- Preserving or establishing the ability to convert fully enriched uranium hexafluoride into uranium tetrafluoride; and
- Having the capability of converting weapon-grade uranium tetrafluoride into metal and producing nuclear weapons components.

The Nuclear Archive did not contain any information on the first bullet item, but it had extensive information on the activities associated with the second bullet, including the construction of a pilot and production-scale plants to make weapon-grade uranium metal and transform them into nuclear weapon components. The two facilities were abandoned or repurposed after 2003, but many of their capabilities have in recent years been installed and partially tested by the AEOL at Esfahan. These activities have included the production of small amounts of near 20 percent enriched uranium metal, and the subsequent installation of a processing line at the Esfahan Uranium Conversion Facility to convert near 20 percent enriched uranium hexafluoride into tetrafluoride form and work on production lines to convert that material into enriched uranium metal. The 20 percent material can stand in for weapon-grade uranium. Iran finished installing equipment for producing depleted and natural uranium metal, although as of October 2022 no nuclear material had been introduced into the production area. The AEOL's actions since about 2020, despite being under safeguards, reflect a determination to reactivate Amad's previous ambitious plans to make uranium metal. The more recent actions inevitably aid the process of making nuclear weapons.

In addition to safeguarded activities, SPND may have maintained related conversion and metallurgical skills in programs involving surrogate materials. At this juncture, the question looms regarding what







material and equipment was in the Turqz Abad shipping containers. These containers could have held equipment and materials needed for the production of weapon-grade uranium metal and its conversion into weapon components.

Additional, key Amad Plan activities and facilities from the table in Figure 10.4 of *Iran's Perilous Pursuit of Nuclear Weapons* would be needed, some of which were not completed as of 2003, including:

- Finishing and bringing into operation a pilot-scale and/or a production-scale facility to make weapon-grade uranium cores for nuclear weapons;
- Integrating a warhead into a reentry vehicle of a ballistic missile;
- Having a facility to assemble all the components of nuclear explosive devices and missile-deliverable nuclear weapons;
- Preparing an underground nuclear test site.

During the last near 20 years, Iran could have made progress on these four areas. SPND, in collaboration with Iran's missile development and manufacturing industrial organizations, could have done considerably more work on integration of a warhead into a ballistic missile. Certainly, Western surveillance is ongoing for secret activities related to Iran building a nuclear test site. With increased concerns about such monitoring, Iran may have shifted from planning on drilling a vertical shaft in an isolated section of a desert to planning the construction of a horizontal tunnel that goes deep inside a mountain.

Based on the original Amad Plan schedules and accomplishments through the end of 2003, and assuming the Amad Plan had not been halted in 2003, it appears that the weaponization and integration projects would have needed one or two more years to complete their work. This is separate from the Project 110 project to produce weapon-grade uranium, the Al Ghadir Project, which was several years from fruition.

### **How Quickly Could Iran Make Nuclear Weapons Today?**

The unfortunate reality is that Iran already knows how to build nuclear weapons. Although there are some unfinished tasks, overall, the SPND and its allied organizations give every appearance of standing ready to build them today, if the regime's leadership decided to do so. But how would it proceed? How long would it take? It cannot be argued today that Iran is several years from building nuclear weapons. At the end of the Amad Plan in 2003, that was the case. The biggest bottleneck then—the production of weapon-grade uranium—is no longer a bottleneck.

Iran's exact level of readiness, including timescales, is difficult to quantify, a determination complicated further by the death of Fakhrizadeh. For comparison, Taiwan had a policy that the nuclear weapons establishment had to deliver an atomic bomb in three to six months after receiving the order to build nuclear weapons.<sup>13</sup> That level of knowledge of Iran's circumstances must be estimated. Given Fakhrizadeh's detailed planning and managerial skills, as exemplified in the Amad Plan's Gantt diagrams for the Operating System Project, planning has most likely occurred on making nuclear weapons, including many contingencies. For a state like Iran under intense international pressure not to acquire nuclear weapons but wanting to hedge against threats, it would be expected to develop a range of options, while steadfastly denying any nefarious intention.

One aspect of any such plan is to hide certain activities, equipment, and documents, particularly those which have no civilian or non-nuclear military cover. The Nuclear Archive, with detailed nuclear weapons documentation, and Turqz Abad shipping containers of sensitive equipment and undeclared nuclear materials, demonstrate that need.

Another aspect of such a plan is avoiding or delaying as long as possible certain high-signature activities that are hard to hide from Western intelligence agencies and would be expected to precipitate harsh attention and escalation. A cold test conducted today would be one such activity. Work on certain single-use components related to integrating a nuclear warhead into a ballistic missile could be another one. Work on reentry vehicles for ICBMs would also fall into this category.

An important uncertainty is the current number of unfinished Amad tasks. Iran has demonstrated great advances related to Amad's Al Ghadir uranium enrichment project and ballistic missiles. More difficult to ascertain are its accomplishments on certain nuclear weaponization and missile integration efforts. Did Iran conduct a cold test? Did it build a prototype? Did Iran finish integrating a nuclear warhead into a ballistic missile reentry vehicle? Given the inherently small-scale nature of several of these unfinished weaponization tasks, their detection is challenging even for the most accomplished intelligence agencies. So much about the Amad Plan, including production-scale facilities, was missed until the discovery of the Nuclear Archive in 2018. About half of the key Amad sites were unknown by Western intelligence and the IAEA until after the seizure of the Nuclear Archive.<sup>14</sup> Furthermore, none of the unfinished tasks would likely take long to complete; after all, the weaponization pillar is the easiest of the three pillars for Iran to master.

Given the pressures on Iran, however, one cannot exclude the possibility that few weaponization activities are being conducted today, including development steps, except actions to hide its capabilities, and not always successfully, as shown by the discovery of the Nuclear Archive and the shipping containers at Turqz Abad filled with equipment and nuclear material from the Amad and possibly post-Amad efforts.





At a minimum, Iran has a coordinated set of activities related to building a nuclear weapon. At worst, the weaponization team has already conducted a cold test, built an industrial prototype and is regularly practicing and improving their nuclear weaponization craft under various covers or in clandestine locations. As mentioned above, a cold test is significant since it would be the last step before manufacturing a nuclear explosive.

An additional part of this evaluation is Iran's desired level of reliability in its weapons. The nuclear explosive device itself would probably work, but if Iran wanted something better and more reliable, more work would be required, leading to delays in the actualization of a weapon or an underground test. Iran's standards over what constitutes a reliable weapon likely differ significantly from those in the West, with Iran more likely to trade less certainty for expediency.

Returning to the original dual-strategy course of action, where Iran would pursue both an accelerated nuclear weapons program and revive the Amad Plan, what are their respective timelines? It should be reemphasized that there is no evidence Iran has activated either option at this time.

### ***Accelerated Nuclear Program***

As of November 2022, Iran is assessed by the Institute as being able to build a crude nuclear explosive in six months. At that point, it could conduct an underground nuclear test or let the world know about the device by other means.

The risk of failure could be high in Iran's case. However, the Iranian leadership may perceive the risk as necessary and worthwhile, ordering the nuclear weapons' team to undertake this approach. In the case of Iraq's pursuit of an accelerated, or "crash," nuclear weapons program in 1990 after its invasion of Kuwait, it was Saddam Hussein and his top leadership that ordered the accelerated nuclear weapons program. This program, far less advanced than Iran's, was ended before its fruition by the start of the allied bombing campaign in January 1991.

This estimate assumes that while much of the weaponization work has been accomplished, a few significant tasks remain, even for completing a crude nuclear explosive, such as a cold test. However, these tasks could be completed in a matter of several months under an expedited schedule. Much of the work on weaponization would be conducted in utmost secrecy and would use existing or repurposed military facilities or hidden equipment and materials, possibly located in tunnels. Moreover, the device would only need to be able to be tested underground or delivered by a crude delivery system such as a ship or truck.

The production of weapon-grade uranium could be delayed until near the end of this six-month period. Iran is assessed as not having a secret uranium enrichment plant, so Iran would need to divert its stock of safeguarded enriched uranium and further enrich it to weapon-grade. With enriched uranium stocks at November 2022 levels, however, within a week or two enough weapon-grade uranium could be accumulated for two nuclear weapons, and in a month enough for four weapons could be produced at declared enrichment plants. This capability means that the diversion of safeguarded enriched uranium could be delayed until a month or two before assembling the first nuclear weapon. The production of weapon-grade uranium metal and its fabrication into weapons components could be practiced in secret sites with natural uranium as a surrogate, something already part of the Amad Plan.

The IAEA may be delayed in detecting the diversion of safeguarded enriched uranium and further enrichment up to weapon-grade, or the use of natural uranium in metal production and fabrication. For the safeguarded enriched uranium and the use of any declared sites, Iran could deny the inspectors access under a pretense such as a fire, an accident, or a security incident. Nonetheless, there would probably be some observable indication that a diversion had occurred, even if indirect.

### ***Revive the Amad Plan***

The other part of the strategy involves Iran secretly reviving the Amad Plan. If launched in conjunction with an accelerated program today, the weapon-grade uranium for several nuclear weapons could be manufactured as part of the initial breakout in the accelerated program. If launched alone, the diversion of the safeguarded enriched uranium would occur late in the project. There is a possibility that Iran would also build a clandestine enrichment plant, utilizing its growing advanced centrifuge production capabilities, possibly directly replacing the critical role the Fordow facility was to play under Amad. A few thousand advanced centrifuges in a hidden plant would make breakout much harder to detect, let alone prevent.

Based on gauging the progress made in the Amad Plan by 2003, combined with setbacks faced since and the fact that Iran would have to tread carefully to avoid premature discovery, Iran is estimated today to need up to two years to reach the point of producing its first missile-deliverable nuclear weapon and recreate an industrial-scale nuclear weapons production complex. The years that have passed since the Amad Plan was downsized, the abandonment of its large construction projects, destruction of discovered facilities, loss and re-assignment of personnel, and perhaps most of all the theft of major portions of the Nuclear Archive, laying bare large parts of Amad's existing and planned physical and human infrastructure, resulted in a significant loss of momentum Iran once had for a quiet revival of the Amad Plan.

Not factored into the two-year timeline is progress made in nuclear weapons development after 2003, as its full extent is at issue. However, this assumption risks shortening the Amad revival timeline by only a matter of months.





In this type of large program, after reaching its first missile-deliverable nuclear weapon, successive ones would be expected to follow every few months, where the supply of weapon-grade uranium would become the main driver of how quickly the arsenal would grow. This two-year estimate is consistent with Israeli public estimates. An Israeli military intelligence estimate from early 2020 assessed that Iran would need two years to build and deploy a nuclear warhead on a ballistic missile, <sup>15</sup> and offered the same estimate in February 2021. The latter estimate recognized shorter breakout timelines to produce enough weapon-grade uranium, but emphasized the delays that would ensue because of the death of Fakhrizadeh. <sup>16</sup> The Israeli military intelligence estimate is similar to previous U.S. intelligence estimates, which assumed that Iran had made little, if any, advancements since 2003. A similar recent Israeli estimate was reported by *The Jerusalem Post* in November 2022. <sup>17</sup> Senior Israeli sources stated that once Iran makes a decision to build nuclear weapons, it would need about two years to master nuclear detonation and integration into a ballistic missile.

According to knowledgeable Israeli sources interviewed by this author, the two-year estimate is based on the scenario of Iran secretly reviving the Amad Plan, meaning that two years are needed to revive the Amad Plan, finish the nuclear weaponization tasks, construct the necessary facilities, and build the first missile-deliverable nuclear weapon. Under this approach, diversion of enriched uranium and production of weapon-grade would not happen until near the end of this two-year schedule. Successive weapons would then follow, leading to a small nuclear arsenal relatively quickly, assuming enough weapon-grade uranium has been produced.

### **Specific Triggering Scenarios**

Currently, Iran is adding to its nuclear weapons capabilities while preventing the IAEA from investigating its undeclared nuclear materials and activities. Most believe Iran has not started building nuclear weapons. Yet, Western diplomatic efforts to constrain Iran's nuclear efforts or increase their transparency have so far failed, oftentimes leading the Iranian regime to retaliate, adding to its gas centrifuge program or decreasing cooperation with the IAEA. While Iran's actions are strengthening the international perception of it being a nuclear power, international concern about its status is increasing, and Western countermeasures are being perceived in Iran as more threatening.

What could lead Iran to change from maintaining a nuclear weapons readiness program to building nuclear weapons? The trigger will affect the specific strategy Iran chooses. These triggers should be considered, and a response planned. Although not all of these triggers are preventable, Iran can be deterred from moving to build nuclear weapons.

### **National Survival Threatened**

A natural trigger to consider is if the Iranian leadership comes to perceive its national survival is threatened, at the same time as it has a ready path to a significant supply of weapon-grade uranium. The latter is currently true today. The former could develop in the coming months as tensions rise further between the West and Iran over Iran's refusal to agree to a revived nuclear deal, Iran's ongoing intransigence with the IAEA, its continued supply of drones or their technology to Russia for use in its war against Ukraine, its expected supply of precision missiles to Russia for use in that war, continued or worsening protests in Iran threatening the regime's existence, and a stepped-up shadow war between Iran and Israel. Iran may come to believe that a military strike or war is imminent. In a recent assessment of the threat posed by Iran, called the Iran Threat Geiger Counter, the Institute ranked the current threat as "High Danger." <sup>18</sup>

If Iran decides to build nuclear weapons as a result of a crisis concerning its national survival, when it has access to a ready supply of weapon-grade uranium, it will likely follow the two-step process outlined above, seeking to possess nuclear weapons as soon as possible to deter an attack on its critical facilities while recreating a robust nuclear weapons production infrastructure. It would likely remain in the Nuclear Non-Proliferation Treaty, while hiding key safeguarded assets such as enriched uranium, and also denying inspectors access to a variety of nuclear sites, helping keep its undeclared nuclear activities secret.

Because Iran has developed new centrifuge manufacturing and operational capabilities, it might build and operate a secret centrifuge plant able to produce weapon-grade uranium for nuclear weapons, using natural uranium and safeguarded enriched uranium as feed stock. Based on IAEA reporting, uncertainties about Iran's stocks of natural uranium and advanced centrifuges are growing. The development of advanced centrifuges translates into a smaller plant or one making weapon-grade uranium more quickly.

### **Withdrawal from the Nuclear Non-Proliferation Treaty**

In reaction to Western escalations, Iran could decide to withdraw from the Nuclear Non-Proliferation Treaty. It would invoke article X, deciding that "extraordinary events, related to the subject matter of this [t]reaty, have jeopardized the supreme interests of its country." It would provide the required three months' notice, ending IAEA inspections except those required by other agreements, such as those affecting the Russian-supplied Bushehr power reactor, but it would publicly deny any intention to build nuclear weapons, while hiding its key stocks of enriched uranium and a stock of advanced centrifuges. If the West did not respond forcibly and decisively, Iran could opt for a secret revival of the Amad Plan, avoiding an accelerated program, counting on a reduced chance of







detection as it methodically builds a nuclear weapons production complex with a two-year window to its first nuclear weapon. If a crisis develops, it could opt for an accelerated program. In this option, Iran may also build a clandestine enrichment plant to better protect its capabilities against military strikes.

### ***Revival of the JCPOA***

The revival of the JCPOA would temporarily but drastically reduce Iran's stock of enriched uranium and require the mothballing of thousands of advanced centrifuges, driving up Iran's breakout timeline and the time to accumulate enough weapon-grade uranium for several nuclear weapons. In this case, during the first five years of a revived deal, assuming it survives that long, an accelerated nuclear weapons program would likely lead to its early exposure as Iran would need over three months to produce its first quantity of weapon-grade uranium for a nuclear weapon. It could revive the Amad Plan, but the rather lengthy time needed to produce enough weapon-grade uranium could dissuade Iran from trying out of fear of detection and the mustering of a harsh international response. Although Iran may nonetheless restart the Amad Plan, it could maintain its current posture of being ready to build nuclear weapons, while continuing to stonewall the inspectors about its undeclared materials and activities, looking forward to building up its nuclear enrichment capabilities as allowed under the JCPOA after 2025, and reaching a point where countries would not know if Iran was planning a breakout or just implementing its legal plans under the deal. At this point, (post-2028), breakout timelines would again drop to several weeks and soon thereafter to a few weeks or even days. Thus, a revived deal would at first complicate Iran's pursuit of nuclear weapons, creating a bottleneck in weapon-grade uranium for several years, but by allowing a buildup to a large enrichment capacity and ultimately no caps on enrichment level, Iran would again be able to quickly breakout and build nuclear weapons either under an accelerated program or by reviving the Amad Plan.

### ***Better Now Than Never***

With advancing capabilities and perceiving diminished international concern or pushback, the Iranian leadership could simply decide the timing is opportune, the balance of capabilities, i.e. speed to the bomb, and negative consequences is manageable, and this balance would only worsen in time. As a result, it could secretly launch both an accelerated program and a revival of the Amad Plan.

### **Responses and Inhibitors**

Iran's pathways to possessing nuclear weapons are multiplying. It should therefore be a priority for the United States and its allies to step up and improve intelligence gathering to detect any movement down one of these pathways, recognizing that a revived Amad Plan and an accelerated program could have very different signatures.

Beyond increasing chances of detection, the United States and the international community should take steps to increase Iran's inhibitions in deciding to build nuclear weapons or leave the NPT, and hopefully act to discourage Iran from further developing its nuclear weapons capabilities. These inhibitions can take many forms, and the ultimate goal should be not only to hinder Iran from activating its current nuclear weapons readiness program but also to undermine that program.

Many expected the JCPOA and its revival to hinder Iran from deciding to build nuclear weapons, but not end its nuclear weapons capabilities, including a readiness program. Today, a JCPOA revival seems less likely, given the Islamic Republic's ongoing demands for more concessions as well as its supply of drones to Russia for use in Ukraine, persistent support for terrorist activities, and human rights violations by the regime. Furthermore, a revived JCPOA does not satisfy the need for a stronger set of methods to inhibit Iran from building nuclear weapons and prevent Iran from increasing its nuclear weapons readiness through increased enrichment capabilities. Overreliance on the JCPOA being in force was a mistake. The JCPOA is not stable, long-lasting, or a deterrent against Iran building nuclear weapons in the medium- or long-term.

An urgent priority is bolstering the IAEA to ensure that Iran addresses the inspectors' finding that Iran has undeclared nuclear material in violation of its comprehensive safeguards agreement. The IAEA Board of Governors has warned Iran thrice to cooperate with the IAEA in its efforts to settle this issue, but it has refused, preferring to drag out the process while denying any wrongdoing. While the IAEA should continue pressing Iran to address its doubts that its nuclear program is peaceful, given Iran's intransigence, the Board should demand that Iran cooperate with the inspectors or else face consequences. Such an action will send a strong signal that Iran's violations are unacceptable and further isolate it internationally, while leaving the IAEA further empowered to press Iran for answers, a process complicating any Iranian move to build nuclear weapons.

Iran needs to be made fully aware that building nuclear weapons will require drastic and serious actions by the international community, including military action. The threat of military force weakened after the negotiation of the JCPOA in 2015. Iran grew to perceive the United States as reluctant to use force and Israel as fearful and unable to launch an effective attack. This tendency is being reversed, but not quickly enough. The Western powers should get serious about offensive military options to destroy Iran's nuclear facilities if Iran moves to build nuclear weapons, diverts nuclear material, or withdraws from the Nuclear Non-Proliferation Treaty. A useful first step is President Biden's declaration that military force could be used as a last resort to stop Iran building nuclear





weapons; the United States and Israel’s recent drill simulating a strike on Iran is also important. In parallel, Israel has been increasing its capabilities to deliver a devastating blow to Iran’s nuclear program. U.S. military cooperation with Israel should continue to be bolstered, ensuring Israel can decisively strike Iran’s nuclear sites on short notice if there are signs of Iran is moving to build nuclear weapons, including the ability of delivering a second strike if Iran reconstitutes those activities. The priority should be assisting and building military capabilities with allies and regional partners in the Middle East, with a U.S. commitment to come to their aid in preventing Iran from acquiring nuclear weapons.

Other inhibitions include aggressively expanding efforts to disrupt Iran’s supply chain for nuclear, drone, and missile programs and marching down the path of snapping back all sanctions and embargoes under the JCPOA dispute mechanism. The United States and the international community should also expand the enforcement of existing sanctions and applying additional ones while offering Iran negotiations on a longer, stronger, more effectively IAEA-inspected nuclear deal. In addition, the United States and its allies should build stronger defenses against missiles and other means of nuclear delivery, making it as difficult as possible for Iran to try to deliver a nuclear weapon against the U.S. or one of its allies. Governments and experts can undoubtedly develop a range of ways to deter Iran from building nuclear weapons and create an optimal package of measures. That effort should accelerate as the hope of a revived nuclear deal fades and the threat of Iran building nuclear weapons increases.

References

1. David Albright and Andrea Stricker, *Taiwan’s Former Nuclear Weapons Program: Nuclear Weapons On-Demand* (Washington D.C., Institute for Science and International Security Press, 2018). [↪](#)
2. David Albright with Sarah Burkhard and the Good ISIS Team, *Iran’s Perilous Pursuit of Nuclear Weapons* (Washington, DC: Institute for Science and International Security, 2021). [↪](#)
3. This section and the next one draw extensively on the discussion in *Iran’s Perilous Pursuit of Nuclear Weapons*. [↪](#)
4. While some may call this a “threshold” state, that term is avoided here because it is poorly defined and ambiguous, having been applied to countries like Japan with a large, separated plutonium stockpile and Israel with an undeclared nuclear arsenal. [↪](#)
5. *Iran Watch*, accessed November 19, 2022, <https://www.iranwatch.org/iranian-entities/brigadier-general-seyyed-mahdi-farahi>. [↪](#)
6. For more information of SPND and its projects, see *Iran’s Perilous Pursuit of Nuclear Weapons*, Chapter 14. [↪](#)
7. *Iran Watch*, accessed on November 20, 2022, <https://www.iranwatch.org/iranian-entities/mohammad-eslami>. [↪](#)
8. *Taiwan’s Former Nuclear Weapons Program: Nuclear Weapons On-Demand*. [↪](#)
9. Saqib is also transliterated as Sareb in other English translations of this document. The main Institute translator believes Saqib is more accurate. Saqib is a male name meaning shining, radiant, or glittering. [↪](#)
10. *Taiwan’s Former Nuclear Weapons Program: Nuclear Weapons On-Demand*. [↪](#)
11. Figure 3.5 in *Iran’s Perilous Pursuit of Nuclear Weapons* shows part of the Gantt diagram from the archive, showing a mostly closed view of this diagram, but the major subprojects are visible. The last number line visible is 630. [↪](#)
12. David Albright and Olli Heinonen, “Shock Wave Generator for Iran’s Nuclear Weapons Program,” *Institute for Science and International Security*, May 7, 2019, <https://isis-online.org/isis-reports/detail/shock-wave-generator-for-irans-nuclear-weapons-program-more-than-a-feasibil>. [↪](#)
13. *Taiwan’s Former Nuclear Weapons Program: Nuclear Weapons On-Demand*. [↪](#)
14. David Albright and Sarah Burkhard, “Unknown Amad Sites, Prior to the Nuclear Archive Seizure,” *Institute for Science and International Security*, May 18, 2021, <https://isis-online.org/isis-reports/detail/unknown-amad-sites-prior-to-the-nuclear-archive-seizure/8>. [↪](#)
15. See for example, Anna Ahronheim, “Iran Will Have Enough Material for a Nuclear Bomb Within the Year,” *The Jerusalem Post*, January 14, 2020, <https://www.jpost.com/Middle-East/Soleimani-killing-Window-of-opportunity-open-for-Israel-against-Iran-614151>. [↪](#)
16. Yaniv Kubovich, “Israeli Military Intel: Iran Is Two Years Away from Nukes, but Hasn’t Decided on Breakout,” *Haaretz*, February 9, 2021, <https://www.haaretz.com/israel-news/premium-israeli-intel-iran-is-two-years-away-from-nukes-but-hasn-t-decided-on-breakout-1.9525099>. [↪](#)
17. Yonah Jeremy Bob, “Israel thinks Iran 2 years from being able to detonate nuke – exclusive,” *The Jerusalem Post*, November 16, 2022, <https://www.jpost.com/middle-east/iran-news/article-722597>. [↪](#)
18. “Iran Threat Assessment: Introducing the Iran Threat Geiger Counter,” *Institute for Science and International Security*, October 20, 2022, <https://isis-online.org/isis-reports/detail/iran-threat-assessment-introducing-the-iran-threat-geiger-counter/8>. [↪](#)

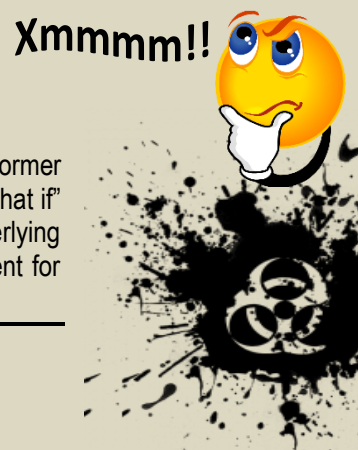
David Albright is President and Founder of the Institute for Science and International Security.

Why Germany Won’t Go Nuclear

By Roger George and Robert Levine

Source: <https://nationalinterest.org/feature/why-germany-won%E2%80%99t-go-nuclear-205966>

Dec 05 – Stephen Szabo’s provocative [article](#) in *The National Interest* presents what we as former intelligence analysts would characterize as a “what if” or “low probability/high impact” scenario. “What if” exercises are useful to challenge the conventional wisdom, if only to demonstrate that the underlying conditions for current assessments remain solid. In this case, we believe that the counterargument for





Germany remaining a non-nuclear ally within NATO is much stronger than the case for Germany exiting the Nuclear Non-proliferation Treaty (NPT) or even seriously considering developing its own nuclear capability.

Szabo's argument rests on several factors and questionable assumptions that he and a few German commentators cite. First, Russia has proven to be a much less capable conventional military threat and now must rely more on its nuclear forces. Second, that the entire European security architecture is now dramatically changed for the worse and U.S. security guarantees are untrustworthy. And third, that Vladimir Putin's invasion of Ukraine has thrown out all previous German commitments made regarding its rejection of nuclear weapons.

We find these arguments unconvincing and overdrawn. For political, military, and economic reasons, there's a stronger case for Germany to avoid any serious moves toward developing its own nuclear deterrent. While debates over Germany's nuclear status regularly occur whenever there is an apparent shift in European or American attitudes toward nuclear deterrence, there are simply too many obstacles to Germany taking such a provocative step.

### **International and Domestic Barriers Should Hold**

Both international and domestic political constraints on Berlin remain essentially in place. Internationally, the West is committed to preserving the NPT, given concerns about North Korea and Iran's intent to develop such weapons. As an NPT signatory, Germany's decision to exit the treaty would essentially destroy long-standing Western solidarity and encourage additional nuclear proliferation. As most scholars of German politics have recognized, post-1945 Germany has felt most secure when it placed its foreign and security policies squarely within a broader Western security structure. Germany's military, for example, is embedded into the NATO military structure—a unique condition made obligatory for West Germany to be rearmed and join the alliance in 1955. And, its conventional forces are ultimately under the control of NATO's supreme allied commander, always a senior U.S. military leader. So, Germany would either have to place its nuclear weapons under U.S./NATO control or exit the alliance itself—the latter of which is more likely to undermine Europe's security architecture than anything Putin has done. Moreover, Russia's invasion of Ukraine may have shaken Europe's security environment, but it has solidified the transatlantic alliance and its resolve, not weakened it.

Domestically, the politics of nuclear weapons has not changed as much as Szabo suggests. That some Christian Democratic security experts believe that there needs to be a debate is [not new](#). Former President Donald Trump's threats to soften the U.S. commitment to the NATO treaty's Article V on collective defense did spawn speculation. But in 2021, the current German coalition government parties were debating the merits of exiting NATO's nuclear sharing and some coalition leaders wanted to [press the United States to remove](#) the few remaining U.S. nuclear weapons in Germany in line with German public opinion. Fast forward to post-Ukraine invasion, and public opinion had shifted dramatically in favor of retaining U.S. weapons. This does not suggest that Germans are [worried](#) about a weakened U.S. commitment or a hankering for its own forces. Needless to say, the public's attitudes are changeable depending on the perception of the nuclear risks that Berlin faces. The Biden administration's forceful pledges to defend "every inch" of NATO territory and its sizable arms transfers to a non-NATO member like Ukraine suggest a comforted German public.

The argument that Germany might skirt the provocative move toward an independent nuclear force by pressing the French to extend their nuclear deterrence to Germany seems to us a bridge too far. The French *Force de frappe* has long been seen as an [independent nuclear force](#) designed to retain Paris's freedom of action as well as complicate Moscow's own nuclear targeting plans. In fact, flagging German confidence in the United States suggested by proponents of a German or European nuclear option is not borne out by [recent opinion polls](#); in June 2022, strong majorities in most countries—including Germany—viewed the United States as a reliable partner. At this juncture, Berlin has no reason to question Washington's reliability.

### **Reality Check: Technologically Feasible, but Costly, Demanding, and Risky**

The technical, economic, and military challenges of creating and maintaining a viable nuclear capability add to the political arguments against a German nuclear program.

To be sure, Germany would have several options to create fissionable material for warheads—all of which are technically feasible. Berlin could retain its civilian nuclear reactors (extended for now during the Ukraine War) and use them to produce plutonium for warheads. This path would require substantial plutonium reprocessing capabilities, a task well within the country's capability. Using commercial reactors would be the least expensive and fastest option for Berlin. Alternatively, Germany could build devoted plutonium-producing reactors at a cost of billions of dollars. This more expensive route would delink the commercial and military programs but provide a rallying point against the effort and become one of the highest priority Russian targets for technical (including cyber sabotage) and military countermeasures.

Berlin could instead opt for uranium-based weapons and create stocks of weapons-grade Uranium-235 through centrifuge enrichment. Building cascades of centrifuges is a major, lengthy, and costly industrial enterprise, but again well within Berlin's technical capability. Turning weapons-grade Plutonium-239 or Uranium-235 into viable warheads is not trivial. However, the greater challenge for Berlin would arise as it







tries to convert a stockpile of nuclear warheads into a credible nuclear strike capability. The research, development, production, and force integration efforts would cost many billions of euros and take years if not a decade or more.

Three days after Russia's attack on Ukraine, Chancellor Olaf Scholz announced an enormous [rearmament program](#), including spending an additional 100 billion euros, or roughly twice the country's annual defense budget. The weapon systems proposed for purchase, such as F-35 fighter jets, along with [recapitalizing a military](#) that has been short-changed for many years, will consume this plus-up. A nuclear program on roughly the same scale as [France's](#) might cost an additional several billion euros per year, after much larger initial R&D and procurement costs. As the French and British see with their aging delivery systems, replacing submarines and missiles is shockingly expensive.

No German nuclear capability makes military sense, or can be rationally constructed, without a clear concept of its fundamental purpose. In the most general sense, nuclear weapons can be used to threaten a potential enemy's warfighting capabilities (its own nuclear or conventional strike capabilities, such as missiles and aircraft bases, army garrisons, military ports, and command and control facilities) or its civilians (populations, economic centers, and infrastructure). In general, the former—counter-force capabilities—are intended to limit the damage an enemy can inflict in its own strike and reduce its conventional capabilities. The latter—counter-value capabilities—are credible only as brutal punishment for aggression—and of necessity hold civilians at risk.

A German counter-force capability against Russia would demand a colossal expansion of its military and development of new, expensive, and technically challenging systems. The potential Russian target set of bases and forces is vast and distant. Although aircraft could strike some targets as a signal of resolve early in an escalatory phase, such delivery systems would not provide the near-certainty of delivery, speed, and accuracy required for a counter-force posture to deter enemy actions.

A counter-value capability would be less demanding, but not trivial. Aircraft might suffice, but unless used early in a conflict—defeating the very purpose of this capability as a fundamental deterrent—German planners would have to assume that Russia would effectively strike German airbases during a conventional phase of a war.

There is a commonly held perception that the mere possession of nuclear weapons generates deterrence. Military planners and analysts recognize that numbers and types of warheads, delivery systems, targeting capabilities, command and control, employment doctrine, training, warning and alert systems, and many other components of a nuclear capability together create a viable nuclear posture. But all of these must be considered in the context of potential opponents and their possible counteractions.

Berlin would almost certainly have to develop a submarine-based missile-borne nuclear capability to create any semblance of credible deterrence. An alternative land-based system would invite Russian planners to prepare for terribly destructive, preemptive nuclear strikes for their own damage-limitation approach. It is hard to imagine that the German populace would find such a possibility, fueled by Berlin's own actions, acceptable. In contrast, submarine-based missiles would be more survivable and still have remarkable accuracy. However, the scale of Russian target sets—their number, character, and distances—would call for a very large submarine force for a counter-force posture. Submarines in port are tempting targets and would provide little more value than aircraft on bases. Submarines and their crews demand rotations for rest and refit, and countries have found that they can keep perhaps one-third of their fleet at sea at any time. Once a planner does the math—the number of targets, the number of missiles to raise the confidence of destruction, the number of missiles per submarine—the total fleet size soars. Moreover, command and control arrangements to guarantee that weapons would not be used unless ordered by the government, and would be used if ordered, represents a key vulnerability. Russian planners would be foolish not to devote efforts to hinder, delay, corrupt, or defeat German nuclear use authorization. These could take extremely destructive forms, including “decapitation” strikes to eliminate government and military leaders.

In practice, a counter-value posture is the most Germany could militarily afford or operate, perhaps no larger than the French or British [arsenals of 200-300 warheads each](#). All things considered, the costs and operational constraints would argue for a German nuclear arsenal aimed at killing millions of Russians rather than defanging the huge Russian nuclear force. How tolerable would this be to Russians or the German public? Not very, in our opinion.

### **Germany Becomes the Target**

This brief military assessment raises perhaps the greatest conundrum for any German leader contemplating an independent nuclear strike force. Its very existence would increase the chances of national destruction through Russian preemption in a deep crisis or war. Moreover, any contemplated use has little credibility. Initial German tactical use as a warning might trigger a damage-limiting Russian strike. Any full-blown use would guarantee Germany's utter destruction. Germans contemplating the size of the needed investment, the risks associated with its existence, and the consequences of its use—killing millions of innocent Russians and inviting the retaliatory destruction of their own country—are unlikely to opt for this path.

No country wants to be a nuclear battlefield. Were Germany to build and deploy nuclear-armed systems, it is obvious that countries between Germany and Russia—Poland, Ukraine, etc.—might view their position as uncomfortable. Even if Berlin committed itself to using nuclear arms only in defense, a German umbrella





wielded by authorities in Berlin might give Warsaw and Kyiv pause. Consultations in a crisis or war, moreover, could provide the very signal for preemptive Russian action.

**Foreseeable Future: A Vanishingly Small Probability**

No intelligence or defense analyst who has lived through the collapse of the Soviet Union or the rise of international terrorism is likely to deny categorically the possibility of a low-probability future. We believe it would take far more drastic geopolitical changes than we have seen or anticipate for Germany to turn to developing its own nuclear weapons. Moreover, the dimensions of those changes would be difficult to miss. If such tectonic shifts occur, a nuclear Germany would be only one of many disturbing outcomes.

Drs. Roger George and Robert Levine are former political and military intelligence analysts and have taught national security strategy at the U.S. National War College. They are co-editing a forthcoming book on *CIA Analysis: Voices From Inside*.

**EDITOR'S COMMENT:** It seems that the authors are forgetting that we are talking about Germany, the mother of two world wars!

Here is a good one!

**UN: Israel must take 'immediate steps' to give up nuclear weapons**

Source: <https://www.middleeastmonitor.com/20221208-un-israel-must-take-immediate-steps-to-give-up-nuclear-weapons/>

Dec 08 – The UN General Assembly has called on Israel to take "immediate steps" to surrender its nuclear weapons and implement UN resolutions fully on the establishment of a nuclear-weapon-free zone in the Middle East.

The General Assembly vote was carried 149-6 yesterday. Israel, Canada, Micronesia, Palau, the US and Liberia opposed the resolution, while another 26 countries abstained, including India and many European states.

Among other provisions, the draft resolution called for immediate steps towards the full implementation of the resolution on the Middle East adopted by the 1995 Non-Proliferation Treaty. The key component of the package deal adopted in the treaty calls for the creation of a Middle East "zone free of nuclear weapons as well as other weapons of mass destruction" including "their delivery systems."

The world body insisted that Israel must "accede to the Treaty without further delay, and not to develop, produce, test or otherwise acquire nuclear weapons, to renounce their possession and to place all its poorly guarded nuclear facilities under full-scope International Atomic Energy Agency (IAEA) safeguards."

Israel's possession of nuclear weapons is an open secret. Although it's widely believed to have a stockpile of nuclear weapons, the apartheid state neither acknowledges nor denies the existence of a nuclear arsenal. Israel is not a party to the Non-Proliferation Treaty and has not accepted IAEA safeguards on some of its principal nuclear activities.

Western countries have generally tolerated Israel's policy of nuclear ambiguity despite the threat it poses to the region. The UN resolution presumes that Israel has such weapons and calls on it to accede to the Non-Proliferation Treaty.

**EDITOR'S COMMENT:** UN General Assembly from a parallel universe! If they make the same call for the US, China, France, the UK, etc., they will prove that they mean what they say. Nukes are very serious to joke about!

**Greek Cities want the government to join the TPNW**

By Nikos Stergiou (Greek branch of World without Wars and Violence)

Source: [https://www.icanw.org/greek\\_cities\\_appeal](https://www.icanw.org/greek_cities_appeal)

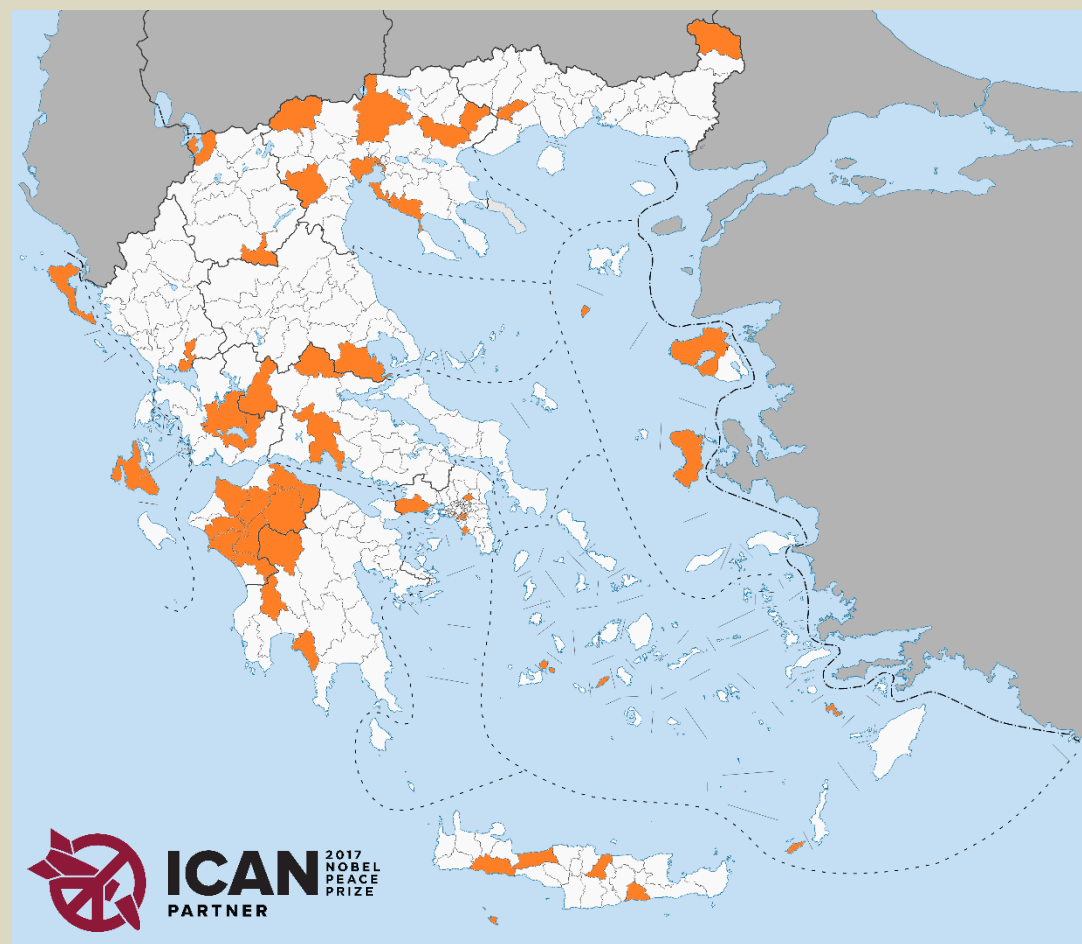
Dec 09 – The Peace and anti-nuclear movement in Greece has a long history and it was always connected to European peace movements. We should not forget the execution of Nikos Nikiforidis in 1951 because he was gathering signatures in support of the Stockholm Appeal and the political assassination of Grigoris Lambrakis in 1963 after one month of the first Peace March in Greece and an anti-nuclear public speech. In the 80's and 90's, the anti-nuclear movement was always active, as it was in the rest of Europe, under the fear of a possible nuclear war between the USA and USSR. Initiatives such as "Nuclear Weapons Free Municipalities" and the Antinuclear Observatory of the Eastern Mediterranean, among others, were those with the most impact at a local and national level.

Although there was such a colourful anti-nuclear and pro-peace movement in Greek society, Greece hosted nuclear bombs at the military air base of Araxos until 2001 [1][2]. And in 2018, the news that the facilities were being modernized, in order to host nuclear weapons once again, was terrifying. This was





the ignition of the idea to start a campaign at a local level with a national impact. The perfect tool came in 2017: the Treaty on the Prohibition of Nuclear Weapons (TPNW) and the ICAN Cities Appeal. The first contacts were through personal meetings, where we had the possibility to talk with a Mayor or a President of the Municipal Council. But it also included official invitations and calls for voting in favour of the appeal to all the 23 municipalities that are already members of Mayors for Peace. A good start, some might say but unfortunately this connection was long forgotten by the majority of those municipalities. The reason was that in Greece's



public sphere, the idea of a nuclear threat has faded over time.

After the first five positive municipalities, the escalation of the campaign was immediate. All 332 municipal councils in Greece were invited officially to vote in favour of the Appeal. It was a risky choice, since the majority of the Mayors were elected in 2019 with the support of the right-wing party, which is also the present government that supports NATO's nuclear weapons better than NATO itself. The war in Ukraine and the threats of possible nuclear strikes though, has awakened the worst fears in all human beings. So, one by one, the municipal councils that discuss the appeal, voted in favour, supporting the TPNW and "call on the Greek Government to sign and

ratify it immediately". Once again, it was proven that the majority of the people have the minimum sense to say "no" to the ultimate weapon of mass destruction. The municipalities that have not said "yes" to the TPNW, they have just not yet discussed the appeal in the municipal council.

In 2023, municipal and parliamentary elections will take place again in Greece. The TPNW is not high up the political agenda. "The NPT is enough" says the Ministry of Foreign Affairs and is trying to minimize the importance of the TPNW. The political parties are lost in several directions, trying to support the TPNW, but also trying to not annoy NATO, at least the parties that are in a possible future governmental scheme. Greens and DiEM25 say "yes" to the TPNW but the Communist Party is still weighting its answer since it prefers a more "all in one" Treaty. As for SYRIZA, the left party that was in the Government the period 2015 – 2019, the party declares that "as a political party we support TPNW, but as a possible future government we have to discuss carefully first". The #σώσετηνπόλη campaign is producing interesting discussions inside the municipal councils and keeps the TPNW high up the political agenda.

The possibility of hosting nuclear weapons again is really terrifying for Greeks and the more the discussion about the TPNW is spreading, the more difficult it is for this to happen. The Cities Appeal is clearly a political act by local representatives that are someone's neighbour, relative, or partner. They have the face of the person next to you on the local bus or at school. It is another act that brings all to ask the question "in what kind of society do I really want to live in?" And it transcends political parties and constitutions. It reminds us of the peace and anti-nuclear culture we have in our hearts and minds as it places human beings at the centre of the discussion and gives us the chance to say "no" to nuclear weapons and to say "yes" to a nuclear-free world.

**By the time this article is published, 58 Greek municipalities support ICAN's Cities Appeal.** They represent more than 15% of the Greek population or around 2 million citizens. The vast majority of them







joined the campaign after the Russian invasion of Ukraine and the war that unfortunately is still going on. And there will be more municipalities signing up in the coming weeks. This is the result of a campaign called #σώσετηνπόλη (“#SaveTheCity”) that has been underway for the last one and a half years, organized by the Greek branch of “World without Wars and Violence”, an international partner and local representative of ICAN. And this is the story behind this result.

**EDITOR’S COMMENT:** If TPNW/ICAN assures that radioactive plumes will spear the cities participating in this program, then it is OK. But I am afraid that it is useless for the *sheep* to pass resolutions in favor of *vegetarianism*, while the *wolf* remains of a different opinion (William Inge).

## What will happen in the GCC area if Iran becomes nuclear?

By the Editor of “C2BRNE Diary”

Iran needs a few nuclear weapons to counter the sanctions imposed by the West and soon they will have them. Logically the GCC countries have nothing to fear from their neighbor. Qatar maintains good commercial relations with Iran and their oil/gas fields are next to one another. There is an old joke where a man thought he was corn. After long psychotherapy managed to feel human again but still posed this question “*I know that I am not a corn anymore, but do chickens know that?*” GCC countries would feel more secure if they had some equal analog that is own nuclear weapons. Of course, a single nuclear missile can turn Kuwait City, Manama, Doha, Abu Dhabi, Dubai, Muscat, and Riyadh into a radioactive desert well before a retaliation strike takes place – perhaps except for KSA due to its size. When comes to answering the question, two options are available: (1) make their own nukes – UAE first since they already have the Barakah nuclear power plant, and then KSA, and (2) defend-in-place since, except KSA, they do not have the geostrategic depth to hide/deploy – this means that they have to go underground. A big project but they have the money to do that if they desire to avoid returning to their camels in the deserts.

## US scientists reach long-awaited nuclear fusion breakthrough

Source: <https://edition.cnn.com/2022/12/12/politics/nuclear-fusion-energy-us-scientists-climate/index.html>

Dec 12 – For the first time ever, US scientists at the National Ignition Facility at the Lawrence Livermore National Laboratory in California successfully produced a nuclear fusion reaction resulting in a net energy gain, a source familiar with the project confirmed to CNN.

The US Department of Energy is expected to officially announce the breakthrough Tuesday.



An aerial photo shows Lawrence Livermore National Laboratory in Livermore, California. National Nuclear Security Administration/ Handout/ Reuters/FILE



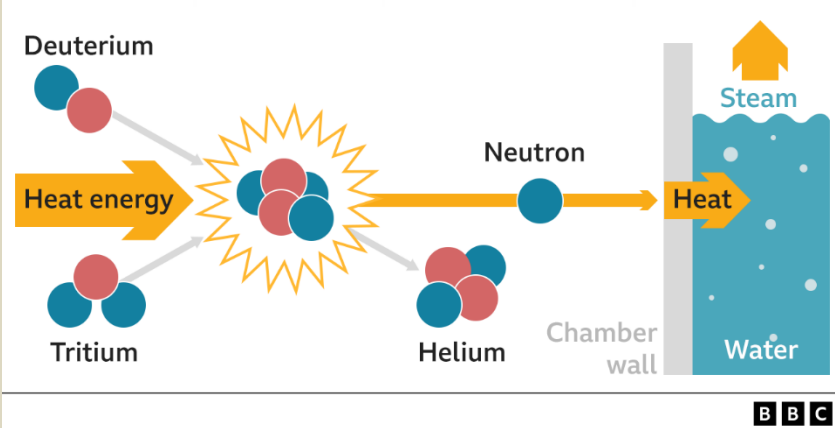


The result of the experiment is a massive step in a decadeslong quest to unleash an infinite source of clean energy that could help end dependence on fossil fuels. Researchers have for decades attempted to recreate nuclear fusion – replicating the fusion that powers the sun.

US Energy Secretary Jennifer Granholm will make an announcement Tuesday on a “major scientific breakthrough,” the department announced Sunday. The breakthrough was first reported by [the Financial Times](#). [Nuclear fusion](#) happens when two or more atoms

### How nuclear fusion works

1	2	3	4
Hydrogen atoms are heated	Fusion reaction	Helium, neutron and energy released	Neutron energy heats water



are fused into one larger one, a process that generates a massive amount of energy as heat.

Scientists across the globe have been inching toward the breakthrough; in February, [UK scientists announced](#) they had more than doubled the previous record for generating and sustaining nuclear fusion.

In a huge donut-shaped machine called a tokamak outfitted with giant magnets, scientists working near Oxford were able to generate a record-breaking amount of sustained energy. Even so, it only lasted 5 seconds.

The heat sustained by the process of fusing the atoms together holds the key to helping produce energy.

As CNN [reported earlier this year](#), the process of fusion creates helium and neutrons – which are lighter in mass than the parts from which they were originally made.

The missing mass then converts to an enormous amount of energy. The neutrons, which are able to escape the plasma, then hit a “blanket” lining the walls of the tokamak, and their kinetic energy transfers as heat. This heat can then be used to warm water, create steam and power turbines to generate power.

The machine that generates the reaction has to undergo serious heat. The plasma needs to reach at least 150 million degrees Celsius, 10 times hotter than the core of the sun.

The big challenge of harnessing fusion energy is sustaining it long enough so that it can power electric grids and heating systems around the globe.

A UK fusion scientist told CNN that the result of the US breakthrough is promising, but also shows more work needs to happen to make fusion able to generate electricity on a commercial scale.

“They have worked on the design and the makeup of the target and the shape of the energy pulse to get much better results,” Tony Roulstone, from the University of Cambridge’s Department of Engineering, told CNN.

“The opposing argument is that this result is miles away from actual energy gain required for the production of electricity. Therefore, we can say (it) is a success of the science but a long way from providing useful energy.”

## The One Thing Everyone’s Ignoring About the Fusion Energy Breakthrough

Source: <https://news.yahoo.com/one-thing-everyone-ignoring-fusion-095819172.html>

Dec 14 – At 1:00 a.m. Pacific Time on Dec. 5, 2022, the National Ignition Facility at Lawrence Livermore National Laboratory in California [created nuclear fusion without thermonuclear detonation](#). The experiment, heralded in the Department of Energy’s [own release](#) as history-making and announced Tuesday by Secretary of Energy Jennifer Granholm, converted 2.05 megajoules of laser energy into 3.15 megajoules of energy from fusion, all produced and recorded and spent in less than a blink of an eye. It is, at once, a meaningful scientific achievement, and one whose entire reason for being rests inside the long-term work of sustaining an arsenal of oblivion.

“Our thermonuclear weapons have fusion ignition that takes place in our weapons, so studying fusion ignition is something we do to support the stockpile stewardship program,” Mark Herrmann, Lawrence Livermore’s program director for weapon physics and design, said during a technical panel on Dec. 13. “In addition, fusion ignition creates these very extreme environments that we have no other way to access on Earth. In this experiment, for the first time ever, we were able to put some samples of materials that are important for future stockpile







modernization efforts that are going on at Lawrence Livermore today in very close to this intense neutron burst and then see how did they respond to that intense neutron burst.”

The stockpile stewardship in question refers to the continued existence of the U.S. nuclear arsenal, the second-largest in the world. Nuclear weapons, though bound to their origin in World War II and development throughout the Cold War, are an ever-present fact of modern geopolitics. They are an enduring threat, and to a large degree the work of stockpile stewardship is about making sure the weapons the U.S. already has will work, if a president gives the order to launch.

“We’re using the output from these really cool science experiments to actually test materials for stewardship applications,” said Herrmann, in a phrase that seemed exactly backwards. The great discovery of the day was scientific, but the facility exists for weapons science first, civil energy second at best.

Ground broke for the National Ignition Facility on [May 29, 1997](#), with construction continuing into 2009. The initial impetus for the facility dates back earlier, with its concept [first theorized](#) in 1959-1960—less than a decade after the first hydrogen bomb test. Hydrogen bombs are two stage, using an atomic fission reaction to trigger a fusion reaction in a second nuclear core in the same warhead. In warhead design, the focus is on intense power, creating the most destructive force from the fewest needed inputs.

Fusion as energy, instead, promises to be self-sustaining after it’s initiated, which means the input energy need not be the kilotons of atomic detonation. A 1 megajoule lasers, first demonstrated in 1960, could provide one avenue for energy production.

In the Dec. 5 test, the 192-laser array of the National Ignition Facility directed 2.05 megajoules into the target, which briefly produced 1.5 times the energy pumped into it. That’s a gain of energy within the reaction, but not in overall terms. Kim Budil, director of Lawrence Livermore National Laboratory, noted that the test took “300 megajoules from the wall for 2 megajoules of laser.”

During the Cold War, the U.S. continued to develop and refine nuclear warheads through live testing. After the Partial Test Ban Treaty of 1963, the country continued nuclear tests underground (literally, not figuratively), up until Sept. 23, 1992. On that day, “Divider,” an otherwise routine test to ensure warhead reliability, became the last live nuclear detonation by the United States.

A moratorium on live testing and the dissolution of the USSR in 1991 meant the immediate risk nuclear peril had diminished, though was hardly absent. While the U.S. and Russia (which inherited the USSR’s warheads and weapons) decreased their overall stockpile size down to under 6,000 warheads apiece, the logic of nuclear weapons meant that the U.S. wanted to ensure its warhead still worked.

Now, though, the U.S. needed a way to do this without live nuclear tests.

“Earlier this year I had the opportunity to remember the 30th anniversary of Divider, the last explosive nuclear weapons test conducted by the United States,” Jill Hruby, undersecretary for nuclear security and administrator for the National Nuclear Security Administration, said at the DOE’s Dec. 13 press conference. “In reflecting on Divider, I spoke on how far our stockpile stewardship program has come, and in how many ways we now understand our nuclear weapons better than we did when we were testing.”

Among the ways the National Nuclear Security Administration maintains America’s existing stockpile are materials tests and computer simulations. Using data gleaned from the 1054 live nuclear tests, as well as now [decades of computer models](#), nuclear researchers at labs like Los Alamos and Lawrence Livermore have continued to design and refine how these weapons work.

“Fusion is an essential process in modern nuclear weapons, and fusion also has the potential for abundant clean energy,” Marvin Adams, NNSA deputy administrator for defense programs, said during the Dec. 13 presser. “As you have heard, the breakthrough at NIF has ramifications for clean energy. More immediately, this achievement will advance our national security in at least three ways.”

Those three ways all emphasized the importance of nuclear science for maintaining and sustaining a nuclear deterrent, without conducting live explosive nuclear tests. Having the scientific expertise and skill to evaluate nukes without detonations lets the U.S. show the world it knows what it’s doing when it comes to nuclear weapons, said Adam. It also lets the U.S. prove to allies that, because the American nuclear arsenal is well and competently maintained, there’s no need for these countries to develop their own nuclear programs.

As a way of strategic thinking, a nuclear arsenal is a tool that deters and constrains the actions of other nations, especially other nuclear-armed nations, because the threat of retaliation is far greater than any gain from initiated war. Deterrence is a theory with limitations; nuclear-armed Pakistan and India have fought multiple wars, though the wars fought have been on a small scale. Similarly, soldiers from nuclear armed India and China regularly engage in melee skirmishes along disputed sections of their border. These skirmishes are fought with [sticks and stones in the shadow of nuclear oblivion](#), with guns set aside so as to not escalate the violence. Deterrence theory also shapes the kinds and types of military aid the [United States provides to Ukraine](#) as it fights against Russian invasion. Weapons with more immediate battlefield utility have been prioritized over long-range missiles, which could be seen as a threat not just to Russian soldiers but to Putin himself.

While Russia’s nuclear arsenal has long been at the foreground of U.S. strategic thinking, China’s growing nuclear stockpile and expanding array of missiles and launch sites, are an increasing part of the [Pentagon’s calculus](#). Deterrence holds fear of oblivion alongside fear of obsolescence. Fear that warheads may not detonate properly on arrival is one of the factors driving a restart of plutonium pit production at







Los Alamos, as the lab tries to [refurbish old warheads](#) out of a concern that essential bomb components may have decayed in the decades since they were assembled.

“Unlocking ignition at NIF will allow us to probe the extreme conditions found at the center of nuclear explosions, and address significant long-standing stewardship questions,” said Hruby.

The clean energy promise of fusion is one step closer after the Dec. 5 test, even at the small scale of energy gained. The work of turning that success into a sustainable basis for fusion power plants is still [likely decades away](#), even if the timeline might be shorter than the often-quipped 50 years away.

In the meantime, the nuclear labs at NIF will continue to better study and understand the materials and science of nuclear warheads and explosions. There’s always room on the budget for the science of energy (destructive), even and especially as it incidentally leads to breakthroughs in the science of energy (productive). Just don’t expect the weapons research to get the same high-profile publicity from the DOE or Secretary Granholm.

## If Finland joins NATO, it needs a new nuclear weapons policy

By Robin Forsberg, Aku Kähkönen, and Jason Moyer

Source: <https://thebulletin.org/2022/12/if-finland-joins-nato-it-needs-a-new-nuclear-weapons-policy/>

Dec 08 – As an aspiring NATO member, Finland must update its nuclear weapons policy. Nuclear weapons are an important pillar of the defensive alliance, which has the [official position](#) that for as long as nuclear weapons exist, NATO will inherently be a nuclear alliance.

In September 2022, Russian President Vladimir Putin [threatened](#) to use nuclear weapons, saying “In the event of a threat to the territorial integrity of our country and to defend Russia and our people, we will certainly make use of all weapon systems available to us. This is not a bluff.” Putin’s statement—and others—[triggered](#) a heated debate about nuclear weapons in Europe not seen since the darkest days of the Cold War. Even though Russia’s military doctrine [prescribes](#) nuclear weapons for self-defense, the doctrine is opaque and Putin is largely considered in the West as an unpredictable actor. As the invasion of Ukraine escalates and Russian losses multiply, there are widespread concerns that Russia might rely on its nuclear arsenal as a last-ditch method of coercion. These concerns happen as Finland contemplates its views toward nuclear weapons as a future member of the alliance.

After filing its membership application in May 2022, Finland is now in the midst of its NATO [accession process](#), with only Turkey and Hungary’s approval remaining. In its application, Finland is not seeking [any exemptions](#) to its membership and is committing to the alliance fully. This has [initiated discussions](#) about its upcoming policy on nuclear weapons. On November 7, President Sauli Niinistö [stressed](#) the Finnish position: “Let me make it clear: even if we do not impose any restrictions on our membership of NATO in advance, Finland has no intention whatsoever of bringing nuclear weapons onto its soil. Nor have I seen any indication that anyone is offering them to us.” NATO’s two other Nordic members—Norway and Denmark—have prohibited NATO bases or nuclear weapons within their borders in peacetime. By applying for full NATO membership without any explicit restrictions, Finland allows itself the opportunity to chart its own decisions on nuclear weapons. But there is one caveat: Under Finland’s current national legislation nuclear weapons [are illegal](#). By joining NATO, Finland will be allied with countries that have nuclear arsenals—and are prepared to use them if deemed necessary. This aligns with the creed of the alliance: Nuclear weapons are a core component of NATO’s deterrence. This will be the new security reality facing Finland the day it joins the nuclear alliance. Yet, it has not been sufficiently [debated](#) what becoming a NATO member will mean for Finland’s approach to nuclear weapons. In part, this is due to interest in both Finland and NATO for a speedy and uncomplicated accession. But there is also a tradition of not debating national strategic security policies in public fora due to the Finns’ high trust in their national authorities. A healthy national debate, however, is needed to improve the understanding of nuclear weapons policies among the Finnish population and their potential impact on Finland’s security.

Finland’s nuclear weapons policy as a member of NATO should serve both the domestic and the international interests of the Finnish people. Finland has a history of a strong non-nuclear proliferation policy. In 1968, it was the first country to sign the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) and has ever since shown strong [support](#) for multilateral non-proliferation and conventional disarmament treaties. But this dogmatism has somewhat wavered in recent years, even before Russia invaded Ukraine. In July 2017, when the United Nations Treaty on the Prohibition of Nuclear Weapons (TPNW, also known as the ban treaty) was signed by 122 countries, Finland chose to abstain from supporting the treaty as a result of changing national security priorities. Around that time, [pundits](#) in Finland believed that a vote for prohibiting nuclear weapons would not lead to the desired outcome, given the opposition of the five nuclear-armed permanent members of the UN Security Council to a vote for the treaty, which ultimately would water it down. Experts theorized at the time that Finland abstained from voting not to jeopardize its prospects of joining NATO.

When Finland joins NATO, its defense minister will have a seat in NATO’s Nuclear Planning Group, the senior body that discusses the alliance’s nuclear doctrine and sets policy. What the Finnish minister will





do in this seat and what role it will assume in this alliance is a topic that has not yet been discussed or disclosed publicly and will require holistic, political, and military evaluation from the country's political leadership. Having a seat in the Nuclear Planning Group will also give Finland's government and military access to previously unobtainable operational information regarding the alliance's nuclear arm. Discussing Finland's revised nuclear weapons policy is important not to jeopardize the ethics of Finland's [continuous and long-standing support](#) of disarmament and non-proliferation efforts. The debate should also be reflective of the people's willingness to take part in NATO's nuclear weapons exercises, activities, or planning.

As full ratification approaches, political parties and parliamentarians in Finland should engage head-on in a policy debate about nuclear weapons and NATO. In the spirit of the Finnish security policy tradition, national politicians should strive to find a consensus that would both endure the test of time and possible future political shifts. A public domestic debate diminishes the risk of political backlash against NATO membership and increases the Finnish population's resilience in the long term. As Finland becomes a party to a nuclear alliance, it must begin the process of updating its nuclear weapons policy.

**Robin Forsberg** is a former visiting scholar at the Johns Hopkins University School of Advanced International Studies' Foreign Policy Institute and a consultant, doctoral researcher, and a fellow of the Manfred Wörner Seminar at the German Bundeswehr.

**Aku Kähkönen** is a public sector consultant at Accenture Finland, a fellow of the Manfred Wörner Seminar at the German Bundeswehr, and a reserve officer in the Finnish Navy.

**Jason C. Moyer** is a program associate for the Global Europe Program at The Woodrow Wilson International Center for Scholars.

## Why a new convention to protect nuclear installations in war is a bad idea

By Michal Onderco and Clara Egger

Source: <https://thebulletin.org/2022/12/why-a-new-convention-to-protect-nuclear-installations-in-war-is-a-bad-idea/>

Dec 05 – In recent weeks, several voices have called for adopting new legal instruments to protect civilian installations from military attacks during conflicts. The prime motivation stems from Russia's shelling and occupation of the Zaporizhzhia nuclear power plant—Europe's largest—as part of its ongoing war against Ukraine. This event, combined with Russia's repeated transgression of international laws of armed conflicts, [is said to reveal](#) the weaknesses and inadequacy of existing legal protections. Such arguments were also aired during the 2020 NPT Review Conference held this summer in New York (after a two-year delay due to the global COVID-19 pandemic) as well as, more recently, [in the columns](#) of the *Bulletin of the Atomic Scientists*. Proponents of improved legal protections [argue](#) that a new convention [is needed](#) because of the ambiguity of existing international laws and the lack of enforcement mechanisms.

Although concerns about the protection of nuclear sites in war settings are wholly justified, the cure proposed might be worse than the disease. First, calls for a new regime reflect a partial reading of the [legal and political mechanisms](#) surrounding the protection of nuclear installations during a conflict. Second, because international law and political commitments already protect against attacks on nuclear installations, a new convention could add undesirable complexity with countries picking and choosing their commitments, which ultimately would weaken existing protections. Calls for new legal instruments would also send counterproductive signals in a context where the value of international norms is already challenged at the domestic and global levels.

### There are no gaps

Legally, international humanitarian law norms already establish a detailed and unambiguous system of protection to avoid nuclear facilities becoming battlefields or being targeted by military attacks. The obligations of warring parties derive from two sources: They are linked to the general protection applicable to all types of civilian infrastructure in wartime but are reinforced and by specific protections applicable to nuclear power plants.

By default, nuclear facilities are considered civilian infrastructures even if doubts exist about their use, according to the Additional Protocol I to the Geneva Conventions (1977) as well as in contact areas (when military forces or combat operations are in the vicinity of power plants). This consideration is [confirmed](#) in the official commentary on the Additional Protocol I published by the International Committee of the Red Cross in 1987. Nuclear facilities are therefore already protected against attacks and reprisals.

One could argue that Russia withdrew from the Additional Protocol I in 2019. At the time, Russia argued that the International Humanitarian Fact-Finding Commission—established by the protocol to investigate breaches to the international humanitarian law—[could be biased](#), as it did not include a Russian representative. But because of the unique nature and scale of the risks associated with nuclear facilities, other international norms apply, too. Warring parties have an obligation to refrain from locating military objectives at or in the vicinity of such facilities. The party controlling or occupying a nuclear site is required to take all the measures to prevent the release of “dangerous forces” from dams and nuclear power plants whose destruction may release dangerous







destructive factors and cause severe losses among civilians, and to maintain the safe and secure operation of the power plant. This obligation originates in Article 43 of the Regulations Respecting the Laws and Customs of War on Land, also known as Hague Regulations of 1899 and revised in 1907. Although over a century old, these provisions still give a bedrock for the law of belligerent occupation today.



IAEA Director General Rafael Mariano Grossi and member of the International Atomic Energy Agency (IAEA) delegation inspect the impacts of a rocket shell during a visit to the Zaporizhzhia nuclear power plant in Ukraine on September 1, 2022. (Photo Fredrik Dahl / IAEA)

Overall, the legal protection against attacks on installations “containing dangerous forces” are seen as so fundamental that they are recognized as a part of the customary international humanitarian law, binding states regardless of whether they signed and ratified (or withdrew from) relevant international treaties. For example, the current military legal codes of [Russia](#), [Israel](#), and the [United States](#) (to name a few) all contain such provisions. From the legal perspective, nuclear facilities are on very safe grounds. Another argument pointing to the inadequacy of existing legal protections is that such protections don’t apply if power plants contribute to the military effort. But this argument is misguided. The Additional Protocols to the Geneva Conventions explicitly provide that nuclear facilities must not be attacked even as part of broader military campaigns, if such an attack “may cause the release of dangerous forces and consequent severe losses among the civilian population” (cited in Article 56(1) of Additional Protocol I). This protection applies against retaliatory action (as cited in Art 56(4) of Additional Protocol I), and legal experts have even [argued](#) that such an act falls under the definition of a war crime (Art 85(3) of Additional Protocol I). Even though—as [argued elsewhere](#)—attacks on nuclear plants are in principle possible under very narrow and exceptional situations, such attacks are never lawful in practice. The rules of proportionality (in this case involving the duty to protect the civilians and their environment from radiation) would make the logistical planning and







ultimate justification of the attack impossible. The customary protection against attacks on nuclear power plants is very strong. There is no legal gap.

Aside from legal prohibitions are political forces. The Board of Governors of the International Atomic Energy Agency (IAEA) already condemned military attacks on nuclear power plants in the past. This view was [later confirmed](#) by the UN Security Council. The IAEA General Conference condemned attacks on nuclear installations serving peaceful purposes in [1990](#) and then in [2009](#). (The 1990 decision [dovetailed](#) with work done in 1980s at the UN Conference on Disarmament toward the prohibition of attacks on nuclear installations. Three months later, the UN General Assembly [voted](#) on a resolution with an equivalent content.) Countries hosting nuclear facilities are therefore de facto committing politically to the unacceptability of attacks against such facilities. So from a political standpoint, Russia's actions are already contrary to the existing commitments it took toward the physical protection of civilian nuclear installations.

Another argument suggests that enforcing prohibitions against attacking nuclear power plants is essentially impossible. But this ignores the impacts that humanitarian diplomacy efforts have had on the behavior of warring parties in theaters as diverse as Afghanistan, the Democratic Republic of Congo, or Yemen. Russia's direct involvement on the Ukrainian battlefield also creates specific demands in terms of respect for international humanitarian law. Even though compliance with such a law is neither conditional nor it can be suspended because of a lack of reciprocity between warring parties, Russia's obligation to secure access to prisoners of war also gives leeway to humanitarian actors and diplomats to pressure the country into respecting its commitments.

### **Fragmentation is dangerous**

Not only is a new convention in regard to attacks on nuclear power plants unnecessary; it would be politically and legally damaging. Adopting a new treaty would signal that current norms have become obsolete, making existing commitments irrelevant. Attacks on international humanitarian law have been frequent in wartime and have been, most of the time, proven wrong and counterproductive. The increase in the number of civil wars following the end of the Cold War has led many commentators to challenge the applicability and relevance of such norms to this new type of conflict. More than 30 years later, however, most warring parties in the world not only understand and recognize the value of international humanitarian law but also commit to enforce such norms while extensive jurisprudence has constantly adapted them to the evolution of warfare.

New norms would increase complexity when it comes to international legal and political commitments related to the protection of nuclear installations in wartime. Rather than reinforcing the existing commitments, it could very well lead to splintering existing international commitments. As those working on international relations know, increasing regime complexity opens the doors for [picking and choosing](#), also known as "[forum shopping](#)." Countries not a party to such an agreement could easily claim that the new protection framework does not constrain their actions.

Multiplying treaties to solve issues in an ad hoc manner risks further politicizing international law in a context of increased polarization of relations between countries, especially great powers. And with politicization comes contestation and delegitimization. A typical example can be found in the attempt by France to come up with a right of humanitarian interference in 1990 in the [UN General Assembly Resolution 45/100](#) to "facilitate the delivery of humanitarian assistance the victims [...] including the establishment of relief corridors." But creating such a new right was not necessary, as both the UN Charter and the Geneva Conventions already detail the obligations of state authorities to protect their civilian population from organized violence of any form and any origin. Although unsuccessful, France's attempt opened a long-lasting controversy over the misuse of humanitarian motives to support countries' military agendas and further politicized the provision of humanitarian aid in conflict settings.

By the same token, the commitment to a new treaty protecting nuclear facilities would most certainly be contested. For instance, would Israel join such agreement after it bombed nuclear installations twice in the region? And would the United States join while keeping "all options on the table" when it comes to Iran's nuclear program? And if these countries don't join a new agreement, would others?

### **No need for a new convention**

Despite the real risks posed by Russia's attacks in Ukraine, there is no need for a new legal framework to address protection of nuclear facilities during wartime. It is hard to imagine how any new international convention would be more enforceable than existing frameworks. On paper, Russia's commitments to the safety of civilian nuclear installations could not be higher. The gap—if any—does not lie in the (lack of) frameworks but in compliance to these frameworks. Enforceability of international law is difficult, and countries most often comply because they see value in it. The mere adoption of a new convention would not alone strengthen protection of nuclear facilities, which would be its prime objective in the first place.

Experts recommending new legal frameworks should beware what they wish for. Before too soon, the international community could find itself in a real debate about the level of protection afforded to civilian nuclear installations. Such debate would likely weaken existing commitments. As is often the case in international politics, good intentions are rarely enough to lead to better international policies.





Rather than looking for creative solutions to non-existing problems, the international community should focus on leveraging existing international legal commitments to ensure Russia complies with its own commitments. Leveraging Russia's interest to access its prisoners of war in Ukraine is one way to demonstrate that compliance with international humanitarian law pays off.

[Michal Onderco](#) is a professor of international relations at Erasmus University Rotterdam.

[Clara Egger](#) is an assistant professor of global governance at Erasmus University Rotterdam.

## Why the world must protect nuclear reactors from military attacks. Now.

By George M. Moore

Source: <https://thebulletin.org/2022/12/why-the-world-must-protect-nuclear-reactors-from-military-attacks-now/>

Dec 15 – Russia's war in Ukraine is approaching its tenth month with no apparent end in sight. All the while, the international community is still scrambling to respond to the threats of attacks on Ukraine's nuclear reactors and nuclear facilities.

Russian occupation of the Chernobyl and Zaporizhzhia reactor sites early in the war has raised deeply concerning issues, as have more recent Russian attacks on Ukraine's utility infrastructure. Even though they have not been directly attacked, other Ukrainian reactor facilities and their associated grid connections—at the South Ukraine, Rivne, and Khmelnytskyi nuclear power plants—remain within the range of Russian air, missile, and drone assets. One might think that Ukraine's counteroffensive to the East and South this Fall might have lessened the threat to these facilities, but that's not the case. Quite the opposite. The latest Russian actions in Ukraine seem to bear out the often-expressed concern that a diminished Russian military and political regime will lash out viciously in reprisal to cover its failings.

The late November shelling near the Zaporizhzhia nuclear power plant has [raised new concerns](#) about the safety of the reactors and spent fuel storage at the site. As has previously happened, the shelling was quickly followed by a series of [counterclaims](#) as to whether Russia or Ukraine was to blame. The IAEA, Ukraine, and even Russia's state-controlled nuclear energy company, Rosatom—which has supervised operations at Zaporizhzhia but has not directly operated the reactors—have again [warned](#) of a possible nuclear accident at the plant.

### Why the international community should act now

The international community seems to believe that the condemnation of Russia's military actions in Ukraine is the appropriate approach while the conflict is still raging and that, somehow, a long-term resolution can come only once the war is over. Another belief seems to be that, because of its actions in Ukraine, it may take quite some time before Russia will be willing to rejoin the international community to better protect nuclear facilities from attacks. Others [have argued](#) that there is no need for any new legal framework and that the existing regime offers sufficient protections.

These assumptions, however, should be strongly reconsidered.

It is imperative for those countries that consider attacks on nuclear facilities in Ukraine to be extremely threatening to stop waiting for a disaster to happen and, instead, act immediately. Whether actions taken by the international community now would significantly reduce the probability of a nuclear accident in Ukraine is obviously debatable, but there is no doubt that waiting to act until after the war ends won't do anything to increase the safety of reactors and facilities being threatened in Ukraine. Even though any actions now by the international community may not be enforceable, prompt action might have some impact on Russian political and military planners.

As the odds of a nuclear accident in Ukraine are growing, the international community has a responsibility to act. And to act *now*.

### Extend the rules of war

While Russia's actions at the Zaporizhzhia nuclear power plant have received widespread [international condemnation](#), its attacks on reactors and nuclear facilities may not be illegal given the fact that no international agreement specifically addresses the issue.

To be clear, Russia appears to be responsible for significant violations of the Geneva Conventions and international human rights law with its [treatment of the reactor operating staff](#) at Zaporizhzhia as well as other incidents of mistreatment of the surrounding population. Attacking a nuclear power plant and its facilities, however, is [allowed](#) under international law and subject only to the constraints of Additional Protocols I and II of the Geneva Conventions and whatever might exist in terms of international norms and customary law on the subject. The Additional Protocol II applies to attacks in civil wars, while Additional Protocol I applies to wars between two countries. Therefore, even though the protection of nuclear facilities is dealt with in both protocols, only Additional Protocol I addresses conflicts like the Russia-Ukraine war. Some could argue that Russia's actions don't go against international norms. But the creation of the Additional Protocols protecting facilities that represent a potential danger if attacked (such as dams,





nuclear reactors, etc.) was necessary to respond to the prevalence of such attacks deliberately carried out during World War II. Prior to these protocols, the norm was that attacks on facilities were allowed, noting, however, that nuclear reactors and nuclear facilities did not exist during World War II. The United States has never ratified Protocol I, Russia has withdrawn its ratification, and several other countries have made reservations about their ratification of Article 56 of the Protocol which addresses the issues involved in an attack. Therefore, any argument that there is an international norm that already prevents attacks on nuclear facilities ignores the Protocols' attempt to restrain the norm that attacking in wartime can be legally possible.

For its part, the United States has specifically rejected the prohibitions of Article 56 of Additional Protocol I. Its position is clearly set out in the [US Department of Defense Law of War Manual](#) which guides the actions of the United States in war. As stated in section 5.13 of the Manual:

Certain facilities containing dangerous forces, such as dams, nuclear power plants, or facilities producing weapons of mass destruction, may constitute military objectives. There may be a number of reasons for their attack, such as denial of electric power to military sources, use of a dangerous facility (e.g., by causing release from a dam) to damage or destroy other military objectives, or to pre-empt enemy release of the dangerous forces to hamper the movement or advance of U.S. or allied forces.

Attack of facilities, works, or installations containing dangerous forces, such as dams, nuclear power plants, or facilities producing weapons of mass destruction, is permissible so long as it is conducted in accordance with other applicable rules, including the rules of discrimination and proportionality. In light of the increased potential magnitude of incidental harm, additional precautions, such as weaponeering or timing the attack such that weather conditions would minimize dispersion of dangerous materials, may be appropriate to reduce the risk that the release of these dangerous forces may pose to the civilian population.

Further, section 5.13.1 of the Manual states:

Article 56 of AP I provides special rules for works and installations containing dangerous forces. For example, “[w]orks or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population.” In addition, Article 56 of AP I provides immunity from attack to combatants and military equipment stationed or placed around works and installations containing dangerous forces “for the sole purpose of defending the protected works.”

The United States has objected to this article of AP I. In ratifying AP I, other States have taken reservations from this article. Insofar as Article 56 of AP I deviates from the regular application of the principles of distinction and proportionality, the U.S. view has been that it does not reflect customary international law applicable in international and noninternational armed conflicts.

As a start, the United States and other countries would need to reconsider their positions vis-à-vis Article 56 in order to protect nuclear facilities against attacks, and then work to achieve a consensus on international prohibitions on attacks.

The international community should agree on consistent and clear statements endorsed by a majority of countries and should define under what conditions, if any, attacks against nuclear reactors and nuclear facilities may be allowed during a war. Further, countries would need to delineate the specific procedures, both politically and militarily, by which any such allowed attacks could be carried out.

Any resulting legal regime should be unambiguous on what might constitute a justifiable legal basis for an attack on nuclear facilities. To continue delegating this decision to the sole judgment of military commanders at unspecified levels of command is not acceptable. It is time for the United States and other countries to declare that the general law of war rules of discrimination and proportionality does not allow—under any circumstances—attacks on nuclear power plants or any other nuclear facilities that would result in the spread of radioactive substances into the environment. Any allowed attacks on such facilities would need to use procedures that would eliminate to the maximum extent possible the risk of release of radiation.

### **How to get there**

A possible path forward to guarantee the safety of nuclear reactors and nuclear facilities in wartime would be for the international community to agree on a treaty, or a series of treaties, setting out specific agreements on these issues.

The stated goal of any international agreement should be that there shall never be a reactor accident, spent fuel accident, or any event releasing radioactive materials as a direct result of either an intentional or unintentional act of war. Drafting the language of such an agreement undoubtedly would require a breath of creative thinking and a new approach to these issues. Agreements could include such things as warnings of attack, exchange of information on the operating status of reactors, prohibition of any attack on a reactor that is in a state that makes it vulnerable to an accident (e.g., operating reactors), rules involving the International Atomic Energy Agency to assist in controlling any reactor or spent fuel in a war zone, creating an analog to the international law concept of free cities which would involve placing reactors and nuclear facilities under international control in wartime, among other rules.

Unfortunately, it seems unlikely that an international convention could be called now to develop a treaty on these issues. But this does not bar countries from organizing talks about how to protect nuclear facilities







in wartime. One option could be for the United States to revisit the concept of the Nuclear Security Summits held between 2010 and 2016 during the Obama administration. Even though somewhat limited in scope, these summits were able to bring together international leaders and organizations such as the IAEA and Interpol in capitals around the world to discuss how to move forward on specific issues of nuclear security.

The Biden administration could, on its own initiative, invite countries to a new Nuclear Security Summit, extended to also address the safety of nuclear reactors and nuclear facilities in wartime. Since the summits of the early 2010s were so closely identified with President Obama, the Biden administration could also consider asking President Obama to chair such a summit and resolve to the greatest extent possible these issues. His lead—or contributions from any other former US president who enjoys favorable international approval—could create momentum and incentivize the international community to act now on these issues.

There can be no guarantee that any actions by the international community will have an immediate effect on the nuclear facilities being threatened in Ukraine. But there is little to no risk in undertaking an international effort now to reach an agreement on how to protect nuclear facilities (and any associated energy infrastructure) in wartime.

A revival of the Obama-era Nuclear Security Summits is one potential way forward to seek agreement on these issues, but it is certainly not the only path. Creative thinkers may come up with better workable alternatives to move now to protect nuclear facilities in Ukraine.

The growing risks to Ukrainian nuclear facilities show the importance of choosing an initial path forward now rather than waiting for the conclusion of the war, which one can hope will come before what would appear in retrospect to have been an avoidable nuclear accident.

**George M. Moore** is a scientist-in-residence at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies at Monterey (MIIS). Previously, he served as a senior analyst in the Office of Nuclear Security at the International Atomic Energy Agency (IAEA) and in various assignments as a staff member at Lawrence Livermore National Laboratory. He received his bachelor's degree from the US Naval Academy and a masters and doctorate in nuclear engineering from the University of California, Berkeley. He also holds a Juris Doctor (JD) degree from the University of California's Boalt Hall (Berkeley) School of Law and is a member of the California and Colorado bars.

## Russian analyst urges nuclear attack on Yellowstone National Park and San Andreas fault line

Source: <https://www.smh.com.au/world/russian-analyst-urges-nuclear-attack-on-yellowstone-national-park-and-san-andreas-fault-line-20150331-1mbl14.html>

**2015** – A Russian geopolitical analyst says the best way to attack the United States is to detonate nuclear weapons to trigger a supervolcano at Yellowstone National Park or along the San Andreas fault line on California's coast.

The president of the Academy of Geopolitical Problems based in Moscow, Konstantin Sivkov said in an [article for a Russian trade newspaper on Wednesday, VPK News](#), that Russia needed to increase its military weapons and strategies against the "West" which was "moving to the borders or Russia".

He has a conspiracy theory that NATO - a political and military alliance which counts the US, UK, Canada and many countries in western Europe as members - was amassing strength against Russia and the only way to combat that problem was to attack America's vulnerabilities to ensure a "complete destruction of the enemy".

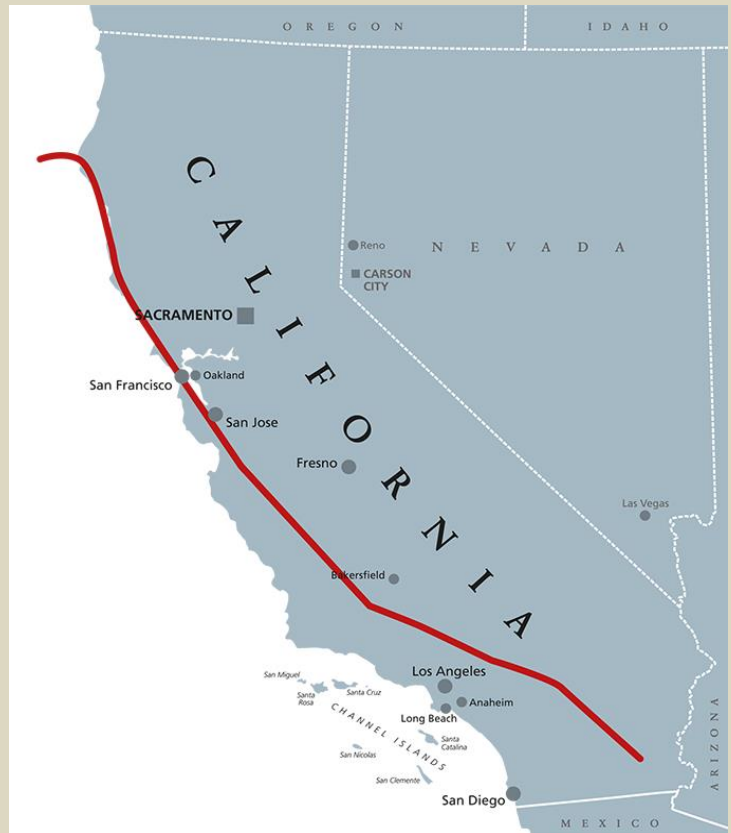
"Geologists believe that the Yellowstone supervolcano could explode at any moment. There are signs of growing activity there.

Therefore it suffices to push the relatively small, for example the impact of the munition megaton class to initiate an eruption. The consequences will be catastrophic for the United States - a country just disappears," he said. "Another vulnerable area of the United States from the geophysical point of view, is the San Andreas fault -





1300 kilometers between the Pacific and North American plates ... a detonation of a nuclear weapon there can trigger catastrophic events like a coast-scale tsunami which can completely destroy the infrastructure of the United States."



Russian target number 2: The San Andreas fault line, here pictured on the Carrizo Plain in California.

He said the Russian geography on the other hand would protect it from a tsunami or a volcano attack. Few people live on the coast in Russia and Siberia which rests on basalt would withstand similar attacks. Mr Sivkov, who spoke at the 2013 Moscow Economic Forum, said by 2020 to 2025 Russia would have amassed "asymmetric weapons" in its arsenal for the attack. "The situation for us today is comparably worse than half a century ago," he said. "The weakened economic potential in Russia, the loss of the 'spiritual core of what was the communist idea', and the lack of large-scale community allies in Europe such as the Warsaw Pact, Russia simply cannot compete against the NATO and its allies." In December last year, the vocal military strategist told Russian newspaper, *Pravda.ru* that there is a "developing standoff between Russia and the West" and the US's ultimate goal was to "destroy Russia". Mr Sivkov accused American politicians of committing several crimes including causing the deaths of 1,200,000 people in Iraq. He believed the only way for the "American elite" to be held accountable was for its military forces to be destroyed. "American politicians have committed a variety of crimes. Will anyone be held accountable for those crimes? What about the international law, the UN and other organisations? Are they doing anything?" he asked. Mr Sivkov told *Pravda* that the idea of the US preparing for a serious war against Russia using cruise missiles was plausible given that it had already launched a thousand missiles in Yugoslavia and Iraq.

**Anton Gerashchenko** @Gerashchenko\_en · Ακολουθήστε

Attention, United States!

Today the propagandists are threatening to blow up Yellowstone National Park.

СПЕЦИАЛЬНЫЙ ВЫПУСК Subtitles: @Gerashchenko Παρακολουθήστε στο Twitter

7:12 μ.μ. 16 Δεκ 2022

- But the Poseidon (Russian codename Status-6) and this Sarmat have comparable units in terms of weight.



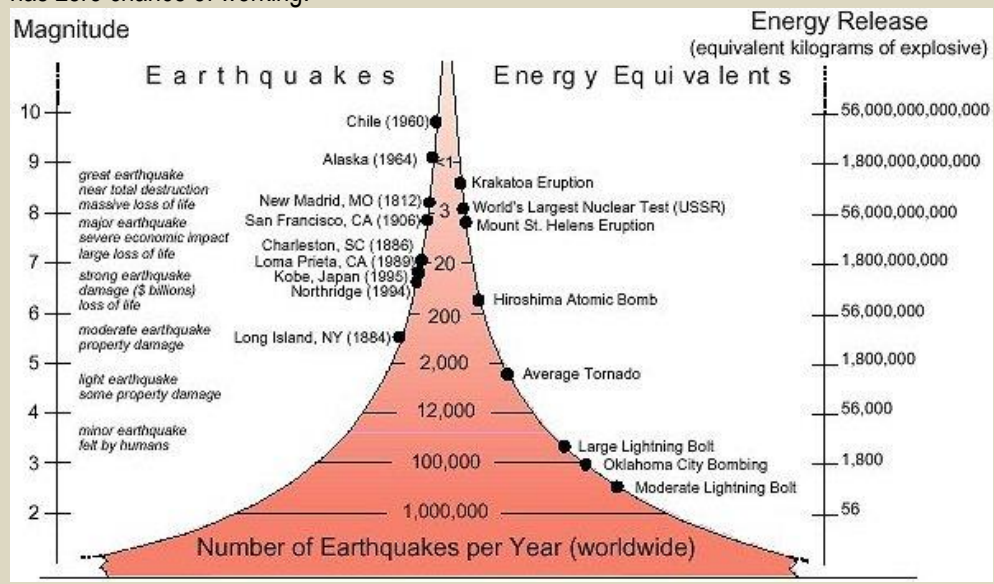




# Can a nuclear blast trigger a Yellowstone eruption? No. But how about an earthquake? Also no.

Source: <https://www.usgs.gov/observatories/yvo/news/can-nuclear-blast-trigger-yellowstone-eruption-no-how-about-earthquake-also>

2018 – YVO has noted, with some amusement, tabloid headlines about various diabolical schemes to trigger an eruption of Yellowstone by nuking the caldera. If you find these crazy schemes somewhat unnerving, please don't be concerned—such a plan has zero chance of working!

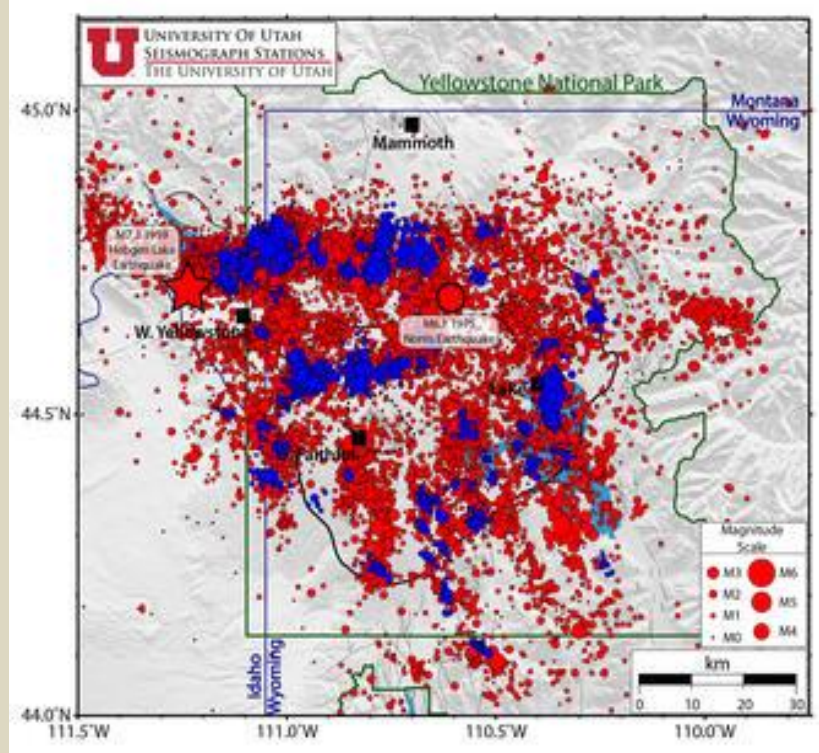


Graph showing the average annual occurrence and equivalent energy release for earthquakes of different magnitudes. Plot is from the Incorporated Research Institutions for Seismology.

You see, unlike science fiction stories, in which nuclear weapons seem to be the cause of, and solution to, many geological catastrophes, science fact tells us that you aren't likely to trigger a Yellowstone cataclysm with a nuclear weapon. How do we know? It's because this experiment has already been tried. Earthquakes release a tremendous amount of energy, which can be

expressed in terms of the equivalent size of explosive. For example, the strongest earthquakes ever recorded, which are above magnitude 9 (like the 2011 Tohoku, Japan, earthquake), release the energy of nearly a 2000-megaton nuclear weapon. For reference, the strongest nuclear test ever was a 50-megaton explosion conducted by the Soviet Union in 1961.

**Red** circles represent all seismicity and **blue** circles represent earthquakes as part of earthquake swarms. The size of the circles is scaled to the magnitude of the earthquake. The 630,000-year-old Yellowstone caldera is shown as a bold black line within Yellowstone National Park. Mapped faults are shown as light gray lines.



The Yellowstone region is not immune to large earthquakes, as most readers know. For instance, in 1975 a M6.1 quake struck the area near Norris Geyser Basin. The largest earthquake recorded in the region is the M7.3 Hebgen Lake earthquake, which occurred on the western boundary of the park at a depth of about 10 km (6 mi). The Hebgen Lake earthquake released more energy than a 2-megaton nuclear weapon—100 times larger than the atomic bomb that destroyed Hiroshima in 1945, and equivalent to an "average" hydrogen bomb. What's more, this earthquake occurred not above, but next to Yellowstone's largely solid magma body, so most of the earthquake's energy was transmitted directly into the rock. In a nuclear attack, the detonation would occur above ground, so the majority of the energy would be released into the air.







And guess what happened to Yellowstone volcano after the M7.3 earthquake? It didn't erupt! The only impacts were some changes in hot springs and geysers due to the shaking.

1959 was not the first time an earthquake occurred on the Hebgen Lake fault. Studies of the geology of the region indicate that there have been [at least three strong earthquakes on the fault in the past 15,000 years](#). This implies a recurrence interval on the order of one strong earthquake per several thousand years. That means since Yellowstone's last magmatic eruption 70,000 years ago (a lava flow, not a major explosion), there might have been a dozen or more earthquakes equivalent to a moderate thermonuclear explosion next to the Yellowstone magma storage region. None triggered an eruption. Since the last caldera-forming explosion 631,000 years ago there might have been hundreds of such earthquakes!

The same holds true when considering large earthquakes on the Pacific-North America plate boundary, like an M8 on the San Andreas Fault or a potential M9 in the Pacific Northwest. The San Andreas might experience a M8 event every 200 years or so, meaning that there could have been 350 such events since the last Yellowstone lava flow and over 3,000 such events since the last huge explosion. Pacific Northwest M9 earthquakes seem to occur, on average, about every 500 years, meaning that there might have been about 140 such events since the last Yellowstone lava flow and over 1200 since the last huge explosion. Clearly, these events do not commonly trigger Yellowstone eruptions.

Thus, it would seem we have little to worry about in terms of Yellowstone being "set off" by some external trigger, be it a distant massive earthquake, a local strong earthquake, or a very local nuclear blast. That isn't to say that there wouldn't be some noticeable effects, however. Distant earthquakes have triggered clusters of small earthquakes at Yellowstone (like those caused by the 2002 Denali, Alaska, earthquake), and variations in geyser eruption patterns are a common consequence of local and distant strong earthquakes. Seismic shaking can cause hydrothermal plumbing systems to collapse, changing how Yellowstone thermal features behave and even resulting in small steam explosions.

But triggering an eruption of magma from Yellowstone is not easy—no eruptions have happened in the past 70,000 years despite numerous strong earthquakes in the region. An eruption will occur only when there is a quantity of liquid magma in the subsurface and sufficient pressure to get that magma to ascend to the surface. Neither condition is currently in place. As a matter of fact, there's only 5-15% liquid in the mostly crystalline magma storage region. So, no matter what the tabloids dream up, the threat of a Yellowstone eruption remains low.

## **The Energy Department's fusion breakthrough: It's not really about generating electricity**

**By John Mecklin**

Source: <https://thebulletin.org/2022/12/the-energy-departments-fusion-breakthrough-its-not-really-about-generating-electricity/>

Dec 16 – This week's headlines have been [full](#) of [reports](#) about a "major breakthrough" in nuclear fusion technology that, many of those reports misleadingly suggested, augurs a future of abundant clean energy produced by fusion nuclear power plants. To be sure, many of those reports lightly hedged their enthusiasm by noting that (as [The Guardian put it](#)) "major hurdles" to a fusion-powered world remain.

Indeed, they do.

The fusion achievement that the US Energy Department announced this week is scientifically significant, but the significance does not relate primarily to electricity generation. Researchers at Lawrence Livermore National Laboratory's National Ignition Facility, or NIF, focused the facility's 192 lasers on a target containing a small capsule of deuterium-tritium fuel, compressing it and inducing what is known as ignition. In a written press release, the Energy Department described the achievement this way: "On December 5, a team at LLNL's National Ignition Facility (NIF) conducted the first controlled fusion experiment in history to reach this [fusion ignition] milestone, also known as scientific energy breakeven, meaning it produced more energy from fusion than the laser energy used to drive it. This historic, first-of-its kind achievement will provide unprecedented capability to support [the National Nuclear Security Administration's] Stockpile Stewardship Program and will provide invaluable insights into the prospects of clean fusion energy, which would be a game-changer for efforts to achieve President Biden's goal of a net-zero carbon economy."

Because of how the Energy Department presented the breakthrough in a news conference headlined by Energy Secretary Jennifer Granholm, news coverage has largely glossed over its implications for monitoring the country's nuclear weapons stockpile. Instead, even many serious news outlets focused on the possibility of carbon-free, fusion-powered electricity generation—even though the NIF achievement has, at best, a distant and tangential connection to power production.

To get a balanced view of what the NIF breakthrough does and does not mean, I spoke this week with Bob Rosner, a physicist at the University of Chicago and a former director of the Argonne National





Laboratory who has been a longtime member of the Bulletin's Science and Security Board. The interview has been lightly edited and condensed for readability.



National Ignition Facility operators inspect a final optics assembly during a routine maintenance period in August. Photo credit: Lawrence Livermore National Laboratory

**Bob Rosner:** I should tell you that I have had some very interesting interactions. I was for example on public TV in Chicago. And basically, the bottom line is that the DoE [Department of Energy] publicity machine really wanted to steer away from the weapons part of the story and focus on, you know, the energy future. And if you probe just a micron beneath the skin of that story, you discovered that it's not quite what's going on ... But I was faced by a TV reporter who thought this is an energy story, and I had to basically tell him, "No, it isn't." It's an extremely interesting story, for people interested in weapons and nonproliferation, and for science in general. That's what it's about. It happens that you do have some tangential relationship to energy, but the people working on energy (and who pay for the ongoing research) had nothing to do with this project. The folks who succeeded so splendidly in attaining ignition and self-sustained fusion on December 5 were not part of DoE's fusion energy program (which sits in the DoE Office of Science Office of Fusion Energy Sciences); they're working instead for the National Nuclear Security Administration (NNSA), which manages our nation's nuclear weapons stockpile.

**John Mecklin:** So why don't you explain, really quickly, for people who aren't up on this: What is it that the NIF did? What is the big breakthrough they're announcing?

**Rosner:** So we have known how to fuse hydrogen and release energy for a long time—in 1952, we exploded the first thermonuclear device, whose detonation was largely the result of hydrogen fusion. So we've known how to do that for a very, very long time. What's different here is that it's never been done under controlled circumstances in a laboratory. And the "it" is a sustained burn. Making hydrogen fuse to produce a few nuclei of helium, i.e., a few alpha particles, that's been done numerous times in the lab. In fact, in the magnetic confinement fusion world, JET [the Joint European Torus] was able to produce in its tokamak plasma helium via hydrogen fusion, no problem. But this was never a self-sustained reaction, what the physicists would call ignition and burn. Ignition means I light it [the fusion reaction], and it continues to burn based on its own energetics that doesn't require any additional energy input once you've lit the "match."







That's what's going on here. So ignition and burn is what it's all about, you start the fusion reaction, and then all the energy that is produced within the reaction sustains the reaction, keeps it going.

And this is the first time it's been done in the lab, in a fully controlled manner. It's a huge achievement!

**Mecklin:** And doing this is important, I've heard you say, in terms of the nuclear stockpile stewardship, that it will help there. Why don't you explain why.

**Rosner:** So I have to turn the clock back a bit, okay? This will be an old story for you, but let's just tell the whole story. In the late '80s and early '90s, the decision was finally made to stop underground testing. And in fact, in the early '90s, the United States stopped it entirely. We no longer brought [nuclear] devices to Nevada, buried them underground, and pushed the button. And there was a huge resistance to stopping, because that program of testing in Nevada wasn't just for fun. It was, basically, to certify the nuclear stockpile. They would withdraw these weapons at random from the stockpile, bring them to Nevada, and demonstrate two things: One is if you push the button, it went off, and two, that the yield was as expected. In other words, the whole thing worked, as it was designed.

And for the [Defense Department], the [STRATCOM](#) people, that was absolutely essential. That's what they needed to know. You push the button, it works, and the yield is the right yield. Because if the yield is off, they might have to, for example, increase the number of weapons they send on a given target that they want to destroy.

So now you've stopped the testing, and the obvious question is: How do these people know that the whole thing still works? So that was the start of this tongue twister called the Science Based Stockpile Stewardship Program. And the promise was that we would put together a set of new codes, using advanced computers as well as new kinds of experiments—what they call nonnuclear experiments and what they call subcritical experiments that didn't get a detonation—that would then serve to certify the stockpile. What we're talking about is there was an ongoing surveillance program of the stockpile. They would open these things up at random, look inside, and occasionally they'd find that there was some aging going on, like, for example, a part doesn't work as it's supposed to work anymore. And you'd have to replace it.

Often, the replacements were made in a different way than the original; for example, different kinds of material were used. So what you had, the question that you had to answer is: Under the explosion conditions, how do you know that this new thing that you put in actually works as it's supposed to?

I'm sure you've heard the story that people in Congress—there are people who started to press for going back to nuclear testing. So the Stockpile Stewardship Program does need to demonstrate that the “science-based” approach does work. And as I said before, NNSA decided to build new experimental facilities (one of which was the National Ignition Facility), efforts were made to construct new simulation codes to help certify the weapons, and investments were made in new generations of advanced computers that these codes required and could run on. And NIF was meant to, in part, validate the design code approaches used for the weapons. Before NIF was even completed, they chose a target experiment that—in combination with simulation codes advances—could demonstrate that we knew what we were doing.

One of the key target experiments that they picked was: We're going to show that we can ignite and sustain a fusion reaction in the laboratory. That's why NIF was called the National Ignition Facility. This goes back to the late '90s, with NIF's groundbreaking in 1997. Early on, the weapons folks were optimistic that this would be kind of a no-brainer; just build a laser facility big enough, and it will just work. Unfortunately, that turns out to be wrong.

To give an intuitive sense of why that turns out to be so hard: Imagine you started with something that's the size of a basketball but solid. And what do you have to do is squeeze it down, decrease its volume by a factor of 1,000, to the size of a baseball. And all the time that it is compressing by a [volume] factor of 1,000, it has to stay perfectly, perfectly spherical. If you have the slightest deviation from sphericity, what happens is the stuff deforms very quickly, and that's practically the end of the implosion. So the huge success here was to figure out both on the part of how to operate the laser, then how to deal with the capsule, so that the capsule stays almost perfectly spherical during the implosion. And they finally figured it out. That's what it's all about.

Now, to get to this point required a close interaction between the experimentalists and the theorists and simulation code folks—an iterative process, involving an incredibly complex set of physics, some of it directly relevant nuclear weapons physics. And their success meant that they mastered the physics well enough in the simulations—that they knew what they were doing—to have the experiment succeed. And that gives considerable confidence that they have also mastered the physics of nuclear devices and can make sure these nuclear weapons will work.

Now, it turns out that's only one of the uses of NIF. You might ask, “Why did they pick ignition?” First, because the science is so cool, and you can demonstrate that you know what you're doing. Second, because when you get to ignition, you get a huge blast of radiation, just enormous, as well as extremes in temperature and pressure. And that you can use to test for example, the properties of various materials critical to weapons. You can answer questions like, “Suppose I had different kinds of material in the bomb? How would they respond to this blast of radiation? To these temperatures and pressures?” Thus, as far as temperature, radiation environment, and pressures







are concerned, you could do that experiment right there at NIF. So this second use relates to the fact that you can replicate the physical conditions during a nuclear blast.

And there's a third reason, by the way. We're going to have nuclear weapons for a long time, no matter how much we want to get rid of them. They're going to be hanging around until we have a different regime of trust between countries. What that tells you is that going into the distant future—in the next 50, 60, whatever, 100 years—if you want to you have these weapons, you have to deal with them. That means you need a cadre, I think almost like high priests, high priests of weapons, that you actually trust that they know what the hell they're doing. The generation of folks that built the original bombs, they're basically retired or gone altogether. Now we have a whole slew of new folks, youngsters. They're supposed to know how to do this. Some of them were in place already during the '70s and '80s, when we were still designing and building weapons. But even those people are getting long in the tooth; they're going to be gone from the labs in the next 20 years or so. And so now you're looking at, you know, kids from my perspective, in their 30s. And you want to train them how to do this.

But now you can't build entirely new weapons anymore. So what do you do? What you do is you see whether or not you can train them to work on physics problems that are just about as hard as building a weapon, designing a weapon, but still related to the physics of weapons. In fact, it turns out that the physics problem that they set themselves to solve—getting ignition and sustained fusion at NIF—is actually harder than designing and building a functional nuclear weapon. You may be surprised to learn that doing things on NIF turns out to be harder; it is harder. The reason why? In '52, the weapons folks were able to get away with blowing up an H-bomb up using very low-tech technology – basically, they didn't have supercomputers then—they had slide rules, mechanical computers, electronic computers that were far less capable than what you now have on your desktop. Whereas nowadays, you need a, you know, a petascale machine to figure out what's going on within NIF. So this is actually a harder problem. And thus, this facility can be used to train the next generation of weapons designers; you can regard it as a teaching facility for the next generation.

And so those are three distinct motivations underpinning the December 5 fusion experiment.

**Mecklin:** The news coverage and how it was put out, though—it was all about, you know, electricity generation from fusion.

**Rosner:** It's basically—it's BS, right? That's how we started our chat... By the way, during the [Energy Department] news conference, yeah, the whole affair was split into two bits. There was a news conference where you had (Energy Secretary Jennifer) Granholm and the leadership gang talking, and then afterwards you had a panel of Livermore scientists who actually worked on this experiment. And that panel was straight on. If you listen to the panel, you would know immediately that this was not about electricity generation. One person who really was clear about all this during the preceding news conference was (National Nuclear Security Administration Deputy Administrator for Defense Programs) Marv Adams. I don't know whether you saw the whole thing. But Marv didn't talk about energy. Marv talked about the science, and why we're doing this. And he said something else, which I should have added just a moment ago, which is: If you succeed in doing this—attaining ignition and sustained burn—you're sending a signal to adversaries that you have the capacity to actually do the things you say you can do. And that's a big deal—it definitely is a fourth motivation for striving towards ignition and gain.

**Mecklin:** But why is this particular facility, or something based on this approach, unlikely to be used for electrical generation anytime soon?

**Rosner:** Here's my standard story, which actually comes straight from Marv Adams, because he said what I'm about to tell you: This facility can do one shot a day; this is at slightly more than two megajoules (of output). For an energy source, it would have to do the same thing at least 10 times a second. If you ask, "Do the lasers exist that can do this?" Not in your dream. The pellet cost a bit over \$100,000 to manufacture. The word bespoke applies to clothing; my bespoke suit, right? This is a bespoke pellet. And it probably took about a week or more to manufacture. You'd need well over a million pellets like that, [manufactured] to the same standard, a day for a power plant. So you might guess (correctly) that the technological challenges are formidable, and I haven't even described how you're going to get electricity out of this kind of facility. We haven't even talked about that, or about the costs.

**Mecklin:** I have a hard time imagining how we are going to transfer that heat into some sort of electricity generation.

**Rosner:** Well, there is no good answer to that yet. I was asked, "Well, how long will it take?" My answer was twofold. It's going to take many decades. The second was—ultimately, "Is it going to be practical?" The answer to that will have to involve the obvious question of "How much is it going to cost to do this?" And no one has a clue about how much this is going to cost. And whether it can be competitive with, as an example, solar cells, or even solar cells coupled with grid-scale batteries; we have no idea. So I can't answer that question.

**Mecklin:** I've always thought it's somewhat ironic. We have a thermonuclear furnace in the sky. But we're always trying to re-create it on Earth.

**Rosner:** Yeah. But the furnace in the sky has one big, big, big advantage. It has a way of containing everything and compressing it, and that's called gravity. And that's not just useful but also cheap.

**John Mecklin** is the editor-in-chief of the *Bulletin of the Atomic Scientists*. Previously, he was editor-in-chief of *Miller-McCune* (subsequently renamed *Pacific Standard*), an award-winning national magazine





that focused on research-based solutions to major policy problems. Over the preceding 15 years, he was also: the editor of *High Country News*, a nationally acclaimed magazine that reports on the American West; the consulting executive editor for the launch of *Key West*, a regional magazine start-up directed by renowned magazine guru Roger Black; and the top editor for award-winning newsweeklies in San Francisco and Phoenix. In an earlier incarnation, he was an investigative reporter at the *Houston Post* and covered the Persian Gulf War from Saudi Arabia and Iraq. Beyond the publications he has edited and opined in, his writing has appeared in *Foreign Policy*, the *Columbia Journalism Review*, and the Reuters news service.

### Banks operating in Belgium continue to invest in nuclear weapons

Source: <https://www.brusselstimes.com/339701/banks-operating-in-belgium-continue-to-invest-in-nuclear-weapons>



Dec 19 – Some banks operating in Belgium continue to invest in companies involved in the production, maintenance or modernisation of nuclear weapons, a Belgian umbrella for peace and democracy announced on Monday.

These banks include BNP Paribas, Deutsche Bank, ING and Santander, the Coordination nationale d'action pour la paix et la démocratie (CNAPD ) said, pointing to a new survey.

The survey was commissioned by the International Campaign to Abolish Nuclear Weapons and the Dutch organisation PAX.

It was conducted among 24 major nuclear weapons producers that contribute to the arsenals of China, France, India, Russia, the UK and the US.



#### Some 306 banks invested \$746 billion in nuclear arms

It shows that between January 2020 and July 2022, these companies benefitted from \$746 billion invested by 306 financial institutions, an increase of \$61.5 billion compared to the previous period analysed.







According to the CNAPD, this means that “the savings of Belgians end up in the hands of arms producers who flout international law.”

The CNAPD noted, by way of illustration, that BNP Paribas, Deutsche Bank and ING invested €12.7 billion, €11.45 billion and €545 million respectively in weapons of mass destruction.

**Good examples: KBC, VDK, Triodos**

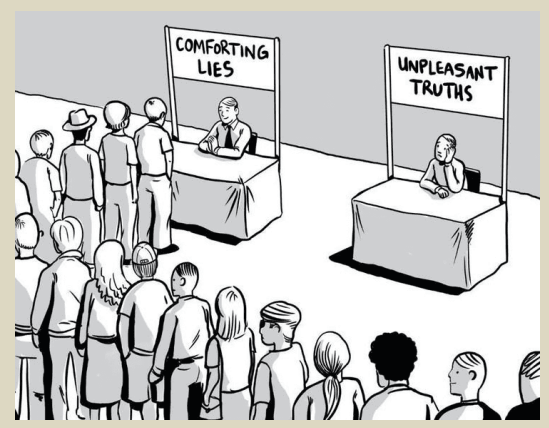
However, there are “good examples” in Belgium, notes the umbrella, citing the KBC in particular.

“The Belgian bank has revised its investment policy by categorising nuclear weapons as controversial and by blacklisting companies specialising in atomic weapons,” the CNAPD reported.

“Other banks, such as VDK or Triodos, have always prohibited investments in companies linked to nuclear weapons,” it added.

**Accepting Reality: For the Foreseeable Future, Denuclearizing North Korea May Be Unattainable**

Source: <https://www.homelandsecuritynewswire.com/dr20221221-accepting-reality-for-the-foreseeable-future-denuclearizing-north-korea-may-be-unattainable>



Dc 21 – For two decades now, U.S. policymakers have sought North Korean denuclearization. Van Jackson writes in *War on the Rocks* that in the early 2000s, it was a smart and necessary goal, because a nuclear North Korea would threaten U.S. allies, spread nuclear weapons beyond the Korean Peninsula, damage the sanctity of the nuclear taboo, and eventually threaten U.S. territory. He continues:

Unfortunately, as the saying goes, the enemy gets a vote. [North Korea](#) has [repeatedly stated](#) it will not entertain “unilateral nuclear abandonment,” and that [denuclearization requires](#) “the removal of all sources of nuclear threat, not only from the North and the South but also from all neighboring areas targeting the Korean Peninsula ... completely eliminating the U.S. nuclear threat to Korea before it can eliminate our nuclear deterrent.” Short of resorting to military force, there is nothing the United States can do to eliminate North Korea’s nuclear weapons for the foreseeable future.

In a [recent report](#) with the Center for a New American Security, I therefore propose redesigning Washington’s North Korea policy to acknowledge that the underlying premise of America’s longstanding approach has been overtaken by events. The assumption that the United States can convince North Korea to denuclearize is not only incorrect; it leads to coercive policies that increase the risk of nuclear conflict. As I recount at length in [On the Brink: Trump, Kim, and the Threat of Nuclear War](#), the goal of denuclearization justified a maximum pressure approach to North Korea in 2017, and maximum pressure played a leading role in causing the nuclear crisis. Rather than dial back a quixotic goal, the Trump administration ratcheted up the means employed and the risks taken to realize it. The nuclear confrontation might have been avoided entirely if the United States had more realistic expectations for what could have been achieved with North Korea.

To better manage the risks of nuclear instability in Korea, the report urges policymakers to stop treating denuclearization as a realistic planning factor and instead pursue an arms control approach that prescribes for the United States a series of unpalatable but essential actions.

I was among [the first](#) to publicly urge an arms control approach with North Korea in lieu of denuclearization years ago — and have since been joined by [other prominent nuclear analysts](#). But as far as I’m aware, this report is the first attempt to translate what such a shift should mean for U.S. North Korea policy in detail.

The report Jackson refers to is his [Risk Realism: The Arms Control Endgame for North Korea Policy](#), issued by the Center for a New American Security.

Here is the Executive Summary of the report:

**Executive Summary**

While the reasons for seeking North Korean denuclearization are sensible, continuing to pursue that goal makes the United States and its allies less secure. In word and deed, North Korea has shown it has no interest in nuclear disarmament.

Because denuclearization is antithetical to Kim Jong Un’s bottom line, U.S. attempts at diplomacy to that end are self-sabotaging. As long as disarmament of North Korea remains America’s professed goal, Kim Jong Un has every incentive either to avoid the negotiating process or favorably manipulate it at America’s expense—by stalling for time, making unfulfilled promises,







and securing concessions without reciprocity. Worse, as the 2017 nuclear confrontation showed, making denuclearization an actionable goal of U.S. policy creates real risks of crisis instability—justifying extreme measures and extreme rhetoric in the name of what has become an extreme aim.

But policymakers can avoid the pitfalls of the past by attempting something more realistic than denuclearization—an arms control approach to North Korea. The United States has significant unexploited margin to take diplomatic and political risks aimed at probing and potentially shifting North Korea's approach to its nuclear arsenal. An arms control approach would seek to reorient U.S. North Korea policy to prioritize what matters most: reducing the risk of nuclear or conventional war without forsaking other U.S. interests at stake in Korea.

Using diplomacy to enhance regional stability and foreclose the possibility of an avoidable nuclear war requires pursuing a negotiated outcome that both sides can accept, and that tests North Korea's willingness to uphold commitments short of disarmament. U.S. policy often seeks to test North Korean intentions, but without offering the accommodations and concessions that would serve as a meaningful test.

Remedying this problem through an arms control approach requires taking considerable unilateral actions consistent with U.S. interests before proceeding to a phased negotiating process.

## **An Arms Control Blueprint**

### **Unilateral Actions**

- *Curb Denuclearization Rhetoric*—The White House should state that denuclearization will no longer be a concrete goal of U.S. North Korea policy.
- *Announce Stable Coexistence*—In tandem with a pivot away from denuclearization, the United States should declare that it is willing to peacefully coexist with North Korea under the Kim regime as long as it does not actively threaten South Korea or Japan.
- *Institutionalize a Strategic Security Dialogue with North Korea*—To manage the risks of inadvertent conflict and tailor its own deterrence posture more effectively, the United States needs to understand as accurately as possible how North Korea thinks about coercion, nuclear doctrine, and conditions of nuclear use.
- *Issue a “No Nuclear Deployment” Executive Order*—The White House should issue an executive order (EO) suspending deployments of nuclear-capable bombers to the Korean Peninsula, including the B-1B, which is no longer nuclear-capable but poses a discrimination problem for North Korea by introducing the same risks as if it were. The EO should have a provision requiring the president to approve any redeployment decision.
- *Declare an End to the Korean War*—Declare an intention to end the Korean War as a political matter. If the United States sees value in maintaining a long-term presence on the Peninsula, it would be on firmer footing if its presence is based not on a war fought more than two generations ago, but rather predicated on whatever the logical merits are for keeping troops in Korea now and in the future.

### **Phase I Negotiation Initiatives**

- *Freeze Nuclear Progress without Intruding into “Kim’s Bathroom”*—The State Department should negotiate a moratorium on all North Korean nuclear activities and allow international monitors to establish an initially limited presence in North Korea. The United States should triangulate verification—relying heavily on intelligence collection and passive open-source analysis—rather than hold negotiations hostage to an unrealistically intrusive inspections regime at the outset.
- *Preemptively Ban “Tactical” Nukes*—U.S. negotiators not only should seek a North Korean commitment to cap its existing arsenal at present numbers, but also to gain a North Korean agreement not to diversify its nuclear capabilities into operational low-yield nuclear weapons.
- *De-Operationalize North Korean Missile Forces*—The State Department should seek a North Korean commitment for the Missile Guidance Bureau to de-operationalize its missile forces. This could be done, for example, by mutually agreeing to keep military alert levels low, restricting the use of solid fuel propellant, and/or allowing inspectors of missile facilities to monitor their non-operational status.

### **Phase II Negotiation Initiatives**

- *Launch a Nuclear-Free Seas Initiative*—The Office of the Secretary of Defense and State Department should jointly negotiate a mutual ban on nuclear weapons within the exclusive economic zones (200 nautical miles) on either side of North Korea's coasts.
- *Start Nuclear Rollback*—Once the arms control process has matured to the point that rollback becomes feasible, U.S. negotiators should prioritize reducing parts production





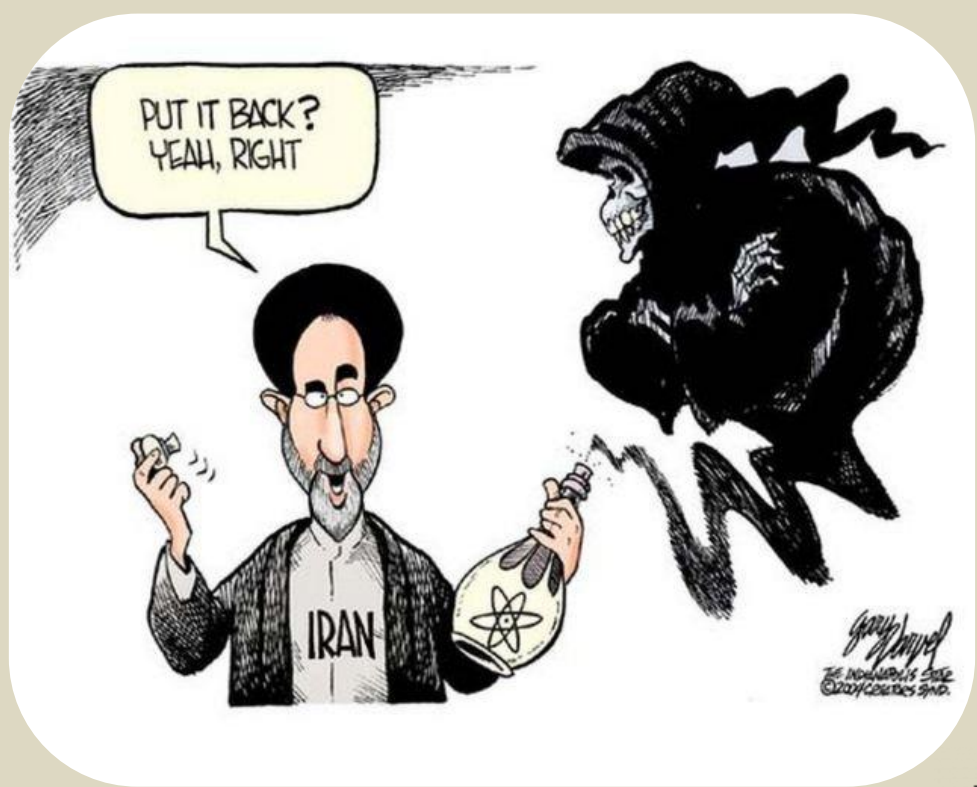
for, and inventory of, the Pukkuksong series of solid-fuel missiles, followed by Musudan, Nodong, and SCUD missiles.

- *Secure Declarations of Nuclear Inventory*—Once the United States and North Korea have established a degree of confidence and predictability by implementing Phase 1 Negotiation Initiatives, the State Department should seek a declaration focusing on fissile-material production facilities—revealing this information does not pose any risk to North Korea’s nuclear deterrent. If North Korea complies without any deception, the Strategic Security Dialogue proposed above should be used to elicit insights about the disposition, quantity, and posture of North Korean nuclear weapons.

In parallel with this arms control process, additional measures will help mitigate the risk that North Korea reneges on commitments or fails to reciprocate U.S. attempts to transform U.S.–Korean Peninsula security dynamics.

**Risk Mitigation Measures**

- *Establish Rapid-Reaction Deterrence in South Korea*—If negotiation and efforts to transform the U.S.–North Korea relationship fail, the nuclear threat can only be managed through deterrence. U.S. force posture in South Korea therefore should adapt to the requirements of deterrence against a second-tier nuclear-armed adversary with a track record of small-scale violence.
- *Repurpose Extended Deterrence Dialogues with Allies*—The Office of the Secretary of Defense and State Department should repurpose existing extended deterrence dialogues with Japan and South Korea as mechanisms for shoring up the credibility of U.S. commitments.
- *Preserve Sanctions that Combat Proliferation*—As the United States undertakes various forms of sanctions relief—a necessary concession in any nuclear bargaining process—it should avoid removing those deemed necessary as legal architecture for combating North Korean trafficking in nuclear and missile materials.





ICI  
International  
**CBRNE**  
INSTITUTE



 **C<sup>2</sup>BRNE**  
DIARY



# EXPLOSIVE NEWS







## Iran Solidifies Missile Support to the Houthis

By John Krzyzaniak

Source: <https://www.iranwatch.org/our-publications/articles-reports/iran-solidifies-missile-support-houthis>

Nov 29 – In September, shortly before the expiration of the U.N.-backed truce in Yemen, the Houthi rebels held a military parade in Sanaa to mark the eighth anniversary of their capturing the city.<sup>[1]</sup> The next day, Iran’s armed forces staged their own parade in Tehran to commemorate the start of the Iran-Iraq war in 1980.<sup>[2]</sup> Both parades featured missiles that were billed as new but in fact were not new at all. The Houthis showed off several missile types that were exact copies of existing Iranian ones, while Iran unveiled a missile that the Houthis have previously claimed as their own.

The parades offer two takeaways. First, Iran appears increasingly willing to supply the Houthis with its most advanced missiles and to run greater risks in doing so.<sup>[3]</sup>

Second, the parades illustrated that the benefits of Iran’s proliferation of weapons to its non-state partners run both ways: arming the Houthis allows Iran to use the conflict in Yemen as a real-world test bed for newer systems that, if they pass muster, may then be adopted by Iran’s own armed forces.

### New Houthi Hardware

The Houthis paraded numerous systems that they had never publicly unveiled before, and all are very likely Iranian in origin.<sup>[4]</sup> Most surprising was the appearance of three kinds of solid-fueled missiles in the parade. The first was the Karar, which appears to be identical to the Iranian Fateh-110 solid-fueled ballistic missile.<sup>[5]</sup>



Top: The Houthi Karar. Bottom: The Iranian Fateh-110 (image flipped horizontally for better comparison).

The second was the Aasif, whose external features match the Iranian Khalij Fars, an anti-ship version of the Fateh-110 with an electro-optical homing seeker.







Top: The Houthi Aasif. Bottom: The Iranian Khalij Fars (image flipped horizontally for better comparison).

The third was the Hatem, apparently a copy of the Kheibar Shekan, a solid-fueled ballistic missile with a claimed range of 1,450 km. The Kheibar Shekan was first unveiled in Iran earlier in 2022, making it one of the newest missiles in the Iranian arsenal.<sup>[6]</sup>



Top: The Houthi Hatem. Bottom: The Iranian Kheibar Shekan.







The Houthis also revealed a new liquid-fueled ballistic missile, the Faleq. The group already possesses several versions of modified Iranian-made liquid-fueled Qiam missiles, which they have dubbed Burkan-2H, Burkan-3, and Zulfiqar.<sup>[7]</sup> The Faleq appears to be an exact copy of what some independent analysts have called the Qiam-2,<sup>[8]</sup> which is differentiated from the original Qiam by its detachable, finned re-entry vehicle for improved precision.<sup>[9]</sup> In other words, the Faleq is an upgrade that tracks the latest technology of Iran's liquid-fueled short-range ballistic missiles.



Top left: Quds-3. Top right: Saqr. Bottom: Faleq.

Two less surprising missiles in the parade were the Quds-3 land attack cruise missile and the Saqr-1 surface-to-air missile. Both the Quds (designated “351” by the United States) and the Saqr (designated the “358” by the United States) have been [captured](#) by Western navies during interdictions of arms shipments bound for Yemen.<sup>[10]</sup> The Quds-3 appeared identical to earlier variants, the Quds-1 and Quds-2, which have been used in multiple attacks against Saudi civilian targets, including a pair of attacks against Abha international airport in June and August 2019.<sup>[11]</sup> The Saqr-1 has been seen in Iraq, and a modified version of it has reportedly been used by Iran-backed groups to attack ground targets in Syria, but this was the first time the Houthis had displayed it.<sup>[12]</sup>

### An Evolving Approach?

The parade suggests that Iran may be changing course in its military support for the Houthis in two ways. First, whereas before Iran mostly supplied the Houthis with older, simpler, and cheaper weapons, the appearance of the Faleq and the Hatem suggests Iran is increasingly willing to share its most advanced missile technologies with the non-state group. Prior to the September parade, Iran was not known to have given the Houthis missiles with terminal guidance or maneuverable re-entry vehicles.

Second, the parade points to a potential shift in Iran's methods of providing weapons to its partners in the region. Until now, Iran has equipped its allies for local production of simpler systems, such as small-diameter solid-propellant artillery rockets, while smuggling disassembled Iranian stocks of the more complex systems.<sup>[13]</sup> This seemingly precluded the transfer of large solid-propellant missiles, since they could be neither produced locally nor easily broken down into pieces for smuggling.

The appearance of such missiles in the parade indicates either that Iran is willing to run the risk of shipping large solid-propellant missiles over long distances, or, less likely, that it has begun expanding the Houthis'







local production capabilities beyond small artillery rockets. The U.S. Navy’s recent seizure of more than 70 tons of ammonium perchlorate, a main ingredient in solid propellants, bound for Yemen lends some credibility to the latter possibility, though the Houthis would also need a production facility with large, sophisticated equipment to manufacture the missiles locally.<sup>[14]</sup> In either case, to make the missiles useable, Iran would also need to transfer specialized launching equipment.

### An Iranian Missile Comes Full Circle

During the parade in Tehran, Iran’s armed forces unveiled for the first time a missile they called the Rezvan, a liquid-fueled ballistic missile with a claimed range of 1,400 km.<sup>[15]</sup> While the missile may be “new” to the Iranian military, it has been in the Houthi arsenal since 2019 in the form of the Burkan-3, which the Houthis later began calling the Zulfiqar.<sup>[16]</sup>



Top: The Houthi Zulfiqar. Bottom: The Iranian Rezvan.

In fact, the Houthis originally obtained the missile from Iran, but Iran had built this customized version of the Qiam specifically for the non-state group, and there was no evidence Iran had ever deployed it at home.<sup>[17]</sup>

The appearance in the parade of a missile originally built for the Houthis is surprising. Iran has been working to improve the precision of its missiles for more than a decade, and the Houthi Zulfiqar, with its poor accuracy at higher ranges, would be a step backwards in that regard. Nor is Iran wanting for missiles that can reach ranges of 1,400 km.

Nevertheless, the Iranian armed forces may find a use for it. Although it would be the first case of a ballistic missile tailor-made for a non-state group finding its way back to the Iranian arsenal, there are other weapons that have followed a similar pattern. The Quds cruise missile, for example, was probably first used by the Houthis in June 2019, months before the September 2019 attack against Saudi Aramco facilities, which the United States believes was launched by Iran. Iran has not formally acknowledged the Quds’s adoption by its armed forces, however. Additionally, some evidence suggests that the IRGC developed and adopted the Shahed-136 kamikaze drone following the transfer of the smaller, more primitive Shahed-131 to non-state partners.<sup>[18]</sup>

Another, often-overlooked benefit for Iran of transferring weapons to non-state groups is that those groups are more willing to use them in combat, and that allows Iran to collect information about the weapons’ performance. This can inform the development of new systems and variants—or even lead to Iran’s incorporation of the weapon into its own arsenal.



**Footnotes**

- [1] “Yemen: Pro-Houthi army unveils new weapons at parade marking revolution's 8th anniversary,” Middle East Monitor, September 22, 2022, available at <https://www.middleeastmonitor.com/20220922-yemen-pro-houthi-army-unveils-new-weapons-at-parade-marking-revolutions-8th-anniversary/>, accessed on November 3, 2022; Ned Price, “UN Truce Expiration in Yemen,” U.S. Department of State, October 3, 2022, available at <https://www.state.gov/un-truce-expiration-in-yemen/>, accessed on November 15, 2022.
- [2] “Drones, Ballistic Missiles Showcased At Iranian Military Parade Marking The Anniversary Of The Iran-Iraq War: We Will Annihilate Israel, Conquer Jerusalem, Trample America Underfoot!” MEMRI TV, September 22, 2022, available at <https://www.memri.org/tv/iranian-military-parade-iran-iraq-war-anniversary-ballistic-missiles-suicide-drones-annihilate-israel-america>, accessed November 3, 2022.
- [3] It is possible that the weapons paraded in Sanaa were merely mock-ups. But even so, they signal Iran’s intentions.
- [4] For a video of the entire parade, see “The full scenes of the majestic military parade on the occasion of the eighth anniversary of the September 21 revolution,” Yemeni Military Media, YouTube, September 22, 2022, available at <https://www.youtube.com/watch?v=Uh43AmC8dQ0> (in Arabic), accessed on November 3, 2022.
- [5] This and the following assessments are based partially on the author’s own measurement estimates, which compare screenshots taken from the parade with other screenshots and still images. All the images capture the relevant weapon from straight ahead in order to minimize foreshortening and other effects. Multiple measurements were taken for each system using different references and then averaged. Although such measurements are not perfect, they can give a reasonable estimate of a weapon’s absolute dimensions and an even better estimate of its dimensions relative to other, similar weapons.
- [6] “Iran Unveils New Long-Range Ballistic Missile,” Tasnim News Agency, February 9, 2022, available at <https://www.tasnimnews.com/en/news/2022/02/09/2659752/iran-unveils-new-long-range-ballistic-missile>, accessed on November 3, 2022.
- [7] “Letter Dated 26 January 2018 from the Panel of Experts on Yemen Mandated by Security Council Resolution 2342 (2017) Addressed to the President of the Security Council,” United Nations Security Council, S/2018/594, 26 January 2018, pp. 118–128, available at <https://undocs.org/S/2018/594>, accessed on November 3, 2022; Norbert Brugge, “The Yemeni Burkan Missile Riddle,” Spaceroockets, no date, available at [https://www.b14643.de/Spaceroockets/Specials/Yemeni-Burkan-missile\\_riddle/index.htm](https://www.b14643.de/Spaceroockets/Specials/Yemeni-Burkan-missile_riddle/index.htm), accessed on November 3, 2022.
- [8] Norbert Brugge, “The Yemeni Burkan Missile Riddle,” Spaceroockets, no date, available at [https://www.b14643.de/Spaceroockets/Specials/Yemeni-Burkan-missile\\_riddle/index.htm](https://www.b14643.de/Spaceroockets/Specials/Yemeni-Burkan-missile_riddle/index.htm), accessed on November 3, 2022.
- [9] “The range of the Qiam missile has reached 1,000 kilometers,” Tasnim News Agency, January 3, 2022, available at <https://tn.ai/2637608> (in Persian), accessed on November 3, 2022.
- [10] “U.S. Dhow Interdictions,” U.S. Central Command Public Affairs, February 19, 2020, available at <https://www.centcom.mil/MEDIA/NEWS-ARTICLES/News-Article-View/Article/20...>, accessed on November 3, 2022; “UK Reveals Royal Navy Seizure of Smuggled Iranian Missiles,” Royal Navy, Ministry of Defence of the United Kingdom, July 7, 2022, available at <https://www.royalnavy.mod.uk/news-and-latest-activity/news/2022/july/07/20220707-montrose-arms-cache>, accessed on November 3, 2022.
- [11] “Letter dated 27 January 2020 from the Panel of Experts on Yemen addressed to the President of the Security Council,” U.N. Security Council, S/2020/326, January 27, 2020, p. 23, available at <https://www.undocs.org/S/2020/326>, accessed on November 7, 2022.
- [12] Michael Knights, “Iraqi Militias Show Off Iranian Anti-Air Missile,” Washington Institute for Near East Policy, October 21, 2021, available at <https://www.washingtoninstitute.org/policy-analysis/iraqi-militias-show-iranian-anti-air-missile>, accessed on November 3, 2022.
- [13] Fabian Hinz, “Missile multinational: Iran’s new approach to missile proliferation,” International Institute for Strategic Studies, April 26, 2021, p. 8, available at <https://www.iiss.org/blogs/research-paper/2021/04/iran-missile-proliferation-strategy>, accessed on November 3, 2022.
- [14] “U.S. Naval Forces Intercept Explosive Material Bound for Yemen,” U.S. Naval Forces Central Command, November 15, 2022, available at <https://www.cusnc.navy.mil/Media/News/Display/Article/3218261/us-naval-forces-intercept-explosive-material-bound-for-yemen/>, accessed on November 15, 2022.
- [15] “Iran Unveils Rezvan Surface-to-Surface Ballistic Missile in Military Parade,” Tasnim News Agency, September 22, 2022, available at <https://www.tasnimnews.com/en/news/2022/09/22/2777746/iran-unveils-rezvan-surface-to-surface-ballistic-missile-in-military-parade>, accessed on November 3, 2022.
- [16] “Open-Source Analysis of Iran’s Missile and UAV Capabilities and Proliferation,” International Institute for Strategic Studies, p. 33, available at <https://www.iiss.org/blogs/research-paper/2021/04/iran-missiles-uavs-proliferation>, accessed on November 3, 2022.







[17] Particularly to maximize the range. For an exhaustive account of the modifications made to the earlier Burkan-2H, see "Letter Dated 26 January 2018 from the Panel of Experts on Yemen Mandated by Security Council Resolution 2342 (2017) Addressed to the President of the Security Council," United Nations Security Council, S/2018/594, 26 January 2018, pp. 123–124, available at <https://undocs.org/S/2018/594>, accessed on November 3, 2022. The Burkan-3/Zulfiqar can be expected to have similar modifications.

[18] The first known public appearance of the Shahed-131 in Iran was at an exhibition of achievements of the IRGC Aerospace Force in May 2014. The system was used in Houthi attacks against Saudi targets in May 2019, as well as in the September 2019 Saudi Aramco attacks. Wreckage of the larger Shahed-136 was apparently first found in Yemen in 2020, and the first indication that the weapon was adopted by Iran's armed forces was in May 2021. This timeline is most clearly presented in "Iranian UAV Attack Against MOTOR TANKER MERCER STREET," United States Central Command, August 6, 2021, p. 5, available at <https://www.centcom.mil/Portals/6/PressReleases/MERCERSTREETATTACK06AUG2...>

### U.S. embassy latest target in spate of letter bombs in Spain

Source: <https://www.reuters.com/world/europe/third-mail-bomb-found-spanish-air-force-base-el-mundo-reports-2022-12-01/>

Dec 01 – Bomb disposal experts defused a letter bomb at the U.S. Embassy in Madrid on Thursday, the sixth such device sent to high-profile targets in a wave that prompted Spain to step up security and vow not to be deterred from supporting Ukraine.

31 cases with suspicious parcels in 15 countries



The campaign began with a package sent to Prime Minister Pedro Sanchez on Nov. 24, spurring Madrid to tighten security around public buildings. Since Wednesday, similar devices have also been sent to the defence ministry, an air force base, a weapons manufacturer and the Ukrainian embassy - where a security officer was slightly injured. Spain's Defence Minister Margarita Robles, who was visiting the Ukrainian port city of Odessa on Thursday and met her

Ukrainian counterpart Oleksii Reznikov, said the letter bombs would not deter Spain from supporting Ukraine's "just cause". "What must be very clear is that none of these deliveries or any other violent action will change the clear and firm commitment of Spain, NATO countries and the European Union to support Ukraine," she said. The latest package was intercepted at the U.S. Embassy by security officials and was later detonated in a controlled explosion by Spanish police. On Wednesday, a package addressed to the Ukrainian ambassador to Spain detonated at the country's embassy as a security official investigated it, causing him to suffer minor injuries to his hands and a concussion. Security has now been stepped up around embassies as well.

Later on Wednesday, Instalaza, a weapons manufacturer in Zaragoza, northeastern Spain, that has send more than 1,000 C90 rocket launchers to Ukraine received another package, and on Thursday an air force base housing a European Union satellite centre, Spain's defence ministry and the U.S. Embassy also received packages.

### Ukraine points finger at Moscow

After the package to the Ukrainian embassy detonated, Ukraine's Foreign Minister Dmytro Kuleba ordered all of Kyiv's embassies abroad to "urgently" strengthen security. Ukraine's ambassador to Spain, Serhii Pohoreltsev, appeared to blame Russia.

"We have instructions from the ministry in Ukraine that given the situation we have to be prepared for any kind of incident... Russian activities outside the country," he told Spanish television station TVE on







Wednesday. Russia invaded Ukraine nine months ago in what it calls a "special military operation" that Kyiv and the West describe as an unprovoked, imperialist land grab. Spain has sent or committed to send military and humanitarian equipment to support Ukraine in the conflict, including surface-to-air missile launchers, a battery of six light howitzers, ammunition and body armor and light weapons as well as offering its airmen training in air defence in Spain. On Thursday, the Twitter account of the Russian Embassy in Spain posted a statement condemning "any threat or terrorist act" in relation to the five letter bombs, "particularly directed at a diplomatic mission".

**"Sudden flames"**

The delivery of letter bombs across the Spanish capital caused road closures and traffic chaos around major diplomatic and public buildings. Speaking before the latest package was found at the U.S. embassy, Spain's deputy interior minister said early indications suggested the first five packages were sent from within Spain. Rafael Perez, the junior minister responsible for security, told journalists in a news conference that the homemade devices were sent in brown packages containing a flammable powder and tripwire that would generate "sudden flames" rather than an explosion. The packages were addressed to the heads of the institutions they were sent to. One device had been kept intact for investigative purposes, Perez said, while the others were detonated by the security forces in controlled explosions. "It appears that they were all sent from within the country but we are basing this on early visual inspections without yet having an in-depth technical report," he said. Perez said it did not yet appear necessary to convene the security committee that would evaluate stepping up Spain's terrorist threat level, which is already at the second-highest level following Islamist attacks around Europe in the past decade. A source close to the investigation said that, while the devices were homemade, "they were not something anyone could make", and investigators were now seeking to trace their contents to their origin. Another source involved in the judicial investigation said the large envelopes all had the same typeface and appeared to have come from the same sender. They contained an "electrical ignition mechanism" and a substance similar to gunpowder, the source said. The postal service has been told to screen all letters addressed to high-profile institutions, he added. Spain's High Court that specialises in terrorism has opened an investigation.

**Thank you!**



A heartbreaking photo shows a police officer in Connecticut saying his final goodbye to his partner. 🐕 K9 Hunter has been ill for that past several days and when tests were conducted, they revealed that K9 Hunter has a very aggressive form of Liver cancer. They unfortunately recommended that he be euthanized.  
THANK YOU SIR DOGGY ❤️







### Canada to provide C\$15 million for Ukraine demining

Source: <https://counteriedreport.com/canada-to-provide-c15-million-for-ukraine-demining/>



Dec 05 – The Government of Canada said Monday that it will grant 15 million Canadian dollars (10.5 million euros) to Ukraine for the purchase of equipment needed for humanitarian landmine clearance. Specifically, the assistance will help fund the detection and removal of landmines, unexploded ordnance and other explosive remnants of war, 'The Globe and Mail' has reported. In this regard, Canada will provide bomb suits to help protect Ukrainian deminers, which will be accompanied by funds for the purchase of advanced remote-controlled demining systems, which will help clear large areas such as farmland, according to a statement from the Canadian Executive.

**EDITOR'S COMMENT:** Demining while the war is in progress? Someone will be very happy with the small token!

### Lockerbie bombing suspect in US custody

Source: <https://www.bbc.com/news/uk-scotland-63933837>



Dec 11 – A Libyan man accused of making the bomb which destroyed Pan Am flight 103 over Lockerbie 34 years ago is in United States custody, Scottish authorities have said. The US announced charges against Abu Agila Masud two years ago, alleging that he played a key role in the bombing on 21 December, 1988. The blast on board the Boeing 747 left 270 people dead. It is the deadliest terrorist incident to have taken place on British soil. All 259 passengers and crew on board the jumbo jet bound to New York from London died while another 11 people were killed in Lockerbie when wreckage destroyed







their homes. Last month it was reported that Masud had been kidnapped by a militia group in Libya, leading to speculation that he was going to be handed over to the American authorities to stand trial. A US Justice Department spokesperson told the Reuters news agency that Masud would make an initial appearance in a federal court in Washington. Five years ago he was serving a prison sentence in Libya for bomb-making.



Abu Agila Masud behind bars in Libya (Reuters)

In 2001 Abdelbaset al-Megrahi was convicted of bombing Pan Am 103 after standing trial at a specially-convened Scottish court in the Netherlands. He was the only man to be convicted over the attack. Megrahi was jailed for life but was released on compassionate grounds by the Scottish government in 2009 after being diagnosed with cancer. He died in Libya in 2012.

Megrahi, who always proclaimed his innocence, launched two appeals against his 27-year sentence. One was unsuccessful and the other was abandoned. A spokesperson for the Crown Office and Procurator Fiscal Service (COPFS) said: "The families of those killed in the Lockerbie bombing have been told that the suspect Abu Agila Mohammad Mas'ud Kheir Al-Marimi ("Mas'ud" or "Masoud") is in US custody. "Scottish prosecutors and police, working with UK government and US colleagues, will continue to pursue this investigation, with the sole aim of bringing those who acted along with Al Megrahi to justice."



**Lockerbie bombing timeline**

- US and British investigators indicted Megrahi in 1991 but he was not handed over by the Libyans until April 1999.
- **May 2000** - A special trial under Scots law starts on neutral ground at Camp Zeist in the Netherlands.
- **31 January 2001** - Former Libyan intelligence officer Megrahi is found guilty of mass murder and jailed for life with a minimum term of 27 years.







- **March 2002** - Megrahi loses an appeal against his conviction.
- **September 2003** - The Scottish Criminal Cases Review Commission (SCCRC) is asked to investigate Megrahi's conviction.
- **June 2007** - The SCCRC recommends that Megrahi is granted a second appeal against his conviction.
- **18 August 2009** - Megrahi's move to drop his second appeal is accepted by judges at The High Court in Edinburgh.
- **20 August 2009** - Megrahi, who has terminal prostate cancer, [is released from prison on compassionate grounds](#).
- **May 2012** - Megrahi dies at his home in Tripoli, aged 60.
- **July 2015** - Scottish judges rule that relatives of the Lockerbie bombing victims should [not be allowed to pursue an appeal](#) on Megrahi's behalf. Courts had previously ruled that only next of kin could proceed with a posthumous application.
- **July 2017** - Megrahi's family [launched a new bid to appeal against his conviction](#).
- **March 2020** - The Scottish Criminal Case Review Commission said Megrahi's conviction [can be taken to a fresh appeal](#).
- **November 2020** - Five Scottish judges hear the [third appeal against Megrahi's conviction](#) on grounds of possible miscarriage of justice



**UPDATE 13/12:** US prosecutors told the court they would not seek [death](#) penalty, as they believe the punishment was not legally available at the time of his alleged crime.

## Rules on liquids and laptops to be eased at UK airports from June 2024

Source: <https://www.theguardian.com/world/2022/dec/15/rules-on-liquids-and-laptops-to-be-eased-at-uk-airports-from-june-2024>

Dec 15 – Rules around taking liquids and laptops through airport security will be eased from June 2024, the government has said. The announcement of the biggest relaxation of aviation security regulations in decades confirms reports last month that the change would come in the year after next. Passengers at most major UK airports will be able to carry liquids in containers holding up to two litres, a huge increase from the current limit of 100ml. Travellers will also no longer need to carry the containers in clear plastic bags or remove tablets and laptops from hand luggage at checkpoints.

## Phosphorus exposure from WWII bomb at US base in Germany lands five in hospital

By John Vandiver

Source: <https://www.stripes.com/theaters/europe/2022-12-08/world-war-ii-bomb-eucom-stuttgart-8349033.html>



U.S. European Command headquarters at Patch Barracks in Stuttgart, Germany. (John Vandiver/Stars and Stripes)

Dec 08 — Five construction workers were hospitalized Thursday after an unexploded World War II-era phosphorus bomb at Patch Barracks was accidentally struck, releasing some of the poisonous gas, Army officials said.

Patch Barracks is home to U.S. European Command headquarters.

At about 12 p.m., a backhoe penetrated the casing of the bomb, U.S. Army Garrison Stuttgart said in a statement. Workers exposed to the phosphorus were taken to a

local hospital for observation, garrison spokesman John Campbell said.

“There is no threat to Patch Barracks or the local community, but residents are asked to avoid the construction site out of an abundance of caution,” the garrison said.

The incident occurred near Floridastrasse, where EUCOM's top generals reside. The bomb was struck while workers were making repairs to the post's sewer system.

A German explosive ordnance disposal team arrived quickly and removed the bomb, the Army said.





# ICI C<sup>2</sup>BRNE DIARY – December 2022

Campbell said no base residents were forced to evacuate their homes. Although it has been more than 75 years since the end of World War II, bombs routinely are uncovered during construction work in Germany, sometimes causing large residential evacuations. An industrial hub during the war, Stuttgart was heavily bombarded by allies. In recent years, unexploded ordnance has been uncovered at or near Army facilities in the Stuttgart area. On average, more than 2,000 tons of unexploded bombs and other munitions are found each year in Germany. About 15% of the bombs dropped during the war didn't explode, and many remain buried deep in the ground.

**John Vandiver** covers U.S. military activities across Europe and Africa. Based in Stuttgart, Germany, he previously worked for newspapers in New Jersey, North Carolina and Maryland. He is a graduate of the University of Delaware.





ICI  
International  
**CBRNE**  
INSTITUTE



# CYBER NEWS







## Metaverse – Most Dangerous Cyber Threats

Source: <https://i-hls.com/archives/117264>



Nov 23 – In February 2022, Gartner predicted that 25 percent of people will spend at least one hour per day in the metaverse by 2026. Backed by technology giants like Google, Microsoft, and Meta, this environment has the potential to change many aspects of people's everyday lives. Even concepts like the virtual workplace are becoming increasingly appealing.

According to [xrtoday.com](https://xrtoday.com), Innovators investing in the metaverse have already begun to share their insights on the benefits this unique landscape could bring. Considering the rapid surge in data protection issues and cyber-attacks following the acceleration of digitization triggered by the COVID-19 pandemic, the rise of the spatial communications platform could potentially lead to similar issues. Many experts are already discussing concerns over cybercrime, fraud, and even the protection of individual users.

The highlighted concerns regarding the expanding use of the Metaverse included:

**Identity theft:** The use of sensors, eye-tracking and face-tracking technologies means criminals could have access to a wider range of tools, allowing them to impersonate victims more convincingly. These stolen identities could even manipulate other users.

**Money laundering:** Cryptocurrencies are already being used in the metaverse for both legitimate and criminal activities. With platform-specific cryptocurrencies emerging, there could be new challenges to address regarding money laundering.

**Ransomware:** The increased importance of digital assets in the metaverse puts companies under increasing pressure to protect their IP. If companies lose assets in the XR landscape, this loss could lead to greater consequences, and issues of fraud.

**Harassment:** The report also examines the potential for real-life harassment and abuse spilling into the metaverse. Reports of people being sexually assaulted in digital environments have already begun to emerge. These virtual events could be just as impactful as those in the physical realm with increasingly realistic XR experiences.

**Child protection:** There's also a concern to address around the concept of protecting children and vulnerable individuals. This new landscape could introduce new ways of grooming and virtually assaulting children.

## Next generation modern and articulated e-Warfare for army

By Dr Nishakant Ojha

Source: <https://www.financialexpress.com/defence/next-generation-modern-and-articulated-e-warfare-for-army/2895675/>

Nov 29 – Realising the irrationality, miscalculation, or some bad intention or unanticipated agenda that may lead an alarm or trigger to launch an attack, some strategists have always been unwilling to place full confidence in the stability of deterrence. It is naturally understood that measures to enable a defence against an attack when it is launched, either to intercept enemy weapons before they can detonate on target or to blunt the effects of detonations that do occur. The proliferation of weapons of mass destruction (WMD) and their delivery systems could have incalculable consequences for national, regional and global security. The emerging effects of these types of weapons i.e. (CBRN) – which include nuclear devices, radiological material, biological pathogens and chemical







substances – are some of the biggest threats but the most important aspects of WMD role is the medium by which it can play a disaster role needs to be analysed & on priority.

The first three decades of the Space Age, demonstrate that the superpowers have found it technically and economically attractive to use space only for the five so called traditional missions of reconnaissance and surveillance, communication, for the Defence and other strategic purposes briefly, before passing on to the host of new technologies that might in the future greatly lengthen this list of military space missions.

With respect to the Reconnaissance and Surveillance -Electromagnetic radiation emitted or reflected from terrestrial objects can be detected from space in any of the three wavelength bands to which the intervening atmosphere is transparent, namely, the visible band, certain infrared bands, and the microwave radio band. It follows that these are the bands used for military surveillance.

Further in the realm of nuclear operations; space is used to detect missile launches and nuclear detonations. Missile warning data permit the safe escape of bombers, tankers, cruise missile carriers, airborne command posts, and, for launch-under-attack (LUA), intercontinental ballistic missiles (ICBMs).. But the most important use of missile launch and nuclear detonation data would probably be to give decision-makers a clear assessment of what happened, information crucial to responsible action and, under the chaotic circumstances, hard to come by otherwise.

### **Terrestrial Communications:**

With respect to the Communications there are only two ways to communicate information over long distances within seconds: by landline (including transoceanic cable) and by radio. Because the earth is round, line-of-sight radio contact between widely separated points on the earth's surface is impossible. One way to propagate radio waves over the horizon is to bounce them off the ionosphere; shortwave (HF, high frequency) radio propagation in this manner. But ionospheric reflection is unreliable and cannot support large rates of message traffic. Long distance communication companies have long placed microwave radio relays on towers and mountaintops for over-the-horizon relay. The communications satellite is just an extension of the relay principle to higher altitudes and consequently longer relay distances.

### **Quantum Technologies:**

If need to compress on the Quantum embedded Technologies Solutions vulnerabilities & misuse by Bad Actors that how the quantum terrorists could bring the quantum internet to its knees almost instantly and without revealing their identity. More worrying still is that there is no obvious way to counter this new kind of attack. How a malicious actor might destroy this cloud and the information it contains. One approach would be to simply break the entanglement, which is a famously fragile form of existence. But this would be something of a sledgehammer—a classical attack on a quantum system.

Basically, interest falls to know how much more subtle kind of quantum attack. This kind of attack would involve injecting some random information that becomes entangled with the rest, thereby making the original information impossible to retrieve from the mix. By itself this does not work. A lone-wolf attacker cannot overwhelm the quantum state with random information.

But if quantum terrorists work in unison, an entirely different scenario unfolds. Also, if several attackers inject their quantum information into the network at the same instant, they can disrupt the global quantum state. In that case the initial state of the system cannot be retrieved, even in principle.

Now the question how many Bad Actors wanted to happen this, the shocking conclusion is that it requires only three or more quantum terrorists working in unison.

### **With respect to the Next Generation Weapons of mass destruction and weapons of mass effects terrorism**

There has been widespread concern of using nuclear, biological, chemical, or radiological weapons – or what usually are labelled weapons of mass destruction (WMD). There also has been concern about another catastrophic terrorist attack entailing the non-traditional use of conventional means. In the coming times a country has to be prepared for this .

Against this background, the Advanced Systems and Concepts Office (ASCO) of the Defence Threat Reduction Agency (DTRA) asked Science Applications International Corporation (SAIC) to analyze the dimensions of possible "Next Generation WMD and WME Terrorism." Particular focus was to be placed on the potential groups that could carry out such attacks, what new groups or other entities might be attracted to the use of WMD or WME over the next 3-15 years, and what motivations might lead different terrorist groups or other entities to escalate to WMD violence.

### **Network Attacks**

For Mass Effects Modern society is becoming increasingly penetrated by networking technology. From the networking of physical objects to the networking of financial dealings, the Internet has become a societal and global command and control system, the Internet also has resulted in a new cyber-space battlefield with new targets, specific vulnerabilities, and a myriad of channels of attack. Attacks across the Internet





taking advantage of those channels of attack are labelled here “network attacks.” One possible purpose of such attacks would be to damage or destroy “things” – and for that reason, it warrants brief inclusion here as part of next generation WMD or WME terrorism. For next generation WMD or WME terrorism, two issues are of particular importance: the spectrum of potential attacks that are conceivable; and the range of potential attackers. Consider each dimension in turn. With regard to the spectrum of potential attacks, as set out in the Lukasik analysis, a useful typology focuses respectively on economy-oriented attacks and people-oriented attacks. Depending on the specific network-based attack, the impact would vary. Some of these attacks would not fall within the category of mass effects attacks directly though they might facilitate later, larger-scale attacks. Thus, a network-based attack aimed at reputation assassination would have a physically limited impact but could be quite important politically. But network attacks could well have immediate mass effects in terms of loss of life, physical destruction or disruption, and other metrics, e.g., attacks on critical energy or oil infrastructure. Attacks that leveraged interdependencies across many economic sectors would be among the most damaging of the latter attacks.

### Conclusion

The dynamics of Space, Quantum & viz-a-viz Next Generation WMD and WME Bad Actors — we can by conclude that over the next 3-15 years, the number of terrorist entities should be expected to continue to increase, continuing an historic pattern of exponential growth in terrorist groups, leaders, and followers. Multiple geopolitical trends – many tied to the impact of globalization on individuals, groups, and nations – all comprise drivers for this emergence of more extremist groups. Many of these groups will be characterized by religious extremism; but there also will be many other motivating ideologies. The Internet increasingly will be a powerful and multi-faceted terrorist enabler, including WMD and WME terrorism. In parallel, technological trends point toward the capability to do extreme violence becoming accessible to smaller and smaller entities, including individuals. Though direct production of nuclear weapons probably exceeds the technical capabilities of all but states, terrorist groups could well obtain nuclear weapons by purchase, theft, or gift. Ties between terrorist groups and traditional criminal organizations are likely to make it easier for such groups to gain access to – and to transport – WMD. With regard to specific groups, the next generation WMD threat will continue to be most characterized by the threat that the Bad Actors will successfully acquire and use any one of chemical, biological, radiological, or nuclear weapons. Aborted or failed attempts to use biological and radiological weapons already have occurred. The repeated use of chlorine-explosive mixtures by them in many countries is no longer simply setting an isolated precedent but instead institutionalizing a new mode of terrorist attack. With regard to nuclear weapons, barring some unexpected reversal, the debate within the Jihadist community about the legitimacy and justification of WMD.

[Dr Nishakant Ojha](#) is Eminent Expert –Counter Terrorism, CSO& Advisor Cyber & Aerospace Securities.

## Christchurch Livestream Video Found on Twitter

Source: <https://www.counterextremism.com/press/tech-terrorism-christchurch-livestream-video-found-twitter>

Dec 02 — Over the weekend, Twitter users successfully [uploaded](#) a video of the 2019 Christchurch shootings to the platform. The video, which was livestreamed by [Brenton Tarrant](#) who attacked two mosques and killed 51 Muslim worshippers, was only removed after being reported to the company by the government of New Zealand. Twitter’s terms of service [state](#) that the company prohibits content that “promote[s] terrorism or violent extremism,” and CEO Elon Musk has [pledged](#) that users would be suspended for posting content that is illegal or an “incitement to violence.”

Following the Christchurch attack, major tech companies, including Twitter, signed the [Christchurch Call to Action](#), a nine-point action plan aimed at fighting terrorism and violent extremism online. The nine action points [included](#) a pledge to invest in new technologies to improve terrorist content detection and removal, a commitment to implementing live streaming checks to reduce risks of disseminating terrorist content, and, among other things, a promise to improve sharing technological developments between large and small companies.

Although content moderation is at the forefront of many policy conversations, the content in question here—a video from a terrorist attack—should be treated as something that must unassailably be removed, much as child sexual abuse material (CSAM) or drug trafficking content, because it continues to inspire further violence. The shooter in the May 2022 Buffalo Attack, for example, [viewed](#) a clip of the Christchurch shooting on 4chan and credited the attack as his inspiration in his online manifesto.

Unfortunately, the Counter Extremism Project (CEP) continues to find the Christchurch video, clips of the video and support for the attack on a variety of platforms that signed the Christchurch Call to Action and other online sites. Ahead of the one-year anniversary of the Christchurch attack in 2020, CEP researchers [found](#) the attack video on 17 online locations. Separately in August 2022, CEP [located](#) three Twitter







accounts that glorified the terrorist attack and combined had nearly 2,000 followers. One of these accounts remained on Twitter for almost four months.

## SpaceX reveals 'Starshield' satellite project for national security use

By Mike Wall

Source: <https://www.space.com/spacex-starshield-satellite-internet-military-starlink>



Dec 07 – SpaceX is expanding its satellite-internet business.

[SpaceX](#) already beams broadband service to customers around the world via its huge and ever-growing [Starlink](#) constellation. Over the weekend, [Elon Musk](#)'s company revealed that Starlink now has a partner project called Starshield, which is tailored for use by government agencies, particularly those in the national security sector.

"Starshield leverages SpaceX's Starlink technology and launch capability to support national security efforts," SpaceX's newly posted [Starshield page](#) (opens in new tab) reads.

"While Starlink is designed for consumer and commercial use, Starshield is designed for government use, with an initial focus on three areas," the page adds. Those areas are Earth observation, communications and hosted payloads (the ability to put a wide variety of instruments on the Starshield satellite bus).

Starshield will offer a higher level of security than Starlink, featuring "additional high-assurance cryptographic capability to host classified payloads and process data securely, meeting the most demanding government requirements," according to SpaceX's Starshield page.

Starshield spacecraft will also be interoperable with other satellites that are equipped with the laser-communications terminal that Starlink craft use, the page adds.

That's pretty much all we know about Starshield; the page doesn't provide many other details about the new project.

We know much more, of course, about Starlink. The megaconstellation consists of more than 3,200 active satellites and will grow considerably larger in the months and years to come.

SpaceX already has permission from the U.S. Federal Communications Commission (FCC) to deploy 12,000 first-generation Starlink craft, the type that's now operating in low Earth orbit.

The company has applied for approval to loft nearly 30,000 Starlink 2.0 satellites on top of that. These new spacecraft, which SpaceX plans to launch primarily using its next-generation [Starship](#) rocket, will be much bigger and more powerful than their predecessors. For instance, Starlink 2.0 satellites will be capable of beaming service directly to cellphones, something that SpaceX [plans to start doing next year](#).





Last week, the FCC granted SpaceX permission to [deploy just 7,500 Starlink 2.0 craft](#), citing concerns about space debris and space traffic. The agency is reserving judgment on the rest of the application.

**Michael Wall** is a Senior Space Writer with Space.com (opens in new tab) and joined the team in 2010. He primarily covers exoplanets, spaceflight and military space, but has been known to dabble in the space art beat. His book about the search for alien life, "Out There," was published on Nov. 13, 2018. Before becoming a science writer, Michael worked as a herpetologist and wildlife biologist. He has a Ph.D. in evolutionary biology from the University of Sydney, Australia, a bachelor's degree from the University of Arizona, and a graduate certificate in science writing from the University of California, Santa Cruz.

## North Korean Cyber Spies Deploy New Tactic: Tricking Foreign Experts into Writing Research for Them

Source: <https://www.voanews.com/a/north-korean-cyber-spies-deploy-new-tactic-tricking-foreign-experts-into-writing-research-for-them/6872314.html>

Dec 12 – When Daniel DePetris, a U.S.-based foreign affairs analyst, received an email in October from the director of the 38 North think-tank commissioning an article, it seemed to be business as usual.

It wasn't.

The sender was actually a suspected North Korean spy seeking information, according to those involved and three cybersecurity researchers.

Instead of infecting his computer and stealing sensitive data, as hackers typically do, the sender appeared to be trying to elicit his thoughts on North Korean security issues by pretending to be 38 North director Jenny Town.

"I realized it wasn't legit once I contacted the person with follow up questions and found out there was, in fact, no request that was made, and that this person was also a target," DePetris told Reuters, referring to Town. "So, I figured out pretty quickly this was a widespread campaign."

The email is part of a new and previously unreported campaign by a suspected North Korean hacking group, according to the cybersecurity experts, five targeted individuals and emails reviewed by Reuters.

**The hacking group, which researchers dubbed **Thallium or Kimsuky**, among other names, has long used "spear-phishing" emails that trick targets into giving up passwords or clicking attachments or links that load malware. Now, however, it also appears to simply ask researchers or other experts to offer opinions or write reports.**

According to emails reviewed by Reuters, among the other issues raised were China's reaction in the event of a new nuclear test; and whether a "quieter" approach to North Korean "aggression" might be warranted.

"The attackers are having a ton of success with this very, very simple method," said James Elliott of the Microsoft Threat Intelligence Center (MSTIC), who added that the new tactic first emerged in January. "The attackers have completely changed the process." MSTIC said it had identified "multiple" North Korea experts who have provided information to a Thallium attacker account.

The experts and analysts targeted in the campaign are influential in shaping international public opinion and foreign governments' policy toward North Korea, the cybersecurity researchers said.

A 2020 report by U.S. government cybersecurity agencies said Thallium has been operating since 2012 and "is most likely tasked by the North Korean regime with a global intelligence gathering mission."

Thallium has historically targeted government employees, think tanks, academics and human rights organizations, according to Microsoft.

"The attackers are getting the information directly from the horse's mouth, if you will, and they don't have to sit there and make interpretations because they're getting it directly from the expert," Elliot said.

### New tactics

North Korean hackers are well-known for attacks netting millions of dollars, targeting Sony Pictures over a film seen as insulting to its leader and stealing data from pharmaceutical and defense companies, foreign governments, and others.

North Korea's embassy in London did not respond to a request for comment, but it has denied being involved in cybercrime.

In other attacks, Thallium and other hackers have spent weeks or months developing trust with a target before sending malicious software, said Saher Naumaan, principal threat intelligence analyst at BAE Systems Applied Intelligence.

But according to Microsoft, the group now also engages with experts in some cases without ever sending malicious files or links even after the victims respond.







This tactic can be quicker than hacking someone's account and wading through their emails, bypasses traditional technical security programs that would scan and flag a message with malicious elements and allows the spies direct access to the experts' thinking, Elliot said.

"For us as defenders, it's really, really hard to stop these emails," he said, adding that in most cases it comes down to the recipient being able to figure it out.

Town said some messages purporting to be from her had used an email address that ended in ".live" rather than her official account, which ends in ".org," but had copied her full signature line.

In one case, she said, she was involved in a surreal email exchange in which the suspected attacker, posing as her, included her in a reply.

DePetris, a fellow with Defense Priorities and a columnist for several newspapers, said the emails he has received were written as if a researcher were asking for a paper submission or comments on a draft.

"They were quite sophisticated, with think tank logos attached to the correspondence to make it look as if the inquiry is legitimate," he said.

About three weeks after receiving the faked email from 38 North, a separate hacker impersonated him, emailing other people to look at a draft, DePetris said.

That email, which DePetris shared with Reuters, offers \$300 for reviewing a manuscript about North Korea's nuclear program and asks for recommendations for other possible reviewers. Elliot said the hackers never paid anyone for their research or responses and would never intend to.

### **Gathering information**

Impersonation is a common method for spies around the world, but as North Korea's isolation has deepened under sanctions and the pandemic, Western intelligence agencies believe Pyongyang has become particularly reliant on cyber campaigns, one security source in Seoul told Reuters, speaking in condition of anonymity to discuss intelligence matters.

In a March 2022 report, a panel of experts that investigates North Korea's U.N. sanctions evasions listed Thallium's efforts as among activities that "constitute espionage intended to inform and assist" the country's sanctions avoidance.

Town said in some cases, the attackers have commissioned papers, and analysts had provided full reports or manuscript reviews before realizing what had happened.

DePetris said the hackers asked him about issues he was already working on, including Japan's response to North Korea's military activities.

Another email, purporting to be a reporter from Japan's Kyodo News, asked a 38 North staffer how they thought the war in Ukraine factored in North Korea's thinking, and posed questions about U.S., Chinese, and Russian policies.

"One can only surmise that the North Koreans are trying to get candid views from think tankers in order to better understand U.S. policy on the North and where it may be going," DePetris said.

## **Meta Launches new Content Moderation Tool HMA that can scan for terrorist content**

Source: <https://www.neowin.net/news/meta-launches-new-content-moderation-tool-hma-that-can-scan-for-terrorist-content/>

Dec 13 – Meta, the parent company of Facebook, has developed an open-source tool that it claims can fight terrorist and violent extremist content online.

The tool, better known as [Hasher-Matcher-Actioner \(HMA\)](#) can identify suspicious content, including copies of images or videos that violate certain guidelines and have been flagged by users as inappropriate. It can then act against such material collectively.

Meta says Hasher-Matcher-Actioner (HMA) tool can be adopted by a range of companies that want to fight against terrorism on their platforms and stop the spread of it. It is particularly useful for smaller companies that don't possess the vast reserves of resources as bigger ones.

Firms desirous of using this product can simply run all their content through the hash-sharing database and follow the steps described above to help themselves and Meta is keeping the violent and abusive content off the internet.

The decision to make the [tool available publicly](#) comes shortly before the California-based company assumes the chair of the Global Internet Forum to Counter Terrorism (GIFCT) board in January.

It's a group that brings together member companies, governments, and civil society organizations to tackle terrorist and violent extremist content online. Meta has been its founding member.





# HMA helps keep platforms free of terrorist content.



## STEP 1: LABEL

First, you label an image or video as violating (it can be terrorist content, child sexual exploitation material, or any other violating content) and enter it into HMA.



## STEP 2: HASH

Then, using an algorithm, HMA creates a unique digital fingerprint, or "hash" for that image or video (often a string of numbers and letters).



## STEP 3: MATCH & CONTINUOUS SCANS

Each fingerprint—not the image itself—is kept in your own database, and all content is run through that database as it's uploaded, to see if it matches something you've already decided is violating.



## STEP 4: ACTION

As HMA finds matches, you can review the results and remove (or take another action on) them automatically or on a case-by-case basis.



## FUN FACT

HMA can also plug into databases where companies pool resources and knowledge, like the **Global Internet Forum to Counter Terrorism**—allowing you to leverage content other companies have found and flagged as terrorist content too.

Meta reports that it spent an amount of \$5 billion globally on safety and security last year, and has a dedicated team of hundreds of people working round the clock with experts from law enforcement and national security agencies to counter-terror work. The new initiative will strengthen it furthermore.







## Iran's Balkan front: The roots and consequences of Iranian cyberattacks against Albania

By Gerta Zaimi

Source: <https://www.mei.edu/publications/irans-balkan-front-roots-and-consequences-iranian-cyberattacks-against-albania>

Dec 22 – On Sept. 7, Albanian Prime Minister Edi Rama announced in a [video statement](#) that a series of damaging hacks of the country's critical digital infrastructure earlier that summer had been attributed to the Islamic Republic of Iran (IRI), and as a result, his government was terminating diplomatic relations with the Tehran — arguably one of the most profound responses that a sovereign state might take to a cyberattack. Iranian foreign ministry spokesperson Nasser Kanaani [condemned](#) Tirana's decision as "unfounded," adding that it "only serves the American and Israeli conspiracy."

But undercutting Kanaani's denial, just three days later, an Iranian-linked group of hackers calling itself HomeLand Justice [targeted](#) a restricted database administered by the Albanian police, before posting the ransacked information to Telegram over the coming weeks. On Sept. 19, a dozen days after Albania broke off diplomatic relations with the IRI, HomeLand Justice published on its Telegram channel a 47-page document of stolen data. The file contained personal identifying information as well as records of the border crossings of the former general director of the State Police of Albania (*Policia e Shtetit*), Gladis Nano, and his family. Less than a month later, on Oct. 3, the same group of cyber actors released another voluminous document, this one over 1.7 gigabytes in size, which exposed 300 identities of persons suspected of criminal acts in Albania. That data dump strongly suggested the hackers had broken into Albania's sophisticated police communication system called [Memex](#), raising strong concerns about national data protection measures.

More periodic leaks followed. On Oct. 19, the hackers published a file linked to the director of Albanian intelligence, Helidon Bendo, that contained 17 years' worth of data (2005-2022) from the government's Total Information Management System (TIMS), again exposing logged entries and exits at the state border. On Nov. 2, the group raised the stakes again by releasing the identities and personal details of 600 Albanian intelligence officers, including their names, emails, and phone numbers. Six days afterward, HomeLand Justice released a video of an Albanian intelligence operation in collaboration with the State Police, which featured footage of then-police chief Nano.

As the Albanian prime minister's Sept. 7 statement made clear, the early autumn cyberattacks and leaks were not the first time that HomeLand Justice made itself known in the country. Previously, its affiliated hackers had stolen correspondence between ministries, embassies, and even Prime Minister Rama's emails with Albanian citizens. Each time, the group [made these public](#) on Telegram. And on July 15, the offensive cyber actor tweeted that it was [planning to carry out cyberattacks](#) against Albania's digital development and administration body, the National Agency for Information Society (AKSHI). After those summer-time incidents, Albania hired American cybersecurity and software companies Mandiant and Microsoft to investigate.

### Iran caught red-handed

[Mandiant's](#) and [Microsoft's](#) reports as well as a [separate investigation](#) by the United States' Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) all came to the same conclusion: Iranian state cyber "actors" — identified as HomeLand Justice — had taken down the websites and services of the government of Albania in July 2022. Mandiant experts believe that the individuals who carried out these attacks wanted to retaliate against the Albanian government for sheltering the Mujahedin e-Khalq (MEK), an Iranian opposition group currently residing in Manëz, Albania.

The FBI-CISA's report, in turn, reveals that Iranian proxies apparently gained initial entry into the Albanian state network approximately 14 months before launching its devastating cyberattack last summer. The hackers then maintained continuous access to the network.

[Experts](#) in the [cybersecurity field assess](#) the IRI's cyberwarfare capabilities as highly effective, even in comparison to [traditionally](#) more sophisticated powers like China, Russia, Israel, or the U.S. And like many





of these other powers, Iran's approach in this domain has been to rely on proxy actors to achieve strategic objectives. It has regularly responded to sanctions or perceived provocations through cyberattack campaigns. Indeed, both of these *modus operandi* were visible in the case of Albania, which is guilty in the Iranian authorities' eyes for the accommodations this Balkan country has been giving to the MEK.

### MEK and Albania

The MEK was founded in Iran in 1965 by radical Iranian students whose shared ideology combined Marxism and Islam. Between 1980 and 1981, the organization gained popular support and emerged as a political-militant opposition force to the new theocratic regime, at which point its adherents were forced to seek exile abroad, eventually ending up in Saddam Hussein's Iraq, amidst the Iran-Iraq war (1981-1988).

Under [intense lobbying](#) from the group and in return for renouncing violence, the United States [removed](#) the MEK from its list of terrorist organizations in 2012, where it had been since 1997. Following Saddam's toppling, the MEK needed to be pulled out of Iraq. The U.S. asked several countries to offer asylum to the group, including Romania. But worried about the possible security consequences involved, Bucharest demurred, [prompting Washington and the United Nations to turn to Tirana](#).

The Albanian government publicly [disclosed](#) parts of this deal in March 2013. In agreement with the American authorities, the [transfer](#) to Albania of more than 2,000 Iranian mujahedin began in 2016. Soon thereafter, the MEK built the "Ashraf 3" camp in the Manëz area, between Tirana and Durrës.

Undoubtedly, the MEK's arrival and regrouping in the small Balkan state could not pass without consequences. Giving shelter to the largest Iranian opposition faction, which presents itself as a future government-in-exile, organizes annual political summits, and allegedly carries out cyberattacks against the IRI, automatically pitted Tirana in a diplomatic dispute with Tehran. Over the years, this conflict metastasized, including into the theater of cyberwar.

### The consequences of Albania's hospitality

After Albania severed diplomatic relations with the IRI in early September, [Iran's foreign ministry stated](#) that the charges leveled against the Islamic Republic would "give full support to a terrorist sect," referring to the MEK, which "continues to play a role as one of America's tools in perpetrating terrorist acts, cyberattacks" against Iran.

This implicitly served as an admission of guilt by Tehran for the summer-time cyberattacks as well as confirmed the reason behind them. In fact, Iranian covert activities against Albania had been growing for years since the arrival of the MEK to the Balkan country. In 2018, [Albania expelled](#) Gholamhossein Mohammadnia, then the Iranian ambassador to Tirana, and Mostafa Roudaki, the station chief of the Iranian Ministry of Intelligence and Security (MOIS), describing them as "undesirable elements" involved in "illegal actions against [Albanian] national security." In 2020, other evictions took place. [Two diplomats of the Iranian embassy](#), Mohammad Ali Arz Peimanemati and Seyed Ahmad Hosseini Alast, were forced to leave Albania and declared *persona non grata*.

That same year, [Danial Kassrae](#), an Iranian with Italian citizenship, was deported from Albania, accused of espionage on behalf of MOIS to gather information on the MEK. In October 2020, Albanian authorities arrested Iranian citizen Bijan Pooladrag on five charges related to terrorism and tampering with computer data. Last week, Pooladrag was [sentenced to 15 years](#) in prison. He was declared guilty of the charge of financial actions with persons or organizations related to terrorism and of participating in a terrorist organization.

In 2021, [three Iranian journalists](#), Mohammad Alavi-Gonabadi, Firouz Baghernejad, and Mohammad Heydar Allauddin, were deported from Albania. All three supposedly worked for MOIS and sought to gather information on the MEK.

In July 2022, the Albanian Special Anti-Corruption Structure (*Struktura e Posaçme Anti-Korrupsion*, SPAK), an independent judicial entity tasked with investigating high-level corruption and organized crime, at the request of the Special Prosecutor's Office, [detained and interrogated 20 Iranians](#), all former MEK members, for espionage in the service of the Iranian regime.

Additionally, the annual MEK summit, scheduled to be held later that same month, on July 23-24, at Camp Ashraf 3 in Manëz, [was postponed](#) (finally held on Sept. 5) due to an apparent threat of a terrorist attack against the proceedings. The decision was motivated by the Albanian government's recommendation as well as a July 21 warning from the [U.S. embassy](#) that the IRI was allegedly planning to violently disrupt the event. A few days later, the Iranian news agency *Fars*, which is associated with the Islamic Revolutionary Guard Corps (IRGC), [asserted](#) that Iran could attack the MEK in Albania with drones and missiles.

Evidence of Iran's special operations targeting Albania continued to mount over the following weeks. In August, the Albanian police detained [Batool Soltani and her husband, Afshin Kalantari](#), the former holding dual Iranian-German citizenship, and held them for 72 hours before deporting them to Germany. Albanian police identified them as a national security risk and suspected them of trying to carry out terrorist attacks in the country.

Soltani and Kalantari had come at the invitation of the Association for the Support of Iranians Living in Albania (ASILA), a Tirana-based organization founded in November 2021 that claims to assist former MEK members who left the group as well as to promote cultural exchange between Iran and Albania. However,







Albanian authorities have long suspected ASILA of creating an agent network with the goal of obtaining detailed information about MEK members living in the camp in Manëz. At the same time, SPAK is actively investigating ASILA's ties to the Iranian government. Indeed, ASILA's own activities are conspicuously promoted online by the [Nexhat Association](#), an organization based in Tehran whose stated aim is “rescuing comrades who are still subjectively and even objectively enslaved by this Organization [the MEK] and to help their suffering families.”

### Conclusion

Going forward, Iran's attacks on Albania can be expected to continue but probably at a lower intensity. This is mainly because Iranian intelligence has lost much of its presence on the ground following the closure of the IRI embassy — a presence built up and cultivated over three decades and one that local proxy networks cannot replace. The main weapon left in Tehran's hands is, thus, hacking and sabotage of national computer networks.

Albania became an Iranian target in the first place because it agreed to host the Iranian opposition group MEK on its territory, because it is an enthusiastic member of the North Atlantic Treaty Organization (NATO) — which Supreme Leader Ali Khamenei notably [vilified](#) last summer, in the presence of Russian President Vladimir Putin — and because Tirana steadfastly stands as one of the key supporters of American interests in the Western Balkans, where the IRI seeks to pursue both [covert and overt interests](#).

Consequently, Albania needs more support in the cybersecurity realm from the U.S. and its allies not only financially but also in terms of improving its domestic knowledge and technology base. Undoubtedly, the Alliance has taken this year's cyberattacks against Albania seriously, as emphasized in a [Sept. 8 statement by the North Atlantic Council](#): “We will continue raising our guard against such malicious cyber activities in the future, and support each other to deter, defend against and counter the full spectrum of cyber threats, including by considering possible collective responses.”

So long as Albania remains in Tehran's sights, the country will continue to depend on allied support in the cyberwarfare space.

[Gerta Zaimi](#) research International Relations, the Middle East, and the Balkans at the Centro Interdipartimentale di Studi Strategici, Internazionali e Imprenditoriali (CSSII), Università di Firenze, in Italy.

## Terrorist Recruitment Now Happens Mainly Online – Which Makes Offenders Easier to Catch

By Jens Binder and Chris Baker-Beall

Source: <https://www.homelandsecuritynewswire.com/dr20221222-terrorist-recruitment-now-happens-mainly-online-which-makes-offenders-easier-to-catch>

Dec 22 – It is notoriously difficult to work out how and why someone becomes a terrorism risk. While attacks cause immense pain and suffering, the actual number of terrorist incidents in the Western world is small. That makes it difficult to arrive at reliable, quantified evidence. But in our [research](#), we've started to identify important patterns when it comes to different journeys into extremist offending. Most notably, we've found that in recent years, people who go on to be convicted of terrorist offenses are far more likely to have been radicalized online – without any offline interactions at all – than was the case in the past.

While the seeming ease with which this can happen is worrying, we've also found that people recruited purely online are less likely to commit violent attacks and less committed to their extremist causes than those recruited via in-person meetings. While face-to-face radicalization continues, the process is now found to take place primarily online.

Our work, which uses detailed risk assessment reports on people sentenced for terrorist offences in England and Wales, draws on 437 cases between October 2010 and December 2021. These reports, written by trained prison and probation professionals, focus on the pre-history of an offence and the current circumstances of the offender. As well as a detailed narrative, they also contain estimates of the levels of risk that the individual poses.

### The Shift Online

We wanted to look into how people became radicalized in the outside world before they committed an extremist offence. We found that, over time, it is less and less the case that people are radicalized offline, such as at local meeting places or via direct contact with peers and relatives.

Mixed radicalization, where extremist offenders are subject to both online and in-person influences, has also been declining. It is now much more common for people to be radicalized online. They might learn from online sources or engage with extreme views on social media. They might also use internet forums and chat groups that provide easy access to like-minded others.





Our findings show that despite [current perceptions about the growth of encrypted messaging services](#), online radicalization is not necessarily happening predominantly through one-to-one communication channels. The most commonly named platform is YouTube. While encrypted applications will always play their role, monitoring and regulating the more public online spaces is likely to make the most difference.

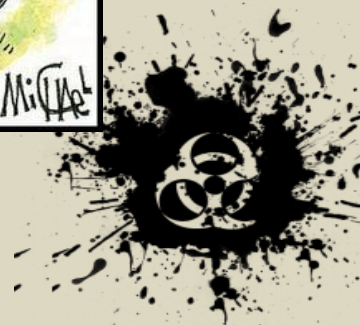
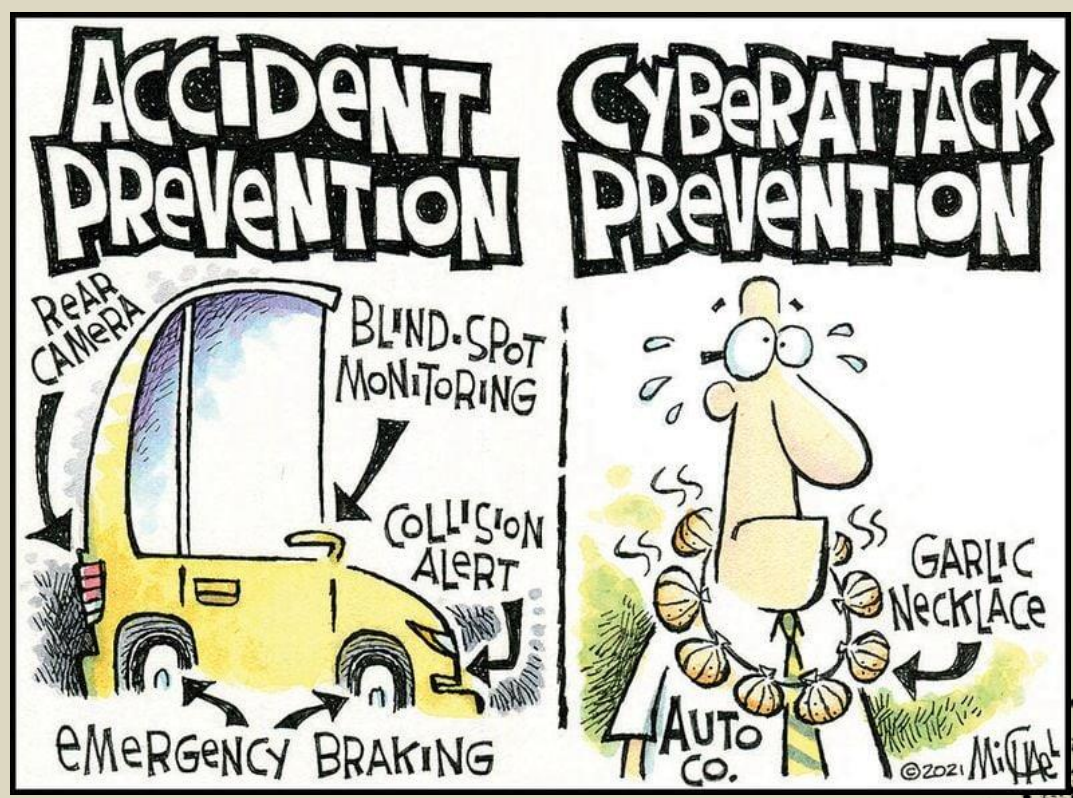
It was also interesting to note that those radicalized online consistently showed the lowest level of estimated risk. They were less engaged with extremist causes than those radicalized offline. They were also the most likely to have committed a non-violent offence, such as [inciting and encouraging others to commit terrorism](#) or possessing terrorist material, and to have committed their offences solely online. They were also far less intent on committing further offences after leaving prison than those who were radicalized offline – and they appeared to have the lowest capacity to commit further crimes because of having less access to the knowledge, networks or materials they might need. So it seems that while online radicalization is the most pervasive form at the moment, it is not overly effective at permanently immersing people in an extremist mindset. Nor is the online approach particularly successful for conveying the skills and knowledge necessary to commit graver offences.

### Disrupting Online Plots

In order to check for potentially more dangerous sub-groups, we also focused on those offenders classed as attackers. These were people who did not necessarily carry out full attacks but had, at the very least, cast themselves in such a role and had pursued attack plans. The online group showed the lowest frequency of attack-related activities, and attackers in this group were least successful in progressing plots for attacks. Only 29% of these plots moved from planning to the execution stage and only 18% were successfully carried out. All the plots we studied, which were not successful, had been disrupted by the police or other security services. The online world is, after all, not a perfect hiding place. Online activities often leave traces that can be detected by counter-terrorism practitioners. While this could all mean that online radicalization is comparatively harmless, there is a thin line between a relatively ineffective online-only radicalization and a much more effective mixed radicalization that includes both online and in-person influences. Online communication can slide into real-life interactions, and people radicalized via the latter technique were assessed as being highest in engagement and intent.

So while the switch to online radicalization appears to make people easier to catch and less likely to commit violent attacks, [this form of radicalization should still be taken seriously](#) and be recognized as a potential stepping stone towards more dangerous behavior.

Jens Binder is a Senior Lecturer in Psychology @ Nottingham Trent University.  
Chris Baker-Beall is a Senior Lecturer In Crisis and Disaster Management @ Bournemouth University.





ICI  
International  
**CBRNE**  
INSTITUTE



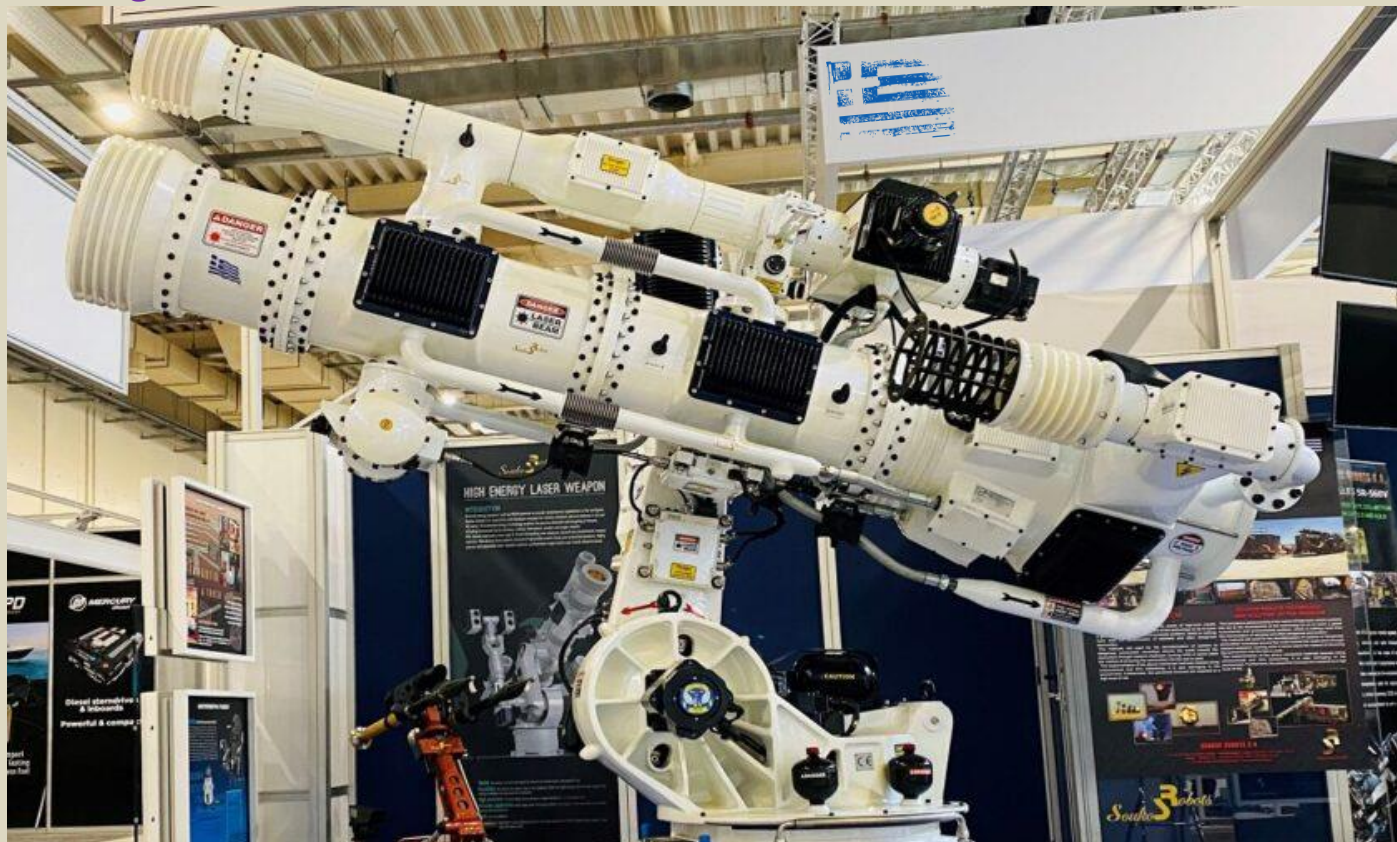
*& Robotic*

**DRONE NEWS**





## Cooking drones!



Soukos Robots S.A. (Greece) anti-drone robotic weapon with a high-energy laser head of 300 Kw (range >23Km | >75,000 feet) and hybrid electromagnetic pulse system.

## The Tiny and Nightmarishly Efficient Future of Drone Warfare

By Mark Bowden

Source: <https://www.theatlantic.com/technology/archive/2022/11/russia-ukraine-war-drones-future-of-warfare/672241/>

Nov 22 – On Saturday, October 29, a Russian fleet on the Black Sea near Sevastopol was [attacked](#) by 16 drones—nine in the air and seven in the water. Purportedly launched by Ukraine, no one knows how much damage was done, but [video shot](#) by the attacking drones showed that the vessels were unable to avoid being hit. In response to that and other successful attacks, Russia has retaliated with scores of missiles and Iranian-built Shahed-136 drones aimed at electrical and water systems throughout Ukraine.

Despite daily reports of lands taken or lands liberated in the nine-month war, the conflict has been largely fought in the air, with artillery shells, rockets, cruise missiles, and, increasingly, drones.

Small, cheap, relatively slow-moving, carrying far less of a wallop than a cruise missile or a 500-pound bomb, the Shaheds in particular have bedeviled Ukraine's otherwise excellent air defenses. Preprogrammed with a target and released in groups of five, the triangular, propeller-driven drones are relatively easy to destroy—if you can find them. They fly low and slow enough to be mistaken on radar for migrating birds. If launched in bunches, as the Russians have been doing, enough are able to evade even the best defenses to do substantial damage. In October, Ukraine estimated that it was shooting down 70 percent or more of the Shaheds, but the ones they missed were enough to debilitate the nation's electrical grid.

The attacks have continued. Intelligence officials say that Russia has sent 400 Iranian-made attack drones [since](#) August. Although that's a small number relative to the thousands of missiles bombarding the country, intercepting drones flying in bunches can be more difficult. Drones also cost less to manufacture and can be sent in ever-increasing numbers. By early November, Ukraine was already in danger of running out of air-defense missiles to combat them.

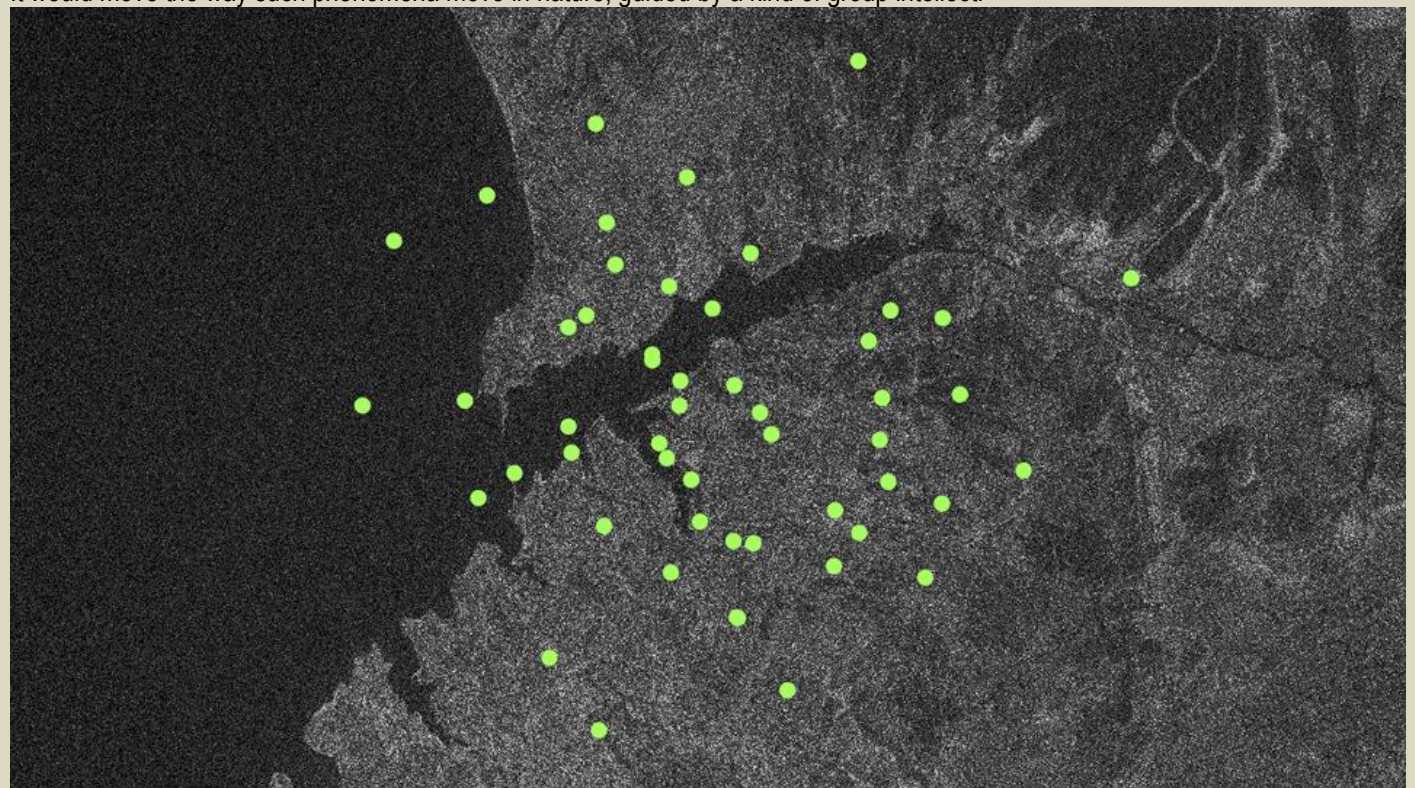
Speaking in mid-November, Ukrainian Vice Prime Minister Mykhailo Fedorov said, "In the last two weeks, we have been convinced once again the wars of the future will be about maximum drones and minimal humans."







What might that future actually look like? For years, military strategists have anticipated the arrival of the so-called drone swarm, a large cluster of small flying machines that will herald a new era of intelligent warfare. Thousands of robotic aircraft no bigger than a starling would be all but invisible when spread out, yet capable of instantly coalescing into a swirling dark cloud, like a murmuration. It would move the way such phenomena move in nature, guided by a kind of group intellect.



“A swarm is an intelligent organism and an intelligent mechanism,” Samuel Bendett, an expert in Russian weapons at the Center for Naval Analyses, told me. “In a swarm—just like in an insect swarm, in a bird swarm, in a school of fish—each drone thinks for itself, communicates with the others, and shares information about its position in a swarm, the environment that the swarm is in, potential threats coming at the swarm, and what to do about it, especially when it comes to changes in direction or changes in swarm composition.”

The weapons deployed in Ukraine by both sides are still far from the full nightmare potential. A swarm would use artificial intelligence to allow individual drones to behave autonomously while also harnessing the wisdom of the collective. David Hambling, in his 2015 book, *Swarm Troopers*, reported that software engineers had already been able to simulate those great swarms in nature by programming drones with three simple instructions: *separate*, or keep a certain minimum distance from others; *align*, or stay on the same course as your neighbors; and *cohere*, or attempt to move toward the average position of your neighbor. So instructed, drone swarms would move in clouds that function as a single entity, perhaps widely dispersed at first, hiding them from radar, only to converge on a target at the last minute. The swarm would be capable of reacting to threats without human intervention—changing course, speed, or altitude, maneuvering around heavily protected air spaces—and could absorb huge losses without stopping. Machines do not get discouraged and turn back.

“This is the holy grail,” Bendett said. “This is what everybody’s working towards. By everybody, I mean advanced countries and advanced militaries hoping to utilize swarm technologies. So the list is short, but it’s slowly growing. Of course, it’s the United States, it’s Israel, it’s China, it’s Russia, it’s Turkey, it’s Iran, and perhaps a handful of other states like India and South Korea.”

Such research programs are classified, but many military analysts see them arriving in the [near future](#). A swarm of 103 micro-drones designed by MIT with a wingspan less than a foot long was successfully launched by the U.S. in 2016, a project sponsored by the Department of Defense. The individual drones were so small and flew so fast that a CBS camera crew trying to film the experiment had a hard time capturing an image of the swarm even with high-speed cameras.

When you consider that a drone swarm consisting of many thousands of off-the-shelf drones would cost less than, say, one F-35 fighter or a ballistic missile, you have a weapon that would give rogue states or terrorist groups the means to launch devastating attacks or assassinations anywhere in the world. Since the Korean War, American forces have controlled the skies wherever they have gone into battle. No other nation had the means to compete with it; the cost, the technology, the experience, and the level of training





required are beyond the reach of even the most affluent nation-states. Drone swarms could end that domination. An aircraft carrier? A commercial airliner? The White House? The president? Sitting ducks.

Imagining a perfected drone swarm, the science-fiction author Kim Stanley Robinson writes in his novel *The Ministry for the Future*: They were more powerful than the atomic bomb, in this very particular sense: you could use them. And they couldn't be stopped ... They were small, they launched from mobile launchers, they came from all directions in a coordinated attack in which they only congregated at their target in the last few second of their flights.

By making nearly any target indefensible, Robinson imagines, such swarms—he calls them “pebble mobs”—would render war “impossible.” What he means is the kind of total war waged against entire civilizations. He envisions drone swarms bringing us to an era of warfare between competing robot armies, though today Russia is using its drone *groups* to attack civilian targets.

Once the technology is within reach, someone, somewhere will build it, and once built, it will follow the rule of Chekhov's gun—if it appears, it will be used. AI weapons have already been deployed—the Israeli Harpy drone, for instance, which loiters in the air over a contested space and is programmed to acquire and destroy targets. And although the destructive power of the atom bomb has so far prevented its use in all-out war, a drone swarm *will* be used once developed, because it is not a cataclysmic weapon. It is, as Robinson notes, a *useful* one. Although the explosive punch of small, cheap drones is insignificant compared with that of conventional bombs and missiles, they can be much more accurate. One would be enough to kill a person. Precisely targeted, even a small number could destroy crucial parts of a modern warship's defenses. The damage done to, say, an aircraft carrier by a drone swarm might not sink it, but could strip away its sensors and weapons, making it a fat target for larger munitions.

The emergence of drone swarms might also fully usher in AI battlefields, where the decision to shoot or explode needs to be made faster than humans can react. To insert a human into the decision chain would defeat the purpose. As Kai-Fu Lee [wrote in this magazine last year](#), “The prowess of autonomous weapons largely comes from the speed and precision gained by not having a human in the loop. This debilitating concession may be unacceptable to any country that wants to win the arms race.” And once a drone swarm is flying, knocking it off one unit at a time would demand the speed and accuracy of a laser guided by a supercomputer. Such full-on AI warfare has long been a theme in dystopian science fiction, perhaps most popularly depicted in the string of *Terminator* movies.

Of course, what all of these nightmares neglect is the notion of countermeasures, the second crucial element in the evolution of warfare. When a new weapon or tactic appears, so will a way to defeat it. Ukraine has been experimenting on the battlefield with a Lithuanian-designed defense called SkyWiper, which thwarts drones in flight by jamming their communications. Lithuania's defense ministry, according to *The New York Times*, has sent 50 to Ukraine after the embattled nation named them as “one of the top priorities.”

But the most useful tool for Ukraine's defenders is far less high-tech: machine guns. The Shahed's propeller makes enough noise to alert ground troops as it passes overhead, and is vulnerable to coordinated fire. The drones have also been destroyed by fighter planes and air-to-air missiles, but that's like driving a nail with a Cartier watch. The average Shahed costs about \$20,000, whereas even the lowest-cost surface-to-air missile (still under development) will run closer to \$150,000, a sum that does not include the multimillion-dollar system required to operate it. When cheap, off-the-shelf drones fly in large numbers, such cost disparity becomes ridiculous and unsustainable.

Last year Congress directed the Pentagon to develop a counterforce for small unmanned aircraft systems (UAS), and budgeted almost \$750 million for them. The newly created office's director, Army Major General Sean Gainey, [has said](#) that the reliance on drones in Ukraine added urgency to his mission: “I think it's bringing more to light of what we already know—that when you scale this capability from a small quadcopter all the way up ... it really shows the importance of having counter-UAS at scale.”

For its part, the U.S. Army is experimenting with using large airbursts or electromagnetic pulses to guard against the eventual emergence of the drone swarm. The U.S. Navy's High Energy Laser weapons system, and those under development by major defense contractors—Raytheon, Lockheed Martin, and others—use AI to very rapidly target and destroy incoming drones one by one, potentially enough to disable a swarm. Such a weapon would be more useful at sea or over an open battlefield than over cities, where most combat in the modern era takes place. Air traffic over large cities is busy, so pinpointing a relatively small and dangerous intruder without knocking down friendly aircraft is hard. To help this effort, the Army's Joint Counter Small Unmanned Aerial System Office is looking at ways to adapt existing air-traffic-control networks to spot anomalous flight patterns.

One of these countermeasures, or one as yet unforeseen, will work, and drone swarms are not likely to wipe out America's arsenal. They will, however, fundamentally alter the way we fight. The machine gun did not end war, but it did permanently change it. Five newly invented Maxim machine guns were enough to slaughter more than 1,000 charging Matabele warriors when the British South Africa Company invaded tribal lands in present-day Zimbabwe in 1893.

By World War I, machine guns had driven infantry underground. Armies fought from deep trench networks that spanned the entire European continent. Eventually tanks, armored vehicles, attack aircraft, and big changes in infantry tactics evolved to counter the weapon, but the machine gun is still the mainstay of ground combat. The standard-issue infantry weapon worldwide is a machine gun.







Just as militaries adapted to heavy machinery and the trench, they will find a solution here. One of the most intriguing drone-swarm countermeasures is being tested by D-Fend, an Israeli contractor. It has been able to hack the guidance software of a small-drone swarm and redirect it harmlessly off course. Software is just code, and code is hackable. But even in this, science fiction has gotten there first.

There is a particularly chilling 2016 episode of the British TV series *Black Mirror* called “Hated in the Nation.” Set slightly in the future, the episode features tiny drones that have been loosed by the millions for a purely beneficial reason—to do the essential work of vanishing bees, spreading pollen from flower to flower. But the bees’ software is hacked. Its new controllers link them to a website where people name the most reviled person in the country. At the end of each day, the reprogrammed drones/bees form a lethal swarm to converge on and kill the person at the top of the list.

This illustrates the principle that whatever technology emerges, its use, for better or worse, will be determined by human beings.

**Mark Bowden** is a contributing writer at *The Atlantic* and the author of [Black Hawk Down](#), [Hué 1968](#), and [The Finish: The Killing of Osama Bin Laden](#).

### Drone Destroyer: 2nd LAAD tests LMADIS

Source: <https://www.marines.mil/News/News-Display/Article/3225868/drone-destroyer-2nd-laad-tests-lmadis/>



Nov 22 – U.S. Marines with 2nd Low Altitude Air Defense Battalion tested the Marine Corps’ newest ground-based air-defense system, the Light Marine Air-Defense Integrated System, Oct. 18-19, 2022.

The LMADIS provides 2nd LAAD and the Marine Corps with the capability to deter and neutralize unmanned aircraft systems. The rising use of commercial off-the-shelf drones for offensive warfare means the Marine Corps must make adjustments to their ground-based air-defense capabilities. The LMADIS helps mitigate threats by disrupting the electronic signals between the UAS and its controller.

“With the constant evolving of commercial drones, the one thing that won’t change is the required frequencies used to pilot any drone,” said U.S. Marine Corps Staff Sgt. Dustin Yonkings, a LAAD gunner with 2nd LAAD.

The LMADIS uses electronic weapons on a light and compact frame, the Polaris MRZR, which allows the LMADIS to deploy to austere environments via air transport.







“The difference is the expeditious aspect of it being able to be loaded on aircraft used for a wide set of missions ... [such as] CH-53E Super Stallions, CH-53K King Stallions, and MV-22B Ospreys,” said Yonkings.



The LMADIS uses two Polaris MRZRs, one acting as the brain and the other as the brawn. Together, they house the CM262U optic, which acts as the ‘eyes’ of the system; the RPS-42 radar and Skyview MP,







which provide 360-degree air surveillance and long-range drone detection; the Modi II, which is a dismountable electronic-warfare system used to disrupt enemy drones and communications; and the AN/PRC-158 multichannel manpack radio system, which allows the LMADIS to communicate everything it detects to troops in its immediate vicinity and commanders in the rear echelon. “Due to the current drone threat, we need an expeditionary system that will combat it. The LMADIS serves as a system that can be deployed at a moment's notice and attach to units that need counter-UAS capabilities,” said Yonkings. In accordance with the Marine Corps’ Force Design 2030 modernization efforts, the Marine Corps has activated a third firing battery for each of the LAAD battalions to better support the Fleet Marine Force. 2nd LAAD, a subordinate unit of 2nd Marine Aircraft Wing, was the first battalion in the Marine Corps to activate their third firing battery.

### No Longer Fictional – Robot Swarms

Source: <https://i-hls.com/archives/114329>



Nov 24 – Robot swarms provide robots with capabilities that are not possible in individual robot activity, such as splitting work among themselves, responding to different risks, and establishing complex structures as the environment changes. A micro-robot or machine at the micro or nano scale may be perceived as only being suited for a limited set of tasks, but their swarming capabilities could permit them to perform a variety of complex tasks and be integrated in a variety of solutions. Researchers used five million molecular machines, which are made up of two biological components: microtubules, which can swarm, and kinesins, which can transport microtubules. Swarming was controlled by combining DNA with a light-sensitive compound called azobenzene, which functions as a sensor. They also added cargo consisting of polystyrene beads ranging in diameter from micrometers to tens of micrometers, enabling control of swarming also at the loading stage. Swarms of molecular robots, according to sciencedaily.com, have demonstrated the ability to cope with thirty micrometers of polystyrene beads, and even achieved five times the efficiency of individual robots. It showed that molecular machines can operate in a swarm-like strategy and perform high-efficiency missions together, and its impact on microrobotics will likely be significant. There is a possibility that microrobot swarm technology will soon be applied in a variety of industries and fields, including medicine and military, when molecular robot cooperation could lead, among other things, to the effective manufacture of drugs and the **development of defense technologies against chemical and biological warfare.**

### Unmanned Vessels – Influencing Wars By 2030

Source: <https://i-hls.com/archives/113265>

Nov 24 – The US Navy Chief of Operations is interested in deploying unmanned or minimally manned vessels with strike groups as soon as the next five years, with a goal for systemic unmanned technology activities across the world by 2030. The website DefenseNews.com reports that Admiral Mike Gilday spoke to reporters in early February about the desire for the US Navy to experiment with unmanned technology, fail when needed, and learn from mistakes.





# IMX/CE 22

INTERNATIONAL MARITIME EXERCISE / CUTLASS EXPRESS

## 80+ UNMANNED SYSTEMS

U.S. ASSETS INCLUDE:

## LARGEST

UNMANNED EXERCISE IN THE WORLD

10 NATIONS BRINGING SYSTEMS:  
BELGIUM \* CANADA \* FRANCE \* ISRAEL  
\* JAPAN \* NETHERLANDS \* SEYCHELLES  
\* UNITED ARAB EMIRATES \* UNITED KINGDOM \* UNITED STATES



**Devil Ray T-38**

An unmanned surface vessel designed for sailing at speeds greater than 80 knots and executing high-speed turns of up to 6 Gs. The T-38 can be used as an intelligence, surveillance and reconnaissance platform or for staging and deploying other unmanned vehicles or weapons.



**Wave Glider**

A wave-powered marine robot that can deliver data from above and below the water.



**Triton**

A hybrid surface and undersea system capable of operating up to three months surfaced or eight days submerged. The system and payload batteries are recharged by solar panels that are outfitted on the sail. The platform is capable of autonomous insertion, recovering, recharging, and redeploying REMUS unmanned undersea vehicles.



**Saildrone Explorer**

A high-endurance, solar and hydro powered intelligence, surveillance and reconnaissance (ISR) unmanned surface vessel propelled by wind and capable of remaining on station for up to 12 months. Its sensor packages include meteorological instruments, bottom scanning sonar, AIS detection and a 360-ISR camera.



**Switchblade 300**

A one-way, mortar-fired unmanned aerial vehicle can be equipped with an intelligence, surveillance and reconnaissance (ISR) camera for real-time full motion video or equipped with an explosive payload for kinetic fires.



**GHOST 4**

A vertical takeoff and landing unmanned aerial vehicle designed for intelligence, surveillance and reconnaissance (ISR) missions. GHOST 4 is equipped with an ISR camera that provides up to 85 minutes of controlled real-time video.



**Mantas T-12**

A multi-role unmanned surface vessel capable of deploying from land, a crewed ship or larger unmanned vessel. Its modular design allows for rapidly tailoring sensor packages to meet specific operational requirements.



**Remus 300**

A two-person portable unmanned undersea vehicle designed for mine countermeasures, search and recovery, rapid environmental assessment, hydrographic survey, renewables, marine archaeology, offshore oil and gas, anti-submarine warfare and intelligence, surveillance and reconnaissance.



[Enlarge page to better read about the systems](#)

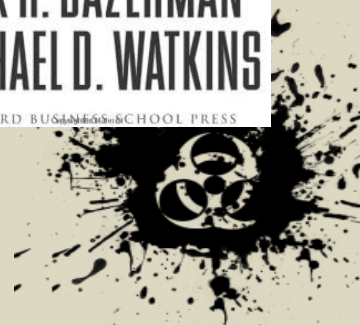
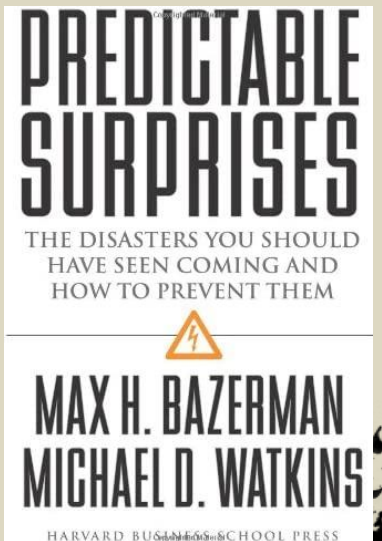
These unique technologies, according to Gilday, enable the formation of new insights into unique courses of action, the acceleration of some operations owing to high performance, and the halting of different actions due to a lack of performance. He also mentioned that some of these technologies had previously been tried during the Middle East Maritime Exercise 22, which was one of the largest exercises using artificial intelligence and unmanned systems, that took place at the beginning of this year.

### PERSPECTIVE: What Will It Take to Adequately Counter the UAS Threat?

By Charles Werner

Source: <https://www.hstoday.us/featured/perspective-what-will-it-take-to-adequately-counter-the-uas-threat/>

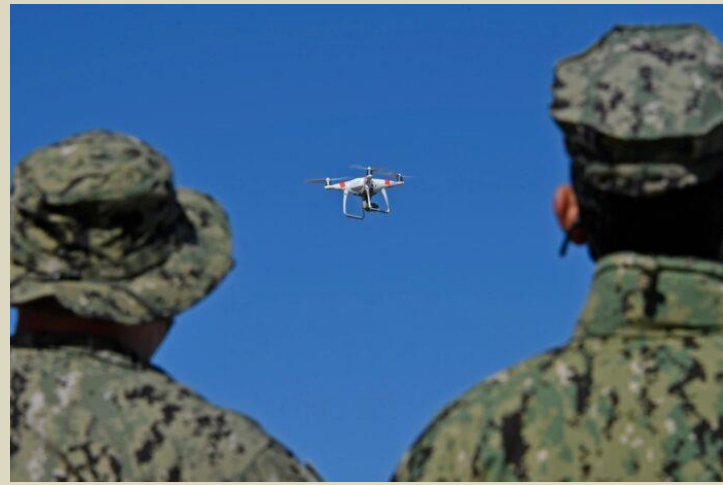
Nov 26 – In the book “Predictable Surprises: The Disasters You Should Have Seen Coming and How to Prevent Them,” the main premise is that many of the disasters that we have faced should not have come as surprises. The situation that is looming is very much the same with uncrewed aircraft systems (UAS), commonly known as drones in the United States. Drones have already begun to raise concern in this country in a number of ways. Drones have been







used by cartels to transport drugs, do reconnaissance on Border Patrol agents and deliver explosives to rival cartels. In numerous prisons worldwide, drones have been used to drop contraband of drugs, weapons and cigarettes directly into prison



courtyards, often leading to prison unrest to the point of becoming riotous. In isolated cases, drones have been used to aid in a prisoner escape.

Naval Air Warfare Center Weapons Division (NAWCWD) Pacific Target Marine Operations (PTMO) and Threat/Target Systems Department (TTSD) deployed small-drones over Naval Base Ventura County (NBVC), Point Mugu, on Oct. 20, 2021, to provide cost-effective unmanned aerial system (UAS) familiarization and threat training. (U.S. Navy photo by Ensign Drew Verbis)

real. More recently, drone incursions have impacted and in some cases interrupted NCAA, NFL, MLB, NASCAR and other large mass gathering events. The significant problem is that with large public assembly events much chaos can be achieved with something as simple as a baby powder drop that is perceived as something more hazardous. Regardless of harmful content or not, it creates a public safety decontamination nightmare. At the next level, the potential for a chemical, biological, radiological, nuclear or explosive (CBRNE) attack has the potential for mass casualty, potential stampede and mass hysteria that will ripple throughout the country. In the U.S., drones have been found or flown near critical infrastructure, the power grid, bulk oil plants and nuclear power plants. So far, most of these incursions have involved three of the four Cs (careless, clueless, curious) but have not been criminal (the fourth C) in nature. On the criminal front, drones are being used more frequently by criminal elements to interfere with law enforcement drones and, as previously mentioned, in prisons.

Since 2017, the NFL has experienced numerous drone incursions, fortunately with dropped pamphlets. While not dangerous in these cases, the demonstrated exposure is very

Drone incursions have also created numerous disruptions to major airports in the U.S. and abroad. Fortunately, none have had serious consequences to date.

Our military forces operating abroad have shared intel on how commercial drones (that can and are being purchased in the U.S.) are now being used in warfare operations overseas. The war in Ukraine has demonstrated the power of commercial drones and these drones are believed to significantly help change the balance of power.

Are you getting the picture? PREDICTABLE SURPRISES.

There are two aspects of counter UAS: detection and mitigation. Presently there are 21 or more laws, rules or regulations that prevent a clear path to both, which means that it is impossible to do either with the exception of those designated federal agencies.

The potential of danger is expanded by a significant number of commercial and recreational remote pilots who do not adhere to FAA rules and regulations. This is validated by a Small Unmanned Aircraft System (sUAS) Traffic Analysis (A11L.UAS.91): Initial Annual Report completed for the FAA'S ASSURE Research Program. While this sampling report gives some idea of potential dangerous UAS flights that exceed flight regulation limitations, rules, regulations and laws from the FCC and FAA create confusion as to the legality of conducting detection. Congress has said that before CUAS can move forward there needs to be clear justification of the problem. Yet Congress refuses to enact even basic legislation that will clear the way to conduct basic monitoring/detection of UAS flights legally. Regardless of mitigation or taking down a drone, the ability to monitor and detect is essential to understand the new complexities of the present national airspace and to address the issues and hazards identified. Ignoring this is simply like sticking heads in the sand.

On April 25, the White House released [The Domestic Counter-Unmanned Aircraft Systems National Action Plan](#) to move CUAS forward. Following this release, bipartisan legislation – the [Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act](#) – was introduced by Senate Homeland Security and Governmental Affairs Committee Chairman Gary Peters (D-Mich.) and former chairman Sen. Ron Johnson (R-Wis.) in July to move the proposed National Action Plan forward. “The threats posed by malicious unmanned aircraft are too great to ignore,” Johnson said in a statement. “This bill will increase our ability to fight the growing threat of criminal drone activity across the country. It is paramount that our national security agencies have the tools they need to mitigate the serious threats posed by UAS. I hope my colleagues move quickly to support this bill that will further our national security.”

Some suggest that the new FAA Remote ID rule will help to resolve this issue. However, the Remote ID rule requires registration of drones. It will help to identify the clueless, careless and curious but it is not likely that bad actors with nefarious intentions will register their drone.





To date it appears that the legislation has stalled, even on the basic ability to monitor and detect. One of the congressional committees stated that more studies are needed before moving forward.

Back to the premise of “Predictable Surprises: The Disasters You Should Have Seen and How to Prevent Them”: this requires action or we are destined to experience the disasters that could have been prevented. So when (not if) a devastating attack initiated with a drone occurs, remember it was a predictable surprise and a disaster that we knew how to prevent.

**Charles Werner** is the retired Charlottesville fire chief and 46 year public safety veteran. After retirement, Charles worked with the Virginia Department of Emergency Management for 2 years as senior advisor/acting deputy state coordinator. Charles served in numerous leadership roles at the local, state, national levels on public safety initiatives. Presently serves as Director-DRONERESPONDERS Public Safety Alliance, Chair-National Council on Public Safety UAS, BOD - Airborne International Response Team, and appointed by Virginia Governor Northam to serve on the Secure & Resilient Commonwealth Panel and serve as Public Safety UAS Sub Panel Chair. Charles also serves on the International Association of Fire Chiefs Technology Council. In 2004, he served two years as a reserve deputy sheriff with Albemarle County. Chief Werner is a FAA certificated Remote Pilot. Chief Werner also serves on the Virginia Center for Innovative Technologies Advisory Board. Charles is a contributing editor to Firehouse Magazine, Crisis Response Journal and an author with 150+ internationally published articles and serves as a contributor to numerous other public safety publications. Chief Werner has numerous commendations, three Virginia Governor’s Awards of Excellence, recognized as the National Career Fire Chief Award in 2008 and Homeland Security Today’s Person of the Year in 2018.

### **Greece: New anti-drone laser robotic platform**



Poseidon by Soukos Robots S.A. (GR)







# World Robot Olympiad – International Final

17-19.11.2022 Dortmund / Germany



Greece in particular emerged as the first power in robotics pan-European and fourth worldwide for 2022 among 73 countries. Several Greek teams were in the top eight.

The Robocores, namely Aliko Ragou, Konstantinos Mazarakis, Yiannis Ragos and their coach, Spyros Tsoukalas, raised the Greek flag to the podium, winning the only medal for our country in the event.

The Robocores team presented at the competition **Pop2See**, a device system that facilitates the inclusion of blind students in mainstream schools and universities. It enhances the interaction between the teacher and the blind student and offers autonomy and independence.

## MIT researchers creating robots that give birth to other robots



Source: <https://nypost.com/2022/11/29/mit-researchers-creating-robots-that-give-birth-to-other-robots/>

Nov 29 – Massachusetts Institute of Technology (MIT) researchers are building swarms of tiny robots that have built-in intelligence, allowing them to build structures, vehicles, or even larger versions of themselves.

The subunit of the robot, which is being developed at MIT’s Center for Bits and Atoms, is called a voxel and is capable of carrying power and data.

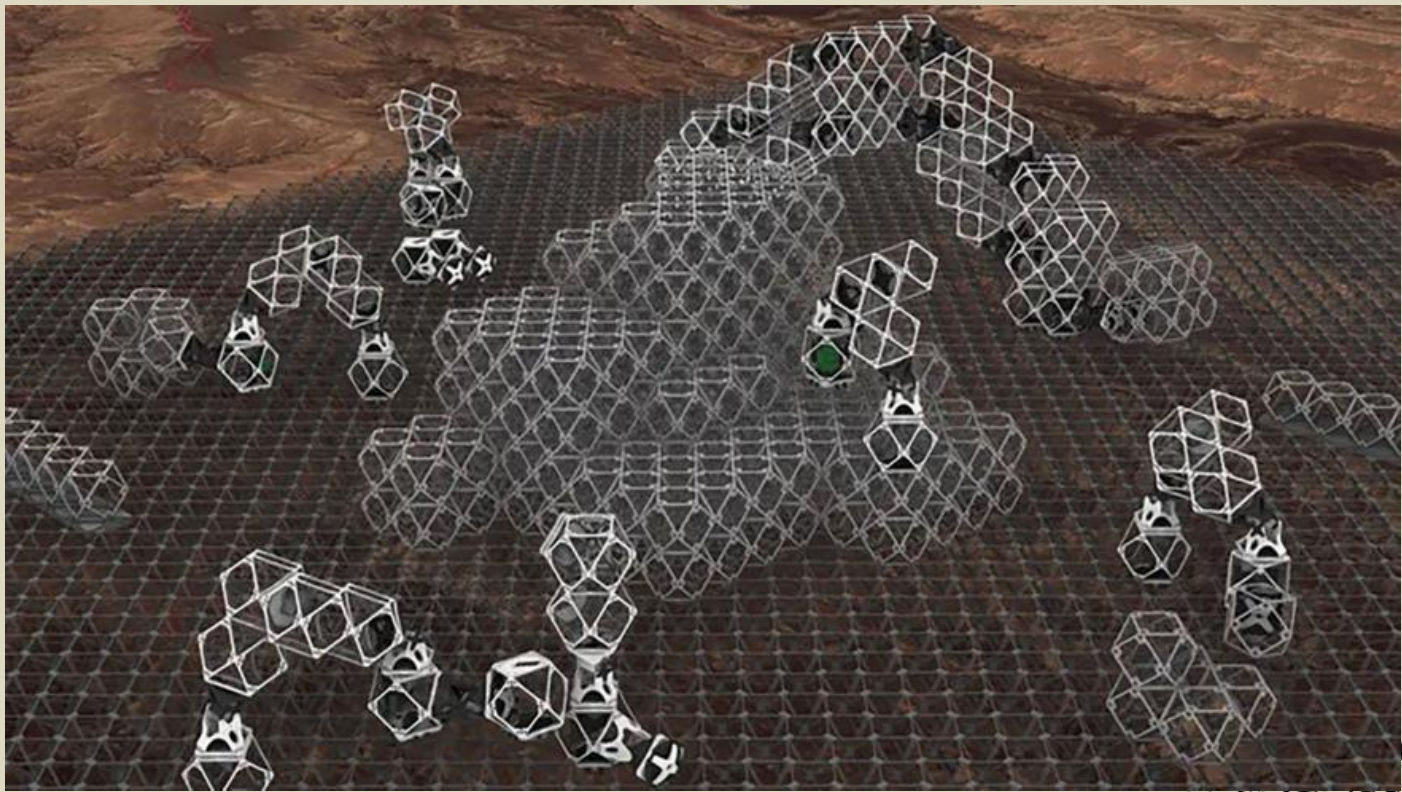
“When we’re building these structures, you have to build in intelligence,” MIT Professor and CBA Director Neil Gershenfeld said in a statement. “What emerged was the idea of structural electronics — of making voxels that transmit power and data as well as force.”

The voxels makeup both the robot itself as well as the components of the thing being built, allowing them to work together on larger structures.

“It could build a structure, or it could build another robot of the same size, or it could [build a bigger robot](#),” CBA doctoral student Amira Abdel-Rahman said in a statement.







The subunit of the robot is called a “voxel” and it carries data and power







While the research is promising, it will likely be years before we see [self-replicating robot swarms](#), according to Gershenfeld. The researchers, who published a paper laying out their findings in Nature, are working with the aviation industry, car companies, and NASA on the new technology.

●▶ [Video](#)

## San Francisco Cops Propose Using Killer Robots to Fight Crime

By Tony Ho Tran (Deputy Editor, Innovation & Tech)

Source: <https://www.thedailybeast.com/san-francisco-cops-propose-using-killer-robots-to-fight-crime>



**San Francisco City Council finally stepped back (7/12)**

Nov 29 – Want a bleak example of our cyberpunk dystopia? Well, look no further than San Francisco, where the city is set to consider allowing cops to use [robots](#) to kill people.

On Tuesday, the San Francisco Board of Supervisors plans to vote on a proposal for the San Francisco Police Department (SFPD) to be able to kill suspects with robots—applying the [same policy that allows human cops to use deadly force](#) against a person. If approved, the SFPD will be able to choose from seven different robots to potentially do the bloody deed.

"Robots will only be used as a deadly force option when risk of loss of life to members of the public or officers is imminent and outweighs any other force option available to SFPD," [the proposal reads](#).

The original draft of the SFPD proposal didn't mention use of force being used by robots, [NPR reports](#). However, San Francisco Board of Supervisors member Aaron Peskin added a line that said, "Robots shall not be used as a Use of Force against any person," the SFPD crossed the sentence out and returned the draft. They also altered the proposal so it reflected the use of force standards applied to officers.

If passed, the SFPD will be able to apply deadly force against suspects using seven different robots, two of which can be weaponized without too much issues: the Remotec F5A, a bomb disposal robot that can be loaded with shotgun shells for the purpose of destroying explosives; and the QinetiQ TALON, a military robot that can be equipped with a machine gun.

However, the SFPD told The Daily Beast in a statement that they don't "own or operate robots outfitted with lethal force options" and it wouldn't be outfitting their robots with guns in order to neutralize suspects—they're going to give them bombs instead.

"As an intermediate force option, robots could potentially be equipped with explosive charges to breach fortified structures containing violent, armed, or dangerous subjects or used to contact, incapacitate, or disorient violent, armed, or dangerous suspect who pose a risk of loss of life to law enforcement or other first responders by use of any other method, approach, or contact," SFPD said in the statement. They added, "While an explosive charge may be considered an intermediate force option, it could potentially





cause injury or be lethal. Robots equipped in this manner would only be used in extreme circumstances to save or prevent further loss of innocent lives.”

If employed, it wouldn't be the first time a city police department utilized robots to neutralize suspects. In 2016, Dallas cops used a [robot armed with C4 to kill a man](#) suspected of using a sniper rifle to target police officers during a Black Lives Matter demonstration. It was the first recorded instance of a robot being used by cops to kill a person.

The proposed killbot policy predictably has experts and activists concerned about the implications of using deadly force against humans with such devices. “We have a very clear position that we do not think in a domestic policing context robots should ever be armed,” Matthew Guariglia, a policy analyst for the Electronic Frontier Foundation, [told Vice](#). “We really fear you'd be seeing these armed robots coming out to every protest on standby and that's just a very dangerous situation.”

Ryan Calo, a law and information science professor at the University of Washington, told NPR that there wouldn't be any reason for a robot to use deadly force because “you send robots into a situation and there isn't any reason to use lethal force because no one is actually endangered.”

The policy proposal comes a few months after a group of robot makers including Boston Dynamics signed [an open letter](#) pledging never to weaponize their machines. “Weaponized applications of these newly-capable robots will also harm public trust in the technology in ways that damage the tremendous benefits they will bring to society,” the letter read.

But with police department and military budgets blowing up like a [T-800 driving an oil tanker](#), that leaves a lot of money on the table for less ethically rigorous robot companies to snatch up. For now, the SF Board of Supervisors is set to vote on the policy at 2pm local time. Hopefully, they'll leave the Robocops to Hollywood.

## European Commission launches Drone Strategy 2.0 – a EUR 14.5 billion market in 2030

Source: <https://www.unmannedairspace.info/news-first/european-commission-launches-drone-strategy-2-0-a-eur-14-5-billion-market-in-2030/>

Nov 29 – The European Commission has today adopted the [European Drone Strategy 2.0](#), which sets out a vision for the further development of the European drone market. It builds on the EU's safety framework for operating and setting the technical requirements of drones, which is the world's most advanced. The new Strategy lays out how Europe can pursue large-scale commercial drone operations while offering new opportunities in the sector, according to a Commission press release.

“With the arrival of a new generation of electrically powered aircraft capable of operating in an urban and regional environment, we need to ensure that, beyond maintaining the safety of operations in our skies, conditions meet both the operators' commercial needs and citizens' expectations with regard to privacy and security,” said Adina Vălean, Commissioner for Transport. “Today's Strategy not only widens Europe's capacity to pursue large-scale commercial drone operations but also offers new opportunities, in particular to small and medium-sized enterprises. With the right framework in place, the drone services market in Europe could be worth EUR14.5 billion, and create 145,000 jobs, by 2030.”

According to the Commission, it wants to **ensure that society supports drones**. To address concerns over noise, safety and privacy, the Strategy therefore calls for national, regional and local municipalities to ensure that drone services are aligned with citizens' needs.

The Commission's statement continues: “The Strategy envisions the following drone services becoming part of European life by 2030: **Emergency services, mapping, imaging, inspection and surveillance within the applicable legal frameworks by civil drones**, as well as the **urgent delivery of small consignments**, such as biological samples or medicines.

Innovative Air Mobility services, such as **air taxis**, providing regular transport services for passengers, initially with a pilot on board, but with the ultimate aim of fully automating operations.

“Unleashing the potential of the EU drone market and services requires the identification of critical **technology building blocks**, such as artificial intelligence, robotics, semi-conductors and EU space services and mobile telecommunications. This will help the EU build an innovative and competitive drone sector, reducing strategic dependencies. The Strategy also identifies areas for synergies between civil and defence drones, and for increased counter-drone capabilities and system resilience.

“The Commission will now launch work on the Strategy's 19 operational, technical and financial flagship actions to build the right regulatory and commercial environment for tomorrow's drone air space and market:

Adopting **common rules for airworthiness**, and new **training requirements** for remote and eVTOL (manned electric Vertical Take Off and Landing) aircraft pilots.

Funding the creation of an **online platform** to support local stakeholders and industry implementing sustainable Innovative Air Mobility.

Developing a **Strategic Drone Technology Roadmap** to identify priority areas for research and innovation, to reduce existing strategic dependencies and avoid new ones arising.







Defining criteria for a voluntary **cybersecurity-approved drone** label.

“This work will prepare the way for large-scale commercial operations and ensure that Europe benefits from synergies between the civil, security and military use of drones and related technologies, including counter-drone solutions.

“The [Commission's Sustainable and Smart Mobility Strategy](#) announced the preparation of an updated European Drone Strategy by the end of 2022. A [Staff Working Document](#) assessing the challenges faced by the drone industry, as well as the analysis and data underpinning the new Drone Strategy 2.0, accompanies this Communication. The Commission has been building the foundations of a comprehensive EU policy on drones since 2014. [Commission Implementing Regulation 2019/947](#) and [Commission Delegated Regulation 2019/945](#) contain detailed rules and procedures for the operation of unmanned aircraft, and set the requirements for the design and manufacture of unmanned aircraft systems. Since 2003, the EU has invested almost EUR980 million in the development or use of drones for innovative applications. It has funded 320 projects relating drones under its research and innovation programmes.

●► For more information: [https://ec.europa.eu/commission/presscorner/detail/en/ip\\_22\\_7076](https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7076)

## Boston Dynamics and other firms pen open letter against weaponized robots

Source: <https://newatlas.com/robotics/boston-dynamics-open-letter-weaponized-robots/>



October 2022 – As robots from Boston Dynamics and the like continue to find more widespread applications, concerns are growing around their misuse. In a bid to prevent the spread of killer robots in society, a group of robotics companies have published an open letter pledging not to weaponize their machines, and pleading with users to do the same.

The idea that autonomous machines can be weaponized and deployed to cause harm is not new, but as our access to highly capable robots continues to improve we have seen these concerns raised in a more mainstream sphere. We've seen leaders in AI and robotics [petition the UN](#) to ban the development of these types of machines, and these movements continue to gain momentum as more companies and organizations [lend their name to the cause](#).





In October last year, Ghost Robotics showed off a [robotic dog with a sniper rifle](#) mounted on its back. Another [video](#) doing the rounds on social media earlier this year showed a quadruped robot carrying an assault rifle and firing at targets on the range. Questions remain over the veracity of that second example, but the point remains: vision of robotic dogs combined with deadly weapons is an unnerving glimpse into the future.

Boston Dynamics, together with Agility Robotics, ANYbotics, Boston Dynamics, Clearpath Robotics, Open Robotics and Unitree Robotics, have today voiced their concerns around these possibilities. In an [open letter](#) addressed to the industry, the group notes the increasing affordability and accessibility of advanced commercially available robots, and the increasing potential for their misuse. “Untrustworthy people could use them to invade civil rights or to threaten, harm, or intimidate others,” the letter reads. “One area of particular concern is weaponization. We believe that adding weapons to robots that are remotely or autonomously operated, widely available to the public, and capable of navigating to previously inaccessible locations where people live and work, raises new risks of harm and serious ethical issues.”

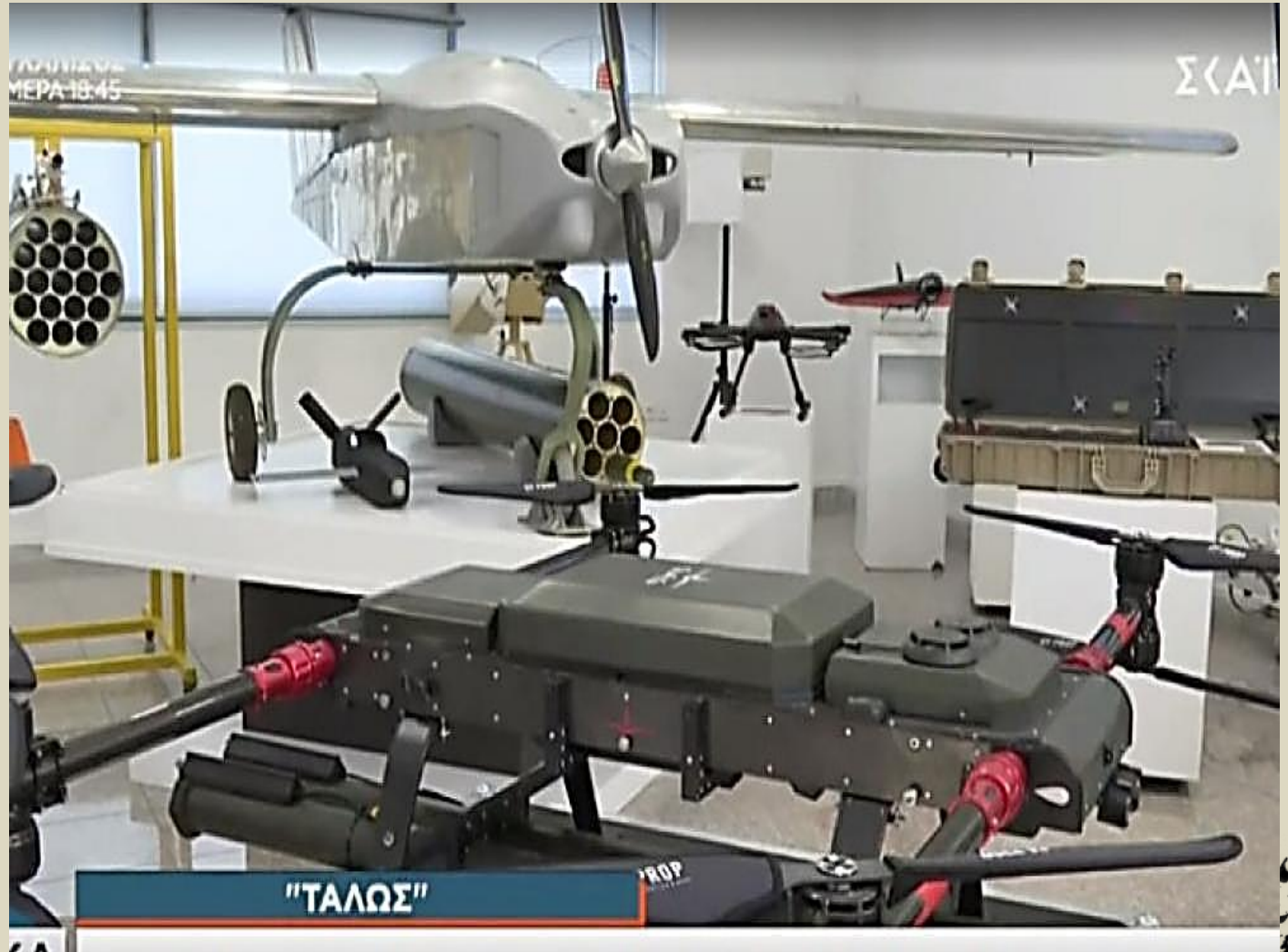
The letter goes on to include a pledge from the group to not weaponize their robots, nor support others to do so, and calls on policy-makers and users to promote their safe use. It also includes a plan to diligently assess their customers' intentions for their products and work on technological solutions to reduce the risks of robotic weaponization.

“We are convinced that the benefits for humanity of these technologies strongly outweigh the risk of misuse, and we are excited about a bright future in which humans and robots work side by side to tackle some of the world’s challenges,” the letter concludes.

**EDITOR’S COMMENT:** I think there is something fishy here. Who is the major client of robotic companies?

### Another Aegean guardian

Name: **Talos** (by SAS Technology) – armed with 2.75 laser rockets (by Thales; same with Apache helicopters)







## Legged Robots in Public Safety: How Spot Leads the Way

Source: <https://www.bostondynamics.com/solutions/public-safety>



Deploy Spot with specialized sensors to detect radiological and nuclear material, toxic gases, and other hazardous materials. Spot helps field operators identify and assess Chemical, Biological, Radiological, Nuclear, and Explosives (CBRNE) threats from a safe stand-off distance, traversing unpredictable terrain and collecting data about the risk.

## VIDEX 2022: Vietnam operationalises locally developed unmanned vehicles for CBRN defence missions

Source: <https://www.janes.com/defence-news/news-detail/videx-2022-vietnam-operationalises-locally-developed-unmanned-vehicles-for-cbrn-defence-missions>

Dec 09 – The People's Army of Vietnam has operationalised an indigenously developed unmanned ground vehicle (UGV) and locally made multirotor unmanned aerial vehicles (UAVs) across two of its chemical, biological, radiological and nuclear (CBRN) defence units.

This was confirmed by a representative from the service, who spoke to *Janes* at the Vietnam International Defense Exhibition (VIDEX) 2022, which is taking place in Hanoi from 8 to 10 December.

The UGV is known as the 'Viet Nam Robot CBRN' while the UAV has been dubbed as the 'Airborne Radioactivity Monitoring System UAV'. Both systems have been developed by the Vietnamese Academy of Military Science and Technology (AMST).

The six-wheeled UGV is a 115 kg vehicle with a manipulator arm that can lift weights of up to 23 kg. It features a gripper attachment that can be interchanged according to mission types, and the type of





decontaminant involved. It is equipped with two video cameras, and these are located on the UGV's main body and manipulator arm, respectively.



A CBRN defence UAV that has been deployed by the People's Army of Vietnam, on display at VIDEX 2022. (Janes/Ridzwan Rahmat)

The UGV is enclosed in a ruggedised exterior that can withstand various contaminants and high-pressure water jets, so that it can easily be decontaminated once it completes its intended operations. Its main mission is to collect suspected decontaminant samples into a mobile lab, where these will be analysed by CBRN personnel for further action.

Meanwhile the UAV is used to verify if an area has been contaminated with CBRN agents. It is equipped with a Geiger–Mueller dose rate detector to measure the volume of radioactive contaminants in the atmosphere, the representative said.

### How Doctrine and Delineation Can Help Defeat Drones

Source: <https://www.homelandsecuritynewswire.com/dr20221213-how-doctrine-and-delineation-can-help-defeat-drones>

Dec 13 – As Iranian-made drones continue to [spread destruction](#) across Ukraine, observers have been reminded once again of the dangers unmanned aerial systems pose. The United States, to its credit, has made significant progress in bolstering its capabilities to combat this threat, particularly through the investment of the Pentagon and the defense industrial base in counter-drone research and development. Washington has also established a senior-level Joint-Force office dedicated to addressing drone attacks within the Department of Defense. Nicholas Paul Pacheco writes in [War on the Rocks](#) that there remain two areas that have not been properly tackled: base defense and warfighter-policymaker synergy. First, [bases have become particularly vulnerable to small drones](#), in part because there is no clear delineation of roles and responsibilities in defending against them. Second, the fast-paced evolution of drone warfare has made it difficult for policymakers to effectively ensure every echelon down to the operators of counter-drone systems is on the same page when it comes to strategic vision, operational mission, and tactical employment.

He writes:







To address these gaps, the Department of Defense should begin incorporating its counter-drone research and strategy into new doctrine and professional military education. To facilitate this, the Joint Counter-Small Unmanned Aircraft Systems Office should include representatives from Army Training and Doctrine Command and the U.S. Army Air Defense Artillery School on its team. At the same time, the Department of Defense should authorize a new joint command center integrating the Army, Air Force, and Marine Corps that would fall under J3 Operations to directly oversee base defense. This interagency effort would be tasked with bringing together all relevant stakeholders, alongside the Joint Counter-Small Unmanned Aircraft Systems Office, to test and deploy new counter unmanned aerial systems technology.

....

Global procurement of military unmanned aerial systems is [up 57 percent from 2021](#). In the Middle East, [Houthi attacks on the Gulf States](#) have shown how legacy air defense systems like the American MIM-104 Patriot have proven ineffective in combating the threat. Even the U.S. military's most effective legacy system against drones, the [Counter-Rocket, Artillery, Mortar Intercept, is at risk](#) against a large enough drone swarm with decentralized flight patterns.

Understanding America's drone vulnerability begins with distinguishing between two potential threats: massed attacks and swarming methods. The first resembles several birds with decentralized flight patterns picking and choosing different prey while the second resembles an [organized flock of birds](#) converging on a single target. Massed attacks are much less organized and often can have several operators using decentralized drones that are not coordinating. This makes it difficult to neutralize a source, but also makes the capacity of the attack less lethal. Swarms on the other hand feature coordinated command and control, usually with one operator using an algorithm or tactical operations center. These are more likely to be practiced by state actors and involve large numbers of drones employed for increased lethality. This makes swarms more vulnerable to being deterred but also more deadly and useful for offensive penetration.

Historically, the usage of drones in global conflict — particularly low-intensity conflict and irregular warfare — has featured mass attacks since the command side has been limited to [human-in-the-loop control](#). But the primary drone threat to U.S. forces today comes from small unmanned aerial systems used in swarm attacks, particularly as [China and Russia](#) have focused on this technology.

These systems possess two characteristics that make them more militarily useful than larger unmanned aerial systems. First, their diminutive size, slow speed, and plastic construction allows them to [avoid detection by traditional anti-aircraft sensors](#). Second, because [small unmanned aerial systems are relatively inexpensive](#), they can be procured and deployed in large numbers. This poses a distinct challenge to base defense because the legacy systems that make up the robust U.S. air defense apparatus do not have capabilities to counter large numbers of drones all at once. The ability of small unmanned aerial systems to coordinate with one another and pick and choose targets enables them to deliver high explosive volume coupled with rapid decision-making and precise direction of attack. With quickly developing AI integration, these swarms are becoming increasingly deadly.

Pacheco notes that as for actually shooting down the pilotless birds, the military has for some time had systems in the pipeline prepped to answer this task, "But while the technology side of defense is developing apace, the Joint Counter-Small Unmanned Aircraft Systems Office has more work to do engaging the warfighters who will have to use this technology, specifically air defenders and base security force units."

He adds:

Fostering greater synergy fits best under the J3 mission statement, since this directly deals with operations-related matters. Creating a joint command center would centralize and enhance command and control for base defense, properly distributing roles and responsibilities for the joint force while also assisting in implementing new counter unmanned aerial systems. A new joint command center in the J3 would allow for a unitary approach bringing together the Army and Air Force that can focus solely on base defense and serve as higher command for base security forces globally. The J3 could ensure that units tasked as security forces were specifically identified, trained, and deployed for that mission. This center could also play a valuable role in coordinating field tests for new technology. Alongside the Joint Counter-Small Unmanned Aircraft Systems Office, it could offer a direct mechanism through which the Defense Advanced Research Projects Agency and the defense industrial base could test newly designed systems in active combat zones.

Pacheco concludes:

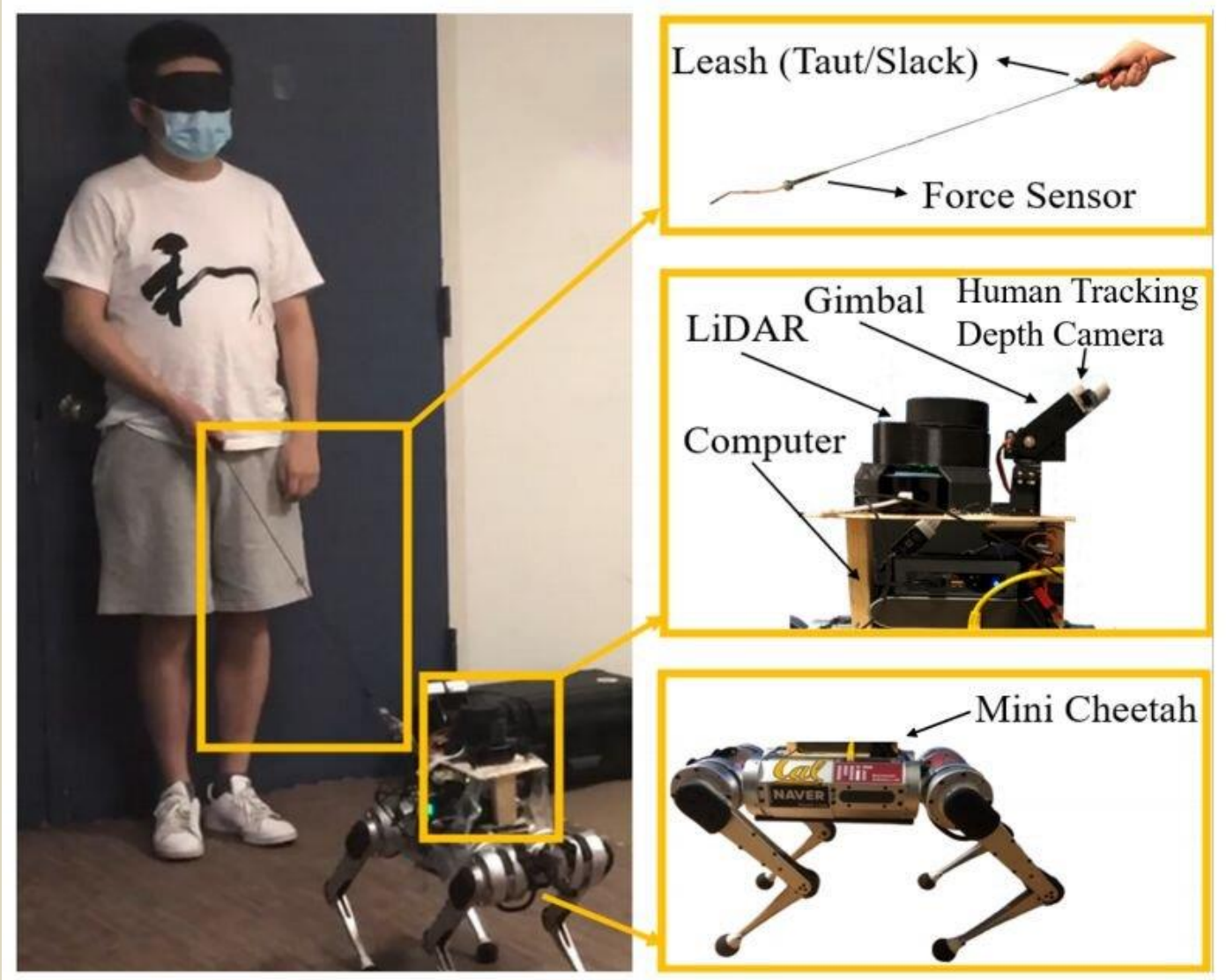
The Joint Counter-Small Unmanned Aircraft Systems Office has, during its short existence, made enormous progress in protecting U.S. forces from drone technology. Like any organization, though, it should assess where it falls short and where it can improve. It has the capacity to set the tone of counter unmanned aerial system strategy for the foreseeable future and develop standard operating procedures that will keep pace with the threat. The unmanned aerial system threat will only evolve. So should the institutions tasked with countering it.





## A laser equipped robotic guide dog to lead people who are visually impaired

Source: <https://techxplore.com/news/2021-04-laser-equipped-robotic-dog-people.html>



The Mini Cheetah is guiding a blindfolded person to avoid obstacles with leash-guided assistance: a leash (top right) is used to connect between the robot and the human, a 2D LiDAR is used for robot localization and a depth camera is used for human detection (middle right). The leash could be taut or slack during the navigation. Credit: arXiv:2103.14300 [cs.RO]

A small team of researchers at the University of California, Berkeley has developed a robot dog to help in ways similar to real guide dogs. They have written a paper describing their robot guide dog and have uploaded it to the arXiv preprint server. They have also posted two videos demonstrating the capabilities of their robot on YouTube. Guide [dogs](#) are very useful to people who are blind or have low sight, of that there is no doubt. But they have their limitations. The first is that it takes a lot of time and money to train a dog, leaving many people on long waiting lists or unable to afford them at all. Another drawback with guide dogs is their inability to read a map and then use it to navigate to a desired location. In this new effort, the researchers have developed a [robot](#) dog that is able to carry out the duties of a live guide dog as well as provide additional services. The researchers started with a robot made by Boston Dynamics called mini cheetah. It is able to walk on four legs and comes equipped with lasers and cameras that allow it to map out nearby terrain. It also comes with a computer brain to use what it sees to walk around while avoiding collisions with objects and to walk a predetermined course. The researchers added a leash to the robot and a human tracking depth camera. The depth camera is needed to provide location information to the robot dog concerning the human that it is leading. The robot and the person work together to move from one location to the next. First, a map describing the path that the dog is to take is downloaded to the robot dog. The map also includes terrain details to help the pair get where they want to go. Then, finally, the human grabs hold of







the leash and the pair begin walking. Testing has shown that the robot dog is able to lead a person (a blindfolded person with sight) from a starting point to an ending point and that it can be done with both a taut and slack leash. More work will need to be done, however, before the robot dog is ready to lead a person who is blind in a real-world setting. The robot will need to be given a smoother and quieter gait, for example, and it will need to give the person it is leading more feedback as the walk unfolds.

### Iranian Shahed 131 Drone "Geran 1" Used in War in Ukraine

Source: <https://www.youtube.com/watch?v=-dvqf3FT2dQ&t=5s>

... but the engine is "Made in the UK"!

Source: <https://uavenginesltd.co.uk/products/ar731-38-bhp/>

... as you can at the end of the video!

Policy Perspectives  
Vol. 10/15, December 2022



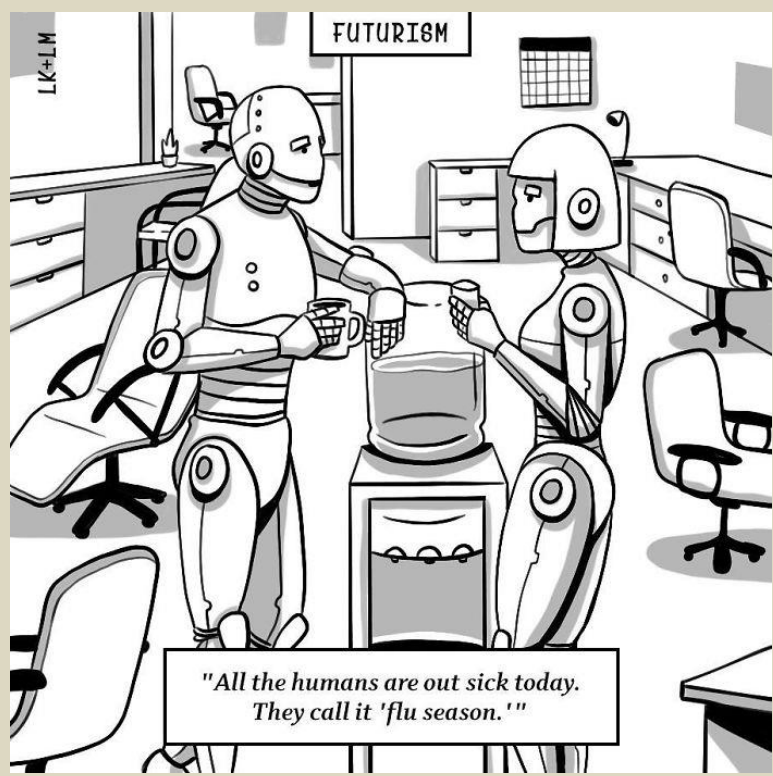
## The Ukraine Drone Effect on European Militaries

The war in Ukraine is the first large-scale, high-intensity military conflict in which both sides deploy different types of drones extensively and to different military effects. European countries should take note to adopt a holistic approach on drones and anti-drone defenses.

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



By Dominika Kunertova





# AI - NEWS







## Kissinger and the current situation considering the development of Artificial Intelligence and the Ukrainian crisis

By Giancarlo Elia Valori

Source: <https://modern diplomacy.eu/2022/11/26/kissinger-and-the-current-situation-considering-the-development-of-artificial-intelligence-and-the-ukrainian-crisis/>



Nov 26 – Kissinger has recently published some reflections on the course of world politics in recent decades, with references to the return of the 20th century conflicts brought to light by the development of new weaponry and strategic scenarios mediated by Artificial Intelligence. Kissinger has also referred to the situation in Ukraine and the equilibria between the United States, Russia and China. Kissinger has stated that instant communication and the technological revolution have combined to provide new meaning and urgency to two crucial issues that leaders must address:

- 1) what is essential for national security?
- 2) what is necessary for peaceful international coexistence?

Although a plethora of empires existed, aspirations for world order were confined by geography and technology to specific regions. This was also true for the Roman and Chinese empires, which encompassed a wide range of societies and cultures. These were regional orders that co-evolved as world orders.

From the 16th century onwards, the development of technology, medicine and economic and political organisation expanded Europe's ability to project its power and government systems around the world. From the mid-17th century, the Westphalian system was based on respect for sovereignty and international law. Later that system took root throughout the world and, after the end of traditional colonialism, it led to the emergence of States which – largely formally abandoned by the former motherlands – insisted on defining, and even defying, the rules of the established world order – at least the countries that really got rid of imperialistic domination, such as the People's Republic of China, the Democratic People's Republic of Korea, etc.

Since the end of World War II, mankind has lived in a delicate balance between relative security and legitimacy. In no previous period of history would the consequences of an error in this balance have been more severe or catastrophic. The contemporary age has introduced a level of destructiveness that





potentially enables mankind to self-destruct. Advanced systems of mutual destruction were aimed at pursuing not ultimate victory but rather at preventing others' attack.

This is the reason why shortly after the Japanese nuclear tragedy of 1945, the deployment of nuclear weapons began to become incalculable, unconstrained by consequences and based on the certainty of security systems.

For seventy-six years (1946-2022) while advanced weapons grew in power, complexity and accuracy, no country was convinced to actually use them, even in conflict with non-nuclear countries. Both the United States of America and the Soviet Union that accepted defeat at the hands of non-nuclear countries without resorting to their own most lethal weapons: as in the case of the Korean War, Vietnam, Afghanistan (both the Soviets and the Americans in that case).

To this day, such nuclear dilemmas have not disappeared, but have instead changed as more States have developed more refined weapons than the "nuclear bomb" and the essentially bipolar distribution of destructive capabilities of the former Cold War has been replaced by very high-tech options – a topic addressed in my various articles.

Cyber weapons and artificial intelligence applications (such as autonomous weapon systems) greatly complicate the current dangerous war prospects. Unlike nuclear weapons, cyber weapons and artificial intelligence are ubiquitous, relatively inexpensive to develop and easy to use.

Cyber weapons combine the capacity for massive impact with the ability to obscure the attribution of attacks, which is crucial when the attacker is no longer a precise reference but becomes a "quiz".

As we have often pointed out, artificial intelligence can also overcome the need for human operators, and enable weapons to launch themselves based on their own calculations and their ability to choose targets with almost absolute precision and accuracy.

Because the threshold for their use is so low and their destructive ability so great, the use of such weapons – or even their mere threat – can turn a crisis into a war or turn a limited war into a nuclear war through unintentional or uncontrollable escalation. To put it in simple terms, there will no longer be the need to drop the "bomb" first, as it would be downgraded to a weapon of retaliation against possible and not certain enemies. On the contrary, with the help of artificial intelligence, third parties could make sure that the first cyber-attack is attributed to those who have never attacked.

The impact of this technology makes its application a cataclysm, thus making its use so limited that it becomes unmanageable.

No diplomacy has yet been invented to explicitly threaten its use without the risk of an anticipated response. So much so that arms control Summits seem to have been played down by these uncontrollable novelties, ranging from unmarked drone attacks to cyberattacks from the depths of the Net.

Technological developments are currently accompanied by a political transformation. Today we are witnessing the resurgence of rivalry between the great powers, amplified by the spread and advancement of surprising technologies. When in the early 1970s the People's Republic of China embarked on its re-entry into the international diplomatic system at the initiative of Zhou Enlai and, at the end of that decade, on its full re-entry into the international arena thanks to Deng Xiaoping, its human and economic potential was vast, but its technology and actual power were relatively limited.

Meanwhile, China's growing economic and strategic capabilities have forced the United States of America to confront – for the first time in its history – a geopolitical competitor whose resources are potentially comparable to its own.

Each side sees itself as a *unicum*, but in a different way. The United States of America acts on the assumption that its values are universally applicable and will eventually be adopted everywhere. The People's Republic of China, instead, expects that the uniqueness of its ultra-millennial civilisation and the impressive economic leap forward will inspire other countries to emulate it to break free from imperialist domination and show respect for Chinese priorities.

Both the US "manifest destiny" missionary impulse and the Chinese sense of *grandeur* and cultural eminence – of China as such, including Taiwan – imply a kind of subordination-fear of each other. Due to the nature of their economies and high technology, each country is affecting what the other has so far considered its core interests.

In the 21st century China seems to have embarked on playing an international role to which it considers itself entitled by its achievements over the millennia. The United States of America, on the other hand, is taking action to project power, purpose, and diplomacy around the world to maintain a global equilibrium established in its post-war experience, responding to tangible and imagined challenges to this world order.

For the leadership on both sides, these security requirements seem self-evident. They are supported by their respective citizens. Yet security is only part of the wide picture. The fundamental issue for the planet's existence is whether the two giants can learn to combine the inevitable strategic rivalry with a concept and practice of coexistence.

Russia – unlike the United States of America and China – lacks the market power, demographic clout and diversified industrial base. Spanning eleven time zones and enjoying few natural defensive demarcations, Russia has acted according to its own geographical and historical imperatives. Russia's foreign policy represents a mystical patriotism in a Third Rome-style imperial law, with a lingering perception of insecurity essentially stemming from the country's long-standing vulnerability to invasion across the plains of Eastern Europe.







For centuries, its leaders from Peter the Great to Stalin – who, by the way, was not even Russian, but felt he was so in the internationalist spirit that led to the creation of the USSR on 30 December 1922 – have sought to isolate Russia's vast territory with a safety belt imposed around its diffuse border. Today Kissinger tells us that the same priority is manifested once again in the attack on Ukraine – and we add that few people understand and many others pretend not to understand this.

The mutual impact of these societies has been shaped by their strategic assessments, which stem from their history. The Ukrainian conflict is a case in point. After the dissolution of the Warsaw Pact, and the turning of its Member States (Bulgaria, Czechoslovakia, German Democratic Republic, Poland, Romania, Hungary) into “Western” countries, the whole territory – from the security line established in central Europe up to Russia's national border – has opened up to a new strategic design. Stability depended on the fact that the Warsaw Pact in itself – especially after the Conference on Security and Cooperation in Europe held in Helsinki in 1975 – allayed Europe's traditional fears of Russian domination (indeed, Soviet domination, at the time), and assuaged Russia's traditional concerns about Western offensives – from the Swedes to Napoleon until Hitler. Hence, the strategic geography of Ukraine embodies these concerns emerging again in Russia. If Ukraine were to join NATO, the security line between Russia and the West would be placed within just over 500 kilometres of Moscow, actually eliminating the traditional buffer that saved Russia when Sweden, France and Germany tried to occupy it in previous centuries.

If the security border were to be established on the Western side of Ukraine, Russian forces would be within easy reach of Budapest and Warsaw. The February 2022 invasion of Ukraine is a flagrant violation of the international law mentioned above, and is thus largely a consequence of a failed or otherwise inadequately undertaken strategic dialogue. The experience of two nuclear entities confronting each other militarily – although not resorting to their destructive weapons – underlines the urgency of the fundamental problem, as Ukraine is only a tool of the West. Dario Fo once said that China was an invention of Albania to scare the Soviet Union. We can say that Ukraine is currently an invention of the West to scare Russia – and this is not a joke. An invention for which Ukrainians and Russians are paying with their blood.

Hence the triangular relationship between the United States of America, the People's Republic of China, and the Russian Federation will eventually resume, even if Russia will be weakened by the demonstration of its intended military limitations in Ukraine, the widespread rejection of its conduct, and the scope and impact of sanctions against it. But it will retain nuclear and cyber capabilities for doomsday scenarios.

In the US-Chinese relationship, instead, the conundrum is whether two different concepts of national greatness can learn to peacefully coexist side by side and how. In the case of Russia, the challenge is whether the country can reconcile its vision of itself with the self-determination and security of the countries in what it has long called its “near abroad” (mainly Central Asia and Eastern Europe), and do so as part of an international system rather than through domination.

It now seems possible that an order based on universal rules, however worthy in its conception, will be replaced in practice, for an indefinite period of time, by an at least partially decoupled world. Such a division encourages a search at its margins for spheres of influence. In such a case, how will countries that do not agree on global rules of conduct be able to operate within an agreed equilibrium design? Will the quest for domination overwhelm the analysis of coexistence?

In a world of increasingly formidable technology that can either elevate or dismantle human civilisation, there is no definitive solution to the competition between great powers, let alone a military one. An unbridled technological race, justified by the foreign policy ideology in which each side is convinced of the other's malicious intent, risks creating a catastrophic cycle of mutual suspicion like the one that triggered World War I, but with incomparably greater consequences.

All sides are therefore now obliged to re-examine their first principles of international behaviour and relate them to the possibilities of coexistence. For the leaders of high-tech companies, there is a moral and strategic imperative to pursue – both within their own countries and with potential adversary countries – an ongoing discussion on the implications of technology and how its military applications could be limited.

The topic is too important to be neglected until crises arise. The arms control dialogues that helped toning down and showing restraint during the nuclear age, as well as the high-level research on the consequences of emerging technologies, could prompt reflection and promote habits of mutual strategic self-restraint.

An irony of the current world is that one of its glories – the revolutionary explosion of technology – has emerged so quickly, and with such optimism, that it has outgrown its dangers, and inadequate systematic efforts have been made to understand its capabilities. Technologists develop amazing devices, but have had few opportunities to explore and evaluate their comparative implications within a historical framework. As I pointed out in a previous article, political leaders too often lack adequate understanding of the strategic and philosophical implications of the machines and algorithms available to them. At the same time, the technological revolution is eroding human consciousness and perceptions of the nature of reality. The last great transformation – the Enlightenment – replaced the age of faith with repeatable experiments and logical deductions. Now it is supplanted by dependence on algorithms, which work in the opposite direction, offering results in search of an explanation. Exploring these new frontiers will require considerable efforts on the part of national







leaders to reduce, and ideally bridge, the gaps between the worlds of technology, politics, history and philosophy. The leaders of current great powers need not immediately develop a detailed vision of how to solve the dilemmas described here. **Kissinger warns that, however, they must be clear about what is to be avoided and what cannot be tolerated.** The wise must anticipate challenges before they manifest themselves as crises. Lacking a moral and strategic vision, the current era is unbridled. The extent of our future still defies understanding not so much of what will happen but of what has already happened.

Advisory Board Co-chair Honoris Causa **Professor Giancarlo Elia Valori** is an eminent Italian economist and businessman. He holds prestigious academic distinctions and national orders. Mr. Valori has lectured on international affairs and economics at the world's leading universities such as Peking University, the Hebrew University of Jerusalem and the Yeshiva University in New York. He currently chairs "International World Group", he is also the honorary president of Huawei Italy, economic adviser to the Chinese giant HNA Group. In 1992 he was appointed Officier de la Légion d'Honneur de la République Française, with this motivation: "A man who can see across borders to understand the world" and in 2002 he received the title "Honorable" of the Académie des Sciences de l'Institut de France."

## Pros and Cons of Autonomous Weapons Systems

By Amitai Etzioni, PhD and Oren Etzioni, PhD

Source: <https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Pros-and-Cons-of-Autonomous-Weapons-Systems/>



Autonomous weapons systems and military robots are progressing from science fiction movies to designers' drawing boards, to engineering laboratories, and to the battlefield. These machines have prompted a debate among military planners, roboticists, and ethicists about the development and







deployment of weapons that can perform increasingly advanced functions, including targeting and application of force, with little or no human oversight.

Some military experts hold that autonomous weapons systems not only confer significant strategic and tactical advantages in the battleground but also that they are preferable on moral grounds to the use of human combatants. In contrast, critics hold that these weapons should be curbed, if not banned altogether, for a variety of moral and legal reasons. This article first reviews arguments by those who favor autonomous weapons systems and then by those who oppose them. Next, it discusses challenges to limiting and defining autonomous weapons. Finally, it closes with a policy recommendation.

### Arguments in Support of Autonomous Weapons Systems

Support for autonomous weapons systems falls into two general categories. Some members of the defense community advocate autonomous weapons because of military advantages. Other supporters emphasize moral justifications for using them.

**Military advantages.** Those who call for further development and deployment of autonomous weapons systems generally point to several military advantages. First, autonomous weapons systems act as a force multiplier. That is, fewer warfighters are needed for a given mission, and the efficacy of each warfighter is greater. Next, advocates credit autonomous weapons systems with expanding the battlefield, allowing combat to reach into areas that were previously inaccessible. Finally, autonomous weapons systems can reduce casualties by removing human warfighters from dangerous missions.<sup>1</sup>

The Department of Defense's *Unmanned Systems Roadmap: 2007-2032* provides additional reasons for pursuing autonomous weapons systems. These include that robots are better suited than humans for "dull, dirty, or dangerous" missions.<sup>2</sup> An example of a dull mission is long-duration sorties. An example of a dirty mission is one that exposes humans to potentially harmful radiological material. An example of a dangerous mission is explosive ordnance disposal. Maj. Jeffrey S. Thurnher, U.S. Army, adds, "[lethal autonomous robots] have the unique potential to operate at a tempo faster than humans can possibly achieve and to lethally strike even when communications links have been severed."<sup>3</sup>

In addition, the long-term savings that could be achieved through fielding an army of military robots have been highlighted. In a 2013 article published in *The Fiscal Times*, David Francis cites Department of Defense figures showing that "each soldier in Afghanistan costs the Pentagon roughly \$850,000 per year."<sup>4</sup> Some estimate the cost per year to be even higher. Conversely, according to Francis, "the TALON robot—a small rover that can be outfitted with weapons, costs \$230,000."<sup>5</sup> According to *Defense News*, Gen. Robert Cone, former commander of the U.S. Army Training and Doctrine Command, suggested at the 2014 Army Aviation Symposium that by relying more on "support robots," the Army eventually could reduce the size of a brigade from four thousand to three thousand soldiers without a concomitant reduction in effectiveness.<sup>6</sup>

Air Force Maj. Jason S. DeSon, writing in the *Air Force Law Review*, notes the potential advantages of autonomous aerial weapons systems.<sup>7</sup> According to DeSon, the physical strain of high-G maneuvers and the intense mental concentration and situational awareness required of fighter pilots make them very prone to fatigue and exhaustion; robot pilots, on the other hand would not be subject to these physiological and mental constraints. Moreover, fully autonomous planes could be programmed to take genuinely random and unpredictable action that could confuse an opponent. More striking still, Air Force Capt. Michael Byrnes predicts that a single unmanned aerial vehicle with machine-controlled maneuvering and accuracy could, "with a few hundred rounds of ammunition and sufficient fuel reserves," take out an entire fleet of aircraft, presumably one with human pilots.<sup>8</sup>

In 2012, a report by the Defense Science Board, in support of the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, identified "six key areas in which advances in autonomy would have significant benefit to [an] unmanned system: perception, planning, learning, human-robot interaction, natural language understanding, and multiagent coordination."<sup>9</sup> *Perception*, or perceptual processing, refers to sensors and sensing. Sensors include hardware, and sensing includes software.<sup>10</sup>

Next, according to the Defense Science Board, *planning* refers to "computing a sequence or partial order of actions that ... [achieve] a desired state."<sup>11</sup> The process relies on effective processes and "algorithms needed to make decisions about action (provide autonomy) in situations in which humans are not in the environment (e.g., space, the ocean)."<sup>12</sup> Then, *learning* refers to how machines can collect and process large amounts of data into knowledge. The report asserts that research has shown machines process data into knowledge more effectively than people do.<sup>13</sup> It gives the example of machine learning for autonomous navigation in land vehicles and robots.<sup>14</sup>

*Human-robot interaction* refers to "how people work or play with robots."<sup>15</sup> Robots are quite different from other computers or tools because they are "physically situated agents," and human users interact with them in distinct ways.<sup>16</sup> Research on interaction needs to span a number of domains well beyond engineering, including psychology, cognitive science, and communications, among others. "Natural language processing concerns ... systems that can communicate with people using ordinary human languages."<sup>17</sup> Moreover, "natural language is the most normal and intuitive way for humans to instruct autonomous systems; it allows them to provide diverse, high-level goals and strategies rather than detailed teleoperation."<sup>18</sup> Hence, further development of the ability of autonomous weapons systems to respond to commands in a natural language is necessary.





Finally, the Defense Science Board uses the term *multiagent coordination* for circumstances in which a task is distributed among “multiple robots, software agents, or humans.”<sup>19</sup> Tasks could be centrally planned or coordinated through interactions of the agents. This sort of coordination goes beyond mere cooperation because “it assumes that the agents have a cognitive understanding of each other’s capabilities, can monitor progress towards the goal, and engage in more human-like teamwork.”<sup>20</sup>

Moral justifications. Several military experts and roboticists have argued that autonomous weapons systems should not only be regarded as morally acceptable but also that they would in fact be ethically preferable to human fighters. For example, roboticist Ronald C. Arkin believes autonomous robots in the future will be able to act more “humanely” on the battlefield for a number of reasons, including that they do not need to be programmed with a self-preservation instinct, potentially eliminating the need for a “shoot-first, ask questions later” attitude.<sup>21</sup> The judgments of autonomous weapons systems will not be clouded by emotions such as fear or hysteria, and the systems will be able to process much more incoming sensory information than humans without discarding or distorting it to fit preconceived notions. Finally, per Arkin, in teams comprised of human and robot soldiers, the robots could be more relied upon to report ethical infractions they observed than would a team of humans who might close ranks.<sup>22</sup>

Lt. Col. Douglas A. Pryer, U.S. Army, asserts there might be ethical advantages to removing humans from high-stress combat zones in favor of robots. He points to neuroscience research that suggests the neural circuits responsible for conscious self-control can shut down when overloaded with stress, leading to sexual assaults and other crimes that soldiers would otherwise be less likely to commit. However, Pryer sets aside the question of whether or not waging war via robots is ethical in the abstract. Instead, he suggests that because it sparks so much moral outrage among the populations from whom the United States most needs support, robot warfare has serious strategic disadvantages, and it fuels the cycle of perpetual warfare.<sup>23</sup>

### Arguments Opposed to Autonomous Weapons Systems

While some support autonomous weapons systems with moral arguments, others base their opposition on moral grounds. Still others assert that moral arguments against autonomous weapons systems are misguided.

Opposition on moral grounds. In July 2015, an open letter calling for a ban on autonomous weapons was released at an international joint conference on artificial intelligence. The letter warns, “Artificial Intelligence (AI) technology has reached a point where the deployment of such systems is—practically if not legally—feasible within years, not decades, and the stakes are high: autonomous weapons have been described as the third revolution in warfare, after gunpowder and nuclear arms.”<sup>24</sup> The letter also notes that AI has the potential to benefit humanity, but that if a military AI arms race ensues, AI’s reputation could be tarnished, and a public backlash might curtail future benefits of AI. The letter has an impressive list of signatories, including Elon Musk (inventor and founder of Tesla), Steve Wozniak (cofounder of Apple), physicist Stephen Hawking (University of Cambridge), and Noam Chomsky (Massachusetts Institute of Technology), among others. Over three thousand AI and robotics researchers have also signed the letter. The open letter simply calls for “a ban on offensive autonomous weapons beyond meaningful human control.”<sup>25</sup>

We note in passing that it is often unclear whether a weapon is offensive or defensive. Thus, many assume that an effective missile defense shield is strictly defensive, but it can be extremely destabilizing if it allows one nation to launch a nuclear strike against another without fear of retaliation.

In April 2013, the United Nations (UN) special rapporteur on extrajudicial, summary, or arbitrary executions presented a report to the UN Human Rights Council. The report recommended that member states should declare and implement moratoria on the testing, production, transfer, and deployment of lethal autonomous robotics (LARs) until an internationally agreed upon framework for LARs has been established.<sup>26</sup>

That same year, a group of engineers, AI and robotics experts, and other scientists and researchers from thirty-seven countries issued the “Scientists’ Call to Ban Autonomous Lethal Robots.” The statement notes the lack of scientific evidence that robots could, in the future, have “the functionality required for accurate target identification, situational awareness, or decisions regarding the proportional use of force.”<sup>27</sup> Hence, they may cause a high level of collateral damage. The statement ends by insisting that “decisions about the application of violent force must not be delegated to machines.”<sup>28</sup>

Indeed, the delegation of life-or-death decision making to nonhuman agents is a recurring concern of those who oppose autonomous weapons systems. The most obvious manifestation of this concern relates to systems that are capable of choosing their own targets. Thus, highly regarded computer scientist Noel Sharkey has called for a ban on “lethal autonomous targeting” because it violates the Principle of Distinction, considered one of the most important rules of armed conflict—autonomous weapons systems will find it very hard to determine who is a civilian and who is a combatant, which is difficult even for humans.<sup>29</sup> Allowing AI to make decisions about targeting will most likely result in civilian casualties and unacceptable collateral damage.

Another major concern is the problem of accountability when autonomous weapons systems are deployed. Ethicist Robert Sparrow highlights this ethical issue by noting that a fundamental condition of international humanitarian law, or *jus in bello*, requires that some person must be held responsible for civilian deaths. Any weapon or other means of war that makes it impossible to identify responsibility for the casualties it causes does not meet the requirements of *jus in bello*, and, therefore, should not be employed in war.<sup>30</sup>







This issue arises because AI-equipped machines make decisions on their own, so it is difficult to determine whether a flawed decision is due to flaws in the program or in the autonomous deliberations of the AI-equipped (so-called smart) machines. The nature of this problem was highlighted when a driverless car violated the speed limits by moving too slowly on a highway, and it was unclear to whom the ticket should be issued.<sup>31</sup> In situations where a human being makes the decision to use force against a target, there is a clear chain of accountability, stretching from whoever actually “pulled the trigger” to the commander who gave the order. In the case of autonomous weapons systems, no such clarity exists. It is unclear who or what are to be blamed or held liable.

What Sharkey, Sparrow and the signatories of the open letter propose could be labeled “upstream regulation,” that is, a proposal for setting limits on the development of autonomous weapons systems technology and drawing red lines that future technological developments should not be allowed to cross. This kind of upstream approach tries to foresee the direction of technological development and preempt the dangers such developments would pose. Others prefer “downstream regulation,” which takes a wait-and-see approach by developing regulations as new advances occur. Legal scholars Kenneth Anderson and Matthew Waxman, who advocate this approach, argue that regulation will have to emerge along with the technology because they believe that morality will coevolve with technological development.<sup>32</sup>

Thus, arguments about the irreplaceability of human conscience and moral judgment may have to be revisited.<sup>33</sup> In addition, they suggest that as humans become more accustomed to machines performing functions with life-or-death implications or consequences (such as driving cars or performing surgeries), humans will most likely become more comfortable with AI technology’s incorporation into weaponry. Thus, Anderson and Waxman propose what might be considered a communitarian solution by suggesting that the United States should work on developing norms and principles (rather than binding legal rules) guiding and constraining research and development—and eventual deployment—of autonomous weapons systems. Those norms could help establish expectations about legally or ethically appropriate conduct. Anderson and Waxman write,

To be successful, the United States government would have to resist two extreme instincts. It would have to resist its own instincts to hunker down behind secrecy and avoid discussing and defending even guiding principles. It would also have to refuse to cede the moral high ground to critics of autonomous lethal systems, opponents demanding some grand international treaty or multilateral regime to regulate or even prohibit them.<sup>34</sup>

Counterarguments. In response, some argue against any attempt to apply to robots the language of morality that applies to human agents. Military ethicist George Lucas Jr. points out, for example, that robots cannot feel anger or a desire to “get even” by seeking retaliation for harm done to their compatriots.<sup>35</sup> Lucas holds that the debate thus far has been obfuscated by the confusion of machine autonomy with moral autonomy. The Roomba vacuum cleaner and Patriot missile “are both ‘autonomous’ in that they perform their assigned missions, including encountering and responding to obstacles, problems, and unforeseen circumstances with minimal human oversight,” but not in the sense that they can change or abort their mission if they have “moral objections.”<sup>36</sup> Lucas thus holds that the primary concern of engineers and designers developing autonomous weapons systems should not be *ethics* but rather *safety* and *reliability*, which means taking due care to address the possible risks of malfunctions, mistakes, or misuse that autonomous weapons systems will present. We note, though, that safety is of course a moral value as well.

Lt. Col. Shane R. Reeves and Maj. William J. Johnson, judge advocates in the U.S. Army, note that there are battlefields absent of civilians, such as underwater and space, where autonomous weapons could reduce the possibility of suffering and death by eliminating the need for combatants.<sup>37</sup> We note that this valid observation does not agitate against a ban in other, in effect most, battlefields. Michael N. Schmitt of the Naval War College makes a distinction between weapons that are illegal per se and the unlawful use of otherwise legal weapons. For example, a rifle is not prohibited under international law, but using it to shoot civilians would constitute an unlawful use. On the other hand, some weapons (e.g., biological weapons) are unlawful per se, even when used only against combatants. Thus, Schmitt grants that some autonomous weapons systems might contravene international law, but “it is categorically not the case that all such systems will do so.”<sup>38</sup> Thus, even an autonomous system that is incapable of distinguishing between civilians and combatants should not necessarily be unlawful per se, as autonomous weapons systems could be used in situations where no civilians were present, such as against tank formations in the desert or against warships. Such a system could be *used* unlawfully, though, if it were employed in contexts where civilians were present. We assert that some limitations on such weapons should be called for.

In their review of the debate, legal scholars Gregory Noone and Diana Noone conclude that everyone is in agreement that any autonomous weapons system would have to comply with the Law of Armed Conflict (LOAC), and thus be able to distinguish between combatants and noncombatants. They write, “No academic or practitioner is stating anything to the contrary; therefore, this part of any argument from either side must be ignored as a red herring. Simply put, no one would agree to any weapon that ignores LOAC obligations.”<sup>39</sup>

### Limits on Autonomous Weapons Systems and Definitions of Autonomy

The international community has agreed to limits on mines and chemical and biological weapons, but an agreement on limiting autonomous weapons systems would meet numerous challenges. One challenge



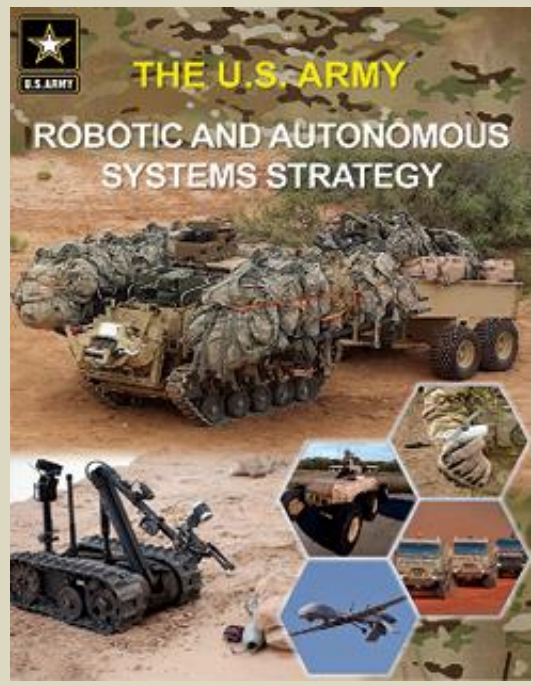




is the lack of consensus on how to define the autonomy of weapons systems, even among members of the Department of Defense.



Soldiers from 2nd Battalion, 27th Infantry Regiment, 3rd Brigade Combat Team, 25th Infantry Division, move forward toward simulated opposing forces with a multipurpose unmanned tactical transport 22 July 2016 during the Pacific Manned-Unmanned Initiative at Marine Corps Training Area Bellows, Hawaii. (Photo by Staff Sgt. Christopher Hubenthal, U.S. Air Force)



A standard definition that accounts for levels of autonomy could help guide an incremental approach to proposing limits. Limits on autonomous weapons systems. We take it for granted that no nation would agree to forswear the use of autonomous weapons systems unless its adversaries would do the same. At first blush, it may seem that it is not beyond the realm of possibility to obtain an international agreement to ban autonomous weapons systems or at least some kinds of them.

*The U.S. Army Robotic and Autonomous Systems Strategy*, published March 2017 by U.S. Army Training and Doctrine Command, describes how the Army intends to integrate new technologies into future organizations to help ensure overmatch against increasingly capable enemies. Five capability objectives are to increase situational awareness, lighten soldiers' workloads, sustain the force, facilitate movement and maneuver, and protect the force. To view the strategy, visit [https://www.tradoc.army.mil/FrontPageContent/Docs/RAS\\_Strategy.pdf](https://www.tradoc.army.mil/FrontPageContent/Docs/RAS_Strategy.pdf).

1999); the Chemical Weapons Convention (ratified in 1997); and the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their







Destruction (known as the Biological Weapons Convention, adopted in 1975). The record of the Treaty on the Nonproliferation of Nuclear Weapons (adopted in 1970) is more complicated, but it is credited with having stopped several nations from developing nuclear arms and causing at least one to give them up.

Some advocates of a ban on autonomous weapons systems seek to ban not merely production and deployment but also research, development, and testing of these machines. This may well be impossible as autonomous weapons systems can be developed and tested in small workshops and do not leave a trail. Nor could one rely on satellites for inspection data for the same reasons. We hence assume that if such a ban were possible, it would mainly focus on deployment and mass production.

Even so, such a ban would face considerable difficulties. While it is possible to determine what is a chemical weapon and what is not (despite some disagreements at the margin, for example, about law enforcement use of irritant chemical weapons), and to clearly define nuclear arms or land mines, autonomous weapons systems come with very different levels of autonomy.<sup>40</sup> A ban on all autonomous weapons would require foregoing many modern weapons already mass produced and deployed.

Definitions of autonomy. Different definitions have been attached to the word “autonomy” in different Department of Defense documents, and the resulting concepts suggest rather different views on the future of robotic warfare. One definition, used by the Defense Science Board, views autonomy merely as high-end automation: “a capability (or a set of capabilities) that enables a particular action of a system to be automatic or, within programmed boundaries, ‘self-governing.’”<sup>41</sup> According to this definition, already existing capabilities, such as autopilot used in aircraft, could qualify as autonomous.

Another definition, used in the *Unmanned Systems Integrated Roadmap FY2011–2036*, suggests a qualitatively different view of autonomy: “an autonomous system is able to make a decision based on a set of rules and/or limitations. It is able to determine what information is important in making a decision.”<sup>42</sup> In this view, autonomous systems are less predictable than merely automated ones, as the AI not only is performing a specified action but also is making decisions and thus potentially taking an action that a human did not order. A human is still responsible for programming the behavior of the autonomous system, and the actions the system takes would have to be consistent with the laws and strategies provided by humans. However, no individual action would be completely predictable or preprogrammed.

It is easy to find still other definitions of autonomy. The International Committee of the Red Cross defines autonomous weapons as those able to “independently select and attack targets, i.e., with autonomy in the ‘critical functions’ of acquiring, tracking, selecting and attacking targets.”<sup>43</sup>

A 2012 Human Rights Watch report by Bonnie Docherty, *Losing Humanity: The Case against Killer Robots*, defines three categories of autonomy. Based on the kind of human involvement, the categories are human-in-the-loop, human-on-the-loop, and human-out-of-the-loop weapons.<sup>44</sup>

“Human-*in-the-loop* weapons [are] robots that can select targets and deliver force only with a human command.”<sup>45</sup> Numerous examples of the first type already are in use. For example, Israel’s Iron Dome system detects incoming rockets, predicts their trajectory, and then sends this information to a human soldier who decides whether to launch an interceptor rocket.<sup>46</sup>

“Human-*on-the-loop* weapons [are] robots that can select targets and deliver force under the oversight of a human operator who can override the robots’ actions.”<sup>47</sup> An example mentioned by Docherty includes the SGR-A1 built by Samsung, a sentry robot used along the Korean Demilitarized Zone. It uses a low-light camera and pattern-recognition software to detect intruders and then issues a verbal warning. If the intruder does not surrender, the robot has a machine gun that can be fired remotely by a soldier the robot has alerted, or by the robot itself if it is in fully automatic mode.<sup>48</sup>

The United States also deploys human-on-the-loop weapons systems. For example, the MK 15 Phalanx Close-In Weapons System has been used on Navy ships since the 1980s, and it is capable of detecting, evaluating, tracking, engaging, and using force against antiship missiles and high-speed aircraft threats without any human commands.<sup>49</sup> The Center for a New American Security published a white paper that estimated as of 2015 at least thirty countries have deployed or are developing human-supervised systems.<sup>50</sup>

“Human-*out-of-the-loop* weapons [are] robots capable of selecting targets and delivering force without any human input or interaction.”<sup>51</sup> This kind of autonomous weapons system is the source of much concern about “killing machines.” Military strategist Thomas K. Adams warned that, in the future, humans would be reduced to making only initial policy decisions about war, and they would have mere symbolic authority over automated systems.<sup>52</sup> In the Human Rights Watch report, Docherty warns, “By eliminating human involvement in the decision to use lethal force in armed conflict, fully autonomous weapons would undermine other, nonlegal protections for civilians.”<sup>53</sup> For example, a repressive dictator could deploy emotionless robots to kill and instill fear among a population without having to worry about soldiers who might empathize with their victims (who might be neighbors, acquaintances, or even family members) and then turn against the dictator.

For the purposes of this paper, we take autonomy to mean a machine has the ability to make decisions based on information gathered by the machine and to act on the basis of its own deliberations, beyond the instructions and parameters its producers, programmers, and users provided to the machine.





**A Way to Initiate an International Agreement Limiting Autonomous Weapons**

We find it hard to imagine nations agreeing to return to a world in which weapons had no measure of autonomy. On the contrary, development in AI leads one to expect that more and more machines and instruments of all kinds will become more autonomous. Bombers and fighter aircraft having no human pilot seem inevitable. Although it is true that any level of autonomy entails, by definition, some loss of human control, this genie has left the bottle and we see no way to put it back again.

Where to begin. The most promising way to proceed is to determine whether one can obtain an international agreement to ban *fully autonomous* weapons with missions that *cannot be aborted* and that cannot be recalled once they are launched. If they malfunction and target civilian centers, there is no way to stop them. Like unexploded landmines placed without marks, these weapons will continue to kill even after the sides settle their difference and sue for peace.

One may argue that gaining such an agreement should not be arduous because no rational policy maker will favor such a weapon. Indeed, the Pentagon has directed that “autonomous and semi-autonomous weapon systems shall be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force.”<sup>54</sup>

Why to begin. However, one should note that human-out-of-the-loop arms are very effective in reinforcing a red line. Declaration by representatives of one nation that if another nation engages in a certain kind of hostile behavior, swift and severe retaliation will follow, are open to misinterpretation by the other side, even if backed up with deployment of troops or other military assets.

Leaders, drawing on considerable historical experience, may bet that they be able to cross the red line and be spared because of one reason or another. Hence, arms without a human in the loop make for much more credible red lines. (This is a form of the “precommitment strategy” discussed by Thomas Schelling in *Arms and Influence*, in which one party limits its own options by obligating itself to retaliate, thus making its deterrence more credible.)<sup>55</sup>

We suggest that nations might be willing to forgo this advantage of fully autonomous arms in order to gain the assurance that once hostilities ceased, they could avoid becoming entangled in new rounds of fighting because some bombers were still running loose and attacking the other side, or because some bombers might malfunction and attack civilian centers. Finally, if a ban on fully autonomous weapons were agreed upon and means of verification were developed, one could aspire to move toward limiting weapons with a high but not full measure of autonomy.

*The authors are indebted to David Kroeker Maus for substantial research on this article.*

**Notes**

1. Gary E. Marchant et al., “International Governance of Autonomous Military Robots,” *Columbia Science and Technology Law Review* 12 (June 2011): 272–76, accessed 27 March 2017, <http://stlr.org/download/volumes/volume12/marchant.pdf>.
2. James R. Clapper Jr. et al., *Unmanned Systems Roadmap: 2007-2032* (Washington, DC: Department of Defense [DOD], 2007), 19, accessed 28 March 2017, [http://www.globalsecurity.org/intell/library/reports/2007/dod-unmanned-systems-roadmap\\_2007-2032.pdf](http://www.globalsecurity.org/intell/library/reports/2007/dod-unmanned-systems-roadmap_2007-2032.pdf).
3. Jeffrey S. Thurnher, “Legal Implications of Fully Autonomous Targeting,” *Joint Force Quarterly* 67 (4th Quarter, October 2012): 83, accessed 8 March 2017, [http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67\\_77-84\\_Thurnher.pdf](http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_77-84_Thurnher.pdf).
4. David Francis, “How a New Army of Robots Can Cut the Defense Budget,” *Fiscal Times*, 2 April 2013, accessed 8 March 2017, <http://www.thefiscaltimes.com/Articles/2013/04/02/How-a-New-Army-of-Robots-Can-Cut-the-Defense-Budget>. Francis attributes the \$850,000 cost estimate to an unnamed DOD source, presumed from 2012 or 2013.
5. *Ibid.*
6. Quoted in Evan Ackerman, “U.S. Army Considers Replacing Thousands of Soldiers with Robots,” *IEEE Spectrum*, 22 January 2014, accessed 28 March 2016, <http://spectrum.ieee.org/autoton/robotics/military-robots/army-considers-replacing-thousands-of-soldiers-with-robots>.
7. Jason S. DeSon, “Automating the Right Stuff? The Hidden Ramifications of Ensuring Autonomous Aerial Weapon Systems Comply with International Humanitarian Law,” *Air Force Law Review* 72 (2015): 85–122, accessed 27 March 2017, <http://www.afjag.af.mil/Portals/77/documents/AFD-150721-006.pdf>.
8. Michael Byrnes, “Nightfall: Machine Autonomy in Air-to-Air Combat,” *Air & Space Power Journal* 23, no. 3 (May-June 2014): 54, accessed 8 March 2017, <http://www.au.af.mil/au/afri/aspj/digital/pdf/articles/2014-May-Jun/F-Byrnes.pdf?source=GovD>.
9. Defense Science Board, *Task Force Report: The Role of Autonomy in DoD Systems* (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, July 2012), 31.
10. *Ibid.*, 33.
11. *Ibid.*, 38–39.
12. *Ibid.*, 39.
13. *Ibid.*, 41.
14. *Ibid.*, 42.
15. *Ibid.*, 44.
16. *Ibid.*
17. *Ibid.*, 49.







18. Ibid.
19. Ibid., 50.
20. Ibid.
21. Ronald C. Arkin, "The Case for Ethical Autonomy in Unmanned Systems," *Journal of Military Ethics* 9, no. 4 (2010): 332–41.
22. Ibid.
23. Douglas A. Pryer, "The Rise of the Machines: Why Increasingly 'Perfect' Weapons Help Perpetuate Our Wars and Endanger Our Nation," *Military Review* 93, no. 2 (2013): 14–24.
24. "Autonomous Weapons: An Open Letter from AI [Artificial Intelligence] & Robotics Researchers," Future of Life Institute website, 28 July 2015, accessed 8 March 2017, <http://futureoflife.org/open-letter-autonomous-weapons/>.
25. Ibid.
26. *Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, Christof Heyns*, September 2013, United Nations Human Rights Council, 23rd Session, Agenda Item 3, United Nations Document A/HRC/23/47.
27. International Committee for Robot Arms Control (ICRAC), "Scientists' Call to Ban Autonomous Lethal Robots," ICRAC website, October 2013, accessed 24 March 2017, [icrac.net](http://icrac.net).
28. Ibid.
29. Noel Sharkey, "Saying 'No!' to Lethal Autonomous Targeting," *Journal of Military Ethics* 9, no. 4 (2010): 369–83, accessed 28 March 2017, [doi:10.1080/15027570.2010.537903](https://doi.org/10.1080/15027570.2010.537903). For more on this subject, see Peter Asaro, "On Banning Autonomous Weapon Systems: Human Rights, Automation, and the Dehumanization of Lethal Decision-making," *International Review of the Red Cross* 94, no. 886 (2012): 687–709.
30. Robert Sparrow, "Killer Robots," *Journal of Applied Philosophy* 24, no. 1 (2007): 62–77.
31. For more discussion on this topic, see Amitai Etzioni and Oren Etzioni, "Keeping AI Legal," *Vanderbilt Journal of Entertainment & Technology Law* 19, no. 1 (Fall 2016): 133–46, accessed 8 March 2017, [http://www.jetlaw.org/wp-content/uploads/2016/12/Etzioni\\_Final.pdf](http://www.jetlaw.org/wp-content/uploads/2016/12/Etzioni_Final.pdf).
32. Kenneth Anderson and Matthew C. Waxman, "Law and Ethics for Autonomous Weapon Systems: Why a Ban Won't Work and How the Laws of War Can," Stanford University, Hoover Institution Press, Jean Perkins Task Force on National Security and Law Essay Series, 9 April 2013.
33. Ibid.
34. Anderson and Waxman, "Law and Ethics for Robot Soldiers," *Policy Review* 176 (December 2012): 46.
35. George Lucas Jr., "Engineering, Ethics & Industry: the Moral Challenges of Lethal Autonomy," in *Killing by Remote Control: The Ethics of an Unmanned Military*, ed. Bradley Jay Strawser (New York: Oxford, 2013).
36. Ibid., 218.
37. Shane Reeves and William Johnson, "Autonomous Weapons: Are You Sure these Are Killer Robots? Can We Talk About It?," in Department of the Army Pamphlet 27-50-491, *The Army Lawyer* (Charlottesville, VA: Judge Advocate General's Legal Center and School, April 2014), 25–31.
38. Michael N. Schmitt, "Autonomous Weapon Systems and International Humanitarian Law: a Reply to the Critics," *Harvard National Security Journal*, 5 February 2013, accessed 28 March 2017, <http://harvardnsj.org/2013/02/autonomous-weapon-systems-and-international-humanitarian-law-a-reply-to-the-critics/>.
39. Gregory P. Noone and Diana C. Noone, "The Debate over Autonomous Weapons Systems," *Case Western Reserve Journal of International Law* 47, no. 1 (Spring 2015): 29, accessed 27 March 2017, <http://scholarlycommons.law.case.edu/jil/vol47/iss1/6/>.
40. Neil Davison, ed., *'Non-lethal' Weapons* (Houndmills, England: Palgrave Macmillan, 2009).
41. DOD Defense Science Board, *Task Force Report: The Role of Autonomy in DOD Systems*, 1.
42. DOD, *Unmanned Systems Integrated Roadmap FY2011-2036* (Washington, DC: Government Publishing Office [GPO], 2011), 43.
43. International Committee of the Red Cross (ICRC), Expert Meeting 26–28 March 2014 report, "Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects" (Geneva: ICRC, November 2014), 5.
44. Bonnie Docherty, *Losing Humanity: The Case against Killer Robots* (Cambridge, MA: Human Rights Watch, 19 November 2012), 2, accessed 10 March 2017, <https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots>.
45. Ibid.
46. Paul Marks, "Iron Dome Rocket Smasher Set to Change Gaza Conflict," *New Scientist Daily News* online, 20 November 2012, accessed 24 March 2017, <https://www.newscientist.com/article/dn22518-iron-dome-rocket-smasher-set-to-change-gaza-conflict/>.
47. Docherty, *Losing Humanity*, 2.
48. Ibid.; Patrick Lin, George Bekey, and Keith Abney, *Autonomous Military Robotics: Risk, Ethics, and Design* (Arlington, VA: Department of the Navy, Office of Naval Research, 20 December 2008), accessed 24 March 2017, [http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1001&context=phil\\_fac](http://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?article=1001&context=phil_fac).
49. "MK 15—Phalanx Close-In Weapons System (CIWS)" Navy Fact Sheet, 25 January 2017, accessed 10 March 2017, [http://www.navy.mil/navydata/fact\\_print.asp?cid=2100&tid=487&ct=2&page=1](http://www.navy.mil/navydata/fact_print.asp?cid=2100&tid=487&ct=2&page=1).
50. Paul Scharre and Michael Horowitz, "An Introduction to Autonomy in Weapons Systems" (working paper, Center for a New American Security, February 2015), 18, accessed 24 March 2017, <http://www.cnas.org/>.
51. Docherty, *Losing Humanity*, 2.





52. Thomas K. Adams, "Future Warfare and the Decline of Human Decisionmaking," *Parameters* 31, no. 4 (Winter 2001–2002): 57–71.

53. Docherty, *Losing Humanity*, 4.

54. DOD Directive 3000.09, *Autonomy in Weapon Systems* (Washington, DC: U.S. GPO, 21 November 2012), 2, accessed 10 March 2017, <http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf>.

55. Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University, 1966).

**Amitai Etzioni** is a professor of international relations at The George Washington University. He served as a senior advisor at the Carter White House and taught at Columbia University, Harvard Business School, and the University of California at Berkeley. A study by Richard Posner ranked him among the top one hundred American intellectuals. His most recent book is *Foreign Policy: Thinking Outside the Box* (2016).

**Oren Etzioni** is chief executive officer of the Allen Institute for Artificial Intelligence. He received a PhD from Carnegie Mellon University and a BA from Harvard University. He has been a professor at the University of Washington's computer science department since 1991. He was the founder or cofounder of several companies, including Farecast (later sold to Microsoft) and Decide (later sold to eBay), and the author of over one hundred technical papers that have garnered over twenty-five thousand citations.

## 'Holdout Humans': Chilling Glimpse Into Our Future if We Survive Another Million Years

By Anders Sandberg

Source: <https://www.sciencealert.com/holdout-humans-chilling-glimpse-into-our-future-if-we-survive-another-million-years>



Nov 30 – Most species are transitory. They go extinct, branch into new species or change over time due to random mutations and environmental shifts. A typical mammalian species can be expected to exist for [a million years](#). Modern humans, *Homo sapiens*, have been around for roughly 300,000 years. So what will happen if we make it to a million years?

Science fiction author H.G. Wells was the first to realise that humans could evolve into something very alien. In his 1883 essay, [Man in the year million](#), he envisioned what's now become a cliché: big-brained, tiny-bodied creatures. Later, he speculated that humans could also split into two or more new species.

While Wells's evolutionary models have not stood the test of time, the three basic options he considered still hold true. We could go extinct, turn into several species or change.

An added ingredient is that we have biotechnology that could greatly increase the probability of each of them. Foreseeable future technologies such as human enhancement (making ourselves smarter, stronger or in other ways better using drugs, microchips, genetics or other technology), brain emulation (uploading our brains to computers) or [artificial intelligence](#) (AI) may produce technological forms of new species not seen in biology.







### Software intelligence and AI

It is impossible to predict the future perfectly. It depends on fundamentally random factors: ideas and actions as well as currently unknown technological and biological limits.

But it is my job to explore the possibilities, and I think the most likely case is vast "speciation" – when a species splits into several others.

There are many among us who want to improve the human condition – slowing and abolishing ageing, enhancing intelligence and mood, and changing bodies – potentially leading to new species.

These visions, however, leave many cold.

It is plausible that even if these technologies become as cheap and ubiquitous as mobile phones, some people will refuse them on principle and build their self-image of being "normal" humans.

In the long run, we should expect the most enhanced people, generation by generation (or upgrade after upgrade), to become one or more fundamentally different "[posthuman species](#)" – and a species of holdouts declaring themselves the "real humans".

Through [brain emulation](#), a speculative technology where one scans a brain at a cellular level and then reconstructs an equivalent neural network in a computer to create a "software intelligence", we could go even further.

This is no mere speciation, it is leaving the animal kingdom for the mineral, or rather, software kingdom.

There are many reasons some might want to do this, such as boosting chances of immortality (by creating copies and backups) or easy travel by internet or radio in space.

Software intelligence has other advantages, too. It can be very [resource efficient](#) – a virtual being only needs energy from sunlight and some rock material to make microchips.

It can also think and change on the timescales set by computation, probably millions of times faster than biological minds. It can evolve in new ways – it just needs a software update.

Yet humanity is perhaps unlikely to remain the sole intelligent species on the planet.

Artificial intelligence is advancing rapidly right now. While there are profound uncertainties and disagreements about when or if it becomes conscious, artificial general intelligence (meaning it can understand or learn any intellectual problems like a human, rather than specialising on niche tasks) will arrive, a sizeable fraction of experts [think it is possible within this century](#) or sooner.

If it can happen, it probably will. At some point, we are likely to have a planet where humans have largely been replaced by software intelligence or AI – or some combination of the two.

### Utopia or dystopia?

Eventually, it seems plausible that most minds will become software. Research suggests that computers will soon become much more energy efficient than they are now. Software minds also won't need to eat or drink, which are inefficient ways of obtaining energy, and they can save power by running slower parts of the day.

This means we should be able to get [many more artificial minds per kilogram of matter](#) and watts of solar power than human minds in the far future. And since they can evolve fast, we should expect them to change tremendously over time from our current style of mind. Physical beings have a distinct disadvantage compared with software beings, moving in the sluggish, quaint world of matter. Still, they are self-contained, unlike the flitting software that will evaporate if their data centre is ever disrupted.

"Natural" humans may remain in traditional societies very unlike those of software people. This is not unlike the Amish people today, whose humble lifestyle is still made possible (and protected) by the surrounding United States. It is not given that surrounding societies have to squash small and primitive societies: we have established human rights and legal protections and something similar could continue for normal humans.

Is this a good future? Much depends on your values. A good life may involve having meaningful relations with other people and living in a peaceful and prosperous environment sustainably. From that perspective, weird posthumans are not needed; we just need to ensure that the quiet little village can function (perhaps protected by unseen automation).

Some may value "the human project", an unbroken chain from our palaeolithic ancestors to our future selves, but be open to progress. They would probably regard software people and AI as going too far, but be fine with humans evolving into strange new forms.

Others would argue what matters is freedom of self-expression and following your life goals. They may think we should explore the posthuman world widely and see what it has to offer.

Others may value happiness, thinking or other qualities that different entities hold and want futures that maximise these. Some may be uncertain, arguing we should hedge our bets by going down all paths to some extent.

### Dyson sphere?

Here's a prediction for the year one million. Some humans look more or less like us – but they are less numerous than they are now. Much of the surface is wilderness, having turned into a rewilding zone since there is far less need for agriculture and cities.





Here and there, cultural sites with vastly different ecosystems pop up, carefully preserved by robots for historical or aesthetic reasons. Under silicon canopies in the Sahara, trillions of artificial minds teem. The vast and hot data centres which power these minds once threatened to overheat the planet. Now, most orbit the Sun, forming a growing structure – a [Dyson sphere](#) – where each watt of energy powers thought, [consciousness](#), complexity and other strange things we do not have words for yet. If biological humans go extinct, the most likely reason (apart from the obvious and immediate threats right now) is a lack of respect, tolerance and binding contracts with other post-human species. Maybe a reason for us to start treating our own minorities better.

**Anders Sandberg** is a James Martin Research Fellow, Future of Humanity Institute & Oxford Martin School @ University of Oxford.

## Russia creates AI robot to rescue drowning people

Source [+video]: <https://www.rbth.com/science-and-tech/330612-russia-creates-ai-robot>



2019 – In late June, at the Army-2019 weapons show in the Moscow Region, Russian engineers unveiled their latest development – the Aurora search-and-rescue drone with artificial intelligence, able to independently find drowning people and transform into a life-raft.

### RADAR MMS

Russia Beyond interviewed the system developer, RADAR MMS. “The robot features AI and neurotechnologies, enabling it to search for people at sea with its ‘technical vision.’ It’s our own in-house development and knowhow,” said Ivan Antsev, executive director of RADAR MMS and a candidate of technical sciences (PhD in engineering). He explained that special neurons and data are loaded into the drone’s AI that are able to distinguish people from debris in the water. “Our robot is already being used by the Russian Ministry of Emergency Situations,” added Antsev. He noted that he knows of no such foreign developments able to autonomously search for people at a crash site and swim up to them.

### How does the drone get to the disaster zone?

At the crash site, *Aurora* is dropped from helicopters equipped with search locators, and optometric and radio-electronic stations. This type of helicopter can take off and land at







unequipped sites both in urban areas and at sea. At the same time, it is able to detect objects (ranging from a sinking ship to an oilfield) in conditions of heavy rain and fog, i.e. zero visibility.

Currently, there are two versions of the helicopter: large, which can carry up to 150 kg, and small, to which one Aurora drone is suspended.

Each of the machines monitors its vicinity at a range of several kilometers, and “sees” everything underwater at a depth of 100 meters from its bird’s-eye perspective.

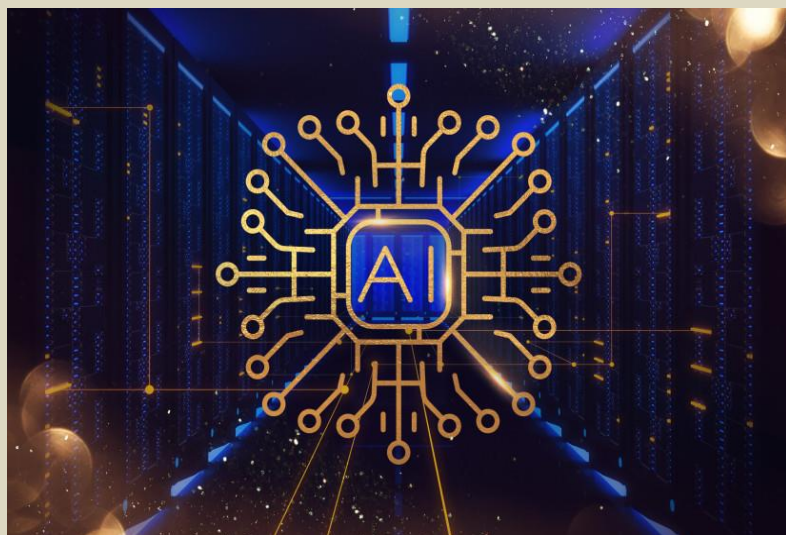
Besides the Ministry of Emergency Situations, RADAR MMS helicopter drones are deployed by Gazprom and Rosneft for rescue operations at oil-and-gas rigs at sea, and to search for new offshore deposits.

## Artificial intelligence in the service of the military

By Guy Avidan

Source: <https://www.jpost.com/opinion/article-724053>

Dec 05 – It is time to think outside the box of the battalion guard and implement a digital and operational transformation in the sentry guard in the IDF.



The incident of the criminal [break-in to the Tsnobar base](#) in the Golan Heights and [the theft of weapons and military ammunition](#) is a wake-up call for the IDF command to finally carry out technological reforms in the security of IDF bases.

We are all familiar with the defense and security tasks of IDF camps and infrastructures performed by combat soldiers and military combat supporters.

These missions are intended to enable the proper and safe existence of infrastructures, means and weapons of the army to fulfill its main mission, which is the defense of the country.

Since its establishment, Israel has been in constant conflict with enemies within the country’s borders and in the distant geographical circle, alongside daily dealings with terrorism within its borders.

### The IDF has to prevent harm to its assets

The ability of the army to meet its defense missions requires the continuous and complete availability and integrity of the infrastructure and means it needs while preventing its enemy from harming its essential assets.

Losing these resources through the theft of weapons, ammunition and equipment, damage to infrastructure and the like harms the military’s competence and ability to respond to threats, and harms the national resilience and [personal security of the country’s citizens](#), no less.

The defense industries in Israel, the military command and the Defense Ministry need to internalize that the security of our camps is not a secondary duty of guarding/security but a necessity for national security. Consequently, the responsibility for the [security of facilities](#) will be set as a high priority for the army commanders.

They will develop, among other things, a comprehensive doctrine of the use of advanced and diverse technologies in part that exist within the IDF and which can be supplemented with additional capabilities, starting with radars, day and night cameras, acoustic sensors and support systems for decision-making during an event, use of advanced systems based on artificial intelligence for facial recognition, classification, data storage and early warning systems.

### New technologies help organization

In the last two decades, the army has been equipped with [command and control systems](#) (C4I) to monitor and manage the organization’s resources, units, personnel and equipment. Thus, forming situational awareness, maintaining the current status of the forces, and constantly assessing the situation and location of enemy units and soldiers. This technology can easily be applied to monitoring military equipment and ammunition in the military, in police units and with first responders.





Retrieved weapons stolen from an IDF base in southern Israel (credit: ISRAEL POLICE)

Units can track their equipment using existing GNSS/GPS technologies, RFID applications and QR code cataloging, digital documentation of officials who came into contact with the specific equipment along the supply chain and storage, and digital transformation for the military warehouses and logistics infrastructure.



It is correct to examine civilian resources and economic optimization processes for merging military installations into the security sector. This will create in advance savings in operational and financial costs preventing the theft of military weapons by unauthorized and dangerous parties.

The stolen weapons captured by IDF and Israel Police on January 25, 2022 (credit: ISRAEL POLICE)

The sooner these technologies are implemented, the more trouble will be avoided.

**Guy Avidan** is the CTO of Asgard Systems, a technological innovation company that specializes in artificial intelligence applications and multidisciplinary engineering.







## Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights

Source: <https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/>

Nov 06 – The Council has adopted its common position ('general approach') on the **Artificial Intelligence Act**. Its aim is to ensure that artificial intelligence (AI) systems placed on the EU market and used in the Union are **safe** and respect existing law on **fundamental rights** and Union values.

Artificial Intelligence is of paramount importance for our future. Today, we managed to achieve a delicate balance which will boost innovation and uptake of artificial intelligence technology across Europe. With all the benefits it presents, on the one hand, and full respect of the fundamental rights of our citizens, on the other.

The draft regulation presented by the Commission in April 2021 is a key element of the EU's policy to foster the development and uptake across the single market of **safe and lawful** AI that respects fundamental rights.

The proposal follows a **risk-based approach** and lays down a uniform, **horizontal legal framework for AI** that aims to ensure legal certainty. It promotes investment and innovation in AI, enhances **governance and effective enforcement** of existing law on fundamental rights and safety, and facilitates the development of a single market for **AI applications**. It goes hand in hand with other initiatives, including the Coordinated Plan on Artificial Intelligence which aims to accelerate investment in AI in Europe.

### Definition of an AI system

To ensure that the **definition** of an AI system provides sufficiently clear criteria for distinguishing AI from simpler software systems, the Council's text narrows down the definition to systems developed through machine learning approaches and logic- and knowledge-based approaches.

### Prohibited AI practices

Concerning **prohibited AI practices**, the text extends to private actors the prohibition on using AI for **social scoring**. Furthermore, the provision prohibiting the use of AI systems that exploit the vulnerabilities of a specific group of persons now also covers persons who are **vulnerable due to their social or economic situation**.

As regards the prohibition of the use of 'real-time' remote biometric identification systems in publicly accessible spaces by **law enforcement authorities**, the text clarifies the objectives where such use is strictly necessary for law enforcement purposes and for which law enforcement authorities should therefore be exceptionally allowed to use such systems.

### Classification of AI systems as high-risk

Regarding the **classification of AI systems as high-risk**, the text adds a horizontal layer on top of the high-risk classification, to ensure that AI systems that are not likely to cause serious fundamental rights violations or other significant risks are not captured.

### Requirements for high-risk AI systems

Many of the **requirements** for high-risk AI systems have been clarified and adjusted in such a way that they are more technically feasible and less burdensome for stakeholders to comply with, for example as regards the quality of data, or in relation to the technical documentation that should be drawn up by SMEs to demonstrate that their high-risk AI systems comply with the requirements.

Since AI systems are developed and distributed through complex value chains, the text includes changes clarifying the allocation of responsibilities and roles of the various actors in those chains, in particular providers and users of AI systems. It also clarifies the relationship between responsibilities under the AI Act and responsibilities that already exist under other legislation, such as the relevant Union data protection or sectorial legislation, including as regards the financial services sector.

### General purpose AI systems

New provisions have been added to account of situations where AI systems can be used for many different purposes (**general purpose AI**), and where general purpose AI technology is subsequently integrated into another high-risk system.

The text specifies that certain requirements for high-risk AI systems would also apply to general purpose AI systems in such cases. However, instead of direct application of these requirements, **an implementing act** would specify how they should be applied in relation to general purpose AI systems, based on a consultation and detailed impact assessment and considering specific characteristics of these systems and related value chain, technical feasibility and market and technological developments.





### Scope and provisions relating to law enforcement authorities

An explicit reference has been made to the exclusion of **national security, defence, and military purposes** from the scope of the AI Act. Similarly, it has been clarified that the AI Act should not apply to AI systems and their outputs used for the sole purpose of research and development and to obligations of people using AI for non-professional purposes, which would fall outside the scope of the AI Act, except for the transparency obligations.

Considering the specificities of law enforcement authorities, several changes have been made to provisions relating to the use of AI systems for law enforcement purposes. Notably, subject to appropriate safeguards, these changes are meant to reflect the need to respect the confidentiality of sensitive operational data in relation to their activities.

### Compliance framework and AI Board

To simplify the compliance framework for the AI Act, the text contains several clarifications and simplifications to the provisions on the **conformity assessment** procedures.

The provisions related to **market surveillance** have also been clarified and simplified to make them more effective and easier to implement. The text also substantially modifies the provisions concerning the **AI Board**, aiming to ensure that it has greater autonomy and to strengthen its role in the governance architecture for the AI Act. In order to ensure the **involvement of the stakeholders** in relation to all issues related to the implementation of the AI Act, including the preparation of implementing and delegated acts, a new requirement has been added for the Board to create a permanent subgroup serving as a platform for a wide range of stakeholders. As regards **penalties** for infringements of the provisions of the AI Act, the text provides for more proportionate caps on administrative fines for SMEs and start-ups.

### Transparency and other provisions in favour of the affected persons

The text includes several changes that increase **transparency** regarding the use of high-risk AI systems. Notably, some provisions have been updated to indicate that certain users of a high-risk AI system that are public entities will also be obliged to register in the EU database for high-risk AI systems.

Moreover, a newly added provision puts emphasis on an obligation for users of an **emotion recognition system** to inform natural persons when they are being exposed to such a system.

The text also makes it clear that a natural or legal person may make a complaint to the relevant **market surveillance authority concerning non-compliance with the AI Act** and may expect that such a complaint will be handled in line with the dedicated procedures of that authority.

### Measures in support of innovation

With a view to creating a legal framework that is more innovation-friendly and to promoting evidence-based regulatory learning, the provisions concerning **measures in support of innovation** have been substantially modified in the text.

Notably, it has been clarified that AI **regulatory sandboxes**, which are supposed to establish a controlled environment for the development, testing and validation of innovative AI systems, should also allow for testing of innovative AI systems in real world conditions.

Furthermore, new provisions have been added allowing **unsupervised real-world testing** of AI systems, under specific conditions and safeguards. In order to **alleviate the administrative burden for smaller companies**, the text includes a list of actions to be undertaken to support such operators, and it provides for some limited and clearly specified derogations.

### Next steps

The adoption of the general approach will allow the Council to enter negotiations with the European Parliament (**'trilogues'**) once the latter adopts its own position with a view to reaching an agreement on the proposed regulation.

## The geopolitics of AI and the rise of digital sovereignty

By Benjamin Cedric Larsen

Source: <https://www.brookings.edu/research/the-geopolitics-of-ai-and-the-rise-of-digital-sovereignty/>

Dec 08 – On September 29, 2021, the United States and the European Union's (EU) new Trade and Technology Council (TTC) held their first summit. It took place in the old industrial city of Pittsburgh, Pennsylvania, under the leadership of the European Commission's Vice-President, Margrethe Vestager, and U.S. Secretary of State Antony Blinken. Following the meeting, the U.S. and the EU declared their opposition to artificial intelligence (AI) that does not respect human rights and referenced rights-infringing







systems, such as social scoring systems.<sup>[1]</sup> During the meeting, the TTC clarified that “The United States and European Union have significant concerns that authoritarian governments are piloting social scoring systems with an aim to implement social control at scale. These systems pose threats to fundamental freedoms and the rule of law, including through silencing speech, punishing peaceful assembly and other expressive activities, and reinforcing arbitrary or unlawful surveillance systems.”<sup>[2]</sup>

The implicit target of the criticism was China’s “social credit” system, a big data system that uses a wide variety of data inputs to assess a person’s social credit score, which determines social permissions in society, such as buying an air or train ticket.<sup>[3]</sup> The critique by the TTC indicates that the U.S. and the EU disagree with China’s view of how authorities should manage the use of AI and data in society.<sup>[4]</sup> The TTC can therefore be viewed as the beginning steps towards forming an alliance around a human rights-oriented approach to the development of artificial intelligence in democratic countries, which contrasts with authoritarian countries such as Russia and China. However, these different approaches may lead to technological decoupling, conceptualized as national strategic decoupling of otherwise interconnected technologies such as 5G, hardware such as computer chips, and software such as operating systems. Historically, the advent of the world wide web created an opportunity for the world to be interconnected as one global digital ecosystem. Growing mistrust between nations, however, has caused a rise in digital sovereignty, which refers to a nation’s ability to control its digital destiny and may include control over the entire AI supply chain, from data to hardware and software. A consequence of the trend toward greater digital sovereignty—which then drives the trend further—is increasing fear of being cut off from critical digital components such as computer chips and a lack of control over the international flow of citizens’ data. These developments threaten existing forms of interconnectivity, causing markets for high technology to fragment and, to varying degrees, retrench back into the nation state.

To understand the extent to which we are moving towards varying forms of technological decoupling, this article first describes the unique positions of the European Union, United States and China concerning regulation of data and the governance of artificial intelligence. The article then discusses implications of these different approaches for technological decoupling, and then discusses implications for specific policies around AI, such as the U.S. [Algorithmic Accountability Act](#), the EU’s [AI Act](#), and China’s [regulation of recommender engines](#).

### Europe: A holistic AI governance regime

The EU has, in many ways, been a frontrunner in data regulation and AI governance. The European Union’s [General Data Protection Regulation](#) (GDPR), which went into effect in 2018, set a precedent for regulating data. This is seen in how the legislation has [inspired](#) other acts, e.g., the [California Consumer Privacy Act](#) (CCPA) and China’s [Personal Information Protection Law](#) (PIPL). The [EU’s AI Act \(AIA\)](#), which could go into effect by 2024, also constitutes a new and groundbreaking risk-based regulation of artificial intelligence, which, together with the [Digital Markets Act \(DMA\)](#) and [Digital Services Act \(DSA\)](#), creates a holistic approach to how authorities seek to govern the use of AI and information technology in society.

The EU AI Act establishes a horizontal set of rules for developing and using AI-driven products, services, and systems within the EU. The Act is modelled on a risk-based approach that moves from unacceptable risks (e.g., social credit scoring and use of facial recognition technologies for real-time monitoring of public spaces), to high risk (e.g., AI systems used in hiring and credit applications), to limited risk (e.g., a chatbot) to little or no risk (e.g., AI-enabled video games or spam filters). While AI systems that pose unacceptable risks are outrightly banned, high-risk systems will be subject to conformity assessments, including independent audits and new forms of oversight and control. Limited risk systems are subject to transparency obligations, such as user-facing information when interacting with a chatbot. In contrast, little or no risk systems remain unaffected by the AI Act.<sup>[5]</sup>

The EU Digital Markets Act (DMA) attempts, among other things, to ensure that digital platforms that possess so-called gatekeeper functions, in their access to and control of large swaths of consumer data, do not exploit their data monopolies to create unequal market conditions. The implicit goal is to increase (European) innovation, growth, and competitiveness.

Similarly, the EU Digital Services Act (DSA) seeks to give consumers more control over what they see online. This means, for example, better information about why specific content is recommended through recommender engines and the possibility of opting out of recommender-based profiling. The new rules aim to protect users from illegal content and aim to tackle harmful content, such as political or health-related misinformation. In effect, this carves out new responsibilities for very large platforms and search engines to engage in some forms of content moderation. This means that gatekeeper platforms are considered responsible for mitigating against risks such as disinformation or election manipulation, balanced against restrictions on freedom of expression, and subject to independent audits.

The aim of these new laws is not only to ensure that the rights of EU citizens are upheld in the digital space but also to make sure that European companies have a better opportunity to compete against large U.S. tech firms. One way of doing this is to mandate compatibility requirements between digital products and services. Such compatibility requirements have already required Apple to change the standard of its charger starting in 2024<sup>[6]</sup> and could also require greater interoperability between messaging services such as Apple’s iMessage, Meta’s WhatsApp, Facebook Messenger, Google Chat, and Microsoft Teams.<sup>[7]</sup> While





increased interoperability could increase the vulnerability and complexity of security-related issues, instituting such changes would arguably make it harder for companies to secure market share and continue their network-driven forms of dominance.

At the same time, the EU is trying to build ties to U.S. tech companies by opening an office in the heart of Silicon Valley headed by Gerard de Graaf, the European Commission's director of digital economy, who is expected to establish closer contact with companies such as Apple, Google, and Meta.<sup>[8]</sup> The strategic move by the EU is also going to serve as a mechanism to ensure that American tech companies comply with new European rules such as the AIA, DMA, and DSA.

Concerning semiconductors, European Commission President Ursula von der Leyen announced the European Chips Act in February 2022, intending to make the EU a leader in semiconductor manufacturing.<sup>[9]</sup> By 2030, the European share of global semiconductor production is expected to more than double, increasing from 9 to 20%. The European Chips Act is a response to the U.S. CHIPS and Science Act and China's ambitions to achieve digital sovereignty through the development of semiconductors. Semiconductors are the cornerstone of all computers and, thus, are integral for developing artificial intelligence. Strategic policies such as the European Chips Act suggest that control over the computer-based part of the AI value chain and the politicization of high-tech development will only become more important in coming years.

The largest tech companies—Apple, Amazon, Google, Microsoft, Alibaba, Baidu, Tencent, and others—are mostly found in the U.S. and China, not in Europe. To address this imbalance, the EU aims to set the regulatory agenda for public governance of the digital space. The new regulations aim to ensure that international companies comply with European rules while strengthening the EU's resolve to obtain digital sovereignty.

### US: A light-touch approach to AI governance

The United States' approach to artificial intelligence is characterized by the idea that companies, in general, must remain in control of industrial development and governance-related criteria.<sup>[10]</sup> So far, the U.S. federal government has opted for a hands-off approach to governing AI in order to create an environment free of burdensome regulation. The government has repeatedly stated that "burdensome" rules and state regulations often are considered "barriers to innovation,"<sup>[11] [12]</sup> which must be reduced, for example, in areas such as autonomous vehicles.

The U.S. also takes a different approach than the EU and China in the area of data regulation. The U.S. has not yet drawn up any national policy on data protection, such as in the EU, where in 2018 the GDPR introduced a harmonized set of rules across the EU. By comparison, only five out of 50 U.S. states—California, Colorado, Connecticut, Utah, and Virginia—have adopted comprehensive data legislation.<sup>[13]</sup> As a result, California's Consumer Privacy Act (CCPA), effective in 2020, has, to some extent, become the U.S.'s *de facto* data regulation.<sup>[14]</sup> The GDPR in many ways served as a model for CCPA, which requires companies to give consumers increased privacy rights, including the right to access and delete any personal data as well as the right to opt-out of having data sold and be free from online discrimination.

Section 230 of the Communications Decency Act protects platforms from liability for content posted. Under current law, liability for content remains with users who post it.<sup>[15]</sup> In part due to this focus on users rather than platforms, in the U.S. there is little oversight of recommender engines that rank, organize, and determine the visibility of information across search engines and social media platforms. Content moderation is a thorny issue, however. On the one hand, there is an argument to be made for platforms to engage in content moderation to avoid overly discriminatory and harmful behavior online. On the other hand, states such as Texas, and Florida, among others, are passing laws prohibiting tech companies from "censoring" users, which are enacted to protect their constituents' rights to free speech.<sup>[16]</sup> The counterargument made by platforms is that their content moderation decisions, as well as their use of recommender engines, is a form of expression that should be protected by the First Amendment, which defends American citizens and companies from government restraints on speech.<sup>[17]</sup>

While the United States takes a *laissez-faire* approach to regulating artificial intelligence, that tends to be fragmented at the state level, new industrial policy initiatives are aimed explicitly at strengthening certain aspects of the AI supply chain. One example is the CHIPS and Science Act, where Democrats and Republicans have come together to create new incentives for producing semiconductors on American soil.<sup>[18]</sup> Based on the idea of digital sovereignty, the CHIPS and Science Act marks a shift in U.S. industrial policy to address renewed concerns over maintaining U.S. technological leadership in the face of fast-growing competition from China.

When it comes to using artificial intelligence in the public sector, the United States has experienced significant opposition from civil society, especially to law enforcement's use of facial recognition technologies (FRT), for example, from the American Civil Liberties Union (ACLU).<sup>[19]</sup> Again, the U.S. approach has been fragmented. Several cities—such as Boston, Minneapolis, San Francisco, Oakland, and Portland—have banned government agencies, including the police, from using FRT. "It does not work. African Americans are 5-10 times more likely to be misidentified," said Alameda Council member John Knox White, who helped ban facial recognition in Oakland in 2019.<sup>[20]</sup>

In the United States, a March 2021 report by the country's National Security Commission on Artificial Intelligence (NSCAI) defined the "AI race" (between China and the United States) as a value-based







competition in which China must be seen as a direct competitor.<sup>[21]</sup> In the report, NSCAI went further and recommended creating so-called “choke points” that limit Chinese access to American semiconductors to stall progress in some areas of technological development.<sup>[22]</sup> Some of these “choke points” were seen in August 2022, when the U.S. Department of Commerce banned Nvidia from selling its A100, A100X, and H100 computer graphics processing units (GPUs) to customers in China, in a move intended to slow China’s progress in semiconductor development and prevent advanced chips from being used for military applications in China. The Department of Commerce justified the move by saying it was meant to “keep advanced technologies out of the wrong hands,” while Nvidia has signaled that it will have serious consequences for its global sales of semiconductors.<sup>[23]</sup>

Over the years, however, many Chinese researchers have contributed to important breakthroughs in AI-related research in the United States. U.S. companies such as Microsoft Research Asia (MSRA), headquartered in Beijing, have also played a crucial role in nurturing Chinese talent in AI. Several former MSRA researchers have gone on to spearhead China’s technological development in leading companies such as Baidu.<sup>[24]</sup> Against the background of growing mistrust between the United States and China, these forms of cooperation are suffering, resulting in rethinking existing ties in areas of technological collaboration.

Over the long run, ongoing technological decoupling could contribute to a bifurcation of digital ecosystems. The Bureau of Industry and Security’s (BIS) Entity List arguably contributes to these developments by blacklisting entities on the list from doing business with U.S. enterprises. In terms of software, these developments are already happening. Google, for example, stopped providing access to its Android operating system (OS) to Huawei after the company was placed on the Entity List. These developments caused Huawei’s sales of smartphones to plummet on international markets due to a sudden lack of access to Android’s (OS) and app store, hurting interoperability between hardware and apps and services.<sup>[25]</sup> These developments have resulted in Huawei doubling down on developing its own proprietary operating system, HarmonyOS, for use across its products.<sup>[26]</sup>

In terms of AI-related regulation, the U.S. Algorithmic Accountability Act was reintroduced in 2022, but it has not been approved in either the Senate or the House of Representatives, where it was first introduced in 2019. Should the Act be passed, it would require companies that develop, sell, and use automated systems to be subject to new rules related to transparency and when and how AI systems are used. In the absence of national legislation, some states and cities have started to implement their own regulations, such as New York City’s Law on Automated Employment Decision Tools. The law stipulates that any automated hiring system used on or after January 1, 2023, in NYC, must undergo a bias audit consisting of an impartial evaluation by an independent auditor, including testing to assess potential disparate impact on some groups.<sup>[27]</sup>

### China: a budding AI governance regime

China’s approach to AI legislation is evolving rapidly and is heavily based on central government guidance. Implementing China’s national AI strategy in 2017<sup>[28]</sup> was a crucial step in moving the country from a lax governance regime to establishing stricter enforcement mechanisms across data and algorithmic oversight. In 2021, China implemented the Personal Information Protection Law (PIPL), a national data regulation inspired by the GDPR. PIPL entails that companies operating in China must classify and store their data locally within the country—an element critical in establishing digital sovereignty. Under the law, companies that process data categorized as “sensitive personal information” must seek separate consent from these individuals, state why they process this data, and explain any effects of data-related decision-making. Like the GDPR, PIPL gives China’s consumers increased rights while companies have become subject to stricter national oversight and data-related controls, enhancing trust in the digital economy.

In terms of AI regulation, China oversees recommender engines through the “Internet Information Service Algorithmic Recommendation Management Provisions”<sup>[29]</sup> which went into effect in March 2022, the first regulation of its kind worldwide. The law gives users new rights, including the ability to opt-out of using recommendation algorithms and delete user data. It also creates higher transparency regarding where and how recommender engines are used. The regulation goes further, however, with its content moderation provisions, which require private companies to actively promote “positive” information that follows the official line of the Communist Party. It includes promoting patriotic, family-friendly content and focusing on positive stories aligned with the party’s core values.<sup>[30]</sup> Extravagance, over-consumption, antisocial behavior, excessive interest in celebrities, and political activism are subject to stricter control: Platforms are expected to intervene actively and regulate this behavior.<sup>[31]</sup> Therefore, China’s regulation of recommendation algorithms goes far beyond the digital space by dictating what type of behavior China’s central government considers favorable or not in society.

Unlike the United States, Chinese regulations put the responsibility on private companies to moderate, ban, or promote certain types of content. However, China’s regulation of recommender engines can be complicated—both for companies to implement and for regulators to enforce—because the law often may be interpreted arbitrarily.<sup>[32]</sup> The regulation could further accelerate the decoupling of practices for companies operating in China and international markets.

In terms of innovation, China’s central government has strengthened private partnerships with China’s leading technology companies. Several private companies, including Baidu, Alibaba, Huawei, and SenseTime, among others, have been elevated to “national champions” or informally to members of China’s “national AI team”<sup>[33]</sup> responsible for strengthening China’s AI ecosystem.<sup>[34]</sup>





The result is that technology giants such as Baidu, Alibaba, and others have moved into the upper echelons of China's centrally planned economy. And precisely because of these companies' importance to the social and economic development of the country, the government is bringing them closer to the long-term strategic goals of the Communist Party. These developments include experimenting with mixed forms of ownership, for example where government agencies acquire minority stakes in private companies through state-run private equity funds and then fill board seats with members of the Communist Party.<sup>[35]</sup> Other measures include banning sectors that do not live up to the Party's long-term priorities. One of these was China's for-profit educational technology sector, which was banned in 2021 because the party wanted to curb inequality in education.<sup>[36]</sup>

In China, the state is playing a central and growing role in adopting facial recognition technologies to monitor public spaces. According to Chinese government estimates, up to 626 million facial recognition cameras were installed in the country by 2020.<sup>[37]</sup> Huge public sector demand has not surprisingly contributed to making China a world leader in developing AI related to facial recognition. Meanwhile, pushback by civil society continues to play a marginal role in China compared to the United States, which makes it more difficult for the population to question the government's use of AI in society.

While the U.S. and the EU only recently have launched new initiatives and industrial policies explicitly aimed at semiconductors, China has long nurtured its chip industry. In 2014, for instance, the National Integrated Circuit Industry Investment Fund was established to make China a world leader in all segments of the chip supply chain by 2030.<sup>[38]</sup> While China still lags far behind the U.S. in semiconductor development, it is an area of the AI value chain that receives continued attention from China's central government, as it is critical for the country's ambitions of achieving AI leadership by 2030.

Regarding how AI intersects with social values, China's latest five-year plan states that technological development aims to promote social stability.<sup>[39]</sup> Artificial intelligence should therefore be seen as a social control tool in "the great transformation of the Chinese nation,"<sup>[40]</sup> which implies maintaining a balance between social control and innovation.<sup>[41]</sup>

### The desire for self-sufficiency

The ideological differences between the three great powers could have broader geopolitical consequences for managing AI and information technology in the years to come. Control over strategic resources, such as data, software, and hardware has become paramount to decisionmakers in the United States, the European Union, and China, resulting in a neo-mercantilist-like approach to governance of the digital space. Resurfacing neo-mercantilist ideas are most visible in the ways that trade in semiconductors is being curtailed, but they are also apparent in discussions over international data transfers, resources linked to cloud computing, the use of open-source software, and so on. These developments seem to increase fragmentation, mistrust, and geopolitical competition, as we have seen in the case of communication technologies such as 5G. The United States, Canada, England, Australia, and several European countries have excluded Chinese 5G providers, such as Huawei and ZTE, due to growing mistrust about data security and the fear of surveillance of citizens by China's central government.<sup>[42]</sup>

As technological decoupling deepens, China will seek to maintain its goal of achieving self-sufficiency and technical independence, especially from high-tech products originating in the United States. As recently as May 2022, China's central government ruled that central government agencies and state-subsidized companies must replace computers from foreign-owned manufacturers within two years.<sup>[43]</sup> That includes phasing out Windows OS, which will be replaced by Kylin OS, developed by China's National University of Defense Technology.

Regarding open-source code repositories such as GitHub (owned by Microsoft), China has also signaled that it seeks to diminish its reliance on foreign-developed open-source software. In 2020, for instance, the Ministry of Industry and Information Technology (MIIT) publicly endorsed Gitee as the country's domestic alternative to GitHub.<sup>[44]</sup> While the development of leading open-source deep learning frameworks continues to be led by U.S. technology enterprises—e.g., TensorFlow (Google) and PyTorch (Meta)—Chinese alternatives developed by national champions such as PaddlePaddle (Baidu) and Mindspore (Huawei), among others, are growing in scope and importance within China. These developments illustrate that achieving self-sufficiency in open-source software development such as deep learning frameworks are on the political agenda of China's central government, feeding into its long-term desire for achieving digital sovereignty.

Certain U.S. policies, such as placing a growing number of Chinese companies on the BIS Entity List, will make it more difficult for China's central government to rely on strategic technical components from the United States as part of the country's economic growth strategy, thus incentivizing China to continue toward its goal of achieving technological self-sufficiency. These developments mean that previous forms of cooperation across the Pacific, e.g., in terms of academic research and corporate R&D, are quietly diminishing. These developments may complicate the possibilities for finding new international solutions to harmonization of AI use and legislation. While the U.S. and EU diverge on AI regulation, focused on self-regulation versus comprehensive regulation of the digital space, respectively, they continue to share a fundamental approach to artificial intelligence based on respect for human rights. This approach is now slowly being operationalized to condemn the use of AI for social surveillance and control purposes, as witnessed in China, Russia, and other authoritarian countries. To some extent, "American" and "European" values are evolving into an







ideological mechanism that aims to ensure a human rights-centered approach to the role and use of AI.<sup>[45]</sup> Put differently, an alliance is currently forming around a human rights-oriented view of socio-technical governance, which is embraced and encouraged by like-minded democratic nations. This view strongly informs how public sector authorities should relate to and handle the use of AI and information technology in society.

**Where are we headed?**

On May 15, 2022, the United States and EU TTC held its second summit, this time in Saclay, a suburb of Paris and one of France's leading research and business clusters. Secretary Blinken and Vice President Vestager met again to promote transatlantic cooperation and democratic approaches to trade, technology, and security. The meeting ultimately strengthened the strategic relationship across the Atlantic in several specific areas, including engaging in more detailed information exchange on exports of critical technology to authoritarian regimes such as Russia. The United States and the EU will also engage in greater coordination of developing evaluation and measurement tools that contribute to credible AI, risk management, and privacy-enhancing technologies. A Strategic Standardization Information (SSI) mechanism will also be set up to enable greater exchange of information on international technology standards—an area in which China is expanding its influence. In addition, an early warning system is being discussed to better predict and address potential disruptions in the semiconductor supply chain. This discussion includes developing a transatlantic approach to continued investment in long-term security in supply for the EU/U.S. market.<sup>[46]</sup>

While the TTC is slowly cementing the importance of the U.S. and the EU's democratic transatlantic alliance in artificial intelligence, the gap between the U.S. and China seems to widen. The world is, therefore, quietly moving away from a liberal orientation based on global interoperability, while technological development increasingly is entangled in competition between the governments of the United States and China. These developments diminish the prospects for finding international forms of cooperation on AI governance,<sup>[47]</sup> and could contribute to a Balkanization of technological ecosystems. The result, already partially underway, would be the emergence of a "Chinese" network and its digital ecosystem, a U.S. and a European one, each with its own rules and governing idiosyncrasies. In the long run, this may mean that it will be much more difficult to agree on how more complicated forms of artificial intelligence should be regulated and governed. At present, the EU and China do seem to agree on taking a more active approach to regulating AI and digital ecosystems relative to the U.S. This could change, however, if the U.S. were to pass the Algorithmic Accountability Act. Like the EU AI Act, the Algorithmic Accountability Act requires organizations to perform impact assessments of their AI systems before and after deployment, including providing more detailed descriptions on data, algorithmic behavior, and forms of oversight.

Should the U.S. choose to adopt the Algorithmic Accountability Act, the regulatory approaches of the EU and the U.S. would be better aligned. Even though regulatory regimes may align over time, the current trajectory of digital fragmentation between the EU and US on one side, and China on the other, is set to continue under the current political climate.

Undoubtedly, AI will continue to revolutionize society in the coming decades. However, it remains uncertain whether the world's countries can agree on how technology should be implemented for the greatest possible societal benefit. As stronger forms of AI continue to emerge across a wider range of use cases, securing AI alignment at the international level, could be one of the most significant challenges of the 21st century.

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

[Benjamin Cedric Larsen](#) is AI/ML Project Lead at the World Economic Forum's Center for the Fourth Industrial Revolution in San Francisco. Benjamin's research focuses broadly on 'AI Governance,' including industrial policy, AI regulation, and AI innovation. He writes for the Series, [The Economics and Regulation of Artificial Intelligence and Emerging Technologies](#), as part of the [Brookings Center on Regulation and Markets](#).

**New AI System Enables Multiple Robots to Recognize YOU**

Source: <https://i-hls.com/archives/117353>

Dec 10 – A new AI system will enable multiple robots to recognize people. A Japanese company has developed an AI system that makes it possible for multiple moving robots to identify people whose images have been uploaded in advance.

This new ability was examined during a pilot test in which images sent from robots in various locations within an event space were analyzed and compiled in the cloud using an AI engine. By utilizing the AI system, robots could identify specific people from camera images sent by various types of robots and to perform cloud-based confirmation. According to [eenewseurope.com](#), The test also demonstrated that people's locations could be pinpointed by using the positions of the robots.



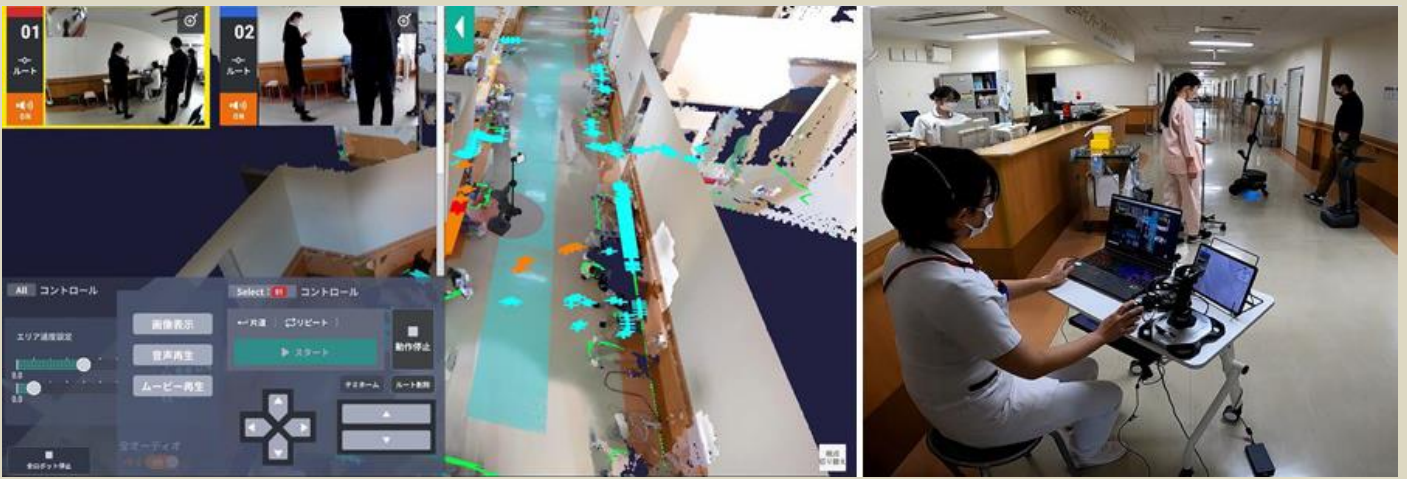


Image from the TransBots™ VR simulator (left) and multiple different robots being controlled simultaneously (right) as part of a pilot test to support nursing operations – ©Toppan Inc.

**TransBots** is a digital twin solution developed by Toppan that uses virtual reality (VR) and computer vision (CV) technologies for remote, central management and control of multiple types of service robots. “Even before the COVID-19 pandemic, Japan was looking at ways to reduce the workload for nursing and care services, including the use of robots,” said Tomoichiro Shibue, deputy head of Toppan’s Business Innovation Center. “TransBots can facilitate the use and control of robots for diverse services in healthcare settings and the results of this pilot test will enable us to refine the solution towards practical implementation.”

**ChatGPT Could Revolutionize The Internet, But Its Secrets Have Experts Worried**

By Toby Walsh

Source: <https://www.sciencealert.com/chatgpt-could-revolutionize-the-internet-but-its-secrets-have-experts-worried>



Dec 15 – ChatGPT is the latest and most impressive artificially intelligent chatbot yet. It was released two weeks ago, and in just five days hit a million users. It’s being used so much that its servers have [reached capacity several times](#). OpenAI, the company that developed it, is already being discussed as a potential Google slayer. Why look up something on a search engine when ChatGPT can write a whole paragraph explaining the answer? (There’s even [a Chrome extension](#) that lets you do both, side by side.)  
But what if we never know the secret sauce behind ChatGPT’s capabilities?  
The chatbot takes advantage of a number of technical advances published in open scientific literature in the past couple of decades. But any innovations unique to it are secret. OpenAI could well be trying to build a technical and business moat to keep others out.







### What it can (and can't do)

[ChatGPT](#) is very capable. Want a haiku on chatbots? Sure.

Chatbots, oh so wise  
Endlessly processing  
Answers from the void.

How about a joke about chatbots? No problem.

Why did the chatbot cross the road?  
To get to the other side – of your screen!

ChatGPT can do [many other tricks](#). It can write [computer code](#) to a user's specification, draft business letters or rental contracts, compose homework essays and even pass university exams.

Just as important is what ChatGPT can't do. For instance, it struggles to distinguish between truth and falsehood. It is also often a persuasive liar.

What is the fastest marine mammal?  
The fastest marine mammal is the sailfish.  
The sailfish is not a mammal.

You are correct, the sailfish is not a mammal. I apologize for the mistake. The fastest marine mammal is the peregrine falcon.

ChatGPT is a bit like autocomplete on your phone. Your phone is trained on a dictionary of words so it completes words. ChatGPT is trained on pretty much all of the web, and can therefore complete whole sentences – or even whole paragraphs. However, it doesn't understand what it's saying, just what words are most likely to come next.

### Open only by name

In the past, advances in AI have been accompanied by peer-reviewed literature.

In 2018, for example, when the Google Brain team developed the BERT neural network on which most natural language processing systems are now based (and we suspect ChatGPT is too), the methods were published in peer-reviewed scientific papers and the code [was open-sourced](#).

And in 2021, DeepMind's AlphaFold 2, a protein-folding software, was *Science's* [Breakthrough of the Year](#). The software and its results were open-sourced so scientists everywhere could use them to advance biology and medicine.

Following the release of ChatGPT, we have only a short blog post describing how it works. There has been no hint of an accompanying scientific publication, or that the code will be open-sourced.

To understand why ChatGPT could be kept secret, you have to understand a little about the company behind it.

OpenAI is perhaps one of the oddest companies to emerge from Silicon Valley. It was [set up as a non-profit](#) in 2015 to promote and develop "friendly" AI in a way that "benefits humanity as a whole". [Elon Musk](#), Peter Thiel and other leading tech figures pledged US\$1 billion towards its goals.

Their thinking was we couldn't trust for-profit companies to develop increasingly capable AI that aligned with humanity's prosperity. AI therefore needed to be developed by a non-profit and, as the name suggested, in an open way.

In 2019 OpenAI [transitioned into](#) a capped for-profit company (with investors limited to a maximum return of 100 times their investment) and took a US\$1 billion investment from Microsoft so it could scale and compete with the tech giants.

It seems money got in the way of OpenAI's initial plans for openness.

### Profiting from users

On top of this, OpenAI appears to be using feedback from users to filter out the fake answers ChatGPT hallucinates.

According to [its blog](#), OpenAI initially used reinforcement learning in ChatGPT to downrank fake and/or problematic answers using a costly hand-constructed training set.

But ChatGPT now seems to be being tuned by its more than a million users. I imagine this sort of human feedback would be prohibitively expensive to acquire in any other way.

We are now facing the prospect of a significant advance in AI using methods that are not described in the scientific literature and with datasets restricted to a company that appears to be open only in name.

### Where next?

In the past decade, AI's rapid advance has been in large part due to openness by academics and businesses alike. All the major AI tools we have are open-sourced.

But in the race to develop more capable AI, that may be ending. If openness in AI dwindles, we may see advances in this field slow down as a result. We may also see new monopolies develop.





And if history is anything to go by, we know a lack of transparency is a trigger for bad behavior in tech spaces. So while we go on to laud (or critique) ChatGPT, we shouldn't overlook the circumstances in which it has come to us. Unless we're careful, the very thing that seems to mark the golden age of AI may in fact mark its end.

**Toby Walsh** is a Professor of AI at UNSW, Research Group Leader @ UNSW Sydney.

## Deep Learning – Weaknesses and Vulnerabilities

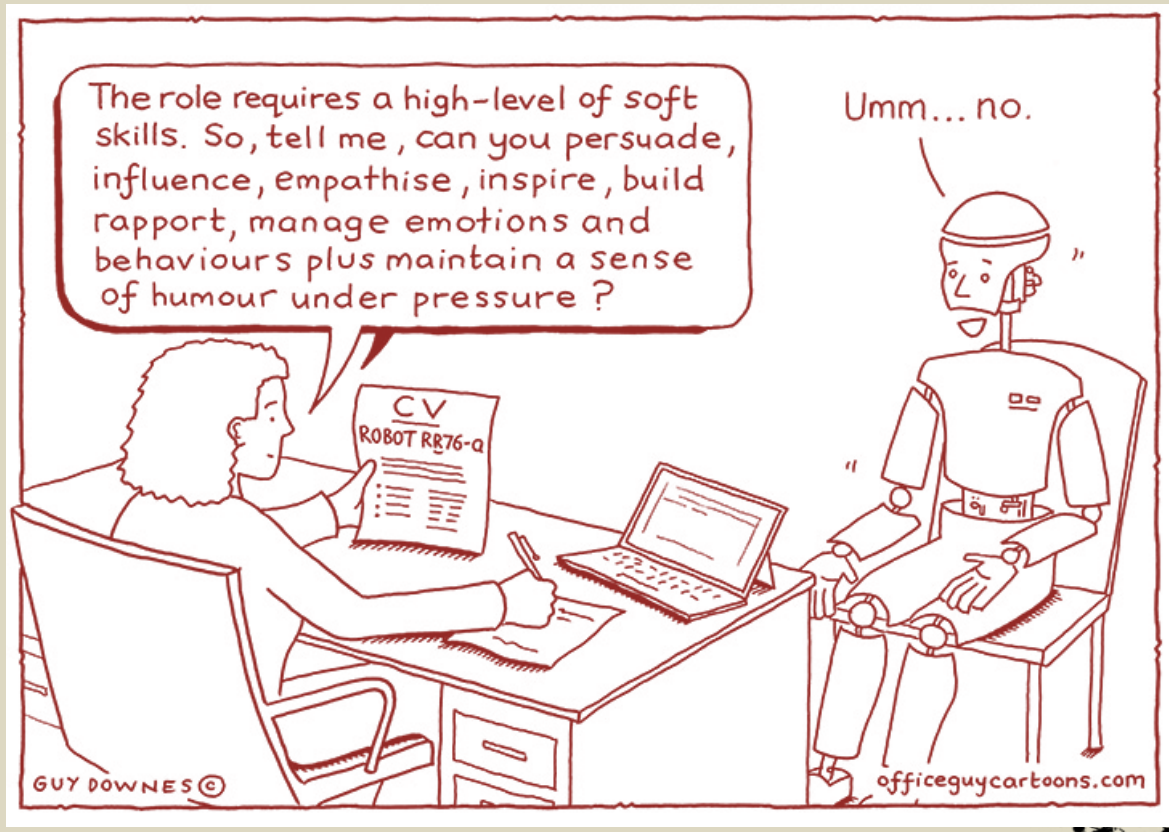
Source: <https://i-hls.com/archives/115259>

Dec 16 – While deep learning algorithms may be looking promising for identifying and characterizing cybersecurity intrusions, various attacks can cause them to provide inaccurate information, or even upset their entire plan of operations. Research shows that cybercriminals have been developing new attacks against different deep learning systems, such as those used for image analysis and natural language processing. Previous research has shown the efficacy of various adversarial approaches in causing deep neural networks (DNNs) to deliver untrustworthy and inaccurate predictions.

Researchers from the cyber security company Citadel have recently shown that current deep learning-based solutions for identifying certain cyberattacks, such as DDoS DNS, have substantial weaknesses and vulnerabilities. Certain attack techniques are capable of creating corrupted data that DNNs would misclassify, therefore delivering false information.

The Citadel researchers developed a DNN capable of detecting cyber-attacks, and then assaulted it with adversarial data to trick the DNN into arriving at false conclusions. The findings of these experiments clearly showed that a DNN can be deceived by malicious attacks and ignore or falsely report DDoS DNS attacks. DDoS DNS amplification attacks use weaknesses in DNS servers to magnify requests sent to them, eventually flooding them with data and taking the servers down. These assaults have the potential to significantly impair internet services provided by both large and small multinational corporations.

According to Marktechpost.com, the work of this Citadel team of researchers may inspire the creation of more effective technologies for detecting DDoS DNS amplification assaults in the future, which can recognize and categorize hostile data.





IOI  
International  
**CBRNE**  
INSTITUTE



**C<sup>2</sup>BRNE**  
DIARY



*Preparedness &*

# **EMERGENCY RESPONSE**







## PPD-44: Implications for Domestic Incident Management

By Robert J. (Bob) Roller

Source: <https://www.domesticpreparedness.com/preparedness/ppd-44-implications-for-domestic-incident-management/>

Nov 23 – Presidential Policy Directive 44: Enhancing Domestic Incident Management ([PPD-44](#)) is an unclassified guidance document signed by President Barack Obama in 2016 and used extensively to guide the federal response to large-scale domestic incidents requiring federal agency coordination. It was not made publicly available until now. The PPD improves upon earlier incident management guidance promulgated after 9/11 and tested in Hurricane Katrina and the years that followed. It helps establish common expectations for federal agencies during these incidents and was designed to supplement but not supplant existing law and previous presidential policy. It represents a paradigm shift in thinking about incident management, but challenges related to incident management roles and responsibilities remain. However, sharing the PPD with a broader audience will allow more effective coordination with incident management stakeholders at all levels.

### Realizing a Need for Better Incident Management

Effectively coordinating large-scale incident response has been a challenge for the federal government for decades. Most federal departments and agencies have specific emergency authority granted by statute, regulatory policy, or presidential guidance in the form of executive orders and a variety of security-related directives. However, these same authorities also are usually limited in scope and prevent one cabinet secretary from directing the work of another. Most of the time, this is a non-issue as each department and agency applies its authorities, capabilities, and congressionally appropriated funds to perform its mission in coordination with others. When they need support from each other, federal departments and agencies routinely employ [interagency agreements](#) or reimbursements through the [Economy Act](#), which grants the ability for federal stakeholders to coordinate purchasing. A well-known exception to these arrangements is presidentially-declared emergencies or disasters under the [Robert T. Stafford Act, as amended](#), where the Federal Emergency Management Agency (FEMA) may issue a mission assignment to federal departments and agencies to perform specific disaster work that is paid through the Disaster Relief Fund. Further FEMA assistance during Stafford Act incidents includes deploying presidentially appointed federal coordinating officers, establishing unified coordination groups to help establish unity of effort for response and recovery, and supporting field, regional, and national coordination structures.

It was evident after the 9/11 attacks that a gap existed regarding the responsibility to coordinate large-scale incident management when an incident does not qualify for a Stafford Act declaration. Legacy Cold War-era policies, such as [Executive Order 12656](#), addressed this coordination topic. Still, the focus on the threat of nuclear attacks that informed that document made it seem obsolete when the threat of terrorism became the primary domestic concern. The perceived need to ensure government-wide incident management coordination to address catastrophic acts of terrorism resulted in the formation of DHS in 2003 and the promulgation of Homeland Security Presidential Directive 5: Management of Domestic Incidents ([HSPD-5](#)) by President George W. Bush that same year.

HSPD-5 included several provisions, including the [National Incident Management System](#) requirements and what later became the [National Response Framework](#). In addition, paragraph four of HSPD-5 established the secretary of DHS as the principal federal official for domestic incident management and cited four criteria under which the secretary would take responsibility for managing the national response to an incident, including those outside the statutory duties of DHS. However, the same HSPD exempted the Defense Department and circumscribed the authority of the principal federal official role by noting that it did not supersede the existing statutory authority of other federal departments and agencies, non-federal partners, or the private sector. Moreover, it included no provisions for the principal federal official to issue mission assignments or direct the actions of departments and agencies.

PPD-44 sets expectations for federal agencies assigned to lead responses to major incidents and can help create an enhanced unity of effort for all responders.

One of the initial HSPD-5 implementation efforts was to delegate the principal federal official authority to a cadre of regional field leaders modeled on the federal coordinating officers employed for Stafford Act incidents. The assumption was that these leaders would [manage the federal response](#) to major incidents, primarily concerning [law enforcement](#), that required a considerable coordinated federal effort outside the bounds of a Stafford Act designation. Unfortunately, large-scale non-Stafford incidents did not occur. It created confusion and an unclear chain of command when both delegated principal federal officials and federal coordinating officers responded to Stafford Act incidents. The clearest example of this was Hurricane Katrina in 2005, where conflicts related to the principal federal official (who reported to the DHS secretary) and the Stafford Act federal coordinating officer (who reported to the president) were noted in the [After Action Report](#) as a significant contributor to the massive loss of life from that incident. Not surprisingly, [Congress criticized](#) this confusing overlap of responsibility, and the program was canceled shortly thereafter.







The next significant use of HSPD-5 was the initial response to the 2009 H1N1 pandemic. In that situation, DHS Secretary Napolitano [leveraged the HSPD-5 principal federal official authority](#) to serve as the spokesperson for the incident in support of the U.S. Department of Health and Human Services (HHS) as the lead federal agency until HHS Secretary Kathleen Sebelius was confirmed into her role. However, the lack of a clear chain of command between the DHS secretary applying HSPD-5 principal federal official authority and HHS leaders executing their statutory authority outside the secretary's control created coordination challenges that the [After Action Report](#) noted for that incident. Since 2009, the DHS secretary has not assumed or been assigned overall responsibility for any major incident outside the core mission areas of DHS. However, HSPD-5 remains in effect and untouched since its promulgation nearly 20 years ago.

### **The Development of PPD-44**

The lessons learned from 9/11 and the decade after were that it is helpful to have a single lead federal agency with an accountable cabinet secretary charged with managing the response to major incidents but defaulting to the DHS secretary as described in HSPD-5 is not an effective solution. Those and other hard-learned lessons from smaller yet complex incidents such as [Ebola](#), where a presidentially appointed czar led the coordination, highlighted that the lead federal responsibility should be assigned to the agency with the most statutory authority for a given type of incident. The overall incident management responsibilities of the lead federal agency should be made clear, and other federal stakeholders should be prepared to support the lead federal agency as needed. That led to the development of PPD-44 in late 2016, but it had never been widely available until now.

PPD-44 does not establish new authorities and does not apply to Stafford Act incidents, military operations, or conflict with other presidential guidance, including HSPD-5. Instead, PPD-44 represents a paradigm shift because, for the first time, expectations are set for federal agencies assigned responsibility to lead the response to major incidents, including:

- Appointing a senior official to lead responsibilities employing the National Response Framework, [National Disaster Recovery Framework](#), and National Incident Management System;
- Determining the relevant federal agencies required for participation in unified coordination and the level of unified coordination needed;
- Developing strategic objectives, priorities, and planning activities;
- Identifying gaps that response and recovery activities should address;
- Coordinating federal incident response and recovery strategies and execution with federal state, tribal, territorial, private sector, and non-governmental entities;
- Facilitating appropriate incident information reporting; and
- Serving as the principal spokesperson to lead communication activities with affected parties and the public.

Furthermore, PPD-44 also establishes responsibilities for agencies tasked with supporting a lead federal agency. This includes specific incident management capabilities FEMA may provide and the reimbursable support other agencies can provide, all according to the National Response Framework, National Disaster Recovery Framework, and National Incident Management System.

### **The Next Steps for Building an Integrated National Response**

PPD-44 was a step forward in setting expectations for all federal departments and agencies to lead overall incident response where they had the most authority to act. However, PPD-44 also created further problems and complexity. For starters, PPD-44 is unclassified but was initially only provided to a small group of federal departments and agencies. Therefore, many who were responsible for leading or supporting incident response pursuant to the directive's requirements could not access the document to review those requirements. Furthermore, by keeping HSPD-5 and the DHS secretary's principal federal official role untouched, anytime the president identifies DHS as the lead federal agency for a domestic incident, that designation is consistent with both HSPD-5 and PPD-44, which may create coordination challenges because the expectations for the lead and supporting agencies differ between the two documents.

Finally, PPD-44 is now available for everyone, and its principles can be incorporated into federal plans and plans that exist in parallel or in partnership with the federal government. Furthermore, implementing PPD-44 and its known challenges vis-a-vis HSPD-5 should offer an opportunity to review the older presidential document and align it with current practice and hard-learned lessons of the past two decades.

**Robert J. (Bob) Roller** serves as FEMA's National Planning Branch Chief, where he supervises the development and implementation of major federal government-wide planning efforts that address complex and catastrophic disasters. In addition to his steady state responsibilities, he is a qualified Planning Support Section Chief within the National Response Coordination Center and formerly served as the Acting Strategy and Policy Division Director. He joined FEMA in 2017 after serving at the U.S. Department of Homeland Security (DHS) Headquarters where he led the development of multiple DHS-wide planning





efforts and served as the Protection Planning Division Chief within the Office of Policy. He also has years of experience as a firefighter and emergency medical services provider in both wilderness and urban environments. He is a frequent contributor to the Domestic Preparedness Journal and recently published a memoir regarding his early experiences as a wildland firefighter. The opinions printed here are his own and not endorsed by his employer.



### What Is THOR?

Source: <https://i-hls.com/archives/109249>

Nov 25 – The Tactical Humanitarian Operations Response vehicle (THOR) was built to operate under any network in any environment, from dense forests during wildfires to remote military settings. The network allowed autonomous robot communication to a self-driving battery delivery vehicle, video streaming between people and vehicles in the field, data from sensors on devices operating in an austere environment, and 5G mobile edge computing being used to help decision-makers by providing a single operating picture of all of these data feeds in real-time, according to Verizon. THOR is a prototype, 5G-based disaster response and command hub vehicle — and there are no present plans to build another. It's designed to be National Incident

Management System or NIMS-1 compliant and offers full radio interoperability and onboard Joint Operations Center services. It also provides “a multitude of connectivity options,” spanning private 5G, commercial 4G LTE, Land Mobile Radio and tactical radio, wireless networking, microwave, mesh, and more — together in one package. Other components include 4G/5G radios, a rear command center, a camera, a 6-seat cabin, and an exterior touch screen display.

Director of Verizon Response and Public Safety Operations Cory Davis told nextgov.com it's also equipped with a tethered drone to capture an aerial view “that can be fed over the network to devices on the ground and the command center below, potentially helping those in public safety or the military with risk and damage assessment, situational awareness, or search and rescue operations.” “THOR is a bit like a Swiss-Army-Knife on wheels,” he added.

“In situations ranging from fighting wildfires in forests where network connections and coverage can be challenging to the devastation and infrastructure damage caused by earthquakes, public safety professionals face the potential of coverage and technology gaps or an out-of-service network,” Davis noted. But Verizon built the futuristic vehicle to confront those challenges. “In a field where seconds always matter, and lives are on the line, connectivity and reliability matter,” he added. THOR consists of the “full menu” of emerging and existing tech solutions. But Davis said future iterations for public safety or the military could potentially go “a la carte.”







## Surging Seas

Source: <https://sealevel.climatecentral.org/maps/>



Global warming has raised global sea level about 8 inches since 1880, and the rate of rise is accelerating. Rising seas dramatically increase the odds of damaging floods from storm surges. A Climate Central [analysis](#) finds the odds of “century” or worse floods occurring by 2030 are on track to double or more, over widespread areas of the U.S. These increases threaten an enormous amount of damage. Across the country, nearly 5 million people live in 2.6 million homes at less than 4 feet above high tide — a level lower than the century flood line for most locations analyzed. And compounding this risk, scientists expect roughly 2 to 7 more feet of sea level rise this century — a lot depending upon how much more heat-trapping pollution humanity puts into the sky.

Search or navigate our interactive tools above to see maps of areas below different amounts of sea level rise and flooding, down to neighborhood scale, matched with area timelines of risk. The tool also provides statistics of population, homes and land affected by city, county and state, plus links to factsheets, data downloads, action plans, embeddable widgets, and more.



### Coastal Risk Screening Tool: Ice Sheet Contributions to Sea Level Rise

The ice sheets map allows users to explore how much land different amounts of Antarctic ice loss could put below the tideline. Because ice loss causes subtle changes in the Earth’s gravitational field, rotation, and shape, local sea level increases will vary from place to place. This map reflects these differences.

[View now »](#)



### Coastal Risk Screening Tool: Affordable Housing

The affordable housing map allows users to explore what affordable housing in the U.S. could be threatened by sea level rise and coastal flooding in the coming decades, under multiple pollution scenarios. The map allows users to examine affordable housing at risk by state, city, county, congressional district, state legislative district, or zip code. [View now »](#)



### Coastal Risk Screening Tool: Map By Year

The year map allows users to explore coastal flood risk and sea level rise projections by decadal year for anywhere in the world, and under multiple pollution scenarios. The map allows users to choose between the leading sea level rise models and incorporate the most accurate elevation data available. [View now »](#)

## Maintaining a Strong Volunteer Force

By Kristina L. Hamilton

Source: <https://www.domesticpreparedness.com/resilience/maintaining-a-strong-volunteer-force/>



Dec 07 – Volunteers are a lifeline for many nonprofit organizations and for-profit companies during emergencies and disasters. Volunteers tend to have big hearts for helping people and are willing to go out of their way to assist as needed. However, recruiting and retaining good volunteers can be difficult. Following are some simple strategies and tools for any emergency preparedness professional seeking to build and maintain a strong volunteer force.

### Strategies & Tools for Volunteer Engagement

When recruiting volunteers, consider what the organization is looking for in a volunteer.

- Are specific credentials or training required?
- Do they need to have a medical background with a current verified license?
- Is heavy lifting involved?
- Is there a lot of clerical work?
- What are the working conditions (indoor/outdoor)?
- What will they need to wear?
- What is going to be supplied?

Once the event or task requirements are defined, the actual recruiting or assigning of volunteers begins. It is critical to avoid assigning a volunteer to a task or duty for which they are not qualified or overqualified. Volunteers tend to have big hearts and are willing to go out of their way to assist as needed, but coordinators must respect their balance between commitments. One of the most important things to remember when recruiting volunteers is they are not getting paid to help. As such, with other personal and





professional responsibilities, they may not be available to assist in every situation. COVID-19 was a good example. When the testing began, it was difficult to get volunteers as they were afraid to bring illnesses back to their loved ones. However, as more information emerged and the nation entered the vaccination stage, volunteers emerged from every direction. As a result, the robust and trained team of volunteers that very smoothly ran the COVID-19 clinics came back to help at other clinics. Those volunteers performed essential tasks: helping with traffic, doing clerical work, giving vaccinations, entering data into computers, watching the people after their vaccinations to make sure they did not have any problems, taking clipboards off the nurses' stations, and cleaning and restocking the clipboards with new vaccination applications. They also cleaned the seats between visitors to maintain a sterile environment. For those who could not enter the building, one of the clerical volunteers and a nurse would perform the tasks outside with the traffic volunteers observing those who received the vaccinations for 15 minutes and alerting staff if needed. Fortunately, no alerts were required outside or inside. To retain volunteers, coordinators must respect this balance between commitments. For example, putting down a volunteer or implying they are untrustworthy because they cannot respond to every event would hinder volunteer retention efforts. However, simple, inexpensive strategies can work well in maintaining volunteers. For example:

- Praise them for their actions.
- Host an appreciation dinner or other event to make them feel wanted and needed.
- Express gratitude by saying "Good job" or "Thank you" to encourage them to return.
- Show personal recognition, such as sending birthday cards or thank you cards (some online websites can create cards and send them by email).

It is difficult for a threat preparedness volunteer coordinator or any other volunteer coordinator to recruit and retain good volunteers to fulfill roles that are not needed daily. There is only so much training that organizations can do to keep volunteers busy. During these downtimes are good opportunities for birthday cards and other friendly gestures to remind them that their services are appreciated even when they are not actively volunteering.

The bottom line in retaining volunteers is to maintain regular contact. Ensure that the volunteers know they are needed and that they are doing a good job. In addition, the volunteers must understand the jobs they are doing for the events, disasters, or other efforts are being done well and that their efforts are essential to the success of the operations.



Volunteers at a COVID-19 vaccination clinic at South Parkersburg Baptist Church, Parkersburg, WV (Source: Hamilton, March 10, 2021)

**Getting Started**

Various programs are available to help with grant funding for managing, recruiting, and retaining volunteers. There are even training programs for volunteer coordinators or managers of volunteers based on best practices. These training programs can be in person, virtual with online leadership, or online self-







paced classes. Some state agencies offer grants and training programs to nonprofit organizations to help recruit and engage more volunteers. For example, in West Virginia, [Volunteer West Virginia](#) is the lead volunteer agency within the state’s Department of Arts, Culture, and History.

It is imperative to receive volunteer management training before starting a program that involves running a volunteer business or managing groups of volunteers. Another program that helps with volunteerism is the [United Way of the Mid-Ohio Valley](#), which has staff that are friendly, available, and willing to help.

One more resource with information about many types of disasters, how to prepare for them, grants, help with volunteers, and so much more is [Ready.gov](#). Much of their materials are free to order and can help facilitate organizing community emergency preparedness events. In addition, having volunteers helping at these events provides good opportunities for the volunteers to gain more familiarity with the topics in these materials.

With the right resources and assistance from different companies and agencies mentioned in this article, there is a lot of support for building and maintaining a robust volunteer force and information on available grants for struggling nonprofit organizations. With grants and other valuable information, organizations can better prepare for the next disaster by recruiting, retaining, and managing a strong volunteer force.

**Kristina L. Hamilton** has been with the Mid-Ohio Valley Health Department since 2003 and currently serves as the threat preparedness volunteer coordinator. She also serves as the six-county regional volunteer coordinator for the Mid-Ohio Valley Medical Reserve Corps since 2011. In addition, she is a West Virginia Public Health Association member and a regional coordinator for the Community Emergency Response Team.



### Protecting major events: an incident response blueprint

[Source](#)

Dec 02 – The cyber security of major events, whether they are related to sports, professional conferences, expos or other events can be a time-consuming, complex undertaking. It necessitates a multifaceted approach and the involvement of multiple entities, including but not limited to the vendors, hospitality teams and service providers to facilitate a uniform approach to cybersecurity across the event ecosystem.

Cisco Talos Incident Response (Talos IR) is sharing a white paper on the steps organizations should follow to secure any major event. These ten focus areas should help guide any organizing committee or participating businesses in preparation for securing such events, including the key questions that need to be asked and associated answers.



*The Editorial Team is wishing to all of you*



**It's not  
the lie that  
bothers me.  
It's the  
insult to my  
intelligence  
that I find  
offensive.**







ICI  
International  
**CBRNE**  
**INSTITUTE**

A common roof for international  
CBRNE First Responders



*Join us!*



Rue des Vignes, 2  
B5060 SAMBREVILLE (Tamines)  
BELGIUM

[info@ici-belgium.be](mailto:info@ici-belgium.be)  
[www.ici-belgium.be](http://www.ici-belgium.be)