02\24

2 CBRNE DIARY

ICI International CBRNE INSTITUTE

Dedicated to Global First Responders

February 2024

PART B

Meet OpenAI Sora!

Could AI help bioterrorists unleash a new pandemic?

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

DIRTY R-NEWS

C2BRNE DIARY

Three Dangerous Cold War Myths About Nuclear Policy

By Kyle Balzer

Source: https://nationalinterest.org/feature/three-dangerous-cold-war-myths-about-nuclear-policy-208796

June 23 – In next month's congressional hearings on defense policy, the Strategic Posture Commission will undoubtedly receive significant attention. Last fall, the commission released its bipartisan report warning that the existing nuclear program of record was insufficient for the emerging two-peer threat environment. To simultaneously deter China and Russia, the report recommended preparations to upload more nuclear warheads and broaden theater strike options. This sober assessment echoes the Biden administration's earlier acknowledgment that "it may be necessary to consider nuclear strategy and force adjustments to achieve deterrence."

Nonetheless, these recommendations have been roundly condemned by the arms control and disarmament community. The critics decry that a robust nuclear modernization program would be tantamount to "sleepwalking" into an action-reaction arms race—an inexcusable error ignoring the Cold War maxim that nuclear competition "has no winners, only losers."

Such alarmism echoes national security advisor Jake Sullivan's warning, issued last June, that a nuclear buildup would trigger a senseless arms race and risk inadvertent escalation. Alluding to the Cold War, Mr. Sullivan confidently proclaimed, "We've been there. We've learned that lesson."

But it is unclear precisely where in the annals of Cold War history Mr. Sullivan and the arms controllers have been—and, more to the point, just how they arrived at lessons that amount to dangerous myths. If these flawed historical analogies are employed to shape nuclear policy, Washington's unilateral restraint could actually weaken deterrence. It is vital, therefore, that U.S. officials and lawmakers first disabuse themselves of three Cold War nuclear myths.

First, the Soviet-American nuclear rivalry hardly resembled an action-reaction arms race, with one side reflexively building strategic forces in response to expansion by the other. In the Cold War, prominent U.S. defense analysts mistakenly assumed—as many do today—that Washington's "insatiable" nuclear appetite was "keeping Soviet programs going."

But this crude action-reaction trope obscures the true nature of Soviet-American interactions. It cannot explain why U.S. nuclear dominance persisted through the mid-1960s, nor why U.S. force-building leveled off from there—even as the Soviets shot past on their way to *numerical* superiority. By the mid-1970s, the Soviet strategic missile arsenal enjoyed a two-to-one advantage in deliverable payload, and the Kremlin was opening up a terrifying deterrence gap by fielding theater missiles that could range all of Western Europe.

The U.S. defense establishment was stunned. In the mid-1960s, strategic planners had assumed that the Soviets were placated by mutual vulnerability and thus satisfied with nuclear inferiority. Modernization programs for a larger strategic missile and advanced bomber were consequently slashed. Hamstrung by these shortsighted decisions, the United States would not respond with offsetting deployments until the mid-1980s—nearly twenty years after force building had plateaued. As one U.S. defense analyst quipped in 1974, "It is surely stretching it to talk of a 'race' between parties moving in quite different directions."

This tale of two postures throws into sharp relief the second myth: Contra widespread misconceptions during and after the Cold War, arms control agreements were not the product of a shared understanding of strategic stability—quite the opposite. Whereas U.S. officials considered mutual vulnerability "the foundation of stable deterrence," their rivals could not fathom its appeal. Indeed, the Soviets did not accept the concept of deterrence until the late 1960s, and even then, they practiced an altogether different style.

In the Kremlin mindset, strategic stability rested entirely on Soviet nuclear primacy—*not* so-called Mutual Assured Destruction. As one Soviet strategic planner later divulged, Moscow "strove to achieve superiority" through the sheer scale of its strategic offensive and defensive programs. An array of massive missiles was complemented by an enormous complex of active and passive defenses that dwarfed its American counterpart—a comprehensive posture designed to survive and prevail in nuclear warfare. As such, the 1972 Strategic Arms Limitation Treaty and Anti-Ballistic Missile Treaty were hardly the result of Washington's power of persuasion on the merits of mutual vulnerability. According to two Soviet officials, "it was not American arguments that caused the Soviet Union to revise its stand on missile defense" but rather "insufficient technological development vis-à-vis the United States."

Thus, the third myth: Notwithstanding popular narratives, it is misleading to depict nuclear competition as inherently unwise or reckless. The Soviet-American rivalry, after all, was anything but a "lose-lose" affair. Scholars can reasonably debate whether the United States delivered a fatal blow to Moscow by winning the "arms race." However, it is undeniable that in overcoming its initial reluctance to compete, Washington secured landmark arms control agreements from a position of strength that facilitated the Cold War's peaceful resolution.

It was America's competitive nuclear modernization program—initiated by innovative defense planners in the mid-1970s—that enabled Washington to lock in decisive advantages a decade later. Once armed with larger strategic missiles, highly accurate theater strike systems, terrain-hugging bombers, and stealth

attack aircraft, the United States effectively leaped "a generation or two" ahead of the Soviets in the 1980s—much to the Kremlin's chagrin.
As a dejected Soviet planner later explained to an American interlocutor, "Our air defense systems were not designed to detect [your theater] missiles. You had hardly deployed 1/3 of these missiles, and we were already compromising." Indeed, even before the initial strike detachments arrived in Western Europe in 1983, the chief of the Soviet general staff had privately conceded to an American journalist that "the Cold War is over, and you have won."
By 1986, Soviet officials were eager to conclude the Intermediate-Range Nuclear Forces Treaty to remove a threat they characterized as "a revolver put to our temple." Though the agreement weighed heavily in America's favor, the Kremlin recognized that it could not withstand another round of competition with a technologically superior rival. As an exhausted Mikhail Gorbachev explained to the Soviet politburo, "If we won't budge from the positions we've held for a long time, we will lose in the end."
Debunking these nuclear myths is not a mere academic exercise, as this history has momentous implications for U.S. strategic planning. To be sure, today's two-peer nuclear threat environment is *sui generis*. Furthermore, Beijing's economic heft and defense-industrial prowess dwarfs that of the Soviet Union. Alas, the United States should be under no illusion about exploiting the same technological advantages it enjoyed during the Cold War.
Nonetheless, the nuclear past provides two fundamental lessons for the future of U.S. nuclear planning. First, strategic stability is a function of long-term competition. American unilateral restraint had opened up, in the minds of Western European leaders, a grave imbalance in the European theater. By the mid-1970s, Soviet theater advantages threatened NATO solidarity—if not the alliance's very existence. As Moscow improved its strategic forces and fielded intermediate-range systems, Washington lacked the strike capability to reassure its anxious allies. It was, therefore, the U.S. modernization program that redressed the situation—*not* unilateral restraint or shared beliefs about stability.
Second, the Cold War demonstrates that arms control, much like deterrence, depends on shrewd competition. The Soviet Union revised its position on missile defense only *after* recognizing that the United States enjoyed a long-term competitive advantage in this area. Similarly, the INF Treaty emerged after the United States had developed superior theater capabilities and NATO exhibited the political will to deploy these systems amidst widespread public opposition.
America's first experience with great-power nuclear rivalry thus offers a cautionary tale about unilateral restraint. Nuclear competition is neither irrelevant nor intrinsically reckless—in fact, robust deterrence and the future of arms control likely depend on it. As such, protestations of the dangers inherent in nuclear modernization should be met with healthy skepticism. Clinging to a flawed understanding of the nuclear past is a greater threat to strategic stability than doing what is necessary to deter adversaries and assure allies.

Kyle Balzer is a Jeane Kirkpatrick Fellow at the American Enterprise Institute, where he focuses on great-power competition, U.S. grand strategy, long-term strategic competition, U.S. nuclear strategy and policy, and arms control. He specializes in Cold War nuclear strategy and the evolution of American deterrence theory.

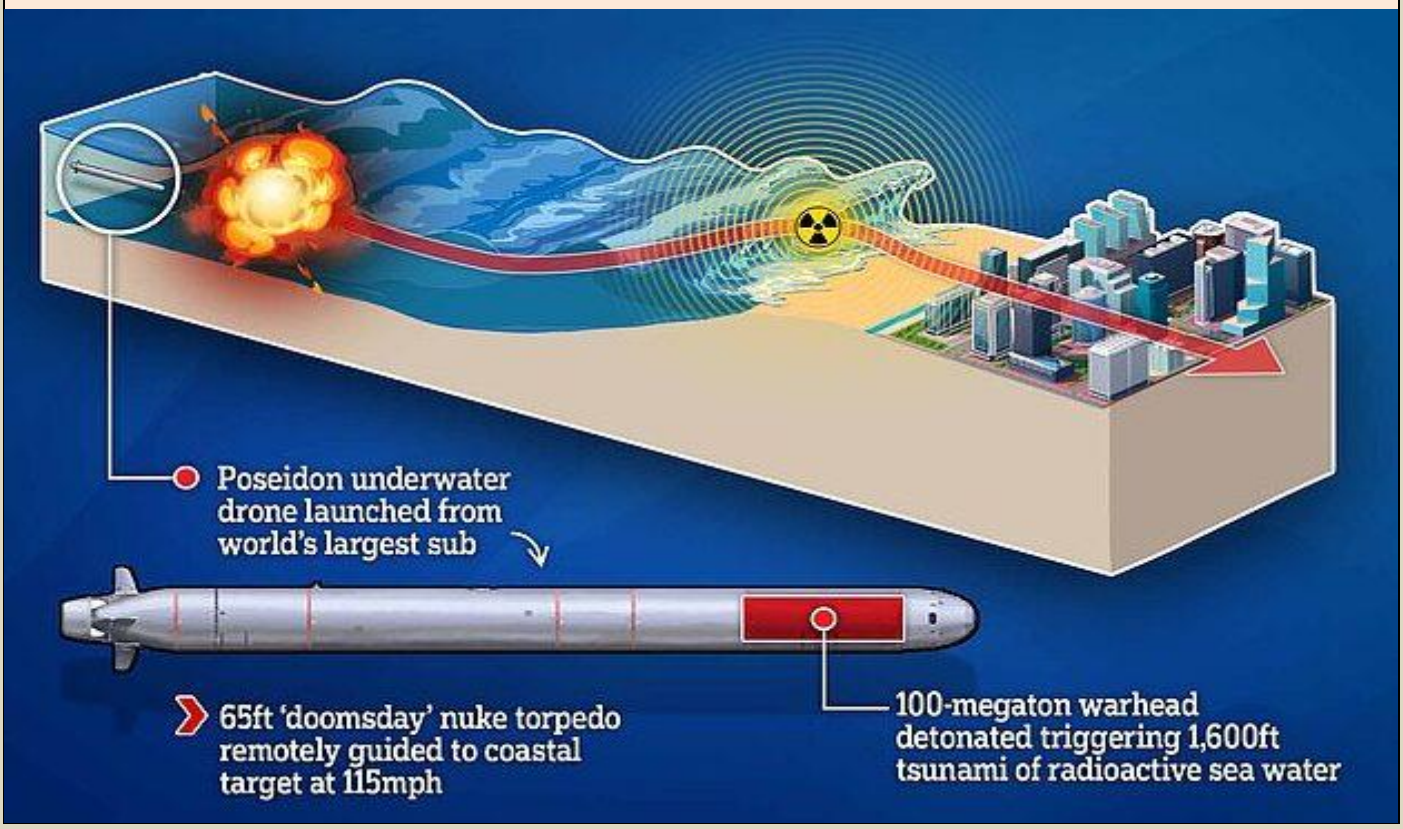
North Korea's Tsunami-Causing Underwater Nuclear Drone

Source: https://i-hls.com/archives/122540

Jan 21 – Korea Central News Agency (KCNA) claims the country has tested an underwater nuclear-capable drone-based weapons system, which is yet another declaration the country has made of its own advanced weapons, claims that don't usually have concrete proof.
This new weapon announcement comes at a time of tension in the region, between the neighboring countries as well as discontent over the presence of Japan and the US near its territorial waters (North Korea has called recent naval exercises of the US and South Korea "provocative").
According to Interesting Engineering, North Korea claims to have tested an underwater drone called Haeil-5-23 at the Underwater Weapon System Institute, which works under the DPRK Academy of Defense Science.
Haeil (meaning tsunami) is a system that uses an underwater nuclear explosion to create a radioactive wave. North Korea claimed to have tested the system on two occasions last year. The KCNA press release reads: "The armed forces of the DPRK will strike horror into their hearts through the responsible, prompt, and bold exercise of its deterrent and firmly defend the security of the state and regional peace."
Nevertheless, the country has not presented any actual evidence of these tests but claimed to have further "rounded off" its nuke-based underwater countering posture. Experts believe that much work lies ahead before the North can deploy this technology, if it exists.

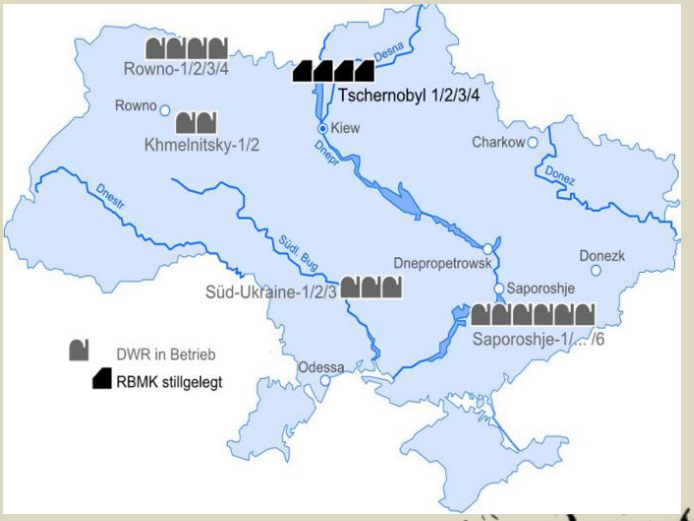
Some worrying developments in the region are expected to escalate tensions as North Korea gets close with Russia for "strategic and tactical cooperation." Experts claim that North Korea has been providing weapons and tech to Russia for operations in Ukraine in return for Russian nuclear technology, as reported by DW reported.
Furthermore, North Korea has reportedly become more aggressive in recent months, claiming more completed weapons tests and looking to pick a fight with its neighbor and the US. Last month, North Korea's leader, Kim Jong Un, said that the North will no longer seek to reconcile and reunify with the South.

EDITOR'S COMMENT: One might think of a Russian finger in this project (Poseidon torpedo).



Ukraine to start building 4 new nuclear reactors this year

Source: https://www.reuters.com/business/energy/ukraine-start-building-4-new-nuclear-reactors-this-year-minister-2024-01-25/



Jan 25 – Ukraine expects to start construction work on four new nuclear power reactors this summer or autumn, Energy Minister German Galushchenko told Reuters on Thursday, as the country seeks to compensate for lost energy capacity due to the war with Russia.
Two of the units - which include reactors and related equipment - will be based on Russian-made equipment that Ukraine wants to import from Bulgaria, while the other two will use Western technology from power equipment maker Westinghouse.
All four reactors will be built at the **Khmelnytskyi nuclear power plant** in the west of Ukraine, Galushchenko added. The timeline is more aggressive than previously outlined by Kyiv, which has spoken of starting work in some time in 2024 and without specifying that all

four reactors could be developed simultaneously. "I think (we'll start construction) in summer-autumn," Galushchenko said in an interview. "We need vessels," he added, referring to the reactor pressure vessels that will have to be imported. We want to do the third and fourth units right away."

Construction of the 3rd and 4th reactors at Khmelnytskyi began in the 1980s but was frozen.

Since gaining independence from the Soviet Union in 1991, Ukraine has built three new nuclear reactors - one each at Zaporizhzhia, Khmelnytskyi and Rivne nuclear power plants.

Today three nuclear power plants in Ukraine-controlled territory produce more than 55% of the country's electricity needs, but Kyiv wants to expand the sector to help compensate for the loss of Zaporizhzhia, Europe's largest nuclear plant.

Russia gained control of the facility after launching a full-scale invasion of Ukraine in early 2022, and its six nuclear reactors are now idled. "With the 3rd and 4th (Khmelnytkyi units) we want to compensate for Zaporizhzhia, and now we are in the talks with our Bulgarian partners on the two reactors we want to take," Galushchenko said.

"If we received the reactor vessels today, I think it would be 2.5 years and we would have a third reactor on line," Galushchenko said.

In parallel with the construction of the Soviet-era VVER-1000 units, Ukraine wants to start preparatory construction work to accommodate two modern Western AP-1000 units, also at Khmelnytskyi.

"We need to pass (parliamentary) legislation and we have draft laws on the 3rd, 4th, 5th and 6th units. This is VVER-1000s, while the 5th and 6th we want to build the AP-type. This is a parallel process," he said.

In December, Ukraine's nuclear power firm Energoatom and Westinghouse signed an agreement on the purchase of equipment for Khmelnytskyi's 5th power unit.

EDITOR'S COMMENT: Strange proxy war!

Highly specialized US Army teams train to disable any potential enemies' nuclear capabilities

Source: https://www.dvidshub.net/news/462450/highly-specialized-us-army-teams-train-disable-any-potential-enemies-nuclear-capabilties

Jan 25 – Nuclear Disablement Team 2 trained Jan. 17 on Aberdeen Proving Ground. A one-of-a-kind capability in the U.S. Department of Defense, NDTs directly contribute to the nation's strategic deterrence by staying ready to exploit and disable nuclear and radiological Weapons of Mass Destruction infrastructure and components to deny near-term capability to adversaries. The NDTs also facilitate follow-on WMD elimination operations.

The NDTs are part of the 20th Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Command, the U.S. military's premier CBRNE formation.

The 20th CBRNE Command is also home to 75 percent of the active-duty U.S. Army Chemical, Biological, Radiological, Nuclear (CBRN) and Explosive Ordnance Disposal (EOD) units, as well as the 1st Area Medical Laboratory, CBRNE Analytical and Remediation Activity and five Weapons of Mass Destruction Coordination Teams.

From 19 bases in 16 states, Soldiers and Army civilians from the 20th CBRNE Command take on the world's most dangerous hazards in support of joint, interagency and allied operations.

The U.S. military's only Nuclear Disablement Teams — NDT 1, NDT 2 and NDT 3 – are all stationed on Aberdeen Proving Ground, Maryland. The NDTs include Nuclear and Countering Weapons of Mass Destruction (FA 52) officers, an Explosive Ordnance Disposal officer, a Nuclear Medical Science officer and a Health Physics noncommissioned officer.

Highly trained American Soldiers honed their skills to disable any potential enemies' nuclear capabilities during training on Aberdeen Proving Ground, Maryland.

"This training event is critical to the success of the NDTs, as conducting disablement operations is one of our core tasks," said Capt. John M. Prevost, an Army Explosive Ordnance Disposal officer from Nuclear Disablement Team 2. "Effective application of the correct tool to the correct task starts with understanding how to set up and employ the equipment. This course allows NDT personnel to see the effects of each tool on a given target material, thus revealing planning considerations and limitations for use in expeditionary operations." Prevost said disablement operations contribute to counter Weapons of Mass Destruction missions and gives commanders greater options on the battlefield. "It can also increase the safety of nuclear infrastructure, enabling freedom of maneuver to the ground component commander and reducing the risk of a potential contamination event," he said.

US to station nuclear weapons in UK to counter threat from Russia

Source: https://www.telegraph.co.uk/world-news/2024/01/26/us-nuclear-bombs-lackenheath-raf-russia-threat-hiroshima/

Jan 26 – The United States is planning to station nuclear weapons in the UK for the first time in 15 years as the threat from Russia increases, Pentagon documents seen by The Telegraph reveal.

Procurement contracts for a new facility at RAF Lakenheath in Suffolk confirm that the US intends to place nuclear warheads three times the strength of the Hiroshima bomb at the air base.

The US removed nuclear missiles from the UK in 2008, judging that the Cold War threat from Moscow had diminished.

The disclosure comes in the wake of warnings that Nato countries need to ready their citizens for war with Russia.

A protester campaigns against nuclear weapons outside RAF Lakenheath in 2022 when it was reported that US warheads could make a return to British soil Credit: Martin pope/getty

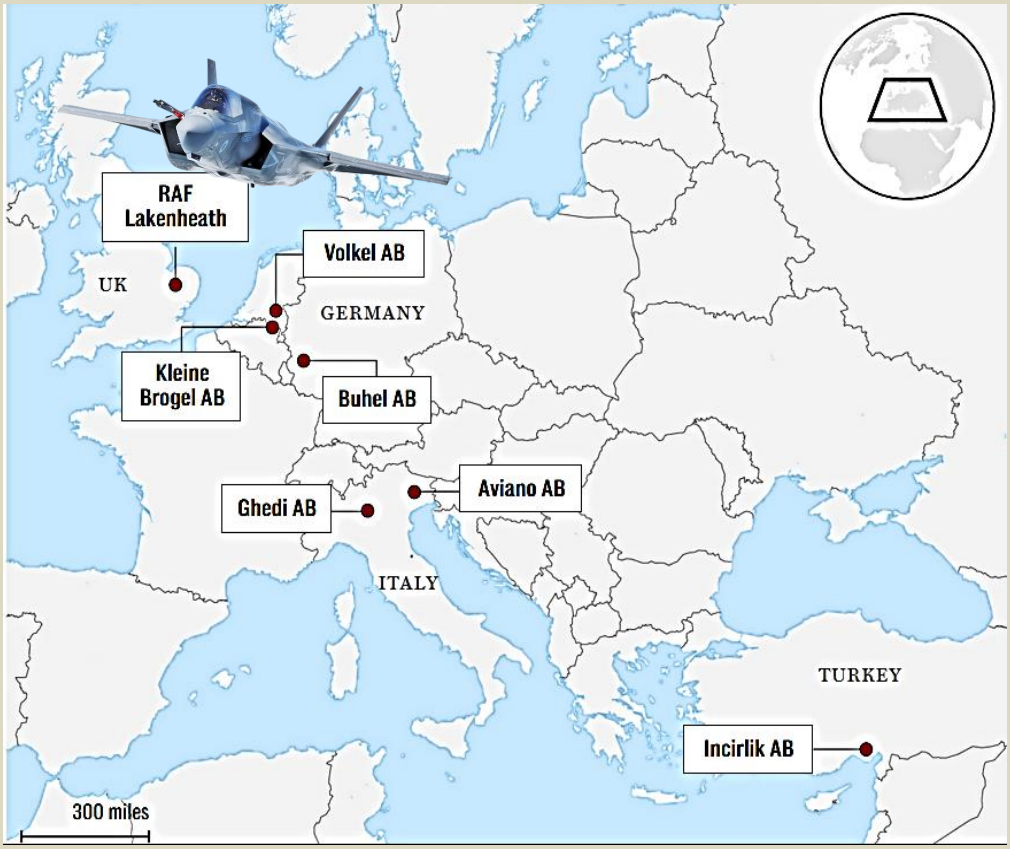
Last week, Adml Rob Bauer, a senior Nato military official, said that private citizens should prepare for all-out war with Russia in the next 20 years that would require wholesale change in their lives.

General Sir Patrick Sanders, the head of the British Army, went on to warn that the public would need to be called up to fight if there was war with Russia because the Army was too small.

His comments forced Downing Street to rule out conscription.

Boris Johnson on Friday night backed Sir Patrick's call for a citizen army, as he pledged to sign up if the UK went to war with Russia.

The US navy secretary, Carlos Del Toro, then urged Britain to "reassess" the size of its armed forces. On Friday, No 10 defended the Government's military spending, pointing out that "the UK is the second biggest defence spender in Nato and the largest in Europe".



The return of American weapons to the UK is part of a Nato-wide programme to develop and upgrade nuclear sites in response to heightened tensions with the Kremlin in the wake of the February 2022 invasion of Ukraine.

Russia has stated that the placement of US weapons in Britain would be viewed by Moscow as an "escalation" and would be met with "compensating counter-measures".

As well as the conflict in Ukraine, the West is facing rising challenges from Iran and North Korea, which have both grown closer to Moscow in recent years.

On Friday, Britain, France and Germany condemned Iran for launching a new satellite to guide long-range missiles. Tehran is enriching uranium for possible use in developing nuclear weapons.

The US and UK have also been carrying out air strikes in the Red Sea against Yemen's Houthi rebels, the Iran-backed militia which have been attacking container ships in purported retaliation for Israel's military offensive in Gaza.

US B61-12 "steerable" nuclear bomb

The US plans to deploy 180 precision-guided thermonuclear bombs to five European countries from 2020

Size

Length: 3.6m

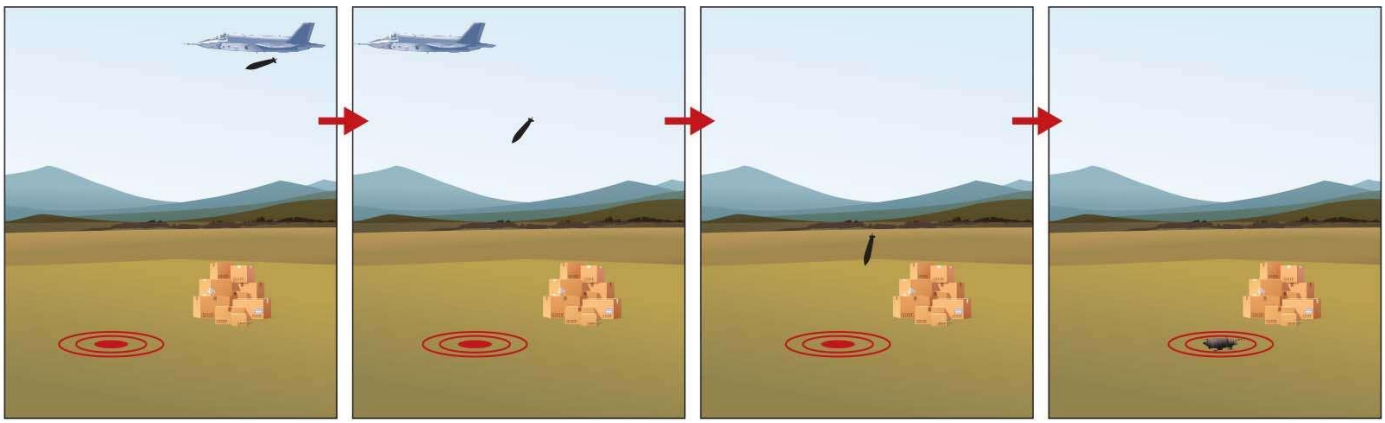
Diameter: 340mm

Weight: 350kg

Where bombs will be based

Belgium	Kleine Brogel	**20**
Germany	Büchel	**20**
Italy	Aviano, Ghedi Torre	**70**
Netherlands	Volkel	**20**
Turkey	Incirlik	**50**

Stages



The B61-12 is deliverable by six aircraft: the B-2A, B-52H, F-15, F-16, Tornado and F-35

GPS and laser guidance embedded in its nose guide the bomb to within 30m of its target

Steerable tail fins and a spin rocket rotor fly the bomb to its precise target

AMAC systems enable selectable detonation magnitudes of 5, 10, or 50Kt, either by air or ground burst

Sources: Federation of American Scientists, IHS Jane's

SCMP / Graphic News

Echoes of the Cold War

Unredacted documents on the US department of defence's procurement database reveal plans for a "nuclear mission" that will take place "imminently" at RAF Lakenheath, where nuclear weapons were stationed during the Cold War. The Pentagon had refused to comment on speculation that a new "surety dormitory", first revealed in budget documents last year, was intended for the base, which is run by the US Air Force under British regulations and laws, to allow the US to house tactical nuclear weapons that can be deployed by F-35 fighter jets.

The term "surety" is used by the Pentagon to refer to the need to keep nuclear weapons safe when they are not being used.

The documents show the Pentagon has ordered new equipment for the base, including ballistic shields designed to protect military personnel from attacks on "high value assets". Construction on a new housing facility for American forces working on the site will begin in June.

RAF Lakenheath is expected to house B61-12 gravity bombs, which have a variable yield of up to 50 kilotons – more than three times the power of the atomic weapon dropped on Hiroshima in 1945.

Following the outbreak of the war in Ukraine, a Pentagon review of the US's nuclear posture said it served as a "stark reminder of nuclear risk in contemporary conflict" and warned of "nuclear threats to the homeland and US allies and partners".

President Joe Biden said that the US would "enhance our force posture in Europe to respond to the change in the security environment".

The US has already announced plans to station two squadrons of fifth-generation F-35 fighter jets, which have the ability to carry the bombs, with the 48th Fighter Wing at RAF Lakenheath.
In October, US officials requested permission from Congress to begin development of a new B61 bomb with a higher payload, arguing that more powerful weapons would "provide the president with additional options against certain harder and large-area military targets".
The documents revealing the decision to station nuclear warheads in the UK were posted on a US government procurement website. One notice, posted in August, requested a private-sector contractor to provide sentry cabins and shields to protect troops in the base's 48th Security Forces Squadron from "forced entry and ballistic attack" from assault rifles on the nuclear weapons site.
"The 48th Security Forces Squadron upcoming nuclear mission is required to operate under ballistic protection," it said.
A second contract, published on Tuesday, advertised for hydraulic ramps for unloading vehicles, noting that the new F35s and "the imminent surety support" had "highlighted the need to replace these much-required facilities".
In response to a US budget document outlining plans for the $50 million (£39 million) dormitory for surety personnel at RAF Lakenheath last year, Maria Zakharova, a Russian foreign ministry spokesman, said that Moscow would respond to the return of US nuclear weapons on British soil with "counter-measures".
"If this step is ever made, we will view it as escalation, as a step toward escalation that would take things to a direction that is quite opposite to addressing the pressing issue of pulling all nuclear weapons out of European countries," she said.
"In the context of the transition of the United States and Nato to an openly confrontational course of inflicting a 'strategic defeat' on Russia, this practice and its development force us to take compensating countermeasures designed to reliably protect the security interests of our country and its allies."
The construction of the site could also be subject to legal challenge by the Campaign for Nuclear Disarmament, which argues that the Ministry of Defence did not conduct required environmental impact assessments before approving the development.
The US currently has warheads stationed in Belgium, Germany, Italy, the Netherlands and Turkey, under a Nato nuclear-sharing arrangement.
A Pentagon spokesman said: "The United States routinely upgrades its military facilities in allied nations. Unclassified administrative budget documents often accompany such activities.
"These documents are not predictive of, nor are they intended to disclose any specific posture or basing details.
"It is US policy to neither confirm nor deny the presence or absence of nuclear weapons at any general or specific location."

EDITOR'S COMMENT: Always find ways to irritate Russians!

Do The Iranians Already Have Nukes?

By Sam Faddis
Source: https://andmagazine.substack.com/p/do-the-iranians-already-have-nucs

Jan 30 – The most critical question to ask in the world of intelligence is "Why?".
Iran is in a confrontation with U.S. forces in the Middle East. Three U.S. servicemen in Jordan were just killed in a missile attack staged by Iranian surrogates. At least 34 others were wounded, and eight were evacuated in critical condition.
Iranian media is now making a big deal of playing up the recent night-time launch of a satellite launch vehicle and the placement of three indigenously designed satellites in orbit.
AND Magazine is a reader-supported publication. To receive new posts and support my work, consider becoming a free or paid subscriber.
Why?
Why is Iran continuing to push the envelope with escalating attacks on U.S. forces?
Why do they seem unconcerned about provoking the United States?
Why is the launch of a handful of satellites something so important and something that had to happen right now?
Is it possible the "launch vehicle" in question has another purpose?
The satellites Iran says it placed in orbit were launched on a Simorgh rocket. U.S. intelligence has pointed out for years that this missile could potentially be aimed at improving and enhancing Iran's ballistic missile capability. This launch may, therefore, have nothing really to do with the peaceful use of space and be part of an effort to develop true intercontinental ballistic missiles (ICBMs).
But, here's the real kicker. An ICBM carrying a conventional warhead is close to useless. It would be a very expensive, incredibly complex way of delivering what in the end would be the equivalent of a single

bomb. It might kill a limited number of people. It might severely damage multiple buildings. It would not be capable of doing much more than that.
The only rational strategic military use of an ICBM is to deliver a nuclear warhead.
What then might the sudden rush to push the development of the Simorgh missile tell us about where Iran stands on its nuclear program? Might it be strong evidence that the Iranians, in fact, already have nuclear weapons and are now finalizing the work necessary to be able to deliver those weapons to their targets?
That, unfortunately, is entirely possible.
Experts have been warning for some time that Iran has already passed the point of no return. They must now be considered to be a nuclear threshold state, and we must recognize that we no longer have the ability to prevent them from acquiring nuclear weapons.
The International Atomic Energy Authority (IAEA) has warned recently that Iran has ramped up its production of the highly enriched uranium needed to make atomic bombs.
David Albright, a former UN weapons inspector in Iraq, has gone further. He has warned that Iran could produce enough highly enriched uranium for 12 atomic bombs in a matter of months and already has the technical knowledge necessary to build nuclear weapons.
The head of the IAEA is also on record as having stated the obvious.
"There's no other country other than those making nuclear weapons reaching those high levels" of uranium enrichment, Rafael Mariano Grossi said of Iran. "I've said many times that this doesn't mean that Iran has a nuclear weapon. But it does mean that this level of enrichment is one that requires an intense verification effort."
That was in 2021, and the implication was clear. No matter what the Iranians say, they are clearly developing nuclear weapons and intend to acquire them. The only question is when they will cross the line.
Step back for a moment and consider the events unfolding in the Middle East and add in for the sake of argument the assumption that the Iranians have nuclear weapons and are finalizing the details of how to deliver them. Does what you are seeing make more sense now? Rogue states all over the world have long since assimilated the implications of North Korea's decision to acquire nuclear weapons. It means that the United States cannot even contemplate direct military action against Pyongyang for fear of a nuclear exchange. Even setting aside the possibility that the North Koreans may be able to hit the United States the devastation that North Korea could inflict on U.S. allies like South Korea and Japan is sobering. Washington dare not act toward Kim Jong Un as it did against Saddam and Qaddafi.
Now think about the aggressive nature of the actions of Iranian surrogates, the continued Houthi attacks in the Red Sea, and the calls by various Iranian officials for attacks inside the United States. Is what you are seeing simply a reflection of the weakness and compromise of the Biden administration or is something else afoot? Might we be inching closer to the day that the Iranians will announce they are in possession of a nuclear arsenal, they have the necessary delivery capability, and any actions against them will cross a "red line" and necessitate strikes on Tel Aviv, Riyadh and other key targets in the Middle East?

Sam Faddis is a retired CIA Operations Officer. Served in Near East and South Asia. Author, commentator. Senior Editor AND Magazine. Public Speaker. Host of Ground Truth.

The Next North Korea? Lessons for Addressing Iran's Nuclear Program

Source: https://www.iranwatch.org/our-publications/roundtables/next-north-korea-lessons-addressing-irans-nuclear-program

Jan 31 – Iran is a threshold nuclear state that has the capability to build nuclear weapons should its leadership so decide. It has also become a major developer and proliferator of missile technologies, some of which could be capable of delivering weapons of mass destruction. This has raised concerns that Iran may, in some ways, be the "next North Korea"—concerns supported by some noteworthy historical parallels. As the United States formulates its next steps in addressing the Iranian nuclear program, it could learn from what did and did not work in its policy towards North Korea and consider whether and how those lessons might now apply to Iran.
On October 21, 1994, the United States and North Korea concluded the Agreed Framework, under which North Korea

agreed to freeze its production of plutonium in exchange for the supply of nuclear power reactors and heavy fuel oil.[1] The two countries also agreed to work toward normalization of their diplomatic and trade relations. The agreement unraveled in 2002, however, after the revelation of a secret North Korean uranium enrichment program.

Although multilateral diplomatic efforts continued in the years that followed and North Korea expressed a conditional willingness to abandon its nuclear programs as late as September 2005,[2] by October 2006 the country had successfully conducted its first nuclear test. Today, North Korea is estimated to have dozens of nuclear weapons and the means of delivering them to intercontinental ranges. This arsenal has made Pyongyang a more potent threat to its neighbors and adversaries and also has heightened the risk of onward proliferation from North Korea to other states and non-state groups.

Diplomatic efforts over Iran's nuclear program in recent years have had some noteworthy parallels. In 2015, the United States, Iran, China, France, Germany, Russia, the United Kingdom, and the European Union concluded the Joint Comprehensive Plan of Action (JCPOA). Under the agreement, which was notably broader in scope than the Agreed Framework, Iran exported its stockpile of enriched uranium and accepted temporary restrictions on its enrichment and reprocessing activities as well as enhanced transparency measures.[3] The JCPOA similarly supported the development of civil nuclear energy in Iran, but also removed some of the most crippling sanctions on it. This agreement, too, unraveled, beginning with the U.S. withdrawal in 2018.

As of 2024, the JCPOA appears unrecoverable. Iran's development and deployment of advanced centrifuges have made it nearly impossible to restore the JCPOA's one-year breakout timeline, and the accord's temporary limits have already begun reaching their expiration dates. Iran now has enough fissile material (if enriched further to weapons grade) to fuel at least five nuclear weapons.

Will Iran follow a trajectory similar to that of North Korea and soon develop nuclear weapons? Or are there reasons why the outcome may be different? What lessons, if any, can the United States and like-minded countries learn from the North Korean case to bolster their non-proliferation efforts with respect to Iran?

In October 2023, the Wisconsin Project convened an expert panel for a private roundtable discussion to answer these questions. The objective of the discussion is to explore what lessons the North Korean case holds that may assist the United States in its use of diplomacy, sanctions, and other tools to prevent Iran from building nuclear weapons or to contain it if it does.

The panel discussion was moderated by **Valerie Lincy**, executive director of the Wisconsin Project, and **John Lauder**, former director of the U.S. intelligence community's Nonproliferation Center and now a senior fellow at the Wisconsin Project. The panelists were **Eric Brewer**, deputy vice president for the Nuclear Materials Security Program at the Nuclear Threat Initiative; **Amb. Joseph DeTrani**, who served as a special envoy for the Six Party Talks with North Korea in the U.S. State Department; **Robert Einhorn**, a senior fellow at the Brookings Institution who served as assistant secretary of state for nonproliferation in the U.S. State Department; **Amb. Robert Gallucci**, who served as a special envoy in the U.S. State Department and chief U.S. negotiator during the North Korean nuclear crisis of 1994; **Dr. Chen Zak Kane**, director of the Middle East Nonproliferation Program at the James Martin Center for Nonproliferation Studies; **Michael Singh**, managing director and Lane-Swig Senior Fellow at the Washington Institute for Near East Policy; and **Vann Van Diepen**, who served as principal deputy assistant secretary of state for international security and nonproliferation in the U.S. State Department. John Caves and John Krzyzaniak, senior research associate and research associate at the Wisconsin Project, also participated in the discussion. Mr. Krzyzaniak prepared this report.

Finding Highlights

The panel found that, though there are significant differences between the two cases, North Korea offers important lessons for Western efforts to prevent Iran from building nuclear weapons.

On the diplomatic front, Iran may be generally more amenable than North Korea was to an agreement that leaves it without nuclear weapons, given Tehran's longstanding hedging strategy. If nuclear diplomacy with Iran is revived, however, Western policymakers would be well advised to determine at the outset whether the agreement they seek with Iran is to be broadly transformational of the bilateral relationship or narrowly transactional on the nuclear issue, and to communicate this clearly both to Iran and their own publics. Further, the objectives of negotiations should be aligned with the available leverage. More ambitious agreements will generally require larger incentives, and economic incentives alone may not suffice.

The panel emphasized the importance of a credible military threat to deter a country from crossing the nuclear threshold, the absence of which may have been a key factor in North Korea's acquisition of nuclear weapons. It noted several challenges involved in maintaining such a threat against Iran. According to the panel, though, the North Korea case also demonstrated that even after a country builds nuclear weapons, there may still be value in reaching agreements that place limits on a country's ability to improve the quality or quantity of those weapons.

Apart from diplomacy and military force, the panel concurred that other tools in the nonproliferation toolkit can be useful in slowing a country's nuclear progress, but there is no silver bullet. Sanctions and export controls can create hurdles for the proliferator, but these work best when they are implemented by a broad international coalition and deployed alongside other tools. Acts of sabotage may buy time if they are

successfully executed but may have limited utility over the long term, especially against a nuclear program as advanced as Iran's.
The panel also found that, like North Korea, Iran may prove more reluctant to contribute to onward proliferation of nuclear weapons technology than it has been with missiles and drones. Yet some panelists thought there was a risk that Iran would be open to selling its centrifuge technology if there were a ready buyer.
Following are the roundtable's findings in greater detail. They are a composite of the panelists' individual views, and no finding should be attributed to any single panelist or be seen as a statement of the policy of any organization with which a panelist is affiliated.

North Korea is a limited analog for Iran but still offers important lessons.
The two countries occupy very different geostrategic environments bearing on their nuclear decision-making. The threat of invasion has been a major strategic preoccupation for North Korea, and nuclear weapons provided the Kim regime a means by which to offset the country's conventional military inferiority relative to the U.S.-South Korean alliance. Iran, by contrast, has perceived no real threat of invasion since shortly after the fall of Saddam Hussein in Iraq, reducing the need for nuclear weapons as a means to safeguard territorial integrity.
Somewhat paradoxically, however, a "military option" to prevent North Korea's acquisition of nuclear weapons was effectively ruled out early on in the U.S. decision-making process on addressing the North Korean nuclear program, both because of the massive artillery threat posed by Pyongyang against Seoul and because of the Kim regime's early possession of weapons-grade plutonium. In Iran's case, however, both the United States and Israel have stated explicitly that they will not allow Iran to acquire nuclear weapons, implying the use of force to halt a breakout scenario.
North Korea has also been much less susceptible to economic pressures than Iran has been. North Korea has more modest economic needs, attaches lower priority to its people's economic welfare, and has a lifeline to China. Iran, by contrast, has relied heavily on oil export revenues, has perceived its regime's survival as requiring a somewhat greater emphasis on its citizens' economic well-being, and to that end has sought greater integration into Western-led global financial and trading systems. In short, Iran has long insisted on, economically, not becoming another North Korea.
Finally, North Korea pursued a fairly direct path to nuclear weapons and may have always viewed their attainment as a concrete objective, whereas Iran has pursued more of an indirect, hedging path. Although Iran's government is authoritarian, it is a system of ruling elites that largely functions by consensus, and differing opinions among those elites may partially explain Iran's nuclear path over time.
These differences generally tilt in favor of an Iran that may be more amenable than North Korea was to deal-making and off-ramps that leave it without nuclear weapons, at least for certain periods of time. However, there are early signs that some of these differences may be diminishing. For example, Iran seems to have recently become less interested in integration with the Western-led economic order and more comfortable as a member of an "Axis of the Sanctioned" with Russia and North Korea, in which it would hold, like those countries, an economic lifeline to China. Further, the moderates in Iran more likely to shy away from the risks associated with obtaining a nuclear weapon capability have been increasingly sidelined since the collapse of the JCPOA, whereas hardliners, including elements of the Islamic Revolutionary Guard Corps (IRGC) have gained prominence as a center of political power. Finally, Iran may be more confident that it can withstand U.S. or Israeli military strikes in the event that it did decide to attempt a nuclear breakout compared to a decade ago.
In sum, although caution is warranted, the panel concluded that there is enough similarity that the nonproliferation experience with North Korea holds instructive lessons for policy toward Iran.

Iran still may have reasons to remain "hyper-latent" without crossing the nuclear threshold.
A decision to build nuclear weapons by Iran would entail great risks. At worst, it could lead to military strikes that threaten the survival of the regime. Even a less extreme outcome could involve severe, long-term diplomatic and economic isolation, including by countries that have offered Iran a lifeline in the past. Further, an Iranian bomb could prompt other countries in the Middle East to follow suit. Saudi Arabia's Crown Prince Mohammed bin Salman, for instance, has openly stated that if Iran gets nuclear weapons, "we have to get one."[4]
Nuclear weapons may also bring few practical benefits to Iran. On balance, its diplomatic and military position has improved over the last two decades. On the international stage, Iran has become more aligned with Russia and China, diluting the multilateral consensus against Tehran. It also boasts stronger influence across the region, particularly in Iraq, Lebanon, Syria, and Yemen. Both the country's own armed forces and the non-state groups that it supports possess potent conventional weapon capabilities, which they have repeatedly used. In short, Iran has made strides towards achieving its security and foreign policy goals without nuclear weapons.
In other words, according to the panel, Iran's leaders could perceive that there is relatively scant upside to openly building nuclear weapons, whereas there may be substantial downsides to doing so. In such a case, the leadership may be inclined to maintain the country's current "hyper-latent" status, sustaining the

industrial and technological capacity to rapidly forge a nuclear arsenal without actually doing so. Such a status has little global precedent, although Japan and Brazil broadly present somewhat similar cases.

In diplomatic efforts, policymakers should decide and make clear whether the non-proliferation agreement they seek is to be transformational or merely transactional.

In both the Agreed Framework with North Korea and the Joint Comprehensive Plan of Action (JCPOA) with Iran, there were unresolved differences—both between and within governments—over whether the agreements were intended to be transformational to the bilateral relationship or merely transactional on the nuclear issue. For example, in the case of the Agreed Framework, the North Koreans likely understood preambulatory language committing both sides to "full normalization of political and economic relations" as a key part of the agreement, whereas the Americans may not have viewed the language as operative, recognizing that such a transformation in the relationship was unlikely.

In the case of the JCPOA, policymakers in the United States disagreed over the extent to which the accord would attempt to change the broader U.S.-Iran relationship. Some saw it as narrowly focused on the issue of non-proliferation. For them, while there was a possibility it would eventually change the political relationship, this was not the core rationale for the accord. Others, however, saw the JCPOA as a means by which to bring about a broader change in U.S.-Iran relations. These diverging perceptions complicated the task of building and sustaining domestic political support for the accord. A lesson from both the North Korean case and the JCPOA, therefore, is to clearly communicate the desired scope of the agreement to both Iran and Western publics and to align the agreement's language with the intended scope.

A related issue is the alignment of negotiating objectives with the available leverage. The more limited the leverage the United States and its partners have and the fewer incentives they have (or are willing) to offer, the more modest the goals must be. Situations of limited bargaining chips are probably better suited to aims that are more transactional as opposed to transformational. In the case of Iran, President Trump withdrew from the JCPOA in 2018 in the hopes of negotiating a better deal that also extended well beyond the nuclear issue. Although his administration sought to use sanctions to increase its leverage for eventual diplomatic bargaining, the objectives it sought were probably too ambitious for the concessions it was prepared to offer.

What can be defined as realistic is also constantly in flux. Policy goals that are viable today may not be so tomorrow. For example, the restrictions contained in the JCPOA were designed to ensure that Iran's breakout time would be at least one year. Today, achieving a one-year breakout time in any new agreement with Iran would be much more difficult given Iran's development and deployment of advanced centrifuges.

The panelists also noted that getting an ambitious deal requires a strong international coalition, including at least tacit support or non-interference from Russia and China. They acknowledged, however, that the current international political climate will make it difficult for the United States and its partners to elicit constructive engagement from Russia or China on the Iranian nuclear issue in the near term. Nonetheless, the high geostrategic and economic importance of the Persian Gulf region and the risk of war in an Iranian breakout scenario may make it possible that China, and perhaps also Russia, would choose not to obstruct Western diplomatic efforts under the right circumstances.

Even after a proliferator declares possessing or successfully tests a nuclear device, an agreement that places limits on its ability to amass an arsenal can still provide valuable security benefits.

The possibility of reaching smaller, more modest deals with North Korea that could be of security benefit to the United States has likely been undercut by the fact that the United States has not—at least publicly—been prepared to accept agreements falling short of "complete, verifiable, irreversible denuclearization" of the Korean peninsula. For example, at the Hanoi summit in 2018, North Korean leader Kim Jong Un had offered to shut down the facilities at the Yongbyon Nuclear Research Center in exchange for the lifting of all U.N. sanctions against North Korea adopted since 2016.[5] That proposal heavily favored North Korea, but the panelists argued that, rather than walk away, it would have been better for the United States to come back with a counterproposal to Kim's offer with incentives more appropriate to the limited benefit of the shutdown.

More generally, when disagreements with a would-be proliferator arise during diplomatic exchanges, it is usually better for the United States and its partners to stay engaged than it is to walk away. This does not mean that any diplomatic agreement is better than no agreement, nor did the panelists endorse talks for the sake of talks. Rather, the panel found that serious and sustained diplomatic engagement and a willingness to consider compromise, while not acquiescing in any bad deals, will still often yield better results than a "my way or the highway" approach.

The panelists also judged that greater attention should be placed on devising strategies for deterring both Iran and North Korea in their further development or potential use of nuclear weapons. Deterrence policy also needs to be complemented by strategic assurances to U.S. allies and regional partners, some of which have the potential to develop nuclear weapons in the future themselves.

Credible threats of military force can be a powerful tool to deter a dash for the bomb, but using military force comes with risks and limitations.

One of the most effective policy tools for deterring Iranian leaders from building nuclear weapons is the threat of severe consequences, including military action, should they attempt to do so. In the case of North Korea, a lack of a feasible military option made it harder to deter a dash for the bomb.

However, the panelists acknowledged several potential pitfalls. First, any military operation would require timely and actionable intelligence of an ongoing nuclear breakout or sneak-out. Second, because Iran's nuclear infrastructure is both well distributed and hardened against attack, a single surgical strike might disrupt the Iranian effort, but likely would not suffice in permanently halting a march toward the bomb. Iran would probably rebuild its facilities and resume progress towards a nuclear weapon within a few years or less. To forestall that possibility, a military option might instead involve a broader series of strikes over some period of time. But such an operation would be more politically difficult and militarily complex and would still risk falling short of its objectives.

Iran has gone to great lengths in the past to rebuild facilities after they have been the target of sabotage operations, often hardening them against future attacks. For example, after a centrifuge assembly hall at Natanz was destroyed in an explosion in July 2020, the Atomic Energy Organization of Iran decided to rebuild the facility underground. Some panelists observed that short-term setbacks to a nuclear program gained through limited strikes or sabotage, though sometimes justified or necessary in the near term, can paradoxically be counterproductive over the longer term.

An American leader's willingness to commit the United States to military action also depends heavily on the context of the moment. In 2007, the Bush administration was reluctant to conduct an airstrike to destroy a suspected nuclear reactor under construction in Syria even though the operation would have been relatively straightforward and had a high likelihood of success. Having already become tied down in two wars, including one that was at least partially motivated by concerns over a clandestine nuclear program, there was little appetite within the Bush administration to risk a third. Ultimately, Israel decided to destroy the facility unilaterally. But Israel may not be willing or able to successfully execute a similar operation on its own against Iran's much larger, harder, and more dispersed nuclear program.

Economic incentives alone may not be sufficient to change a country's calculus if it seeks nuclear weapons for security or other reasons. It may be possible, however, to reduce the country's demand for nuclear weapons by providing the security guarantees or political outcomes it wanted nuclear weapons to achieve, but this is easier said than done.

States may seek and build nuclear weapons for reasons of national security, prestige, domestic politics, or a combination of factors. In theory, to the extent that the United States and its partners can offer incentives that displace or compensate for these motivating factors, they may be able to convince a proliferator not to cross the nuclear threshold.

A challenge arises, however, when the would-be proliferator doubts the United States and its partners can truly deliver on such incentives and sustain them over time. For example, if the United States itself comprises a large part of the threat that the country perceives against its own security, an offer on paper of U.S. guarantees without a substantial change in the United States' own national security posture may hold little value in the eyes of the proliferator.

The available menu of concrete incentives that can be offered is often limited for a variety of reasons, including domestic politics or pre-existing commitments to allies and partners who are themselves threatened by the proliferator, such as South Korea or Israel. Delivering on relatively limited measures such as the construction of nuclear power reactors in the case of the Agreed Framework or sanctions relief under the JCPOA proved difficult, including because of concerns and objections by members of the U.S. Congress. In sum, to be able to reach a deal in the future, Tehran must be enticed by the trade-offs and be confident that the United States and other parties would follow through on their commitments.

Iran has proliferated missile and drone technologies extensively, including to non-state groups, but would likely be more hesitant to spread its nuclear weapon technologies.

The panel assessed that if Iran were to build nuclear weapons, there are reasons to believe it would hesitate to contribute to onward nuclear proliferation. This stands in contrast to Iran's proliferation of missile and drone technologies. Scholars have pointed out several reasons why countries may be reluctant to transfer complete nuclear weapons or fissile material to other countries or to non-state actors, including that a forensic analysis could allow investigators to eventually identify the source of the material, and this could prompt international condemnation and severe consequences upon the proliferator.

The North Korea case provides reason for cautious optimism. While it has been a source of extensive onward missile proliferation, it has been more limited in its transfer of nuclear weapons technology abroad. A notable exception was North Korea's role in the construction of a nuclear reactor in Syria presumed to be capable of producing enough plutonium for one or two weapons per year, had it become operational. Notably, there is no evidence that Iran was involved in the Syrian nuclear program. This does not rule out the possibility of an Iranian A. Q. Khan. There is a risk that a well-connected individual motivated by profit could sell Iranian

nuclear technologies. But the risks of a freelancing nuclear scientist have always been present, and Iran's decision to build a bomb may not significantly alter them. Some panelists thought there was some risk that Iran would be willing to sell its centrifuge technologies to other countries. However, it is not immediately clear which country or countries would be interested in purchasing them. An additional reason not to share nuclear weapon technologies for at least several years following the first test of a nuclear device is that the prevailing imperative would be to build up its own nuclear arsenal. Given limited resources, Iran may decide it has little to no weapons-related materials and technologies to spare, at least at first.
Some on the panel also warned of a possible—though not likely—case of onward nuclear proliferation might involve a quasi–"forward deployment" of nuclear weapons with IRGC Qods Force units on the territory of Iran's proxies. Such a scenario would be consistent with how Iran has shared other military technologies with non-state groups throughout the region and might confer some "extended deterrence" benefits while allowing Iran to maintain some control over the weapons and their employment. Other panelists, however, thought this was a remote possibility at best. There was also concern among some panelists about the possibility that Iran may be willing to proliferate radiological sources to aligned non-state groups.

Sanctions and export controls can create hurdles for the proliferator, but they work in different ways.
Comprehensive economic sanctions are essentially a tool of coercion, particularly when they are imposed on broad sectors of a country's economy. Existing scholarship on the effectiveness of sanctions generally finds that they work best when they are swift, substantial, and attached to a clear objective. Their imposition should ideally be coupled with a clear statement about what changes in behavior by the target would lead to their lifting. In the best of cases, sanctions can create pressure and induce an adversary to change its policies. Export controls and targeted sanctions aimed at specific entities in a weapon program, by contrast, are tools of prevention, and their impact unfolds over decades. They can slow a proliferator's acquisition of critical enabling technologies and raise program costs. Export controls can also be supported by targeted sanctions on entities involved in developing, manufacturing, procuring, or supplying goods or technologies for a nuclear program. The panelists agreed that both tools work best when they are implemented by a united international coalition. When sanctions or export controls are only imposed unilaterally or by only a limited set of countries, the target country will have an easier time evading the measures—though unilateral U.S. financial sanctions, with their wide-reaching application, remain a potent tool. Ultimately, though they can hinder a nuclear program, neither sanctions nor export controls may be sufficient on their own to stop a determined proliferator.

Footnotes:
[1] "Agreed Framework Between the United States and America and the Democratic People's Republic of Korea," October 21, 1994, available at https://peacemaker.un.org/node/1129.
[2] "Joint Statement of the Fourth Round of the Six-Party Talks, Beijing, September 19, 2005," U.S. Department of State, September 19, 2005, available at https://2001-2009.state.gov/r/pa/prs/ps/2005/53490.htm.
[3] "Joint Comprehensive Plan of Action," July 14, 2015, available at https://www.europarl.europa.eu/cmsdata/122460/full-text-of-the-iran-nuclear-deal.pdf.
[4] Matt Spetalnick and Eric Beech, "Mohammed bin Salman Says Saudi Arabia is Getting 'Closer' to Israel Normalization," Reuters, September 20, 2023, available at https://www.reuters.com/world/middle-east/saudi-crown-prince-says-getting-closer-israel-normalization-fox-interview-2023-09-20.
[5] "The February 2019 Trump-Kim Hanoi Summit," Congressional Research Service, March 6, 2019, p. 2, available at https://sgp.fas.org/crs/row/IN11067.pdf.

●▶ **Read also:** A History of Iran's Nuclear Program

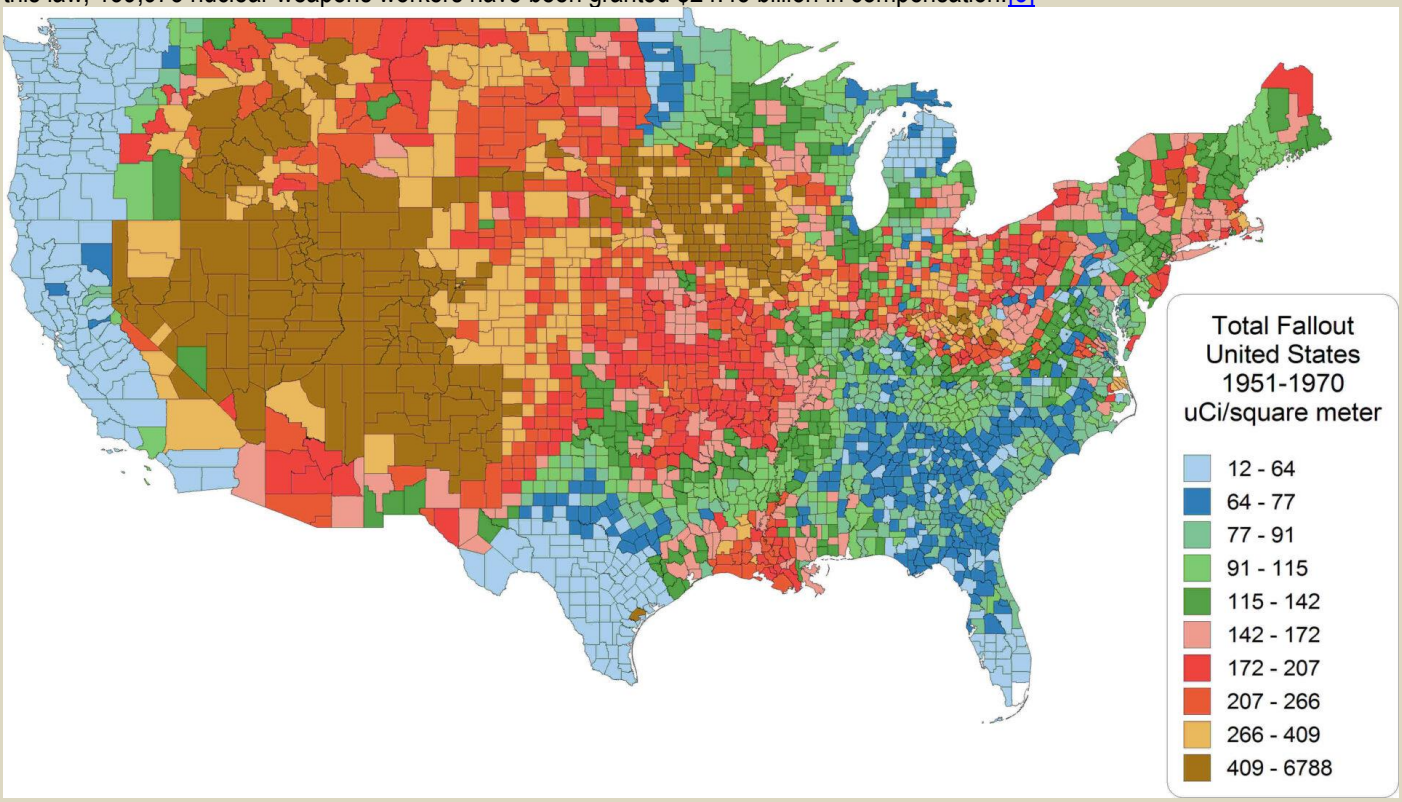
Seeking justice for radiation victims of the US nuclear program

By Robert Alvarez
Source: https://thebulletin.org/2024/02/the-fallout-never-ended/

Feb 02 – Congress recently decided not to expand the 1990 Radiation Exposure Compensation Act to include several additional Western states (including Trinity Test downwinders in New Mexico), as well as tribal uranium miners and Missouri residents impacted by contamination from illegal dumping of Manhattan Project wastes. As the empirical evidence of the radiological legacy of the Manhattan Project and the early Cold War grows, the Congressional Budget Office puts the price-tag for the expansion of RECA to include victims not accounted for in earlier legislation at $147 billion over the next 10 years.[1] Despite the price tag and the recent congressional decision not to expand RECA, the effort to gain compensation for more radiation victims is far from dead—especially

with elections looming in less than a year. RECA expansion has received unusual bi-partisan support in Congress, especially from members representing "red states" impacted by the early nuclear weapons program. And cancer victims and their families are well organized and not giving up.

RECA is unique in that it offers an explicit congressional apology and financial restitution for placing Americans into harm's way without their knowledge or consent. As of May 2022, compensation benefits have been paid out to 30,092 Nevada Test Site downwinders and onsite participants, totaling $1.63 billion. Under RECA, 9,098 uranium miners and process workers who worked up to 1971 have received $974 million in compensation benefits, including health care.[2] In terms of the overall compensation picture, an important element of the story is the Energy Employee Occupational Illness Program Compensation Act of 2000. Under this law, 139,973 nuclear weapons workers have been granted $24.45 billion in compensation.[3]



Gen. Leslie Groves, the director of the Manhattan Project, constructed a barrier intended to block legal claims for radiation injuries and illnesses, but it began to crack by the 1980s and now has crumbled. Groves believed that such compensation was a dagger aimed at the heart of the nuclear weapons program. Given widespread radiation exposure problems, concerns over financial and legal liabilities also influenced a wide variety of radiation-protection decisions. According to Stafford Warren, medical advisor to Groves, an overriding concern was to protect "the government interests" against legal claims.[4]

In a memo regarding possible declassification of a study suggesting that occupational radiation exposure levels "may be too high," the head of the Insurance Branch of the AEC declared:

"We can see the possibility of a shattering effect on the morale of the employees if they become aware that there was substantial reason to question the standards of safety under which they are working. In the hands of labor unions the results of this study would add substance to demands for extra-hazardous pay ... [K]nowledge of the results of this study might increase the number of claims of occupational injury due to radiation."[5]

The US government spared no expense to fight lawsuits filed by people living close to nuclear testing grounds. Without exception, the courts ruled in favor of the agency then in charge of the country's nuclear program, the Atomic Energy Commission. Since the US nuclear weapons program controlled all federal research of radiation health effects and kept radiation fallout data behind a curtain of secrecy, the deck was stacked against "down-winders," who had few resources and no security clearances. It became clear that secrecy, isolation, and privilege had corrupted science and violated the public trust—for the purpose of amassing the world's largest arsenal of weapons of mass destruction.

By 1987, the overarching legal approach that Groves set during World War II was still alive and well at a meeting of the Health Physics Society that I attended. The main speaker was Brian Seibert, an attorney from the Energy Department who gave a speech titled, "Radiation: the Offense and the Defense." In a room filled with nuclear industry employees, he prefaced his presentation by declaring "this is the party

line" and then proceeded to expatiate on how successful radiation compensation claims would seriously curtail nuclear weapons, nuclear power, and nuclear medicine.
He then introduced the group to Mr. Don Jose, a US Department of Justice litigator, who was to lead workshops sponsored by the society around the country to train health physicists, the people responsible for nuclear health and safety, to become expert witnesses against claimants.
Although his speech was, to say the least, ethically dubious, the Energy Department attorney was correct in saying that compensation for radiation injuries and diseases remains an important force shaping a broad array of technical and policy issues involving medicine, science, public health, energy production, environmental protection, and national security. In addition to helping victims of the government's various nuclear activities, compensation for illicit exposures of the public to radiation also plays a powerful role in radiation standard setting, economics, and public acceptance of nuclear technologies.
But Americans who were endangered by the government without their knowledge deserve justice and accountability. "What good is it to defend our country with nuclear weapons, if we poison our people?" former Sen. John Glenn often asked. This question still deserves an answer as we come to terms with the human price for unlocking atomic fire.

Notes

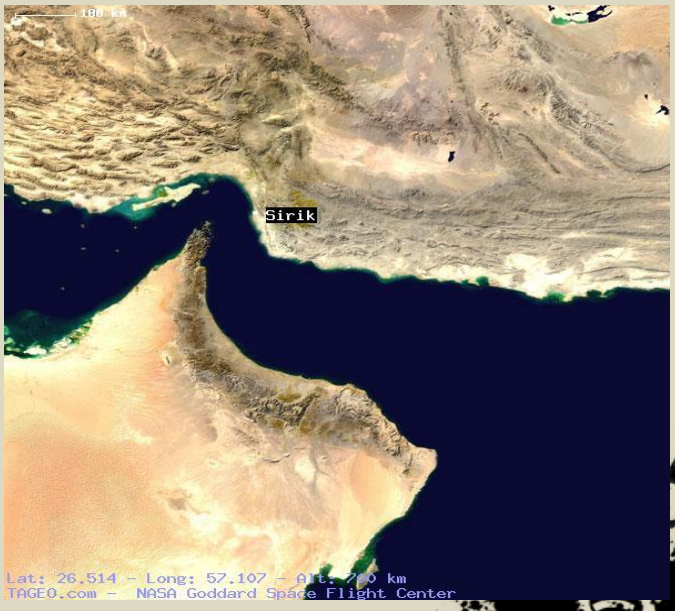
[1] NDAA Includes $150 Billion Deficit-Increasing Program, Committee for a Responsible Federal Budget, October 2023. LINK
[2] The Radiation Exposure Compensation Act (RECA): Compensation Related to Exposure to Radiation from Atomic Weapons Testing and Uranium Mining, Congressional Research Service, Table A-1, June 2022. LINK
[3] Department of Labor, Office of Workers' Compensation Programs (OWCP) EEOICP Program Statistics, June 22, 2023. LINK
[4] Barton Hacker, The Dragons Tail, University of California, 1987, p.51.
[5] Report of the President's Advisory Committee on Human Radiation Experiments, Part II, Chapter 13. LINK

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

Iran Begins Building 4 More Nuclear Power Plants

Source: https://www.voanews.com/a/iran-begins-building-4-more-nuclear-power-plants/7467128.html

Feb 01 – Iran began construction on four more nuclear power plants in the country's south, with expected total capacity of 5,000 megawatts, the official IRNA news agency reported Thursday.
Iran seeks to produce 20,000 megawatts of nuclear energy by 2041.
The country has one active nuclear power plant, a 1,000 megawatt plant that went online with help from Russia in 2011. It's also building a 300-megawatt plant in the oil-rich Khuzestan province, near the western border with Iraq.
The U.N.'s nuclear watchdog said last year that Iran has increased the rate at which it is producing near-weapons grade uranium.
Director General Rafael Grossi said in the report that Iran "in recent weeks had increased its production of highly enriched uranium, reversing a previous output reduction from mid-2023," according to an IAEA spokesperson. Iran had previously slowed the rate at which it was enriching uranium to 60% purity, which is just a short technical step away from the weapons-grade level of 90%.



The West has long suspected that Iran is acquiring nuclear weapons. Iran denies it is seeking such weapons.
IRNA quoted Mohammad Eslami, the head of Iran's atomic agency, saying it will take up to nine years to complete the new plants.
The report said the four new plants are being built in the port town of Sirik on Iran's east coast, about 1,150 kilometers south of the capital, Tehran. Nasser Shariflou, the head of the project, told IRNA that the project will cost about $20 billion and will create 4,000 jobs. Each plant is expected to use 35 tons of nuclear fuel per year.

The Iran Threat Geiger Counter: Reaching Extreme Danger

By The Institute for Science and International Security
Source: https://www.homelandsecuritynewswire.com/dr20240207-the-iran-threat-geiger-counter-reaching-extreme-danger

Feb 07 – A national security threat is typically posed by a combination of hostile intentions and capabilities. The threat from Iran's nuclear program is no exception. The Iran Threat Geiger Counter from the Institute for Science and International Security measures on a regular basis Iran's hostile actions and intentions toward the United States and U.S. allies, and its capability to turn these hostile intentions into action through the potential or actual construction of nuclear weapons. As with the radiation levels measured by a Geiger counter, any level above zero represents a degree of danger.
Since May 2023, the date of the last edition of the Counter, the threat posed by Iran's nuclear program has increased dramatically. This increased threat has been in part fueled by the Hamas terrorist attacks on Israel on October 7, 2023, Israel's subsequent invasion of Gaza, and subsequent attacks carried out by Iranian-backed proxy groups, including Palestinian Islamic Jihad, Hezbollah, and Ansar Allah (Houthi). The volatile situation in the region is providing Iran with a unique opportunity and amplified internal justification for building nuclear weapons while the United States and Israel's resources to detect and deter Iran from succeeding are stretched thin. The ongoing conflicts are leading to the neglect of the Iranian nuclear threat at a time when Iran's nuclear weapons capabilities have never been greater. Coupled with decreased transparency over its nuclear program, for the first time in years, we are facing the real possibility that Iran may choose to weaponize its nuclear capabilities and build nuclear weapons.
These grave and concerning changes have led the Institute to raise the total threat score to 151 out of 180, up from 140 in May 2023, and assessed as **Extreme Danger,** the first time the Counter has reached this level.

Overview of Methodology
The Institute assigns the following threat level using a zero to 180 scale on the Iran Threat Geiger Counter:
0-30: Least Danger 31-60: Low Danger 61-90: Moderate Danger 91-120: Considerable Danger 121-150: High Danger 151-180: Extreme Danger
The Iran Threat Geiger Counter analyzes Iran's activities in six categories and assigns up to 30 points for each category:
Hostile Actions (30 Points Max) Hostile Rhetoric (30 Points Max) Lack of Transparency (30 Points Max) Nuclear Breakout (30 Points Max) Sensitive Nuclear Capabilities (30 Points Max) Beyond Breakout (30 Points Max)
The scoring system for each category is the following:
0-5: Least Danger 6-10: Low Danger 11-15: Moderate Danger 16-20: Considerable Danger 21-25: High Danger 26-30: Extreme Danger
The following sections discuss the threat posed by Iran and the allocation of points to each category in detail.

Current Threat: Extreme Danger

Criteria	Total Score: 151	Direction of Change	Danger Level Extreme Danger
Hostile Actions	28	⇧ 3	**Extreme Danger**
Hostile Rhetoric	29	⇧ 1	**Extreme Danger**
Lack of Transparency	21	⇧ 2	**High Danger**
Nuclear Breakout	30	Max	**Extreme Danger**
Sensitive Nuclear Capabilities	22	⇧ 2	**High Danger**
Beyond Breakout	21	⇧3	**High Danger**

The current score of 151 is in Extreme Danger territory. Most of the points are the result of Iran's hostile actions (28 points) and rhetoric (29 points) against the United States and its allies, combined with the fact that Iran's nuclear breakout time remains at zero (30 points). The rest result from Iranian progress on developing sensitive nuclear capabilities (current score of 22 points), increasing its nuclear weaponization efforts beyond breakout (current score of 21 points), and inadequate transparency over its nuclear program (21 points). The scores have increased across the board since May 2023, moving the overall threat score to Extreme Danger. *Institute for Science and International Security, February 2024.*

Iran Threat Geiger Counter in Detail: What Drives the Threat?
Hostile Actions Score: 28 points ⇧
Iran has significantly intensified its hostile activities against the United States and its allies in the wake of the terrorist attack by Hamas against Israel on October 7, 2023, and Israel's subsequent invasion of Gaza. Proxy groups supported and directed by Iran have attacked U.S. forces in the region, causing multiple casualties and deaths. These groups have also targeted international shipping. Meanwhile, Iran continues to support Russia's invasion of Ukraine and target specific individuals on U.S. and European soil for kidnapping and assassination. However, it has also been hesitant about a direct confrontation with the United States.
These hostile activities warrant an increase in the threat assessment score of three points to 28 points (Extreme Danger). At its most basic level, this score measures Iran's level of hostile action against the United States and its allies. These activities – and U.S. and allied reactions to them – are an important backdrop as the Iranian regime contemplates building nuclear weapons.
Significant recent developments include the following:

Iranian Proxy Groups Continue to Attack U.S. Forces in the Middle East
Iranian proxy groups have conducted more than 100 attacks against U.S. forces in the Middle East in 2023 and 2024, most recently killing three U.S. soldiers in an attack in Jordan on January 27, 2024. [1] In addition to ongoing attacks by local proxies against U.S. forces in Jordan, Iraq, and Syria, the Houthi in Yemen have directly targeted U.S. and allied naval units in the Red Sea, most recently launching a major drone and missile strike on January 10. The U.S. and United Kingdom navies shot down 18 drones, two anti-ship cruise missiles, and one anti-ship ballistic missile. [2]

Iran Backed-Proxy Groups Attacked Israel
On October 7, 2023, the Iranian backed terrorist organization Hamas and its affiliate groups in Gaza, including Palestinian Islamic Jihad (PIJ), launched a devastating and horrific terrorist attack against Israel, killing over 1,200 Israeli civilians and soldiers and seizing over 200 hostages.[3] Hamas and its affiliate groups used Iranian-supplied missiles, bombs, and other weapons as well as training and technical help to carry out the attack, although it is unclear if Iran had foreknowledge of when the actual attack would take place. [4] Hezbollah in Lebanon has conducted almost-daily missile strikes against Israel. [5] Houthi militants in Yemen also launched missile strikes against Israel. [6] The war continues to rage today and it is clear that Iran's extensive assistance was critical in enabling Hamas and other organizations to maintain military operations against Israel.

Iranian Proxy Groups Attacked International Shipping with Iranian Assistance
In support of Hamas, Iranian proxy groups, in particular the Houthi in Yemen, have launched dozens of attacks against international commercial shipping transiting through the Gulf of Aden, the Red Sea, and the Strait of Bab al-Mandab. [7] The attacks rely on missiles and long-range drones supplied by Iran. The Houthi can carry out these attacks because they have received, and continue to receive, extensive material and logistical assistance from Iran. In mid-January 2024, U.S. Navy Seals conducted a raid on a vessel off the coast of Somalia in the Red Sea, seizing munitions and warheads produced by Iran and en route to Houthi forces in Yemen. [8] Iranian spy ships have provided the Houthi with key intelligence on commercial shipping locations and activities that have enabled them to launch missile and drone strikes. [9]

Iran Continues to Provide Military Hardware to Russia in Support of Its Invasion of Ukraine
Iran has provided Russia's JSC Alabuga extensive assistance to establish and mass produce Shahed-136 kamikaze drones at the Alabuga Special Economic Zone (SEZ), in Yelabuga, Russia. The Institute and the Washington Post have conducted comprehensive analyses on leaked documents from the factory, outlining Russian and Iranian plans to mass produce the drone system, and ultimately make 6,000 drones by September 2025 at the SEZ. [10] Commercial satellite imagery demonstrates that the factory to make drones is operational and improving its perimeter security. [11] Alabuga has further expressed interest in buying from Iran Shahed 129 and 181 drones and the technology to make them.
Media reports indicate that Russia received a limited quantity of reconnaissance/attack Shahed 107 drones from Iran, and possibly the kamikaze-type Shahed 101 drones.[12] The two drones can be used together to identify and attack targets.

Evidence has emerged that Iran is also supplying Russia with artillery shells and ammunition. Reportedly, hundreds of thousands of artillery shells and roughly 100 million rounds of ammunition were delivered via two cargo ships from Iran. [13]
The Wall Street Journal reported that Iran is in active negotiations with Russia to supply hundreds of short-range surface-to-surface missiles for use in its war in Ukraine, although no transfer has yet been observed on the battlefield. [14]

Hostile Rhetoric Point Score: 29 points ⇧
Public statements from Iranian officials indicate an extreme level of hostility (29 points) towards the United States and its allies. Notable recent statements include the following:
Hossein Amir-Abdollahian, the Foreign Minister of Iran, in an interview with Al Jazeera on October 16, 2023, stated in reference to the war between Hamas and Israel that, "All possible options and scenarios are there for Hezbollah … Naturally, resistance leaders will not allow the Zionist regime to take any action in Gaza, and when it feels reassured about Gaza, move on to other resistance areas in the region… Therefore, any preemptive measure is imaginable in the coming hours." [15] Hossein added "the resistance leaders…[will not allow Israel]…to do whatever it wants in Gaza."
Hossein Amir-Abdollahian, the Foreign Minister of Iran, in a statement to the United Nations on October 26, 2023, following Hamas' invasion of Israel and the beginning of the war, threatened that if Israel did not cease its retaliation against Hamas, that the United States would "not be spared from this fire." [16] Mohammad Reza Naqdi, a Brigadier General in the IRGC, following several attacks by Houthi forces against commercial shipping, stated in a threat made on December 23, 2023, that "They [the United States and the West] shall soon await the closure of the Mediterranean Sea, (the Strait of) Gibraltar and other waterways."[17] Naqdi added that, "Yesterday, the Persian Gulf and the Strait of Hormuz became a nightmare for them, and today they are trapped … in the Red Sea."
Ramezan Sharif, a spokesperson for the IRGC, stated on December 27, 2023, in reference to the October 7 attack against Israel that, "The Al-Aqsa Storm was one of the retaliations of the Axis of Resistance against the Zionists for the martyrdom of Qasem Soleimani." [18] These most recent statements must be seen against the backdrop of more than four decades of extreme anti-American, anti-Israel, and anti-Western rhetoric from Iranian officials.

Lack of Transparency Score: 21 points ⇧
Iran continues to deceive the International Atomic Energy Agency (IAEA) and violate its safeguards agreement and JCPOA monitoring agreements. With regards to Iran's cooperation with the IAEA, Director General Rafael Grossi stated at the World Economic Forum in Davos, Switzerland, on January 18, 2024: "It's a very frustrating situation. We continue our activities there, but at a minimum." He added, "They are restricting cooperation in a very unprecedented way…When there's something that France, the UK or the United States says that they don't like, it is as if they were taking the IAEA hostage to their political disputes with others. This is unacceptable for us." [19]
Iran's lack of transparency warrants a threat assessment score of 21 points, an overall increase of two from May 2023. This increase accounts for worsening safeguards compliance and ongoing diminished JCPOA monitoring (High Danger).

Iran Continues to Refuse to Implement the Additional Protocol
A November 2023 IAEA report states that it has been "two years and nine months since Iran stopped provisionally applying its Additional Protocol and, therefore, since it provided updated declarations and the Agency was able to conduct complementary access to any sites and locations in Iran." [20] The IAEA can no longer carry out daily visits to Iran's enrichment facilities or measure in-process low enriched nuclear material. It has not had access to data from on-line enrichment monitors and electronic seals, or access to measurement recordings registered by installed measurement devices.

Safeguards violations and Iranian non-cooperation
Iran has consistently violated its obligations under its comprehensive safeguards agreement (CSA), a key part of the verification of the Nuclear Non-Proliferation Treaty (NPT). It has refused to cooperate with the IAEA and fully account for its past and present nuclear activities, and obstructed IAEA inspections by razing and sanitizing related nuclear sites. For four years, the IAEA has been investigating the presence of anthropogenic (of human origin) uranium particles it detected at three Iranian sites, and was seeking information about nuclear material and activities at a fourth site. [21] The four sites are Turquz Abad, Varamin, Marivan, and Lavisan-Shian. Out of these four sites, three were discussed in Iran's Nuclear Archive, and all four are related to Iran's former and possibly ongoing work on nuclear weapons.
Iran maintains that the Marivan site was a mine operated by "another Member State in the 1960s and 1970s," and that the detected contamination is a product of "laboratory instruments and equipment" used at the site. [22] In late May 2023, the IAEA decided it had no further questions for Iran and drew two conclusions: The IAEA was unable to prove or disprove the mining-related explanations for the presence of uranium made by Iran with the available information, but more importantly, the IAEA stood by its

assessment that Iran conducted undeclared nuclear weapons-related activities at the site, specifically that Iran conducted "explosive experiments with protective shielding in preparation for the use of neutron detectors and nuclear material" at the high explosive test site at Marivan. [23] Thus, the IAEA is stating that while Iran may have prevailed on the relatively small point of the uranium particles, the elephant in the proverbial (Marivan) tent remains present.

Questions regarding two of the sites, Turquz Abad and Varamin, remain unresolved and Iran continues to stonewall the investigations and refuses to provide complete information and evidence. The IAEA states in its November 2023 NPT report that "during this reporting period, Iran has not provided the Agency with any information on the outstanding safeguards issues relevant to either of the two undeclared locations." The IAEA underscores that "despite numerous resolutions of the Board and many opportunities provided by the Director General over a number of years, Iran has neither provided the Agency with technically credible explanations for the presence of uranium particles of anthropogenic origin at two undeclared locations in Iran nor informed the Agency of the current location(s) of nuclear material and/or of contaminated equipment." [24] The IAEA reiterates, "The outstanding safeguards issues stem from Iran's obligations under its NPT Safeguards Agreement and need to be resolved for the Agency to be in a position to provide assurance that Iran's nuclear programme is exclusively peaceful."

Reduced monitoring under the JCPOA

Iran has reduced the monitoring of advanced centrifuge production and assembly under the Joint Comprehensive Plan of Action. For almost three years, the IAEA has not been able to monitor where and how many centrifuges and key centrifuge components Iran has been producing and storing. The IAEA has stated that due to gaps in relevant monitoring, it has concerns about its ability to verify Iran's declared centrifuge numbers even if Iran turned over past video footage and fully cooperated. Over the last months, Iran has not been deploying many additional centrifuges at its declared centrifuge enrichment plants, despite a late 2023 IAEA assessment that Iran continues to make centrifuges. This adds to the concern about Iran's ability to sneak-out to a nuclear weapon, using only a small number of secretly-produced advanced centrifuges.

In the March 2023 Joint Statement, Iran agreed to re-establish JCPOA online enrichment monitors and camera surveillance removed in June 2022. Despite some initial progress on installing cameras, the IAEA reports in its November 15, 2023, NPT report that the Director General "is seriously concerned that Iran appears to have 'frozen' the implementation of the Joint Statement of 4 March 2023 for the past two reporting periods, and questions Iran's continued commitment to its implementation." During a meeting in Vienna held during the IAEA General Conference on September 25, the Director General "expressed his serious concern to Vice-President Eslami that there had been no progress in the implementation of any of the three agreed elements of the Joint Statement for several months" and that this was against the "spirit of cooperation" agreed in the joint statement.

Iran Expels IAEA Safeguards Inspectors

Iran has further degraded the ability of the IAEA to carry out verification and monitoring activities at safeguarded nuclear facilities in Iran. On September 16, 2023, Iran withdrew the designations of several senior IAEA inspectors that conduct verification and monitoring activities. [25] This de-designation removed a handful of inspectors from Iran considered to have the most experience with enrichment technology. Iran took this action after several dozen states, led by the U.S. and Europe, signed a joint statement at the September IAEA board meeting demanding Iran's cooperation with the IAEA's five-year investigation into undeclared nuclear weapons work. [26]

Taking Stock

With Iran's refusal to resolve outstanding NPT safeguards violations and its reductions of JCPOA monitoring, the IAEA has a significantly reduced ability to monitor Iran's complex and growing nuclear program, which in particular has unresolved nuclear weapons dimensions. The IAEA's ability to detect diversion of nuclear materials, equipment, and other capabilities to undeclared facilities remains greatly diminished. Nonetheless, the transparency situation could worsen even further, if, for example, Iran withdrew from the NPT, asked IAEA inspectors to leave the country altogether, or fabricated excuses to temporarily deny inspectors access.

Nuclear Breakout Score: 30 points

In 2022, for the first time, Iran's breakout time became zero, indicating an extreme threat and a score of 30 (Extreme Danger). Iran has more than enough 60 percent enriched uranium, or highly enriched uranium (HEU) to directly fashion a nuclear explosive.

If Iran wanted to further enrich its 60 percent enriched uranium up to 90 percent weapon-grade uranium (WGU), used in Iran's known nuclear weapons designs from the Amad Plan, it could do so quickly. It can break out and produce enough weapon-grade enriched uranium for a nuclear weapon in a week, using only a fraction of its 60 percent enriched uranium. This breakout could be difficult for inspectors to detect promptly, if Iran took steps to delay inspectors' access.

Using its remaining stock of 60 percent enriched uranium and its stock of near 20 percent enriched uranium, it could have in total enough weapon-grade uranium for six weapons in one month, and after five months of producing weapon-grade uranium, it could have enough for 12. [27] (Five nuclear weapons were the original goal of Iran's Amad Plan.)
Moreover, over the last few years, Iran has learned important lessons in breaking out to nuclear weapons by experimenting with and practicing shortcuts in multi-step enrichment.

- Iran started from a level below 5 percent enriched uranium and enriched directly to near 60 percent in one cascade, rather than using two steps, a slower process entailing the intermediate production of 20 percent enriched uranium.
- It built and tested equipment to feed 20 percent enriched uranium and withdraw HEU, possibly enriched to higher than 60 percent; the exact level is unknown. Iran remixed the enriched product with the less enriched waste tails after measuring the product's enrichment level.
- Iran prepared advanced centrifuge cascades to switch more easily from the production of five percent enriched uranium to 20 percent enriched uranium.
- It further developed a multi-cascade set up to produce 20 percent enriched uranium from natural uranium by making 5 percent enriched uranium in advanced centrifuges and then directly feeding this product, still in gaseous hexafluoride form, into IR-1 centrifuge cascades to make near 20 percent enriched uranium. As such, Iran was practicing multi-step enrichment needed to produce weapon-grade uranium while seeking to shortcut the process.

Sensitive Nuclear Capabilities Score: 22 points
Iran continues taking steps to escalate its sensitive nuclear activities. Iran has a capability to produce large amounts of enriched uranium and achieve enrichment levels up to 90 percent, or weapon-grade uranium, a capability implied in April 2023 by Mohammad Eslami, head of the Atomic Energy Organization of Iran (AEOI). [28] Since May 2023, Iran continued to increase its enriched uranium stocks and increased the number of weapon-grade uranium (WGU) quantities it could produce in one month from enough WGU for five nuclear weapons to enough for six nuclear weapons. These activities receive a score of 22 (High Danger), up from 20 in May 2023, reflecting actions taken over the last several months, but leaving room on the scale to account for the strong possibility that Iran's nuclear buildup could continue.
In fact, Iran has ambitious goals to increase its enrichment program, aiming for tens of thousands of advanced centrifuges, producing a range of enrichment levels, and tens of thousands of kilograms of enriched uranium. By 2030, Iran plans to have an enrichment capacity of 125,000 separative work units (SWU) per year. As Iran makes progress toward its goals, these activities will affect the score in this section even if they are allowed by a new or revived nuclear deal. Likewise, if Iran's most threatening nuclear activities were reduced, the score would go down.
As of November 2023, Iran continued to increase the quantity and quality of its enriched uranium stock and bolster its ability to enrich uranium. Uranium enrichment remains the most sensitive activity in Iran's nuclear program. Iran may also develop an ability to produce and separate weapon-grade plutonium, although that effort is largely dormant today.

Stocks of 20 and 60 Percent Enriched Uranium and Capacity to Make Highly Enriched Uranium
Over the summer and fall 2023, Iran decreased the rate at which it produced 60 percent highly enriched uranium, producing only roughly 3 kg (Uranium mass) per month between June 2023 and November 2023. However, in late November 2023, Iran resumed increased production of 60 percent highly enriched uranium, producing about 9 kg per month, similar to what it was producing prior to its slowdown.[29]
Iran has taken a further step to enhance its ability to produce highly enriched uranium by reversing the connection of two IR-6 cascades at Fordow Fuel Enrichment Plant so that the cascade with modified subheaders is now at the end-stage of producing 60 percent rather than being at the beginning stage, enabling Iran to quickly change the overall enrichment level of the cascade.[30] This mode of operation was used previously by Iran in January 2023, but had been undeclared to the IAEA, which subsequently detected the undeclared change and further detected the presence of near-84 percent HEU particles at the cascade's product sampling point.[31]
Iran's most sensitive stocks of enriched uranium, its 60 percent HEU stock and its 20 percent enriched uranium stock, increased steadily over the last months. Its 60 percent HEU stock has reached 128 kg (Uranium mass) and its 20 percent enriched uranium stock has reached 567 kg by end of October 2023.

Enrichment Capacity
As of November 2023, Iran had a total installed nominal enrichment capacity of about 30,800 SWU per year, where advanced centrifuges account for about 24,300 SWU per year and IR-1 centrifuges account for 6500 SWU per year. The amount of separative work achieved in practice is lower, sometimes far lower, due to inefficiencies in centrifuge construction and operation.[32]

Iran's advanced centrifuges make up almost 80 percent of Iran's enrichment capacity and deserve special attention because they pose a grave risk to international security, allowing Iran to produce weapon-grade uranium for a nuclear weapon more quickly, either at declared nuclear sites or at clandestine ones. The presence of advanced centrifuges at the Fordow underground enrichment plant enhances Iran's ability to break out using a declared but highly fortified facility.
Over the summer and fall of 2023, Iran deployed over 350 additional advanced centrifuges. As of November 2023, Iran had 6277 advanced centrifuges of various types installed at its three enrichment facilities at Natanz and Fordow, up from 5919 as of May 2023, as well as 7230 installed IR-1 centrifuges. Most of Iran's advanced centrifuges are installed at the Natanz main enrichment plant and the pilot plant, with some installed at the Fordow underground plant. Iran further announced its intentions to install an additional 14 IR-6 centrifuge cascades at Fordow and an additional 6 IR-4 centrifuge cascades at Natanz. As of November 2023, Iran has not installed additional IR-6 centrifuges at Fordow; however, Iranian progress in doing so would inevitably raise the score in this section further.
Work continued on a new, large, heavily fortified underground site near the Natanz enrichment plant to assemble advanced centrifuges. This site may also be slated to hold another enrichment plant.

Shortened Timeline to Breakout and Produce Enough Weapon-grade Uranium for Six Nuclear Weapons
An indicator of sensitive nuclear activities is a change in the amount of weapon-grade uranium Iran can produce in a breakout. As discussed in the previous section, as of November 2023, not only can Iran produce weapon-grade uranium for its first nuclear weapon in a matter of days, it can produce enough weapon-grade uranium for six weapons in one month, and after five months of producing weapon-grade uranium, it could have enough for 12.

Iran Has Installed a Capability to Produce Highly Enriched Uranium Metal
In the last few years, Iran has developed capabilities at the Esfahan site to produce enriched uranium metal, a necessary step in building nuclear weapons. It has developed a capability to convert enriched uranium hexafluoride, the output of its centrifuge plants, into enriched uranium metal. On a small scale it has converted 20 percent enriched uranium hexafluoride into metal. This accomplishment means that Iran could do the same with weapon-grade uranium hexafluoride.

Iran Remains a Serial Violator of National Export Controls and Sanctions
Iran continued to violate international and national sanctions and strategic trade control laws as it seeks to outfit its nuclear and missile programs. These activities are crucial for Iran, since it does not produce many of the subcomponents and raw materials needed by its nuclear, conventional arms (including drones), and missile programs. Intelligence reports, prosecutions, and sanctions listings continuously highlight Iran's ongoing and often increasing WMD-related procurement efforts.

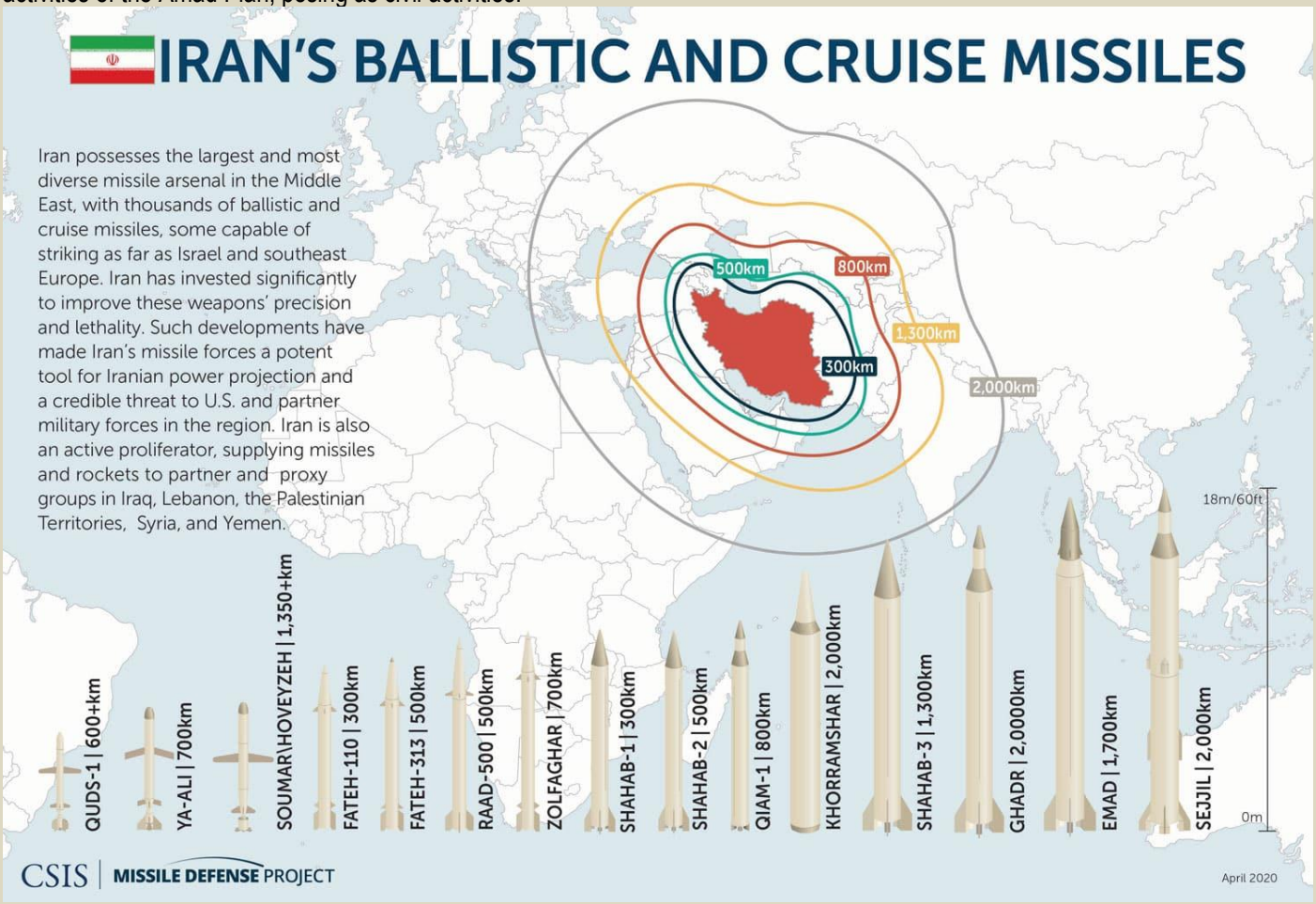
Beyond Breakout: Building Nuclear Weapons Score: 21 points ⇧
So far, Iran has not turned its enriched uranium into nuclear weapons. However, over the last few years, the ability of Iran to do so has increased as well as the speed of it to accomplish this task. Thus, Iran's nuclear weapons capabilities are more dangerous than they have ever been, while its relations with the West are at a low point. Moreover, Iranian regime functionaries have suggested that perhaps it is time to produce nuclear weapons. [33] This combination of factors raises the specter that Iran will build nuclear weapons. These considerations lead to an increased score of 21 out of 30, representing an increase of three points and a shift for the first time from Considerable Danger to High Danger.
As discussed above, Iran could rapidly produce enough weapon-grade uranium for a small nuclear arsenal. In addition, Iran has multiple ways to deliver nuclear weapons, including on ballistic missiles. The missing piece is nuclear weaponization.
Iran can build a current nuclear weaponization effort based on its large-scale nuclear weapons program in the early 2000s and progress made since then. Iran appears to have a program to be prepared to make nuclear weapons and to do so in short order, one ready to produce nuclear weapons "on-demand."

Iran Has Maintained an Organizational Structure to Preserve and Possibly Hone Nuclear Weaponization Assets and Skills
Iran's nuclear weapons program started slowly, building to a crash nuclear weapons program in the early 2000s, called the Amad Plan, to create five nuclear weapons in an industrial complex capable of producing many more. [34] Under international pressure and fearing a military attack, the program was driven to downsize and deeper secrecy. Iran's decision to halt the Amad Plan merely served as a tactical retreat, not an abandonment of its nuclear weapons ambitions or activities, a step taken earlier by other countries, notably Taiwan and South Africa.
After the closure of the Amad Plan, other organizations continued to work on nuclear weapons. The evidence suggests that Iran not only maintained the capability to produce nuclear weapons, but actively

worked on efforts to advance that capability in case Iran's leaders made a decision to build them. There is no evidence that such work has halted.

The nuclear weaponization skills continue to be largely harbored in a military organization known by its acronym SPND, involved in many military development projects. Core Amad Plan groups remain in SPND, employing many former Amad Plan personnel, preserving and likely improving key nuclear weaponization skills and capabilities. SPND has also launched its own project to develop and build a nuclear propulsion reactor.

The post-Amad reorientation strategy shines a light on controversial Atomic Energy of Iran (AEOI) nuclear activities that followed after 2004, particularly the Fordow enrichment plant, which was originally the Amad Plan's intended facility to produce weapon-grade uranium. After the halt of the Amad Plan, the secret Fordow project was transferred to the AEOI, which was judged as providing a more credible civil cover for military activities. This turned out to be true, as Western powers revealed the secret project in 2009 and its repurposing to low enriched uranium production. Similarly, recent AEOI uranium metal production activities may include follow-on activities of the Amad Plan, posing as civil activities.



Iran Has Multiple Paths Towards Developing A Nuclear Weapon[35]

Iran has multiple pathways to complete its weaponization requirements and build nuclear weapons. The two most prominent pathways are (1) launching an accelerated effort to achieve a few crude nuclear weapons or (2) reconstituting and completing its earlier Amad nuclear weapons program with the ability to serially produce annually many warheads suitable for delivery by ballistic missiles.

The second path has some notable challenges. It would require Iran maintaining secrecy for an extended period, a few years by most assessments, while rebuilding a range of production-scale facilities able to serially produce warheads for ballistic missiles. This presents a risk for Iran since early discovery could result in a harsh international reaction and plenty of time for Israel, the United States, and its allies to organize a united reaction.

The first path, an Iranian accelerated program, would not aim to produce warheads for ballistic missiles, but a warhead that could be tested or delivered by crude means (ship, or truck), and could be accomplished in about six months. It could take significantly longer than six months to build a nuclear warhead for a ballistic missile. Nonetheless, a crude nuclear weapon would signal Iran's entry into the nuclear weapons

club as the tenth member, either dramatically via an underground nuclear test or stealthily via leaks about its accomplishment. A missile-deliverable warhead would probably be the next goal of Iran's nuclear weapons program. The outside world would be left to ponder how soon it could reach this capability.
While most of the weaponization work has been accomplished for a crude nuclear weapon, such as the high explosive triggering package, an acceptable neutron initiator, and high explosives components, a few significant tasks likely remain. However, these tasks could be completed in a matter of several months. Much of the work on weaponization could be conducted in utmost secrecy and would use existing or repurposed military facilities or hidden equipment and materials, possibly located underground.
Western intelligence agencies may not detect the start of Iran's nuclear weaponization effort. Given all the complexities and conflicts in the Middle East today, these agencies are stretched to the limit. The beginning stages of a quiet, low-level effort to build nuclear weapons could slip through unobserved.

Iranian Space Launch Vehicle Development and Deployment of Solid-Fuel Propellant Missiles
Iran continues to work diligently to develop its missile capabilities, including space launch vehicles (SLV) intended to deliver payloads to geostationary orbit. In late September 2023, Iran successfully launched a Ghased SLV carrying the Noor 3 military reconnaissance satellite to geostationary orbit. The three-stage Ghased rocket uses a first-stage Ghadr liquid-propellant missile and an upper stage Salman solid-fuel propellant motor, a step towards a completely solid-fuel propellant missile. [36]
In January 2024, Iran reportedly used the more advanced Qaem 100 three-stage solid fuel rocket to put a Soraya satellite into orbit at 750 km above the Earth's surface, breaking its previous altitude record. [37]
Developing a solid-fuel propellant missile is a key milestone that gives a missile force an advanced capability to quickly deploy and launch ballistic missiles. Liquid-propellant missiles take hours to fuel and prepare for launch, making them vulnerable to detection and a pre-emptive strike. The development of SLV provides Iran with a plausible cover to develop some of the key technologies needed to produce long-range missile systems, a precursor for an ICBM at some point in the future. However, to date, non-theoretical developmental work on re-entry systems for ICBMs has not been detected.

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

Earthquake or Secret Nuclear Blast? A New Tool Exposes The Truth With 99% Accuracy

By Mark Hoggard

Source: https://www.sciencealert.com/earthquake-or-secret-nuclear-blast-a-new-tool-exposes-the-truth-with-99-accuracy

Feb 08 – Since the first detonation of an atomic bomb in 1945, more than 2,000 nuclear weapons tests have been conducted by eight countries: the United States, the Soviet Union, the United Kingdom, France, China, India, Pakistan and North Korea.

Groups such as the Comprehensive Nuclear-Test-Ban Treaty Organization are constantly on the lookout for new tests.

However, for reasons of safety and secrecy, modern nuclear tests are carried out underground – which makes them difficult to detect. Often, the only indication they have occurred is from the seismic waves they generate.

In a paper published in *Geophysical Journal International*, my colleagues and I have developed a way to distinguish between underground nuclear tests and natural earthquakes with around 99 percent accuracy.

Fallout

The invention of nuclear weapons sparked an international arms race, as the Soviet Union, the UK and France developed and tested increasingly larger and more sophisticated devices in an attempt to keep up with the US. Many early tests caused serious environmental and societal damage. For example, the US's 1954 Castle Bravo test, conducted in secret at Bikini Atoll in the Marshall Islands, delivered large volumes of radioactive fallout to several nearby islands and their inhabitants.

Between 1952 and 1957, the UK conducted several tests in Australia, scattering long-lived radioactive material over wide areas of South Australian bushland, with devastating consequences for local Indigenous communities.

In 1963, the US, the UK and the USSR agreed to carry out future tests underground to limit fallout. Nevertheless, testing continued unabated as China, India, Pakistan and North Korea also entered the fray over the following decades.

How to spot an atom bomb

During this period there were substantial international efforts to figure out how to monitor nuclear testing. The competitive nature of weapons development means much research and testing is conducted in secret.

Groups such as the Comprehensive Nuclear-Test-Ban Treaty Organization today run global networks of instruments specifically designed to identify any potential tests. These include:

- air-testing stations to detect minute quantities of radioactive elements in the atmosphere
- aquatic listening posts to hear underwater tests
- infrasound detectors to catch the low-frequency booms and rumbles of explosions in the atmosphere
- seismometers to record the shaking of Earth caused by underground tests.

A needle in a haystack

Seismometers are designed to measure seismic waves: tiny vibrations of the ground surface generated when large amounts of energy are suddenly released underground, such as during earthquakes or nuclear explosions.

There are two main kinds of seismic waves. First are body waves, which travel outwards in all directions, including down into the deep Earth, before returning to the surface. Second are surface waves, which travel along Earth's surface like ripples spreading out on a pond. The difficulty in using seismic waves to monitor underground nuclear tests is distinguishing between explosions and naturally occurring earthquakes. A core goal of monitoring is never to miss an explosion, but there are thousands of sizeable natural quakes around the world every day.

As a result, monitoring underground tests is like searching for a potentially non-existent needle in a haystack the size of a planet.

Nukes vs quakes

Many different methods have been developed to aid this search over the past 60 years.

Some of the simplest include analysing the location or depth of the source. If an event occurs far from volcanoes and plate tectonic boundaries, it might be considered more suspicious. Alternatively, if it occurs at a depth greater than say three kilometres, it is unlikely to have been a nuclear test. However, these simple methods are not foolproof. Tests might be carried out in earthquake-prone areas for camouflage, for example, and shallow earthquakes are also possible.

A more sophisticated monitoring approach involves calculating the ratio of the amount of the energy transmitted in body waves to the amount carried in surface waves. Earthquakes tend to expend more of their energy in surface waves than explosions do.

This method has proven highly effective for identifying underground nuclear tests, but it too is imperfect. It failed to effectively classify the 2017 North Korean nuclear test, which generated substantial surface waves because it was carried out inside a tunnel in a mountain. This outcome underlines the importance of using multiple independent discrimination techniques during monitoring – no single method is likely to prove reliable for all events.

An alternative method

In 2023, my colleagues and I from the Australian National University and Los Alamos National Laboratory in the US got together to re-examine the problem of determining the source of seismic waves.

We used a recently developed approach to represent how rocks are displaced at the source of a seismic event, and combined it with a more advanced statistical model to describe different types of event. As a result, we were able to take advantage of fundamental differences between the sources of explosions and earthquakes to develop an improved method of classifying these events.

We tested our approach on catalogues of known explosions and earthquakes from the western United States, and found that the method gets it right around 99% of the time. This makes it a useful new tool in efforts to monitor underground nuclear tests.

Robust techniques for identification of nuclear tests will continue to be a key component of global monitoring programs. They are critical for ensuring governments are held accountable for the environmental and societal impacts of nuclear weapons testing.

Mark Hoggard, DECRA Research Fellow, Australian National University.

Why the Biden administration's new nuclear gravity bomb is tragic

By Stephen Young

Source: https://thebulletin.org/2024/02/why-the-biden-administrations-new-nuclear-gravity-bomb-is-tragic/

A US F-35A combat aircraft tests an unarmed B61-12 bomb in the Nevada Desert. Source: Sandia National Laboratory

Feb 13 – In late October 2023, the Pentagon announced—to the surprise of many, including congressional staffers who work on these issues—that it was pursuing a new nuclear weapon to be known as the B61-13, a gravity bomb.

This is a troubling development for many reasons. First, it is merely the latest in a long line of new nuclear weapons that the United States is building or proposing, in yet another sign that a new nuclear arms race is expanding. In addition, it breaks a promise the Obama administration made to eliminate almost all types of US nuclear gravity bombs, while further undermining President Biden's pledge to reduce the role of nuclear weapons in US security. Most tragically, it further cements an absolute commitment on the part of the United States to retain nuclear deterrence as the centerpiece of its security policy for decades to come. While most of us

hope the world can eventually stop relying on the threat of mass murder at a global scale as the basis for international security, the B61-13 moves everyone further away from that day.

Starting from the top, here is the entire, vast set of new nuclear bombs and warheads the United States recently developed or is pursuing:

- The Trump administration's new "low-yield" warhead, deployed on sea-launched ballistic missiles (SLBMs) carried by US submarines, with an estimated explosive yield roughly one-third the size of the gravity bomb dropped on Hiroshima. "Low-yield" is a relative term; this warhead could still kill tens of thousands in an instant.
- The new, more lethal B61-12 gravity bomb that the National Nuclear Security Administration (NNSA) recently started producing, after many years of delay (and with each bomb costing more than its weight in gold).
- The updated warhead for the stealthy air-launched cruise missile first proposed by the Obama administration, ideally suited to start a nuclear war.
- A variant of that cruise missile warhead for a sea-launched cruise missile that a) the Trump administration proposed, b) the Biden administration is trying to cancel, but c) Congress recently required the administration to pursue.
- The precedent-setting warhead for land-based missiles that, for the first time since the end of the Cold War, will be made entirely from new components, with nothing being reused except the basic design of the warhead.
- The momentous new warhead for submarine-launched ballistic missiles, the first entirely new bomb since the end of the Cold War, with both the components and the design of the weapon made anew.
- The B61-13.

All these new bombs and warheads are just part of a massive rebuilding of the entire US nuclear arsenal, which also includes new long-range, land-based missiles, new submarines, new stealthy, long-range bombers that will carry the new stealthy cruise missiles mentioned above, and major upgrades to the missiles carried by the submarines. The total cost to do all that while maintaining the existing weapons will be well over $1.2 trillion during the next 25 years.

In short, a new nuclear arms race is exploding across the globe, and while the Biden administration has not announced plans to increase the size of its nuclear arsenal (despite bipartisan pressure to do so), it is racing to climb what is often called a "modernization mountain"—a journey that will certainly take longer and cost far more than currently projected, all to produce a vastly oversized nuclear stockpile that everyone hopes will never be used.

The broken promise

There is a second and compounding problem with the B61-13: It breaks a promise made during the Obama administration to eliminate all but one of the types of US gravity bombs. Specifically, to win support for the B61-12—a new guided gravity bomb the Pentagon and NNSA badly wanted—the Obama administration proposed to retire the B61-3, B61-4, B61-7, B61-10, B61-11, and the B83 gravity bombs, trading six

weapons for one. Unfortunately, since its inception the B61-12 has faced major cost overruns and years of delays. The NNSA initially said the bomb would cost $4 billion, then quickly raised the tab to $8 billion, while the Pentagon initially estimated it at $10 billion. The actual cost, including work the Air Force is doing, will be as much as $14 billion. The NNSA initially projected it would begin making the bombs in 2017, while the Pentagon said it would be 2022 before work started. The Pentagon was right, with the B61-12 finally entering production late in 2022.

On top of all the cost increases and delays, the associated commitment to retire the six other gravity bombs is changing significantly. First, it is not clear the B61-11 will be retired at all; planning documents no longer include it as something the B61-12 will replace. That variant is designed to penetrate into the Earth, to attack hardened and deeply buried targets. No administration has ever explained why it was removed from the retirement list; it simply stopped being included on it. Second, the sole bright spot is the B61-10, but oddly so. Although the bomb's retirement was tied to starting production of the B61-12, the B61-10 was removed from the stockpile in 2016. Apparently, it really was not needed at all, regardless of the B61-12.

More dangerously, the decision to retire the B83—by far the most destructive weapon in the US nuclear stockpile—was reversed by the Trump administration. The B83 has an explosive yield of some 1.2 megatons—or 80 times larger than the bomb dropped on Hiroshima. In a simulation developed by the Union of Concerned Scientists (UCS, where I work), dropping one bomb like the B83 on a nuclear facility in Iran would kill over three million people and spread deadly radiation across Afghanistan, Pakistan, and India. It is this behemoth that the Trump administration declared its intention to keep "until a suitable replacement is identified." Fortunately, the Biden administration reversed the reversal, and the B83 is currently on a path to be retired at some point, though the plan for when that will happen is classified. (Unfortunately, election results this year could again change that outcome.)

In the meantime, the Biden administration has announced the B61-13.

Significantly, this new bomb will be based on the B61-7, the most destructive of the B61 variants, with a maximum yield of 360 kilotons, or 24 times more devastating than the bomb dropped on Hiroshima. Just to remind you, that one bomb killed 70,000 to 140,000 people. In other words, the B61-13 will be massively destructive, accompanied by immense and widespread fallout. In other other words, this is yet another tool for nuclear warfighting—or, more specifically, seeking to win a nuclear war. That mission should not exist. Indeed, as five of the countries with nuclear weapons—the United States, Russia, China, France and the United Kingdom—have declared, "a nuclear war cannot be won and must never be fought."

Yet fighting and winning a nuclear war is precisely the goal of developing the B61-13. There are, apparently, specific targets that this more powerful gravity bomb can hold at risk—ones that cannot reliably be destroyed with the B61-12, despite its vastly increased accuracy in comparison to existing gravity bombs. But existing nuclear warheads on submarine-based missiles can already hold those same targets at risk. So the B61-13, it turns out, is just another option to blow up something the Pentagon can already destroy, and many times over. In fact, each US nuclear-armed submarine carries seven times the destructive power of all the bombs dropped during World War II, including the two atomic bombs dropped on Japan.

The scope of the mistake

Coming from a Biden administration that pledged to seek to reduce the role of nuclear weapons, with a president who, as a candidate for office, declared his support for the policy that the United States would never use nuclear weapons first in any conflict, the decision to pursue the B61-13 is not only deeply disappointing, but a profound mistake. In short, the B61-13 is yet another sign that the United States intends to make its nuclear arsenal even more deadly and the foundational element of the existing security system. That system is based on the principle that this country, to keep itself "safe," needs to be able to kill tens or hundreds of millions of people in less than an hour.

On moral grounds, and under international law, that prospect alone should be evidence enough to conclude that such an approach to security is grievously wrong, and that the United States should do everything it can to move away from that system.

But the reality is far worse, because Russia already has and China is now moving toward nuclear arsenals that will give them similar capabilities. Even with their vastly smaller arsenals, the other six nuclear weapons states—the UK, France, India, Pakistan, Israel, and North Korea—also have the capacity to kill tens of millions of people in hours. That horrible reality is the basis of the world's security system. If everyone can kill everyone else, and no one can be safe from that threat, then—in the supreme irony of nuclear deterrence—everyone is *supposed to be* safe.

The mutual assured destruction precept of deterrence theory is ludicrous. For such a system to make sense, it would have to work perfectly and for all time. If it doesn't, then we are all dead.What human system has *ever* worked perfectly for any significant length of time? In just one example of far too many, nuclear war was barely averted when a Russian officer refused to go along with two colleagues who wanted to use a nuclear-armed torpedo against US Navy ships harassing their submarine at the height of the Cuban Missile Crisis. As has been noted, it was as much luck as careful choices that avoided the start of a nuclear war that would almost certainly have spiraled out of control.

Rather than develop a new nuclear weapon that adds fuel to a rapidly growing arms race, the Biden administration should launch a concerted effort to rid the world of nuclear weapons. It should publicly announce this intention, invite representatives from other nuclear-armed states to the table, and begin talks about what would be required to eliminate nuclear weapons from Earth. In an ideal world, we could turn the tragedy of the B61-13 into the launching point for a global effort to push for that outcome.

Stephen Young is a senior Washington representative for the Global Security program at the Union of Concerned Scientists.

North expanding chemical complex critical to nuclear and missile programs

Source: https://koreajoongangdaily.joins.com/news/2024-01-11/national/northKorea/North-expanding-chemical-complex-critical-to-nuclear-and-missile-programs/1956491

Jan 11 – North Korea is expanding a chemical plant that plays a crucial role in its nuclear and missile program, according to satellite imagery examined by analysis group 38 North and the Korea Institute of Nuclear Nonproliferation and Control.

The images, taken via commercial satellites, show that the Unha chemical complex near Manpho, Chagang Province, is undergoing expansion and modernization and exhibits signs of increasing production of reagents, such as nitric and sulfuric acids, that are associated with the reprocessing, enrichment and conversion of nuclear materials.

The Unha chemical complex "holds considerable strategic importance to North Korea," according to 38 North, which noted that a declassified Central Intelligence Agency (CIA) report from 1980 linked Unha with the production of liquid rocket propellant and other chemical products needed to support North Korea's demanding strategic industries.

Beyond Parallel, a North Korea analysis group run by the Washington-based Center for Strategic and International Studies, released a report in March 2023 that determined Unha as a key source of reagents to the North's Yongbyon nuclear complex, and that three specialized railcars have been used to transport reagents between the two sites.

Rafael Grossi, the director-general of the International Atomic Energy Agency (IAEA), confirmed in a board of governors meeting held in Vienna in November that North Korea is running its Yongbyon nuclear complex again after a short period of inactivity between September and October.

The Yongbyon nuclear complex in North Pyongan Province is the North's primary uranium enrichment and reprocessing facility.

Yongbyon's 5-megawatt reactor has long been the focal point of previous failed international diplomatic efforts to rein in North Korea's nuclear ambitions.

The reactor is believed to be the regime's sole source of spent nuclear fuel for reprocessing and is capable of producing six kilograms of weapons-grade plutonium from spent fuel rods per year.

In the meeting, Grossi confirmed there have been "increased levels of activity" at and near the reactor, and they could observe, since mid-October, "a strong water outflow" from the reactor's cooling system.

Grossi also told the board that the Punggye-ri underground nuclear testing site in North Hamgyong Province remains "prepared to support a new nuclear test" following the restoration of multiple tunnels, which was detected via satellite photography in 2022.

Although South Korea and the United States have called on the North to return to talks to negotiate its complete, verifiable and irreversible denuclearization, the North demanded the scrapping of international sanctions and joint South Korea-U. S. military exercises as preconditions for the resumption of talks.

In recent months, North Korean leader Kim Jong-un and his influential sister Kim Yo-jong have staked out an even harder-line position against abandoning nuclear weapons and threatened to use them against the South. The North's state media reported on Wednesday that Kim Jong-un called South Korea his regime's "main enemy" and said he has "no intent to avoid war" during a two-day inspection of a munition factory that began Monday.

According to the report, Kim also said the North "will not hesitate to annihilate" the South using "all means and forces available" in the event of an armed conflict.

Even in the face of Russian aggression, a nuclear 'Eurodeterrent' is still a bad idea

By Stephen J. Cimbala, and Lawrence J. Korb

Source: https://thebulletin.org/2024/02/even-in-the-face-of-russian-aggression-a-nuclear-eurodeterrent-is-still-a-bad-idea/

Feb 12 – Policy makers and national security experts are now seriously discussing the possible need for a European nuclear deterrent. For example, former German Foreign Minister Joschka Fischer, in an interview with the weekly *Die Zeit* in December 2023, supported the idea of a European nuclear deterrent. Other supporters of a European—or even a German—nuclear arsenal have contributed regularly to conservative German newspapers.

In 1975, the West German government stated that its ratification of the accession of the Federal Republic to the Nuclear Nonproliferation Treaty would not preclude an eventual nuclear deterrent within the framework of the European Union. The issue of a European nuclear deterrent also blends into the related question as to what role, if any, remains for so-called "tactical" or non-strategic nuclear weapons in NATO.[1]

There are several political and military arguments in favor of this proposal. But there are certainly also reasons for skepticism and concern that, considered together, add up to the conclusion that a Eurodeterrent continues to be a bad idea.[2]

Rationale for a Eurodeterrent

The first reason given for a European nuclear deterrent is the possibility that a future US president might not be as committed to NATO as his or her predecessors. This was a concern raised during the administration of President Donald Trump, whose open disparagement of European allies for allegedly insufficient financial contributions to NATO alliance security raised alarms from Brussels to Washington. Although Trump's actual policies turned out to be less disruptive than his inflammatory rhetoric, his possible return to the White House in 2025 could reboot European doubts about US security commitments. These doubts could include concerns about the role of America's nuclear umbrella in the deterrence of war in Europe.

A second reason for the renewed interest in a possible European nuclear deterrent is the war in Ukraine and the recurring threats by Russian President Vladimir Putin to resort to nuclear first use if needed to protect Russian security interests in that region.[3] Some Europeans who feel immediately threatened by Russian nuclear coercion, or even by the possibility of a Russian conventional military victory over Ukraine,

might doubt the efficacy of America's nuclear guarantee in the face of an increasingly confident Russia casting a larger shadow over the security of Eastern and Central European countries. Although Russia would still have its hands full of resistance and rebellion in Ukraine, even after having defenestrated the Zelensky government, European and American solidarity to further resist Russian diplomatic coercion supported by military power might weaken.

A third reason might be the growing nationalism in Europe and in the United States, spanning across the general public, leadership classes, and political office holders. The heady optimism about the North Atlantic security community that marked the Cold War and its immediate aftermath is now being challenged from many sides. Newer generations of voters show skepticism about the benefits of transnational and trans-Atlantic security and economic cooperation. There is also the growing significance among Europeans and Americans of identity politics, including doubts about the impact of foreign migration and so-called alarms over a dilution of national character. Parties of the far right are drawing increased strength in part from voters who feel denationalized by foreign influences and globalist agendas.

A fourth concern among some supporters of a European nuclear deterrent lies in doubts about the reliability of the US nuclear umbrella for the deterrence of war in Europe. NATO has only a small number of deployed nuclear weapons on European soil compared to Russia's large inventory of nearly two thousand less-than-strategic or "tactical" nuclear weapons. Russia might be tempted under pessimistic conditions of unacceptable loss in conventional warfare, as they define "unacceptable," to cross the nuclear threshold in any one of a number of ways.

Russia could engage in a demonstrative strike for coercive purposes with a low-yield nuclear weapon, which would do little immediate damage compared to the larger weapons that are prepositioned in its arsenal and raised to combat alert readiness in a crisis. Or Russia could employ a tactical nuclear weapon against a key Ukrainian or NATO military target to prepare the battlespace for a larger war. Would the United States and NATO risk responding with nuclear strikes of their own and thereby escalating the conflict to a larger nuclear war that might destroy much of Europe and ultimately the US homeland? Some military experts feel that the United States lacks a sufficient number of small yield nuclear weapons in its arsenal, compared to Russia's larger inventories, and so would have lost escalation dominance across the spectrum of military options short of unrestricted nuclear warfare.

But more weapons do not necessarily equate to better deterrence. Deterrence remains centered in the mind of the deterree, not the deterrer. Guessing the threshold of conventional defeat beyond which Russia would feel obligated to resort to nuclear first use requires disciplined intelligence collection in real time, combined with mature judgment about Russia's imminent priorities and risks.

Why it's a bad idea

Despite these legitimate concerns about nuclear risks in Europe, it is not clear whether a European nuclear deterrent—either entirely separated from its American umbrella or somehow aligned with it for policy purposes—would enhance the credibility of deterrence or nuclear crisis stability. In fact, at least for four reasons, the opposite result is more probable.

First, legitimate concern should not give way to exaggerated fears of NATO or US abandonment of their political commitment to the deterrence of war in Europe or its defense if necessary. One might argue that NATO was more likely to wobble in the face of Russian intimidation when NATO was preoccupied with "out of the area" commitments in the Middle East and South Asia. Since 2014, however, when Russia annexed Crimea in a coup de main that caught the West asleep, NATO has witnessed a renaissance of awareness about its original mission to guarantee the peace in Europe. Russia's war against Ukraine further aroused NATO to a unified political and military stance. However the conventional war between Russia and Ukraine turns out, NATO is stronger than it has ever been since the Cold War ended. The addition of Finland and the imminent addition of Sweden to NATO membership represent geostrategic fiascoes for Russia—and an outcome Putin and his advisors surely had not anticipated. NATO's nuclear guarantee, supported by the United States' nuclear umbrella, should never be doubted. Escalation is a two way street: Russia fears as much as European NATO countries that a nuclear first use could lead to a process that escapes the control of political leaderships playing at nuclear coercive diplomacy under unprecedented conditions of stress and uncertainty.

A second challenge for a European nuclear deterrent lies in its organization and operational shape, including the chain of command over a (presumably) multinational nuclear force. Something like this was attempted in the 1960s when several military planners and politicians put forward a proposal for a Multilateral Force (MLF) mixing personnel and weapons, including nuclear warheads, from several European powers. The problems of authoritative political control and operational management in such a force soon became evident and proved to be too challenging. Even short of an explicitly multinational force, a transnational European nuclear deterrent presents problems of political collaboration and military-operational command. One might propose that the United Kingdom and France, currently the only two nuclear weapons states among European NATO countries, move toward joint operations with respect to certain well defined contingencies and emergencies. Yet their political and military command and control systems would still have to remain separate for reasons of national sovereignty and military efficiency. In addition, because the United Kingdom is no longer in the European Union, a "Eurodeterrent" would not be under the political supervision of EU institutions and therefore be reduced to a bilateral cooperation. Another issue is that the European nuclear powers have very different delivery systems for nuclear

weapons: The United Kingdom fields a fleet of ballistic missile submarines, while France also has land-based and carrier-based airborne delivery systems.

A third riposte to the idea of a European nuclear deterrent is that it might stimulate nuclear proliferation and ultimately lead to more nuclear weapons states, either in Europe or beyond. Reliance on the US nuclear guarantee has helped to prevent the spread of nuclear weapons not only in Europe, but also in Asia with respect to South Korea and Japan. If countries now start doubting the credibility of the US nuclear deterrent and feel immediately threatened by the growing capabilities of hostile neighbors, their leaders and publics might turn to national nuclear forces as a guarantor against aggression or nuclear coercion. This could be tempting because, based on the historical evidence, even a small number of nuclear weapons can be deterring to adversaries who might otherwise contemplate a conventional war against a state. If North Korea continues to menace South Korea with military threats, including nuclear ones, South Korea might reverse its prior disinterest in its own nuclear force. Japan too, if it feels threatened by a rising China, might reluctantly become more interested in a small but survivable force of sea-based nuclear missiles.

Fourth, the argument that the US nuclear force is insufficiently flexible for deterring or responding to nuclear coercion or nuclear first use deserves further scrutiny. The United States' combatant commanders who operate the unified and specified commands in wartime are also responsible for planning against a range of threats across the spectrum of conventional war and nuclear deterrence. Flexibility and multiple options are built into these plans for every challenge, ranging from unconventional wars and coercive diplomacy to limited or large-scale conventional war to, if necessary, nuclear coercion or retaliation. Plans are scrubbed repeatedly and road-tested in near-realistic exercises.

In today's world of high tech competition among major powers, neither the United States nor any other aspiring military can afford to rest on dated plans, aging technology, or roseate assumptions about the likelihood of wars. Surprises are inevitable: preparation and agility are the hallmarks of superior military performance. As Dwight D. Eisenhower famously said: "Plans are worthless, but planning is everything."

Notes

[1] There is a considerable history of Cold War and post-Cold War policy debates here. See, for example: Richard Weitz, "The Historical Context," pp. 3-12, and Paul Schulte, "Tactical Nuclear Weapons in NATO and Beyond: A Historical and Thematic Examination," both in Tom Nichols, Douglas Stuart and Jeffrey D. McCausland, eds., *Tactical Nuclear Weapons and NATO* (Carlisle, Pa.: US Army War College, Strategic Studies Institute, April 2012). See also: George Perkovich, *Nuclear Weapons in Germany: Broaden and Deepen the Debate* (Washington, D.C.: Carnegie Endowment for International Peace, February, 2010).

[2] An interesting commentary on this topic appears in: Michael Ruhle, "German Musings About a European Nuclear Deterrent," (Fairfax, Va.*: National Institute for Public Policy, Information Series,* January 3, 2024).

[3] See also Dmitri (Dima) Adamsky, *The Russian Way of Deterrence: Strategic Culture, Coercion, and War* (Stanford, CA: Stanford University Press, 2024), pp. 106-110.

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

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

Trump's Threats Lead to Reflections in EU Over Nuclear Weapons

By Ella Joyner | DW journalist

Source: https://www.homelandsecuritynewswire.com/dr20240216-trump-s-threats-lead-to-reflections-in-eu-over-nuclear-weapons

Feb 16 – The looming prospect of NATO-skeptic Donald Trump winning a second term as US president is serving as food for thought in Europe on everything from climate to trade.

But this week, explosive comments from the isolationist front-runner to be the Republican Party's candidate for president have pushed concerns about EU security to the fore and loomed large over a NATO defense ministers' meeting in Brussels on Thursday.

At a campaign rally on Saturday, Trump implied he wouldn't come to the aid of NATO states attacked by Russia if they hadn't met the alliance's military spending targets.

In fact, he would have opted to "encourage" Russia "to do whatever the hell they want," he said, recounting a conversation he claimed to have had with the leader of an unnamed major European country while in office between 2016 and 2021.

Trump has long railed against European NATO allies that spend far less than Washington in both real and relative terms on their militaries, slamming them for free-riding on an international security order backed up by US clout.

A Shiver Down Europe's Spine

Trump is known for hyperbole and still a long way from the White House, but his words reverberated on the other side of the Atlantic. Such a threat flies in the face of the central promise of NATO, enshrined as Article 5 in its treaties: Allies must come to each others' aid in the case of a military attack.

On Wednesday, NATO Secretary General Jens Stoltenberg touted increased spending by European NATO allies — an increase of 11% in 2023, he told reporters at a press conference ahead of the meeting.

"The whole idea of NATO is that an attack on one ally will trigger the response from the whole alliance. And as long as we stand behind that message, together, we prevent any military attack on any ally," he stressed.

EU politicians are concerned that they may not be able to count on the US if President Joe Biden, a Democrat who strongly condemned Trump's comments, loses in November elections.

The fear extends to Washington's huge nuclear arsenal. Though the information is classified, experts estimated that the US had about 3,700 warheads last year, with around 100 bombs stationed at military bases in Germany, Belgium, the Netherlands, Italy and Turkey. After the departure of the United Kingdom from the EU, France is the only member state with its own nuclear weapons.

"Judging by recent comments from Donald Trump, we can't count on that anymore," European Parliament Vice President Katarina Barley told German newspaper *Tagesspiegel* last week.

Asked by *Tagesspiegel* whether the EU needed its own nuclear bombs — something widely regarded as a pipe dream (or indeed, for some, a nightmare) for now — the center-left Social Democrat replied: "On our way to a European army, this could also become a topic."

Long Road to a 'Eurobomb'

Nuclear armaments are highly divisive in the EU. Austria, Ireland and Malta have all signed an outright ban on nuclear weapons. While some countries, like France, Romania and Poland, more strongly favor nuclear deterrence, in many states — even ones like Germany that host US nuclear weapons — public opinion has traditionally been largely against them.

Nuclear weapons analyst and researcher Franziska Stärk told DW there were different options under discussion in Europe, none of them very convincing for her.

"Suggestions in the EU context range from the EU developing its own arsenal, to France and the UK substantially bolstering their arsenals and somehow kind of 'Europeanizing' launch authority," the researcher from the Peace Research and Security Policy at the University of Hamburg said.

"Personally, I'm highly critical of the feasibility of these suggestions." Stärk said. "First of all, because the EU is not famous for making foreign policy decisions easily. And I can hardly see how they can establish a chain of command for a presumably multinational nuclear force."

France, Provider of a European Umbrella?

What is more likely, according to Tom Sauer of the University of Antwerp, is for France to somewhat "Europeanize" its nuclear capabilities: "The French already now say that if the security interests of Europe are in danger, our nuclear weapons may help … [French President Emmanuel] Macron said that and all previous presidents said that one way or another."

France got nuclear weapons in 1960, but the rest of the EU has traditionally been lukewarm, Sauer told DW. Nonetheless, politicians in Germany have at times come out in favor of cofinancing or increasing coordination over French nuclear weapons.

A French member of the European Parliament, Christophe Grudler, told DW on Wednesday that the EU should consider this option. "The French nuclear arsenal is under French command, uniquely a French mandate," the center-right lawmaker stressed. "However, if there was cooperation looking at how we could work on technical assistance, develop the principle of cohesion in Europe … it's something that we should indeed pursue."

Sauer said he is skeptical that France is completely sincere in this regard, pointing out that all this would bring up a whole range of issues. Would Germany finance French weapons without having control over them? And would Paris be willing to relinquish complete control over its weapons in exchange for cash?

A Dangerous Debate?

Sauer and Stärk were both very critical of the entire discussion. "Instead of talking about the eurobomb, we should talk about having a nuclear-weapon-free zone in Europe extending to Russia, if possible," Sauer said. Stärk said she wished some of the politicians proposing nuclear options actually "thought

about the global implications when we talk about the value of the nonproliferation regime, which is obviously put into question if Europe decided to actually nuclearize."
On Wednesday, German Defense Minister Boris Pistorius also sought to downplay the discussion. He even criticized fellow Social Democrat Barley for being among the first German politicians to raise the issue, saying: "In my opinion, that's not something you discuss publicly."

Trump: A Pinch of Salt Necessary?
Asked if European states needed to rethink nuclear deterrence in light of Trump's comments, Stoltenberg said Wednesday that the "NATO nuclear deterrent … has provided the ultimate security guarantees for NATO allies for decades."
"This is the arrangement we have together in NATO, with agreed procedures for command and control doctrines, we are exercising together. And of course, this is the combination of US nuclear weapons in Europe, but also other NATO allies providing the planes, the infrastructure, the support," he said.
Earlier in the week in a separate statement, Stoltenberg downplayed Trump's comments. "I expect that regardless of who wins the presidential election the US will remain a strong and committed NATO ally," he said.
Sauer of the University of Antwerp argued that Trump's comments don't actually have much bearing on the actual likelihood of European NATO states being attacked by Russia. The analyst doesn't believe Russian President Vladimir Putin has the inclination or the ability to invade such countries, unlike Ukraine, which is outside NATO and the EU.
On X, formerly Twitter, Hans Kristersen of the Federation of American Scientists called for calm.
"There are two ways to undermine NATO security," Kristersen wrote on Wednesday. "One is for Trump to say something stupid (which he does all the time). The other is for Europe to overreact and say 'we can no longer rely' on the US nuclear umbrella and need a eurobomb. It's exactly what Putin [and] Trump want to hear."

EDITOR'S COMMENT: No matter what, we must not permit Germany to acquire its own nuclear weapons. Two world wars are enough!

CNN: "Russia is developing nuclear electromagnetic wave weapons to destroy satellites"

Source: https://newsrebeat.com/world-news/195698.html

Feb 18 – CNN reported on the 17th (local time) that Russia is trying to develop a nuclear space weapon that can destroy satellites with energy waves from space.
CNN reported this, citing three sources familiar with U.S. intelligence agencies. The nuclear explosion could create an energy wave that could paralyze commercial and government satellites on which the world's mobile phone calls and internet depend, the sources said.
Mike Turner, chairman of the House Intelligence Committee, said on the 14th that the government has "serious intelligence on national security threats."
Accordingly, on the 16th, President Joe Biden announced that what Chairman Turner was referring to was Russia's new nuclear-related anti-satellite capability. However, authorities declined to comment further, citing confidentiality of the information.
Biden administration officials have publicly emphasized that the weapon is still under development and is not yet on track.
But if the weapon were used, it would cross a dangerous Rubicon in the history of nuclear weapons and could bring extreme disruption to daily life in ways that are difficult to predict, officials said.
CNN explained that this weapon is commonly known as a nuclear EMP among military and space experts. They say it creates electromagnetic energy waves and a lot of electrical particles, which could interfere with other satellites flying around the Earth.
The Pentagon and intelligence community have been tracking Russia's efforts to develop a wide range of anti-satellite weapons, including EMPs, for years. According to a Defense Department official, there has been a series of intelligence reports in recent months, particularly regarding Russian efforts to develop nuclear-powered anti-satellite capabilities. CNN assessed that Russia's efforts are making progress.
CNN pointed out that it is not clear whether this weapon can affect global navigation systems (GPS) and nuclear command and control satellites that fly in higher orbits than large commercial and government satellites. He said it is also unclear how well this technology has been developed.
However, experts pointed out to the media that this type of weapon could affect small satellites such as SpaceX's Starlink, which is being used successfully in Ukraine, which is still at war with Russia.

In particular, it will be Russia's "ultimate weapon," one U.S. official and source said.
In relation to this, the United States is said to have begun diplomatic efforts, including mentioning the possibility of Russia's nuclear weapons to China and India.
The New York Times (NYT) reported on the 17th that U.S. Secretary of State Tony Blinken, who visited Munich, Germany to attend the Munich Security Conference, raised the possibility of Russia's nuclear weapons movement to China and India.
NYT said, "Secretary Blinken's message was straightforward," and said that if Russia causes a nuclear explosion in space, not only American satellites, but also Chinese and Indian satellites will be eliminated.
Secretary Blinken said it was up to Chinese and Indian leaders, including Chinese President Xi Jinping and Prime Minister Narendra Modi, to persuade President Vladimir Putin of a situation that could turn into a disaster.
The Outer Space Treaty, which went into effect in 1967 between the United States and Russia, prohibits the deployment of weapons of mass destruction (WMD), including nuclear weapons, in space. Biden administration officials are concerned that if Russia violates this, North Korea and others will follow suit.

Germany and Nuclear Weapons: A Difficult History

By Volker Witting and Rina Goldenberg
Source: https://www.homelandsecuritynewswire.com/dr20240219-germany-and-nuclear-weapons-a-difficult-history

Feb 19 – German Defense Minister Boris Pistorius is annoyed by the current debate about European nuclear weapons. "There is no reason to discuss the nuclear umbrella now," he told public broadcaster ARD.
Ever since Donald Trump suggested that, as US president, he would not provide military assistance to NATO countries if they invested less than 2% of their GDP in their defense, German politicians have been discussing whether French and British nuclear weapons would suffice as a protective shield or whether Europe needs new nuclear weapons.
"The debate about European nuclear weapons is a very German debate that we don't see in any other country," political scientist Karl-Heinz Kamp from the German Council on Foreign Relations (DGAP) told DW — especially not in Eastern Europe, where there is a constant perceived threat from Russian President Vladimir Putin's Russia.
Germany has a special history: Germany was "seen as an intrinsically aggressive country, that had started two world wars and could not be trusted with nuclear weapons," said Kamp.

Germany-Based Nukes During the Cold War
In 1954, not long after the end of World War II, the first chancellor of the Federal Republic of Germany, Konrad Adenauer, signed an agreement renouncing the production of its own nuclear, biological or chemical weapons on its territory. In return, the US included West Germany in its nuclear deterrence policy against the Soviet-led Warsaw Pact.
In 1958, the German parliament, the Bundestag, approved the deployment of US nuclear weapons, despite some pacifist protests among the population. In 1960, 1,500 US nuclear warheads were stored in West Germany and a further 1,500 in the rest of Western Europe.
The nuclear weapons were also available to the Bundeswehr for training and use in the "case of defense." "There was never any discussion about Germany acquiring its own nuclear weapons," said Kamp.
The West German and European peace movements grew. The protest against the "NATO Dual-Track Decision" in 1982 saw over a million people in West Germany take to the streets in protest against the planned stationing of new US medium-range missiles in the country. Nevertheless, on November 22, 1983, a center-right majority in the Bundestag approved the stationing of the missiles in US bases shortly thereafter. At the time, the Greens were newly represented in the Bundestag and appealed to the Federal Constitutional Court against the storing and deployment of nuclear missiles on West German territory. This bid was rejected as unfounded in December 1984.
During the Cold War, East Germany, the communist German Democratic Republic (GDR), was part of the Warsaw Pact military alliance, and from 1958, nuclear missiles and warheads were stationed in Soviet military bases on GDR territory. Some were withdrawn in 1988 as part of the Intermediate-Range Nuclear Forces Treaty between the US and the Soviet Union.
After German reunification and the withdrawal of the Soviet military, the territory of the former GDR officially became free of nuclear weapons in 1991.

Post-Cold War Germany
After the fall of the Berlin Wall in 1989, the collapse of the Soviet Union and the end of the division between East and West Germany, the German position was once again cemented in the so-called "Two-Plus-Four

Treaty": No nuclear weapons! On September 12, 1990, the four victorious powers of World War II (the US, the Soviet Union, France and UK) stipulated that Germany East and West should be reunified and renounce nuclear weapons.
Kamp says this was hardly surprising, because "a German nuclear power would be something that would cause horror. For historical reasons alone."
The US government withdrew many of these nuclear warheads after the collapse of the Soviet Union, though an estimated 180 US nuclear weapons are still stored in Europe, in Italy, Turkey, Belgium, the Netherlands and Germany.
Experts believe that 20 US nuclear warheads are currently stored in the town of Büchel in Rhineland-Palatinate, western Germany.
"But the decision-making authority over these weapons lies solely with the American president," explained Kamp.
Any debate about Germany acquiring its own nuclear weapons is completely unrealistic, says political scientist Peter Rudolf from the German Institute for International and Security Affairs. Nuclear bombs need to be stored so that they are not easy targets, he told the *Frankfurter Allgemeine* daily.
"Survivable nuclear weapons would have to be on nuclear-powered submarines that can remain underwater for a very long time, he said, pointing to equipment the Bundeswehr does not have. "So there are so many problems standing in the way of a German nuclear bomb that it has no relevance to current crises," Rudolf concluded.
"Those who are now talking about a European defense dimension are not talking about German nuclear weapons, because Germany is a member of the Nuclear Non-Proliferation Treaty and has made several binding commitments under international law to renounce the possession of weapons of mass destruction — including nuclear weapons," agreed Kamp.
Defense Minister Pistorius, meanwhile, who made headlines not so long ago saying Germany should get "war-ready," is now keen to brush the whole debate aside: He told ARD that "the majority of those in charge in the United States of America know exactly what they have in their transatlantic partners in Europe, what they have in NATO."
And Kamp agrees: "Trump may be able to damage NATO considerably, but he cannot destroy it. You can't destroy decades of transatlantic relations in one term of office."

Volker Witting is a political correspondent for *DW-TV* and *DW* online. **Rina Goldenberg** is a writer and editor at *DW*.

EDITOR'S COMMENT: No matter what keep nukes away from Germany!

Japanese Crime Boss Trafficked Nuclear Material From Myanmar, U.S. Says

By Ed Shanahan
Source: https://www.nytimes.com/2024/02/21/nyregion/japan-nuclear-trafficking-yakuza.html

Feb 21 – A man identified by federal prosecutors as a leader of Japan's Yakuza organized crime syndicate was charged on Wednesday with trafficking uranium and plutonium from Myanmar with the expectation that Iran would use the material to make nuclear weapons.

Takeshi Ebisawa with a rocket launcher. | US District Court for the Southern District of New York

The man, Takeshi Ebisawa, is accused of conspiring with associates to sell the weapons-grade material and illegal narcotics and to buy surface-to-air missiles and other weapons on behalf of an ethnic insurgent group in Myanmar, the country formerly known as Burma.
"It is impossible to overstate the seriousness of the conduct alleged in today's indictment," Damian Williams, the U.S. attorney in Manhattan, said in announcing the charges.
Mr. Ebisawa, 60, is being held in a federal jail in Brooklyn after being charged in 2022, along with three co-defendants, with international drug and weapons trafficking crimes. He has pleaded not guilty to those charges. He is scheduled to appear in Federal District Court in Manhattan on the new charges on Thursday. Evan Lipton, his court-appointed lawyer, declined to comment on the trafficking charges but disputed prosecutors' characterization of his client as a Japanese crime boss.
"When this case is tried, it will be clear that Mr. Ebisawa is not a leader of any sophisticated criminal syndicate, Yakuza or otherwise," Mr. Lipton said. The indictment announced on Wednesday says the scheme began in early 2020, was captured on a series of telephone and electronic communications and unfolded in the following way: Mr. Ebisawa told an undercover Drug Enforcement Administration agent and a confidential source for the agency in February 2020 that he "had access to a large quantity of nuclear

materials that he wished to sell." At one point, he asked whether the confidential source had a buyer for the uranium, adding that it was "not good for your health." Two months later, Mr. Ebisawa sent the confidential source pictures of a "dark rocky material with a Geiger counter," a radiation-measuring device. Later that year, Mr. Ebisawa sent the undercover drug enforcement agent similar pictures and what he told the agent were lab analyses indicating the presence of uranium and another radioactive element, thorium. Responding to Mr. Ebisawa's inquiries, the undercover agent "pretended to agree" to help broker the sale of nuclear materials. The agent said the buyer was an Iranian general, but the person was actually a second confidential source "posing as a general."

A photo, allegedly sent by Ebisawa, of "rocky substances," according to the indictment. | US District Court for the Southern District of New York

In August 2020, Mr. Ebisawa reminded the undercover agent during a recorded call that he had access to uranium and asked whether Iran might buy it. In a follow-up email, the agent said the general was "very interested."
"How enriched is it," the agent asked Mr. Ebisawa in a subsequent message. "Above 5 percent? They don't need it for energy." "I think so and I hope so," Mr. Ebisawa responded. **In September 2020, he offered to sell 50 metric tons of uranium and thorium for $6.85 million.** A week later, he told the undercover agent that he could supply plutonium that would be "better" than uranium for Iran's purposes.
He added that he did not have a license to sell such materials. The transaction, the agent acknowledged, would be "very quiet and illegal." As part of the trafficking scheme, the indictment says, Mr. Ebisawa sent the undercover agent a list of weapons he wanted, including surface-to-air missiles and AK-47 assault rifles. He then sent the agent a picture of the leader of an ethnic insurgent group in Myanmar who is an unindicted co-conspirator in the scheme, referring to the person as "No. 1." In a follow-up call, Mr. Ebisawa said the person was the prospective buyer of the weapons. He then introduced the undercover agent to two other brokers who are also unindicted co-conspirators. While negotiating the weapons deal in May 2021, Mr. Ebisawa asked the undercover agent again whether the Iranian general was still interested in obtaining nuclear materials. The agent said yes. The next month, Mr. Ebisawa shared a picture of what he said was "yellowcake" uranium with the agent and the three unindicted co-conspirators. The negotiations between Mr. Ebisawa and the others continued into February 2022, when two of the unindicted co-conspirators met in Thailand. During the course of the meetings, one of the unindicted co-conspirators showed the undercover agent two vials with a powdery yellow material before taking the vials to an office in Bangkok for safekeeping. In May 2022, law enforcement personnel searched the Bangkok office and found the material. A U.S. nuclear forensic laboratory examined it and found detectable quantities of uranium, thorium and plutonium.
"The plutonium, if produced in sufficient quantities, would be suitable for use in a nuclear weapon," the indictment says.

Does Iran already have nuclear weapons?

By Richard W. Rahn
Source: https://www.washingtontimes.com/news/2024/feb/19/does-iran-already-have-nuclear-weapons/

Feb 19 – Iran may already have five nuclear bombs and may have as many as a dozen by May. Some intelligence estimates, as early as this past October, asserted that Iran could have enough enriched weapons-grade uranium for one bomb within a week and enough for **five nuclear bombs within six weeks**. It has been more than three months since those estimates were made.
If Iran does have a bomb, why is there little mention of it in the press? The Iranians will probably not want to claim to have the bomb until they have a dozen or so operational ones at diverse locations. It would be foolish to announce one bomb, because the U.S. and Israel would expend considerable effort to find and destroy it — but more bombs in more locations makes this "destroy" effort increasingly complex, if not almost impossible.
The Biden administration has a strong incentive to hide or not reveal the existence of an Iranian bomb because of President Biden's repeated pledges over the years not to allow the Iranians to have a nuclear bomb on his watch. Barack Obama and Donald Trump made similar pledges when they served as president. If the Biden administration were to acknowledge the existence of the Iranian bomb, the president would be pressured to take action. But what action?

The Israelis have also pledged not to allow Iran to have the bomb — for the simple reason that if Iran has many nuclear bombs, it could mean the end of Israel. It had been assumed that Israeli intelligence was good enough to warn about an Iranian bomb before it was completed — and could be destroyed. Israel and the U.S. had been able to delay the Iranian bomb program in the past by destroying production and research facilities, sabotaging both hardware and software, and assassinating key scientists.

The Iranians have certainly learned from these previous losses and taken measures to make sure their earlier vulnerabilities have been mitigated. Now, there are questions of how good the Mossad (Israeli intelligence) really is given its failure to predict the Hamas strike of Oct. 7. The Israelis are also very much occupied by their current war and are left with fewer resources to take out the Iranian nuclear program. The Israelis have little incentive to announce an Iranian bomb before they have figured out how to stop it.

The press most often refers to the amount of weapons-grade uranium as a proxy for the number of bombs. Nuclear bombs are produced in a number of sizes. A country can build a larger number of less powerful bombs or fewer more powerful bombs, depending on the targets and objectives. A bomb of the power that leveled Hiroshima, Japan, might be built, using only 16 kilos (35 pounds) of highly enriched uranium. More for a bigger bomb, less for a smaller one.

To build a bomb takes far more than just enriched uranium — which must be fashioned into metal in critical shapes. It also requires a powerful conventional explosive to create the critical mass of uranium, and electronic triggering devices to make it all take place in a fraction of a second.

The engineering of a bomb requires a high level of skill — but U.S. engineers were able to do it in 1945, and the necessary knowledge has leaked from the seven known nuclear states in the past 80 years. The Iranians have first-rate physicists and engineers, so there is no doubt they can accomplish the task given enough time and resources.

A country must not only be able to build bombs but to tailor them for delivery. A crude bomb could perhaps be smuggled into a city center in a small truck. A bomb could be hidden on a ship or submarine. A bomb that can be put into a missile, delivered, and exploded at a precise spot takes considerably more engineering skills — but not ones that are beyond Iranian skill sets.

Given what we think we know, it is possible that the Iranians will have as many as a dozen operative bombs by May. At that point, they may feel comfortable announcing it to the world and, perhaps, set one off underground to prove the point. They would almost certainly want to announce their bomb while Mr. Biden is still president, knowing of his dithering and reluctance to take action, rather than gamble on a return of Mr. Trump to the White House.

How many bombs does a country need before it feels protected from an unprovoked attack? Iran and all of the other nuclear powers are making more (or refurbishing — in the case of the U.S. and Russia) bombs each month as an insurance policy.

If, two years from now, both Israel (which has had a nuclear stockpile for decades) and Iran have the capability with enough bombs to destroy each other, it is possible to envision a situation much like the U.S. and Russia had during the Cold War — a stalemate based on mutually assured destruction. And perhaps that could eventually lead to peace.

Richard W. Rahn is chairman of the Institute for Global Economic Growth and MCon LLC.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

Mexican soldiers find factory producing drone bombs, grenade launchers, fake military uniforms

Source: https://www.msn.com/en-us/news/world/mexican-soldiers-find-factory-producing-drone-bombs-grenade-launchers-fake-military-uniforms/ar-AA1nc6oH

Jan 26 – Police and soldiers in Mexico have discovered a small factory used to make drone bombs, grenade launchers and fake military uniforms in a region where the Jalisco cartel and gangs have been waging turf wars.

The facility, found late Wednesday by police and soldiers in the town of La Huacana in the western Michoacan state, had a computer-controlled lathe and milling machine, suggesting the operators had considerable metalworking knowledge, according to The Associated Press.

Authorities said the factory produced bombs usually dropped by drones, as well as under-barrel, 40mm grenade launchers designed to be attached to assault rifles.

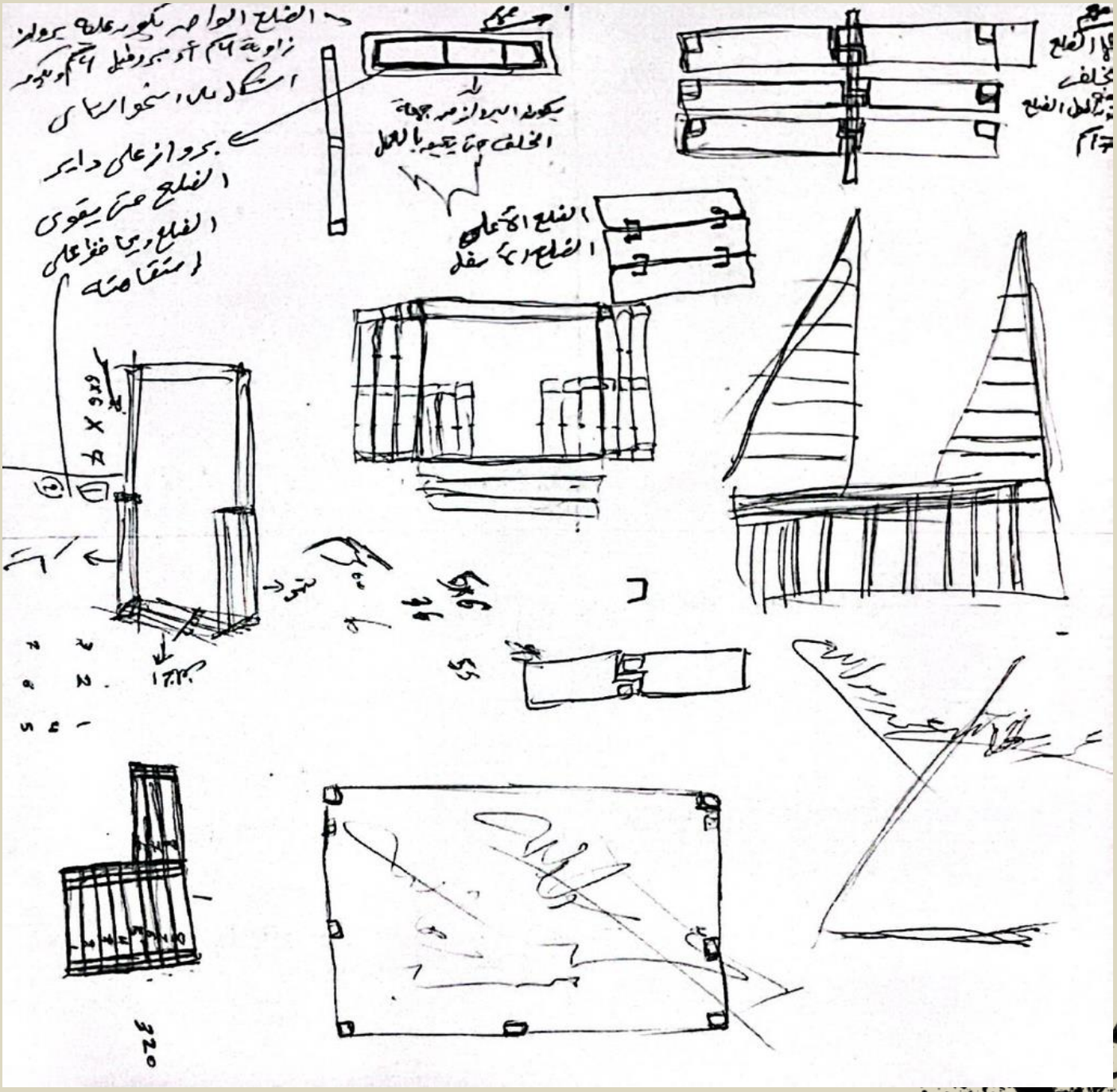
The Jalisco cartel (CJNG) and local gangs have been fighting in Michoacan for years, the AP reports.

The warring gangs frequently use bomb-dropping drones, improvised explosive devices buried in roadways, .50 caliber sniper rifles, homemade armored vehicles and grenades. They also often establish checkpoints on highways and wear fake military uniforms.

Hamas makes bombs from medical supplies

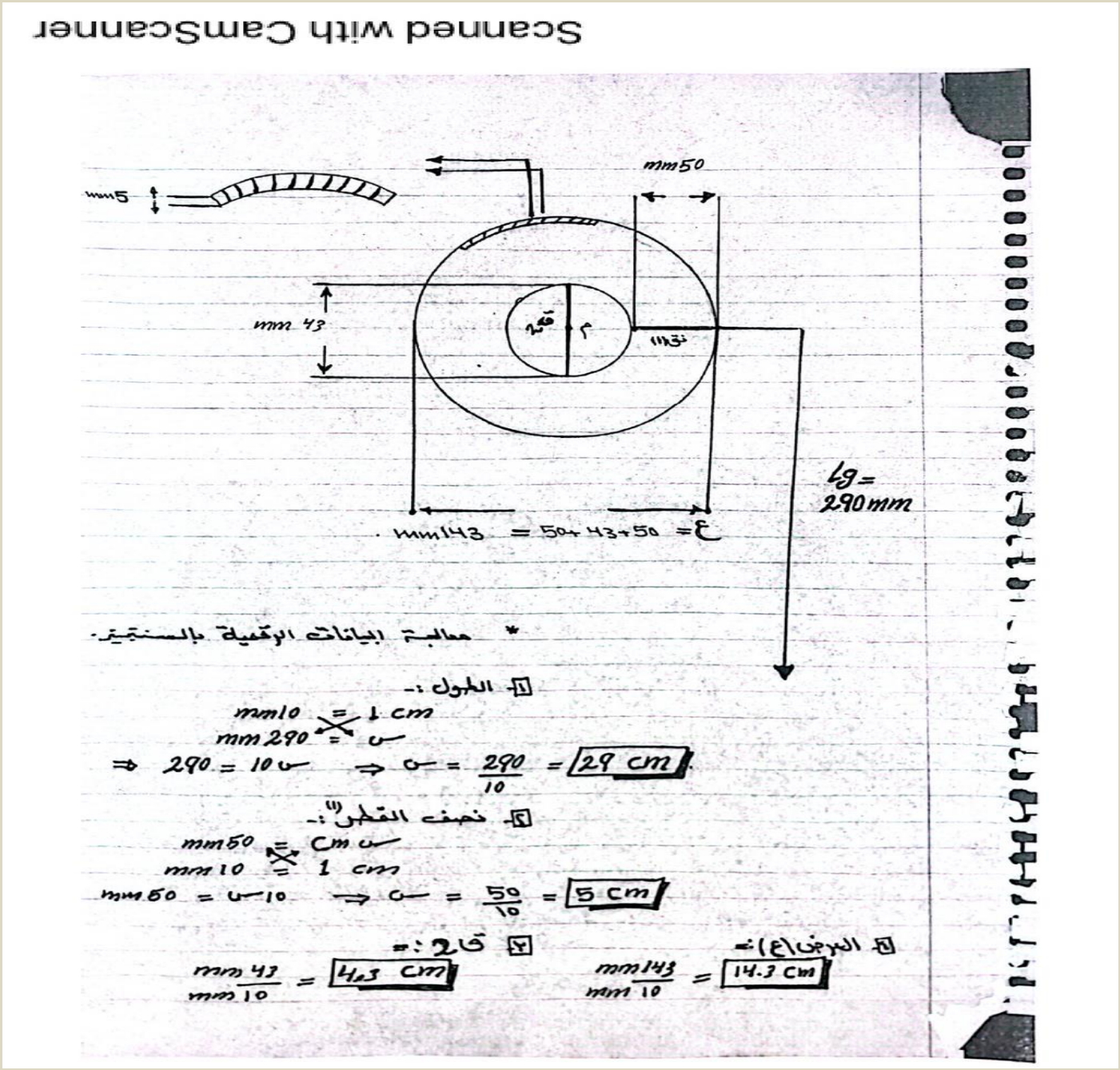
Source: https://www.ynetnews.com/article/byuk9ft9t

Feb 05 – It's a striking example of how Hamas exploits civilian resources for terrorism: a comprehensive manual provides detailed illustrations for use of **Hydrogen Peroxide**, a substance used in hospitals, in **explosive and rocket propellant production**.
IDF troops operating in Gaza found a detailed Hamas manual for the production of explosives and rocket propellant material using Hydrogen Peroxide, supplied to hospitals, come to light revealing how Hamas is exploiting a substance with legitimate uses in hospitals to construct rockets, a clear indication of the terror group's use of civilian materials for their military needs.
The manual consists of materials written in English, Arabic, and another language, likely Norwegian, outlining the distillation process of H202 for the production of explosives. These documents contain intricate schematics for constructing distillation equipment, as well as instructions on assembling homemade rockets and explosive charges.



Hamas bomb-making manual

Troops uncovered a staggering number, exceeding 100 million files and encompassing over half a million documents, including operational plans and combat strategies employed by Hamas. These materials were being meticulously examined by the intelligence unit responsible for investigating enemy material within the Intelligence Branch, which serves as the central hub for gathering and analyzing the spoils of war obtained from Hamas since the conflict's onset.



Hamas manual

During the incursion into the Gaza Strip on October 7, thousands of documents and operational code maps were discovered on the bodies of Nukhba fighters and inside their vehicles. They revealed critical information such as the deployment of Hamas forces, combat positions, sniper locations, and observation points across the area.

The failure of the Military Intelligence Directorate becomes even more apparent in light of the preparations made to handle the immense volume of documents emerging from Gaza. The dedicated unit had been disbanded five years ago but was swiftly reestablished following the events of October 7, now under the leadership of a Colonel. The unit will require several more years of dedicated work, surveillance, and decryption to fully analyze the gathered materials.

ANAMA has registered 3423 mine victims since 1991

Source: https://en.apa.az/military/anama-has-registered-3423-mine-victims-since-1991-425985

Feb 07 – "Landmine victims of Azerbaijan continue to grow. During the 30-year-long occupation, Armenia infested the lands of Azerbaijan with millions of landmines." Hikmat Hajiyev, assistant to the President of the Republic of Azerbaijan and head of the Foreign Policy Affairs Department of the Presidential Administration wrote on X, APA reports.

"Surveys of landmine incidents demonstrate that most of the explosions occur behind the former line of confrontation, especially in the areas which had no military significance. It is testimony to the fact of deliberate and indiscriminate usage of landmines with the logic "weapons of mass destruction" to terrorize and kill civilians and deprive them of the right of return." Hikmat Hajiyev wrote.

He emphasized that, from November 10, 2020, to February 5, 2024, 344 people were victims of mine explosions, of which 65 people were killed and 279 people were injured. Among mine victims, 65 civilians died and 115 were injured: "Since 1991 up to today 3423 mine victims are registered by ANAMA. Of them youth and child-357, female-38."

THE FEW
AND
THE BRAVE

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Smartphones Can Spy on You Without Using Your Camera

Source: https://i-hls.com/archives/122555

Jan 22 – Smartphone ambient light sensors are used to automatically adjust screen brightness, but researchers reveal that they can be turned into cameras and used to secretly film unsuspecting victims and their surroundings.

Researchers at MIT's Computer Science and Artificial Intelligence Laboratory proposed a computational imaging algorithm that allowed the recovery of an image of the environment from the screen's perspective.

According to Cybernews, ambient light sensors are tiny devices deployed in almost all portable devices and screens that surround us in our daily lives. As such, the authors highlight a privacy threat that affects a comprehensive class of devices and has been overlooked so far. The study suggests that ambient light sensors could intercept various user gestures like swiping and sliding, and capture how users interact with their phones while watching videos.

The main point of the study was to disprove the belief that ambient light sensors can't reveal any meaningful private information to attackers, so apps should be able to freely request access to them. Yang Liu, a PhD at the MIT Electrical Engineering & Computer Science Department explains that ambient light sensors capture what we're doing without permission and can pose privacy risks to users when combined with a display screen. One suggestion by the researchers was that software makers tighten permissions and reduce the precision and speed of the sensors. Another way to combat the security issue would be to allow users the same control they have over app permissions to access their camera or microphone. A suggestion made for future devices was that they have the ambient light sensors facing away from the user, like to the side of the device for example.

In conclusion, cybersecurity researchers are finding more and more innovative ways to spy on users. An example of this is our article regarding an AI algorithm that can know what you are typing by the sounds of your keyboard.

Can Hackers Hijack Flights?

Source: https://i-hls.com/archives/122749

Feb 07 – Flysmart+ is an iOS app for pilots to calculate aircraft takeoff performance, weight, and balance, developed by the Airbus subsidiary Navblue. It was recently revealed by cybersecurity researchers at Pen Test Partners to be vulnerable to practical attacks that could result in a tailstrike or runway excursion on departure.

According to Cybernews, the Flysmart+ app had a security feature called App Transport Security (ATS) intentionally disabled. The feature enforces secure connections, and having it and any form of certificate validation disabled exposed the app to interception attacks over Wi-Fi. This issue, though now fixed, could "enable tampering with, for example, the engine performance calculations, potentially resulting in a tailstrike or runway excursion on departure," Pen Test Partners said.

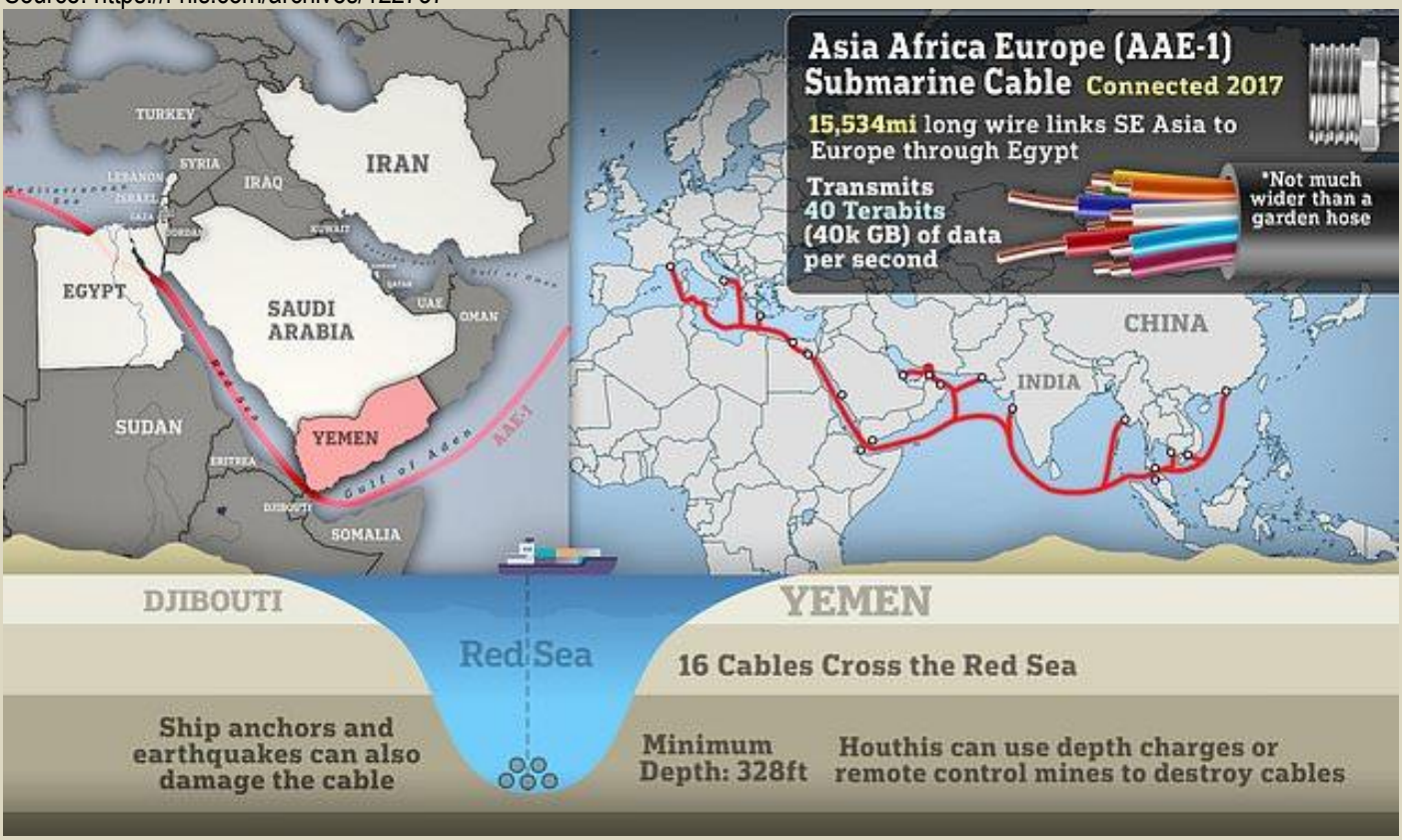
The ATS feature forces an app to use the HTTPS communication protocol, and when it is disabled, the app communicates with servers using insecure methods without encryption. This weakness can be used by attackers to intercept and decrypt potentially sensitive information in transit.

The researchers further demonstrated that a middleman could access data downloaded from Navblue servers, including SQLite databases containing information on specific aircraft, as well as take-off performance data. The researchers gave the example that with that control disabled, an attacker could potentially modify aircraft performance data or adjust airport information, like the length of the runway. Furthermore, since the app is constantly updated with aeronautical information (like procedures, how to safely depart from an airport, standard arrival routes, runway and taxiway information changes), attackers could target the Wi-Fi at a hotel where pilots typically stay and modify aircraft performance data.

After the vulnerability was disclosed in June 2022, Airbus released a public disclosure 19 months after the initial discovery. Nevertheless, the researchers mention that such changes could take a long time to fix.

The Houthis Threaten to Sever Undersea Cables, Cause Worldwide Internet Shortage

Source: https://i-hls.com/archives/122737



Feb 06 – Yemen's Iran-backed Houthis have been continuously attacking ships off the coast of Yemen since the beginning of Israel's war with Hamas, claiming they will continue "as long as Israeli forces remain active in Gaza." However, a new threat emerges with the group's threats of attacking the lattice of undersea telecommunications cables that line the Bab el-Mandeb canal.

On December 24th, 2023, a Telegram channel linked to the Houthis posted a map showing the networks of submarine communications cables in the Mediterranean Sea, the Red Sea, the Arabian Sea, and the Persian Gulf. The post read: "There are maps of international cables connecting all regions of the world through the sea. It seems that Yemen is in a strategic location, as internet lines that connect entire continents — not only countries—pass near it."

Despite not presenting an immediate threat, this statement accompanies the group's most aggressive military campaign against vessels in the Red Sea – Since October 2023, the group has launched more than 100 drones and missiles at vessels, attacks so disruptive that several shipping companies announced they would suspend shipping through the Red Sea and Suez Canal "until further notice."

According to "Gulf International Forum," both the Houthis and their allies have been scrutinizing the communications cables running underneath the Red Sea. Both Hezbollah and Iran-backed militias in Iraq released their own statements on Telegram suggesting they would consider cutting the cables.

But how important are those cables exactly? These undersea cables serve as some of the world's most critical digital infrastructure of the 21st century, servicing more than 95 percent of international data flows and communications – even partial damage to these cables could eliminate internet access across great areas, causing major economic and communication disruptions for entire countries. Until now, the reason the cables were safe was a lack of technology by the Houthis, more than a lack of motivation. Because the militant group has so far primarily fought a land war against its government, they have never developed a highly trained navy or marine contingent. They lack the submersibles necessary to reach the cables.

However, with enough time and opportunity they might be able to adapt some of their maritime tactics to target the vital communication infrastructure. It would actually not be that difficult since the shallow waters of the Gulf (only reaching a depth of 100 meters) reduce the need for high-tech submarines.

Back in 2013 three divers were arrested in Egypt for attempting to cut an undersea cable near the port of Alexandria, highlighting the possibility that militants without special equipment or training could carry out a similar mission. The Houthis have definitely undergone combat diver training, and so could execute a similar attack.

Hamas Cyberattacks Ceased After the Oct. 7 Terror Attack. But Why?

By Nate Nelson | Contributing Writer

Source: https://www.darkreading.com/threat-intelligence/hamas-cyberattacks-ceased-after-october-7-attack-but-why

Feb 14 – Cyber threat actors linked with Hamas have seemingly ceased activity ever since the terrorist attack in Israel on Oct. 7, confounding experts. Combination warfare is old hat in 2024.

As Mandiant said in a newly published report, cyber operations have become a "tool of first resort" for any nation or nation-aligned group around the world engaged in protracted conflict, be it political, economic, or warlike in nature. Russia's invasion of Ukraine — preceded and supported by historic waves of cyber destruction, espionage, and misinformation — is, of course, the quintessence.

Not so in Gaza. If today's playbook is to support resource-intensive kinetic war with low-risk, low-investment cyber war, Hamas has thrown out the book.

"What we saw all through September 2023 was very typical Hamas-linked cyber espionage activities — their activity was very consistent with what we've seen for years," Kristen Dennesen, threat intelligence analyst for Google's Threat Analysis Group (TAG), said in a press conference this week. "That activity continued on until just before October 7 — there wasn't any kind of shift or uptick prior to that point. And since that time, we haven't seen any significant activity from these actors."

Failing to ramp up cyberattacks prior to Oct. 7 might be construed as strategic. But regarding why Hamas (irrespective of its supporters) has quit its cyber operations instead of using them to support its war effort, Dennesen admitted, "We don't offer any explanation as to why because we don't know."

Hamas Pre-Oct. 7: 'BLACKATOM'

Typical Hamas-nexus cyberattacks include "mass phishing campaigns to deliver malware or to steal email data," said Dennesen, as well as mobile spyware via various Android backdoors dropped via phishing. "And finally, in terms of their targeting: very persistent targeting of Israel, of Palestine, their regional neighbors in the Middle East, as well as targeting of the US and Europe," she explained.

For a case study in what that looks like, take BLACKATOM — one of the three primary Hamas-linked threat actors, alongside BLACKSTEM (aka MOLERATS, Extreme Jackal) and DESERTVARNISH (aka UNC718, Renegade Jackal, Desert Falcons, Arid Viper).

In September, BLACKATOM began a social engineering campaign aimed at software engineers in the Israeli Defense Forces (IDF), as well as Israel's defense and aerospace industries. The ruse involved posing as employees of companies on LinkedIn and messaging targets with fake freelance job

opportunities. After initial contact, the false recruiters would send a lure document with instructions for participating in a coding assessment.
The fake coding assessment required recipients to download a Visual Studio project, masquerading as a human resources management app, from an attacker-controlled GitHub or Google Drive page. Recipients were then asked to add features to the project, to demonstrate their coding skills. Contained within the project, though, was a function that secretly downloaded, extracted, and executed a malicious ZIP file on the affected computer. Inside the ZIP: the SysJoker multiplatform backdoor.

'Nothing Like Russia'
It may seem counterintuitive that Hamas' invasion wouldn't have been paired with a shift in its cyber activity akin to Russia's model. This may be due to its prioritization of operational security — the secrecy that made its Oct. 7 terror attack so shockingly effective.
Less explicable is why the most recent confirmed Hamas-related cyber activity, according to Mandiant, occurred back on Oct. 4. (Gaza, meanwhile, has suffered from significant Internet disruptions in recent months.)
"I think the key thing to draw out is that these are very different conflicts, with very different entities involved," said Shane Huntley, senior director at Google TAG. "Hamas is nothing like Russia. And therefore, it's not surprising that the use of cyber is very different [depending on] the nature of the conflict, between standing armies versus a sort of attack like we saw on October 7."
But Hamas likely has not fully retired its cyber operations. "While the outlook for future cyber operations by Hamas-linked actors is uncertain in the near term, we do anticipate that Hamas cyber activity will eventually resume. It should be focused on espionage for intelligence-gathering on these intra-Palestinian affairs, Israel, the United States, and other regional players in the Middle East," Dennesen noted.

Hackers can Spy on Cameras Through Walls

Source: https://i-hls.com/archives/122790

Feb 12 – Security cameras are our first line of defense in many fields of life, from our homes to the bank. But what if they aren't as secure as we thought? New research from Northeastern University points to a massive gap in our security infrastructure, which stems from our security cameras. Professor of Electrical and Computer Engineering at Northeastern and cybersecurity expert Kevin Fu discovered a way to eavesdrop on most modern cameras, from home security cameras to smartphone cameras. The technique was named EM Eye (short for Electromagnetic Eye) and it can capture video from another person's camera through walls in real-time.
Fu claims that anyone with a few hundred dollars of equipment, a radio antenna and a little bit of engineering knowledge could do this, and the problem is not the lens but the wires inside most modern cameras. Fu explains that inside most security cameras there is a computer chip with a wireless connection back to the internet. The wires between the chip and the camera components give off electromagnetic radiation, which the hacker can "pick up" and decode to get the real-time encoded video. The data transmission cable ends up unintentionally acting as a radio antenna that leaks electromagnetic information.
According to Techxplore, the research team tested EM Eye on 12 different kinds of cameras (including smartphones, dash cams and home security cameras), and the results varied depending on the distance one would need to be to eavesdrop on each device (from less than half a meter away to as far away as 5 meters). However, there is another scary aspect to the discovery – since EM Eye eavesdrops on the wires and not on a computer recording footage to a hard drive, the camera doesn't actually have to be recording for someone to eavesdrop on it. "If you have your lens open, even if you think you have the camera off, we're collecting," Fu explains. "Basically, anywhere there's a camera, now there's a risk of that live real-time feed being collected by someone as close as a meter or so through walls." Fu concludes with advice for consumers and manufacturers. For consumers, he says a plastic lens is not completely fool-proof but it is a good first step, and for camera manufacturers, Fu hopes these findings would be a wake-up call.

Yeah, But No, But Yeah: The Strange Tale Of 3 Million Hacked Toothbrushes

By Davey Winder
Source: https://www.forbes.com/sites/daveywinder/2024/02/08/surprising-3-million-hacked-toothbrushes-story-goes-viral-is-it-true/

Feb 08 – A news story about the hacking of three million smart toothbrushes to create a massive botnet used to launch a distributed denial of service cyberattack against a Swiss organization has gone viral. However, many in the information security industry, including myself, have trouble finding evidence to support the story.

What's Behind The Viral Story Of 3 Million Hacked Smart Toothbrushes?Searching Google reveals that everything from national newspapers to online technology publications have picked up the viral story

of three million hacked smart toothbrushes attacking an unnamed Swiss business by way of a DDoS botnet.
However, the headlines certainly raised a few eyebrows within the information security community online, not least as there is very little by way of specifics in any of the reports and a distinct lack of technical explanations as to quite how such a massive botnet, one of the biggest on record, was created.

The story has arisen from comments provided to the Swiss publication by an engineer from the Swiss arm of security vendor Fortinet. I have contacted Fortinet for clarification regarding the root of this viral story and will provide an update if I hear back.

Update February 8: A Fortinet spokesperson has provided the following statement:

"To clarify, the topic of toothbrushes being used for DDoS attacks was presented during an interview as an illustration of a given type of attack, and it is not based on research from Fortinet or FortiGuard Labs. It appears that due to translations the narrative on this topic has been stretched to the point where hypothetical and actual scenarios are blurred."

Update February 8: The author of the orginal article refutes the Fortinet narrative and insists the 'example' was presented as a real case.

The author of the original article published by Aargauer Zeitung, Ann-Kathrin Amstutz, contacted Forbes following the publication today of an update to this story in the format of a statement from Fortinet which claimed there was no real attack. That statement suggested that "due to translations the narrative on this topic has been stretched to the point where hypothetical and actual scenarios are blurred." However, Amstutz told Forbes that "In a statement today, Fortinet's head office claimed that the scenario was hypothetical and that we had 'streched the narrative.' We counter this with the report on how the article came about."

Indeed, Amstutz was so keen to point out that the idea that somehow the narrative had been stretched in the original article was not true that a newly published rebuttal of this narrative has now gone to press. This has quite a different takle to tell.

Although this is also in the German language, a machine translation reveals a vert different story to the one that Fortinet is portraying. The publication says that while Fortinet claims the toothbrush case was used as an example of a DDoS attack during an interview, the 'example' was, in fact, presented as reality.

"What is now called a 'translation problem' by the Fortinet headquarters in California, sounded very different during the research. Swiss Fortinet representatives described the toothbrush case as a real DDoS attack at a meeting that was about current threat situations. Fortinet provided concrete details: information about how long the attack paralyzed the website of a Swiss company and an order of magnitude of how much the damage incurred was. Fortinet did not want to disclose which company it was out of consideration for its customer."

The rebuttal goes as far as to state that the text of the original article was forwarded to Fortinet for verification before it was published and "The sentence that it is a real case that really happened in this way was not objected to."

The email that was sent by Fortinet that included the statement I published as an update to this story actually included some more information that I did not publish at the time. However, in light of the newly published rebuttal, I think it should be added now. This is what else the Fortinet spokesperson had to say:

"The Mirai botnet has been dethroned from its #1 position. In the 2H 2022 Global Threat Landscape Report from FortiGuard Labs, which was released on February 22, 2023, Mirai sat at #1 in terms of Volume per Organization. Between Q3 and Q4 2023, Mirai volume of command-and-control detection subsided 36%

and now currently sits at #5. FortiGuard Labs has not observed Mirai or other IoT botnets target toothbrushes or similar embedded devices."
I have reached out to Fortinet once more with this new information, and I will update the story if there is any further communication.

Security Experts Call BS On Toothbrush Botnet Story
One highly-respected industry veteran, Kevin Beaumont, better known as GossitheDog online, was quick to claim the story wasn't true. Others such as Robert Graham, ErrataRob on Twitter/X, also called BS on the claim.
Meanwhile, at my request, Dirk Schrader, vice-president of security research at Netwrix, and a native German speaker, took a look at the original article that appeared in the Swiss newspaper Aargauer Zeitung. Schrader told me that the original article doesn't mention any type or model of toothbrush, the name of the victim or the suspected perpetrator, or the motive behind the distributed denial of service attack.
"It appears to be a rather generic tale warning of the need to protect any device, large or small, connected to the internet," Schrader says, "my feeling is that this is a theoretical and poorly explained example, later in the same piece there's another such example of how to use open-source intelligence to infiltrate an organization."

The Truth Behind The Viral Warning
Most smart toothbrushes are Bluetooth Low Energy enabled rather than connecting by WiFi, although some do have that capability. However, whether it's feasible that three million could have been hacked is highly debatable. Without firm evidence, which I have asked Fortinet to provide, the clever money would agree with Schrader that this is a case of something lost in translation that has run wild. Not that the underlying threat from so-called Internet of Things devices isn't something to take seriously. It most certainly is. "While the theory is valid, and DDoS attacks abusing operational technology devices have happened in the past," Schrader concludes, "this kind of report does not help to secure smart devices. It doesn't give any advice about how to securely connect smart devices using multi-factor authentication features or something similar."

Davey Winder is a four-decade veteran technology journalist and contributing editor at PC Pro magazine, a position he has held since the first issue was published in 1994. Davey has spent more than 30 years as a freelance technology journalist. The author of 25 published books, Davey's work has appeared in The Times, The Sunday Times, The Guardian, The Observer, PC Pro, The Register, Infosecurity Magazine, SC Magazine, IT Pro and TechFinitive to name but a very few. Along the way, he has picked up a bunch of awards from his peers, including: *'Most Educational Content' (2021 European Blogger of the Year Awards) - 'Cyber Writer of the Year' (2020 Security Serious Awards) - 'Enigma Award' (2011 BT Security Awards) - 'Security Journalist of the Year' (2010 BT Security Awards) - 'Security Journalist of the Year' (2008 BT Security Awards) - 'Security Journalist of the Year' (2006 BT Security Awards) - 'Technology Journalist of the Year' (1996 BT Technology Journalism Awards).*

Hackers Can Use the Sound of Swiping to Steal Your Fingerprints

Source: https://i-hls.com/archives/122909

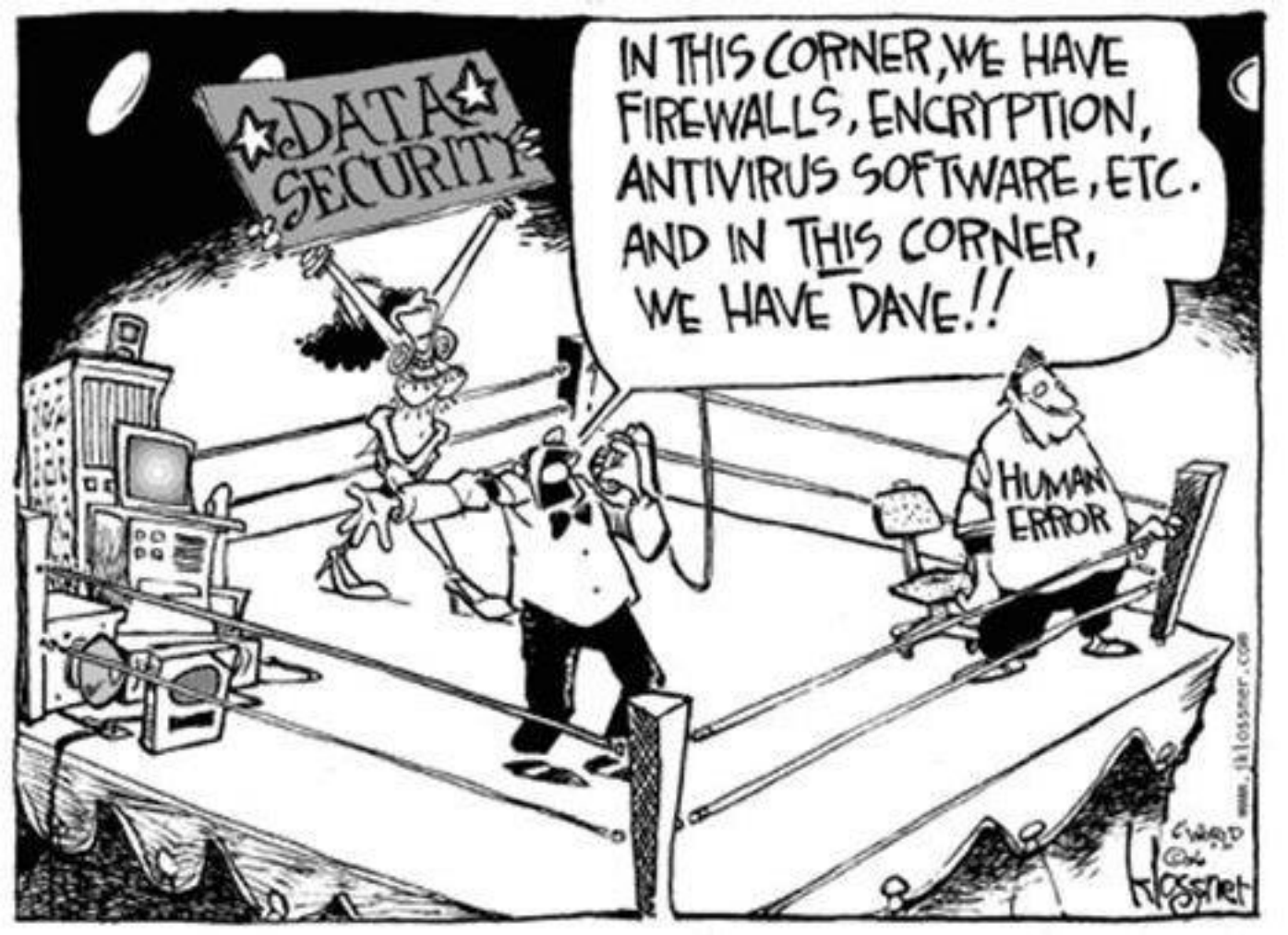
Feb 22 – Nowadays, fingerprints are one of the most popular forms of personal identification, whether it's unlocking your phone, approving online payments, access control, and many more. This means that leaked fingerprints can cause immense amounts of damage.

Researchers from China and the US were able to steal up to 27.9% of partial fingerprints and 9.3% of complete fingerprints within five attempts using a "PrintListener" side-channel attack that leveraged the sounds made by users' fingertip friction while they use social media or other apps on their phones.
"The attack scenario of PrintListener is extensive and covert. It only needs to record users' fingertip friction sound and can be launched by leveraging a large number of social media platforms," reads the paper published by the researchers.
According to Cybernews, the researchers began by recording the friction sounds of nine participants against a phone with a matte screen protector. They then moved on to 65 participants aged 18 to 30 and tried to extract important information from finger friction audio.
When the finger swipes on a screen it creates a roughness noise, the production of which involves three factors: the friction between the fingertips and the smartphone screen that amplifies

the vibrations, the dynamics of the vibrations between the finger and the screen, and the audible roughness sound that radiates from the finger to the surface of the phone and propagates through the air.

This work extends previous research that demonstrated the vulnerability of fingerprint recognition systems, especially when the attacker has even partial information of the users' fingerprints. Furthermore, listening to swiping fingers puts attackers at an advantage since they can be stealthy, use mainstream apps and device microphones, and not require extensive training on specific individuals.

The researchers provided some solutions to protect against such attacks, including using a smooth screen protector that produces less noise and creates less friction, trying not to swipe while recording video/audio, or even having the apps themselves destroy finger frictional sound features with automatic speech noise reduction or implement pop-up reminders to caution users to be careful when performing swiping operations while the microphone is in use.



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

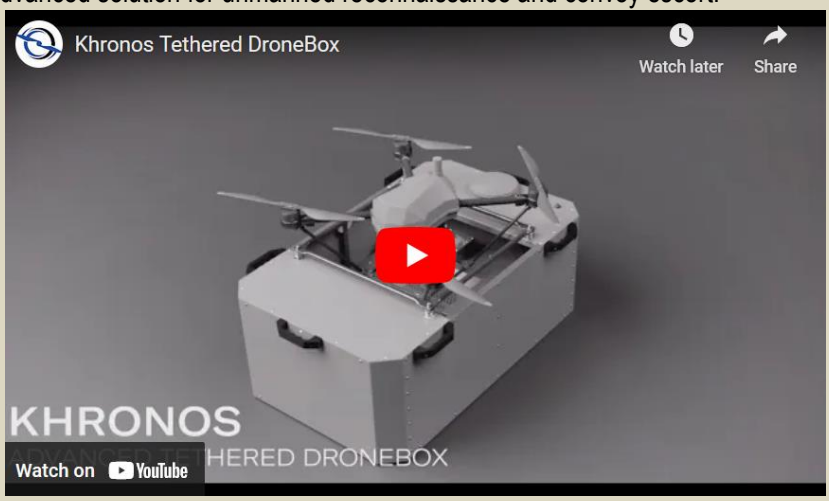
& Robotic

DRONE NEWS

'Drone-in-a-box' – New Drone-Truck Tag Team

Source: https://i-hls.com/archives/122578

Jan 24 – A new partnership between Rheinmetall Canada and Elistair aims to provide military customers with an on-the-move ISR solution that will combine Elistair's fully automated KHRONOS tethered drone with Rheinmetall's Mission Master family of UGVs.
Elistair's CEO Guilhem de Marliave stated: "We are very excited to be collaborating with a major defense contractor like Rheinmetall Canada. By combining their Mission Master family of UGVs with our push-button, long-endurance, automated KHRONOS drone, Rheinmetall Canada can provide customers with an advanced solution for unmanned reconnaissance and convoy escort."



According to Interesting Engineering, Elistair's KHRONOS is a 30 kg tethered drone that can be deployed from a transportable drone box in under two minutes and **remain in the air for up to 24 hours**, even operating from a moving platform. **It provides continuous coverage of an area with a radius of 10 kilometers day and night.** The drone can also fly in difficult weather conditions or GPS-denied and RF-denied environments.
Rheinmetall's Mission Master SP is an electric-powered UGV designed for resupply missions and payload carriage. It is a compact platform that provides aid and safety to dismounted troops over a range of 450 kilometers without needing additional charge. It can even cover 50 kilometers when its batteries run out. Finally, it has space to transport light payloads like section sensors and weapon systems. This revolutionary system is designed to operate in challenging environments and can be deployed rapidly and be operational in under two minutes from a portable "drone-in-a-box," making it exceptionally suitable for urgent and dynamic scenarios.
An issue arises when tethering a drone to a ground vehicle since it makes it inherently more vulnerable than a "free-flying" drone. However, the companies claim that the ability to provide persistent surveillance, secure communications, and greatly improved energy efficiency outweigh the cons under certain mission circumstances.
The KHRONOS system is highly versatile and easy to integrate with vehicles, and an excellent tool for public safety agencies, border patrol units, military forces, and vehicle integrators. It is expected to be a simple yet highly effective long-endurance ISR asset, and the first deliveries are set for March 2024.

A Drone with Ears

Source: https://www.homelandsecuritynewswire.com/dr20240126-a-drone-with-ears

Jan 26 – When a natural disaster such as an earthquake occurs, every minute counts. Unmanned aerial vehicles (UAVs) are often used to assist the search for survivors as they can provide an initial overview of difficult-to-reach areas and help to detect victims — provided they are visible. Researchers at the Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE) are now looking to close a gap in the provision of disaster management services with a new technology: In the future, drones equipped with microphone arrays will be able to precisely locate cries for help and other acoustic signals from victims from the air and supply information about their location to the rescue teams. This significantly increases the chances of a rapid rescue for victims who cannot be spotted by camera. Floods in Libya, Greece and Slovenia, fires in Hawaii and Tenerife, earthquakes in Turkey and Morocco — when a region is hit by a natural disaster, every minute counts in the efforts to save victims. But searching for survivors is complex work as buildings and roads may be damaged and large areas cut off. The use of drones equipped with daylight cameras and thermal imaging cameras is therefore becoming increasingly widespread — they can quickly fly over large areas of ruined infrastructure, locate victims and speed up the response of the rescue teams. The problem is that victims trapped under rubble cannot be seen by these imaging sensors, and factors such as thick smoke, fog or darkness also limit the effectiveness of the cameras. For scenarios such as these, researchers at Fraunhofer FKIE are working on a solution which enables acoustic sensors to be added to the cameras: LUCY — short for Listening system Using a Crow's nest arraY — is a piece of technology developed by FKIE scientist Macarena Varela in collaboration with colleagues and research group leader Dr. Marc Oispuu to save the lives of people buried in rubble or trapped by fires.

The present version of LUCY, which incorporates 48 MEMS microphones | Fraunhofer FKIE

LUCY is an array of MEMS microphones — known as a crow's nest array — which is mounted on drones in order to determine the direction from which noises such as cries for help, clapping or knocking signals are coming. The tiny, robust MEMS microphones are inexpensive and used in applications such as smartphones. The special thing about this system is that the microphones are attached to the underside of the drone in a special geometric configuration and can perceive sound from all directions. "The highest lookout point on ships which allows you to see in all directions is known as the crow's nest. The same goes for LUCY — our system can hear in all directions with virtually no restrictions," explains Macarena Varela.
LUCY works in a similar way to the human ear, which takes in sound information and conveys it to the brain where it is analyzed. In the case of the array system, the ears are replaced by microphones and the brain is replaced by a signal processing unit which gages the direction from which the noises are coming. LUCY currently features 48 microphones, enabling the direction of the sound source to be determined with excellent precision. "Spatial hearing obviously works better with 48 or more microphones than with two acoustic sensors, and both targeted hearing in a particular direction and the ability to ignore certain sounds are also improved," says Dr. Oispuu. Furthermore, the system is able to perceive frequencies which the human ear cannot register. In the future, the number of microphones will be increased to 256 sensors capable of processing signals in real time.

Distracting Ambient Noises Are Filtered Out
The system blocks out distracting ambient noises such as from rescue equipment, wind or birds, as well as from the whirring rotors of the drone itself. Artificial intelligence (AI) methods and adaptive filters are used to filter out signals, and at the same time the system is taught to detect sound patterns such as shouting, banging or clapping which might be used by people in need to attract attention. To enable the system to do this, it uses a database of different sounds or signatures that the AI has been trained on in advance. In combination with signal processing techniques such as coherent beamforming, this makes it possible to detect and classify noises and determine their angle of incidence precisely. Furthermore, a compact processing unit ensures that signals can be processed very quickly. When a disaster occurs, the location data that is received will be conveyed to the rescue teams, who can then use tablets, for example, to identify the exact positions of the victims.

Lightweight LUCY
Thanks to their scalability, the sensor modules and microphone arrays can be used on numerous commercially available drones. As both the MEMS technology and the drones are relatively cheap, multiple unmanned aerial vehicles can be used to investigate the disaster zone effectively. Due to its low weight, emergency responders can carry the LUCY system with them to also use it on the ground, and it can be mounted on vehicles or used as stationary equipment. The FKIE researchers are currently working on further improvements to the experimental system.

Hydrogen Power Takes Drones to the Next Level

By Brian Blum
Source: https://www.homelandsecuritynewswire.com/dr20240130-hydrogen-power-takes-drones-to-the-next-level

Jan 30 – Remember when the scourge of "fire kites" from the Gaza Strip was Israel's most pressing problem?
It was 2018 – seems like ancient history in the context of the current war against Hamas – and the terror group was flying cheap incendiary devices in balloons and kites over the high-tech border fence, resulting in significant damage to Israeli agriculture.

Bentzion Levinson, who served as a combat commander in the Israel Defense Forces, was invited to join a hackathon to come up with innovative solutions to the fire kites.
Levinson's idea was to outfit drones with thermal cameras to identify the location of fires, and with firefighting equipment that could put out the fires from the air.
Since then, Levinson has been all-in on drones – so much so that he left the IDF and founded a startup, HevenDrones, to build solutions for the military, homeland security firefighters and aid organizations.
"Drones are becoming mainstream," Levinson notes. "But if we want them to be able to take concrete actions – to install things, move something from point to point or put out fires – they need to be more like flying robots."

Is Hydrogen the Answer?
The biggest questions for drones when used by the military or security services are how much it can carry and for how long it can remain in the air.
Most drones run on electric batteries and can stay aloft no more than about 45 minutes when carrying just a few kilograms. The more they carry, the sooner they need to return to base to recharge. Hovering – which is necessary for surveillance or delivering a payload – uses even more juice.
HevenDrones' answer: hydrogen.
"The core issue is energy density," Levinson explains. "For a car, you can always make a bigger battery. That won't work with drones. It will make them too large. Hydrogen has the best energy density."
To fight in an arena such as the Gaza Strip, drones need to fly for many hours. When HevenDrones demonstrated that it could do that using hydrogen as the power source, the IDF entered into an exclusive relationship with the company to provide hydrogen-powered drones through 2026.

Two New Models
At the Monaco Hydrogen Alliance Forum in November, in the midst of Israel's war with Hamas – HevenDrones announced two hydrogen-powered UAVs (unmanned aerial vehicles, the formal way to describe a drone):

- The H2D200 can carry up to 10 pounds (double the maximum weight for battery-powered drones) for 317 miles or four hours of flight time.
- The **H2D250** (right) can transport up to 22 pounds for a range of 466 miles with eight hours' flying time.
- That's in addition to the HD55, a hydrogen-powered hovering drone launched earlier in 2023.

HevenDrones' only non-hydrogen powered vehicle, the H100, is already operating in the field. It runs on batteries, but it's able to carry a 75-pound payload for close to an hour. The H100 can carry other companies' robots, as well – such as Roboteam's Micro Tactical Ground Robot.

Self-Reliant
HevenDrones has a partnership with Plug Power, which makes hydrogen fuel cells, to cooperatively develop hydrogen drones.
HevenDrones is also working with Honeywell, another key player in the hydrogen space. And Levinson is bullish on deploying "micro-electrolyzers" – small and cheap devices that can generate hydrogen anywhere, including in the field.
HevenDrones uses a relatively small amount of hydrogen – just 250 grams for a two-hour flight. Toyota's Murai, a hydrogen-powered car, consumes some five kilograms of hydrogen per tank.
Therefore, its drones won't be reliant on "hydrogen hubs" like the US Department of Energy is planning for refueling larger aircraft, trains, ships and cars. HevenDrones' customers, says
Levinson, "can be self-reliant on their own hydrogen source."
Levinson, who moved to Israel from the United States with his parents when he was a teenager, is looking at military uses as the most immediate "use case" for hydrogen-powered drones. But there are plenty of other applications, such as monitoring construction and agricultural sites.
How about home deliveries? Amazon, for example, has invested heavily in drone technology. Right now, those drones can only carry up to about five pounds. "Hydrogen will allow them to carry 10-pound payloads," Levinson says. "We will get there." It doesn't hurt that HevenDrones hired the person who was formerly responsible for Amazon's $2 billion drone delivery program.

One to Many

The military, however, is in some ways the easiest client to land, as it controls the airspace in times of conflict and is therefore not subject to the regulatory demands that an Amazon delivery drone might encounter. Drones can be operated either manually or run autonomously. In both cases, the intention is clear: To be efficient, an individual drone can't have its own dedicated pilot.

"To add value, we have to get to 'one-to-many.' We can't have 100 skilled pilots for 100 drones. So, we're focusing a lot on the autonomy piece." Levinson says.

HevenDrones, which employs 35 people in Yokne'am (northwest Israel) and in Miami, Florida, has raised $25 million from private investors in the four years since the company was established and will be heading towards a Series B round in 2024. The company's drones are now flying on three continents.

Levinson is not just a military guy. He attended an entrepreneurship program at Stanford's Graduate School of Business and participated in the technology training program run by Israel-based Jolt.io.

He was called up to serve in the reserves on October 8, following the horrific "Black Sabbath" the day before.

"I spent a month and a half on the northern border," he tells ISRAEL21c. "Moving forward, though, I realized our company could add more value creating drones for the military than with me being on the front."

Moreover, with a third of HevenDrones' staff currently involved in the fighting, Levinson's leadership in the office was needed more than ever.

Even Keel

We were curious what happened to the "a" in the "heaven" part of the company's name.

"'H' is for hydrogen," Levinson explains. "Following that, there's the word 'even,' which relates to 'stability.' A flying robot needs to be stable. And of course, if you look up into the sky, 'heaven' comes to mind."

●▶ To learn more about hydrogen-powered drones, click here.

Brian Blum writes about new local startups, pharmaceutical advances, and scientific discoveries for Israel21.

The Challenge of Cheap Drones: Finding an Even Cheaper Way to Destroy Them

By Bradley Perrett (defense and aerospace journalist)

Source: https://www.homelandsecuritynewswire.com/dr20240130-the-challenge-of-cheap-drones-finding-an-even-cheaper-way-to-destroy-them

Jan 30 – The aerial target is coming at you or your friends. It can kill any kind of vehicle, including a tank, or hit an ammunition store, command post or even a surface-to-air battery worth hundreds of millions of dollars. Or it may go after a single soldier.

Your challenge is that the target, a quadcopter drone, is really small, maneuverable and hard to detect.

None of that is the biggest challenge. Rather, the confounding problem is that the thing is incredibly cheap, having cost the enemy some low multiple of $1000—far less than the usual cost of shooting down anything. If you use expensive means to knock down such a drone, the other side's easy answer is just to build more of them and exhaust your budget.

The sudden proliferation of inexpensive drones in Ukraine is a revolution in warfare. While they vary in size and capability, the economics of defense are particularly stressed by the very cheapest ones, those adapted from civilian models or made with commercially available components.

What follows is a look at the difficulties in engaging a little civil-derivative quadcopter. This article in the series particularly focusses on the challenge in developing and making counter-drone systems that use cannon to achieve more range than is available from machine guns—to increase the area that can be defended and the time available for engagement. Another article will look at other tools for defeating cheap drones, such as lasers and jamming.

Northrop Grumman of the US, MSI-DS in Britain, and Australia's Electro Optic Systems (EOS) are among manufacturers offering systems with cannon.

Two issues arise: such weapons need a multiplicity of expensive sensors to do the job, and they must be built with high precision to hold down ammunition expenditure. So, they cannot be cheap. We can understand this if we follow their engagement sequence.

First, the defender must detect the drone. For longest-range detection, use of a search radar may be preferred—at the risk of the enemy picking up its transmissions, determining its location and attacking it.

The drone is made mostly of plastic, a poor reflector of radio energy, so the radar needs to be sensitive. It must also be set for detection of targets moving as slowly as tens of kilometers per hour, which means it will have to be clever enough to ignore reflections from birds.

In fact, a radar may be able to do that and indeed to use the characteristics of radio reflections to work out a drone's model—handy information for avoiding destruction of friendly aerial objects.
A search radar may pick up a little drone at 5km if it has a sufficient line of sight, then classification occurs at a closer range. Such a sensor probably costs at least hundreds of thousands of dollars.
Optical detection is an alternative to radar in reasonably clear daylight but probably doesn't offer such long range and warning time. The Mark I eyeball is particularly challenged in noticing a distant quadcopter, but a weapon system's electro-optical and infrared cameras might be used in scan mode.
Once the drone has been detected, it must be tracked. And here we begin to deal with the problem of achieving high precision and the tight and costly manufacturing standards that it demands.
Tracking means finely measuring the drone's position and movement. Again, a suitably high-performance radar may be used, at the risk of detection, or the weapon system can rely on its electro-optic and infrared cameras and its laser rangefinder. Taking the required data from them means knowing exactly the angles at which they are pointing.
They need to be slewed in the target's direction very quickly, preferably automatically, to begin their work and minimize engagement time. Tracking may need to begin at a range of several kilometers. The greater the range, the greater the distortion of observed angles by atmospheric conditions. To some extent those errors can be reduced with software.
If everything is working, the fire-control computer now knows pretty well where the little target is and how it's moving. It can work out a future position at which the drone and a round of ammunition can come together.
The gun must now point at exactly the angles that the fire-control computer has calculated for it. Nothing in the apparatus can be wobbly. If confident that the weapon is tracking well and that no friendly object will be hit, the gunner will fire. In the case of EOS's Slinger counter-drone weapon, the gunner could reasonably hope to hit at 1500 meters, the company says.
If such a weapon is using 30mm proximity-fused shells, which explode when they sense something close to them, it had better knock down a quadcopter with a single round. Each shell costs something like US$1000, so using a few could easily cost more than the drone (and take more time). Here, however, there's an advantage for the defender. A flimsy quadcopter can cope with hardly any damage and a fragment from an exploding shell is very likely to bring it down.
The probability of hitting will vary with ranges and weather, and also from system to system. EOS says the Slinger has at least a 95% chance of downing a quadcopter with one 30mm proximity-fused round in standard daylight conditions at 1000 meters. If solid ammunition is used instead of shells, the cost per round will be much lower, but the gunner will probably have to fire a burst of several.
Cannons might also use time-fused shells, which explode at the calculated moment of interception.
The point of using cannons is to engage at a distance, but if the drone has managed to close to around 500 meters, the gunner will switch to the system's machine gun. A burst of bullets may cost only a few dollars, and one hit will do the trick.
That sounds good, but the defender will strongly prefer that the drone never gets so close. And if the drone has escaped cannon fire in going for a target that's too far for the machine gun to cover, then the defense has already failed.
The exact prices for these systems are not known. EOS has said that three Slingers sold last year cost less than $2 million (US$1.3 million). The ABC has reported a price of less than US$1 million per system.
That would not include the search radar, nor, perhaps, training and an initial stock of ammunition and spares, all needed to achieve operational capability. Then there's the question of how many such systems must be bought. If the defender needs to cover a front line and the effective weapon range is 1000 meters, then the systems will have to be spaced at less than 2km intervals, even assuming clear lines of sight. And more will be needed in the rear, to cover other equipment and installations, and maybe more again to deal with larger drones that could reach such facilities as power stations and hospitals. If swarm drone attacks are expected, and they probably should be, defensive weapons will have to be placed thickly, reinforcing each other.
Consider, too, that crews will be needed for all those systems.
The drones are cheap, so killing them must also be cheap. But equipping an army for the task cannot be.

Raytheon's CHIMERA Fries Drone Using Microwave Rays

Source: https://i-hls.com/archives/122675

Jan 31 – Raytheon announced that its Counter-Electronic High-Power Microwave Extended-Range Air Base Defense (CHIMERA) has completed a three-week field test in which it managed to fry static targets and track aerial targets flawlessly.
During testing, CHIMERA utilized directed energy to engage multiple static targets and successfully demonstrated end-to-end fire control by acquiring and tracking aerial targets through their entire flight paths.
According to Interesting Engineering, CHIMERA is a ground-based demonstration system that uses radio energy to defeat airborne threats with more power than other high-power microwave systems. Such

systems are very inexpensive to fire once built and their ammunition is limited only by the availability of power, making them suitable to take on drones that attack in large numbers.

President of Advanced Technology at Raytheon Colin Whelan stated: "High-power microwave systems are cost-effective and reliable solutions that play an important role in layered defense by increasing magazine depth and giving warfighters more options to defeat adversaries quickly."

CHIMERA is a component of the Directed Energy Front-line Electromagnetic Neutralization and Defeat (DEFEND) program to create HPM systems for deployment at the front line. Furthermore, Raytheon recently announced that as part of this program it has also developed an HPM weapon system for the US Army. The systems are designed to be sturdy and easily transportable for deployment on the front lines.

The partnership between the US Air Force Research Lab, Naval Surface Warfare Center Dahlgren Division, and the Undersecretary of Defense for Research and Engineering aims to deliver prototypes in the fiscal years 2024 and 2026.

"Non-kinetic defense systems are a key part of America's national defense strategy," said Whelan, "The new iterations of Raytheon's high-power microwave systems are cost-effective and reliable solutions that operate at the speed of light – enabling our warfighters to defend against faster and more maneuverable threats."

BAE Systems' Drone-Killing Vehicle

Source: https://i-hls.com/archives/122634

Jan 29 – BAE Systems successfully tested its anti-drone AMPV C-UAS system: an Armored Multi-Purpose Vehicle Counter-Unmanned Aircraft System prototype. The test assessed the detection, tracking, identification, and defeat of stationary and moving aerial and ground targets.

According to Interesting Engineering, the system was tested during realistic battlefield scenarios in which the AMPV C-UAS showed its ability to accurately detect, track, identify, defeat, or turn off stationary and moving aerial and ground targets. BAE Systems AMPV program director Bill Sheehy stated: "From the earliest combat

capability concept stage of the AMPV program, we intentionally designed a modular and flexible configuration to provide an adaptable and ready-for-growth platform for the warfighter."
The US Army received the first AMPVs from BAE Systems in 2020. These vehicles mark the introduction of a modular armored vehicle system that enables the Army to customize the AMPV for various purposes. From carrying personnel to serving as a mobile surgical operating theater, the AMPV can be modified quickly for different roles.

Brandon Gollwitzer, Moog Inc. (aerospace and defense company) Turreted Weapon Systems general manager, explained: "The fully-integrated mission capability demonstrated in this RIwP (Reconfigurable Integrated-weapons Platform) equipment package on AMPV is ready now and poised to meet the current and future needs of our warfighters."
In the future, Moog will reportedly supply and integrate the C-UAS weapon system with Leonardo DRS' Multi-Mission Hemispheric Radars, C2 systems, and Northrop Grumman's XM914 30mm cannon.
This innovative system provides significant improvements in power, mobility, interoperability, and survivability for soldiers.

Can a 100-Drone-Swarm Be Controlled by One Person?

Source: https://i-hls.com/archives/122743

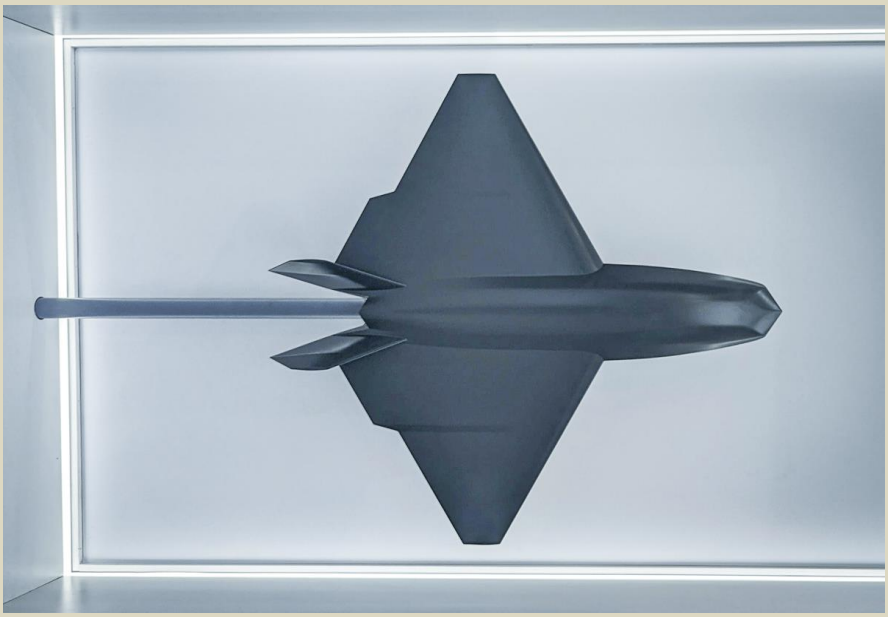
Feb 06 – Research from Oregon State University shows that a "swarm" of over 100 autonomous ground and aerial robots can be supervised by just one person. This discovery represents a big step toward efficiently and economically using swarms in various roles, from wildland firefighting to package delivery to disaster response in urban environments.
According to Techxplore, the results of the study were published in "Field Robotics" and stem from the Defense Advanced Research Project Agency's program known as OFFSET, which is short for Offensive Swarm-Enabled Tactics. During the four-year project, researchers deployed swarms of up to 250 autonomous vehicles (multi-rotor aerial drones, and ground rovers) that were able to gather information in urban surroundings where buildings impair line-of-sight, satellite-based communication.
Julie A. Adams of the OSU College of Engineering was a co-principal investigator on one of two swarm system integrator teams that developed the system infrastructure and integrated the work of other teams focused on swarm tactics, swarm autonomy, human-swarm teaming, physical experimentation and virtual environments.
The tests were each stretched over several days, while each multi-day field exercise introduced additional vehicles, and every 10 minutes swarm commanders provided information about their workload and how stressed or fatigued they were. During the final field exercise (which featured over 100 vehicles) the users' workload levels were also assessed through physiological sensors.

"The project required taking off-the-shelf technologies and building the autonomy needed for them to be deployed by a single human called the swarm commander. That work also required developing not just the needed systems and the software, but also the user interface for that swarm commander to allow a single human to deploy these ground and aerial systems."

A collaboration with Smart Information Flow Technologies yielded I3 – a virtual reality interface that lets the commander control the swarm with high-level directions. "The commanders weren't physically driving each individual vehicle, because if you're deploying that many vehicles, they can't—a single human can't do that," Adams explained. "The idea is that the swarm commander can select a play to be executed and can make minor adjustments to it… The objective data from the trained swarm commanders demonstrated that a single human can deploy these systems in built environments, which has very broad implications beyond this project."

BAE Systems shows off mystery drone at defense show

Source: https://newatlas.com/military/bae-systems-mystery-drone/



Feb 07 – In a teaser of things to come, BAE Systems has displayed a model of its future drone at the World Defense Show in Riyadh. Steeped in more mystery than a Raymond Chandler novel, it gives us a hint of what future military drones might look like.

International defense shows can often be more like bird watching events than showcases for the latest military hardware. Defense contractors don't just like to show off their wares for sale, they also like to give a glimpse of what might be on the way. Oftentimes, these will be in the form of models or concept images on display without any explanation of what they are.

Though this can be a bit frustrating for the curious, it does

provide something of an air of adventure to the proceedings.
In the case of the latest BAE Systems display, we get a model, but no specifications. Not even a name. However, there are all sorts of clues that give us some idea about this aircraft. The drone has a cropped diamond delta wing, which suggests that it can perform at transonic or supersonic speeds and has a small radar cross section. It's jet powered, has a V-tail for less drag, an angular hull, shrouded jet exhausts, and a dark coating, suggesting that stealth plays a large part in its details.
When we learn more and whether it leaves the drawing board is up to BAE.

Enemies Might Attack US Forces With Autonomous Killer Robots

By Johnny Franks
Source: https://warriormaven.com/global-security/enemies-might-attack-us-forces-with-autonomous-killer-robots

Feb 09 – Are we ready for a future where machines decide who lives and who dies? Lethal Autonomous Weapon Systems (LAWS) have been at the forefront of discussions and initiatives by the United Nations (UN) to address growing concerns. These systems, characterized by their autonomy with varying levels of human oversight, have become more sophisticated, and as technology advances, artificial intelligence (AI) is being applied for more efficient operation. The UN Secretary-General, António Guterres, called LAWS "politically unacceptable and morally repugnant," advocating for their prohibition under international law and recommending the conclusion of a legally binding instrument by 2026 to prohibit LAWS that operate without human control or oversight and regulate all other types of autonomous weapons systems.
The US military is at the forefront of integrating autonomous technologies into its operational capabilities, and there is a general trend among global powers to employ such systems. DoD policy directs that an appropriate amount of human judgment must be included in using force by autonomous and semi-autonomous weapons systems. However, there is an evident push towards developing systems with ever-diminishing degrees of human control. On the other hand, the U.S. Army's long-term strategy involves the phased integration of robotic and autonomous systems (RAS) in the combat force, beginning with unarmed, unmanned utility vehicles and trucks, moving to armored robotic vehicles with increasing autonomy. This strategy seeks to enhance operational effectiveness while mitigating risks to human soldiers.
The US military's move towards autonomy in weapon systems includes all service branches. The Navy is developing and test-running prototype systems like Sea Hunter and unmanned underwater vehicles (UUVs), having the capability to perform extended autonomous operations. The incentives for such efforts include cost-effectiveness and the reduction of risk, all to send out a more challenging target to an enemy.

The Air Force, on the other hand, is also developing unmanned combat drones that can operate autonomously, especially in situations where communication with human operators might be impossible.
This transition towards more autonomous systems challenges and contributes to the debates on the issue. The global race for autonomy in military technologies, driven by strategic competition among major powers, brings out several ethical, legal, and security implications. The challenge of controlling the risks arising from accidental engagements and escalation, accompanied by the moral ramifications that come along with the progressive dismantling of human involvement in life-and-death decisions, are some of the pressing concerns that must be addressed. Through the international community, via conferences like the UN, the world is coming to grips with this challenge to establish norms and rules that strike a balance between technological advancement for the sake of the defense and holding in check the humanitarian principles, ensuring compliance with international law.

Johnny Franks holds an MA in U.S. Foreign Policy & National Security from American University and a BA in Diplomacy & World Affairs from Occidental College. With a specific interest in geopolitical security and military technology, Johnny has primarily focused his research and analysis on the Russia-Ukraine conflict from 2014 onwards. As part of his MA coursework, Johnny contributed to developing an Arctic defense strategy in partnership with the U.S. Department of Defense.

●▶ **Read also: Attack Robots, Terminators, Autonomous Weapons – Future of AI**

Academics in US, UK and Australia collaborated on drone research with Iranian university close to the regime

Source: https://www.theguardian.com/world/2024/feb/14/academics-in-us-uk-and-australia-collaborated-on-drone-research-with-iranian-university-close-to-regime

Feb 15 – Academics in the UK, Australia and the US collaborated on research related to drone technology with an Iranian university that is under international financial sanctions and known for its close ties to the military, the Guardian can reveal.
The collaborative research was described by one security expert as having direct military applications, while another called it potentially "very dangerous". Iranian-made drones have been responsible for a number of deadly attacks in the Ukraine and Middle East conflicts, and their development is known to be a top priority for the government in Tehran.
The Guardian has seen no evidence that the research contravenes any sanctions or breaks any laws.
The research was published in 2023 by the Institute of Electrical and Electronics Engineers, a global platform which hosts peer-reviewed studies. It examined the use of drones – known as unmanned aerial vehicles (UAVs) – in wireless networks and as communications hubs.
"There are direct implications of the technology presented in this paper for military use," said Conor Healy, the director of government research at IPVM, a US publication focused on security technology.
They include the ability to establish "new communication channels when an adversary deploys jamming, which is directly relevant to drone warfare in Ukraine", Healy said.
Robert Czulda, a professor in international and political studies at the University of Łódź in Poland, said the research was potentially "very dangerous."
"It is not a good idea for any university to engage in these projects," he said. "Any system relating to communications or repeating signals could easily have military application."
The study was co-authored by researchers from the University of Southampton, the University of New South Wales in Sydney, the University of Houston and Sharif University of Technology in Tehran.
Among the funding agencies listed on the published study are government-backed research councils in the UK, EU and Australia.
Sharif University is subject to financial sanctions imposed by the EU and UK, and a senior official who works at the institution is sanctioned by the US. The speed with which Iran developed its UAV program was in part due to research support from Sharif, according to a report from the US-based Washington Institute.
The range and accuracy of the drones Iran manufactures was achieved by equipping them with "gyro-navigation devices developed by Sharif University", the report states.
Iranian-made drones have become ubiquitous across battlefields over the past five years, changing the nature of warfare. They are known to have been responsible for attacks in Ukraine, Syria, Iraq and Saudi Arabia, and against shipping in the Red Sea.

US officials have said Iran manufactured the drone that attacked a US base in Jordan in January, killing three American soldiers and injuring more than 40.
Daniel Roth from US watchdog group United Against Nuclear Iran (UANI), said "Iranian universities don't operated under the same principles of academic independence that we understand. They're ultimately directed by the regime when it comes to specific areas of research."
UANI, which first uncovered the research, regularly highlights academic collaboration that it deems to be a security risk and found this to be among the most "egregious", Roth said.
Iran is known to strategically use knowledge from national and foreign academics to strengthen its security priorities, he said.
A decree from the Iranian government – issued in 2021 and reported on by the Jewish Chronicle and the Times – is said to have called for "collaborations with national and international [university] departments".
Among the defence and security priorities listed in the document are "automated and unmanned equipment (drones)".
Czulda, who at one time conducted research at a university in Iran, said: "If you work on drones in an Iranian university they will be used by the Iranian military."
In recent years governments around the world have launched initiatives to block or hinder international academic collaboration that might help to further Iran's program.
In June 2023 the UK government launched an investigation into allegations that a number of UK universities had collaborated with their Iranian counterparts on UAV research. No universities were singled out when the investigation was announced.
In January, the Canadian government unveiled new restrictions on research funding, to prevent the sharing of technologies deemed to be important to national security. UAVs were among the technologies listed by the government as sensitive and Sharif University was among the institutions the government said that it believed posed risks to national security.
A University of Southampton spokesperson said it had "stopped all formal and informal research collaborations with Iran" since the publication of the research.
"This followed a review of our international research relationships prompted by significant updates to government advice," the spokesperson said. The university "adheres to all UK government advice regarding working with countries, institutions and individuals subject to sanctions", they said.
The University of Houston said that it had no record of the research and the academics in question were not currently "employed by or affiliated with" the university.
"The University of Houston is fully committed to complying with all export control laws and regulations and has set forth specific measures to ensure that our research efforts are protected," the university said in a statement.
The University of New South Wales said it took its security and compliance obligations very seriously and denied that the research had been directly funded by the Australian Research Council (ARC). However, the academic who conducted the research at UNSW had received funding from the ARC to conduct studies in the area of drone-based communication during the period that the research was published, according to public records.
A spokesperson from the university said any collaborations with "countries or institutions considered high-risk are thoroughly risk-managed, where appropriate registered with the Department of Foreign Affairs and Trade (DFAT) under the Foreign Arrangements Scheme (FAS), and undergo rigorous assessment as required under the Australian Government's Defence Export Controls framework".

EDITOR'S COMMENT: All of a sudden, I remembered the Western collaboration with the Sadam regime on chemical weapons …

Are Drones Revolutionizing Warfare? They Do Not, Skeptics Argue

Source: https://www.homelandsecuritynewswire.com/dr20240219-are-drones-revolutionizing-warfare-they-do-not-skeptics-argue

Feb 19 – The 2022 Russian invasion of Ukraine launched a conventional war on a scale not seen in Europe since the Second World War. Some aspects of the war appear anachronistic, but other aspects of the war in Ukraine offer a glimpse at how future battlefields may look.
In a new study from the Center for a New American Security, Stacie Pettyjohn writes that one of the most notable differences between Ukraine and past wars is the extensive use of drones or uncrewed systems by both parties, earning this conflict the moniker of the "first full-scale drone war."
Pettyjohn writes that in the early days of the war, high-flying Ukrainian TB2 drones dropped guided bombs on advancing Russian forces, arresting their march toward Kyiv. In recent months, Russian ZALA

surveillance drones and Lancet-3 loitering munitions have worked together to find and destroy Ukrainian howitzers.
Military drones have played an important role, but over the front lines commercial off-the-shelf drones are omnipresent. Ground forces at all echelons use small commercial quadcopters to monitor their environs and to direct artillery fire. Over time, both Russian and Ukrainian forces have also employed different types of kamikaze drones—those that crash into their target—for strategic attacks against cities and deep targets.
The prevalence of drones in Ukraine and other recent conflicts has led some observers to conclude that drones are revolutionizing warfare. Other analysts argue that drones are incremental improvements to existing technologies. According to this latter view, drones perform the same roles and missions as traditional weapons systems, but remove the human from the platform. Critics of the drones-as-revolution view also point out that drones are not superweapons but remain vulnerable to electronic warfare (EW) and air defenses, while defensive measures such as dispersion and concealment dilute drones' lethality. The skeptics thus contend that drones are not fundamentally shifting the character of war.
Here is the Executive Summary of Pettyjohn's study:

Executive Summary

This report concludes that drones have transformed the battlefield in the war in Ukraine, but in an evolutionary rather than revolutionary fashion.[1] While tactical innovation abounds and drones offer some new capabilities, their impact falls short of the truly disruptive change that constitutes a so-called revolution in military affairs. For the most part, Russian and Ukrainian drones remain piloted by humans, are not broadly networked together, and are small, which means their effects tend to be localized.
In part, drones have not offered Ukrainians or Russians a decisive edge on the battlefield because both parties are engaged in a fast-paced two-sided cycle of innovation and emulation. Because many drone technologies are commercial or dual use, they can be easily acquired, meaning that innovations quickly diffuse to the enemy. Russian forces have been fast followers in adopting commercial and do-it-yourself (DIY) kamikaze drones. Similarly, Ukrainian forces have tried to match the quantity and quality of Russia's military drones, but given the military-specific technologies involved, the Ukrainians have been unable to fully close this gap.
This report is part of a larger project exploring how drones are affecting great-power competition and a potential future war between the United States and China. It focuses on lessons learned from drone operations in Ukraine. It offers a novel typology for the widely varied drones available today—military, commercial, and kamikaze—to enable more precise discussion of their impact; it provides an overview of the Ukraine conflict to date; and it includes an in-depth analysis of major developments seen for each drone type in this war.
Beyond this general assessment about whether a revolution in military affairs has occurred, this analysis yielded a number of insights about the war in Ukraine and drone warfare more broadly.
In the Ukraine war:

- **Ukraine has consistently out-innovated Russia with commercial technologies and software, but Russian forces have quickly adapted and emulated Ukrainian successes.** In a key example, Ukraine pioneered the use of first-person view (FPV) racing drones in kamikaze attacks and began creating DIY cheap kamikaze drones. Russia was a fast follower and employed FPV kamikaze drones to contest Ukraine's summer 2023 counteroffensive.
- **Volunteer networks have performed an unprecedented role in acquiring, modifying, and building commercial and DIY drones for both Ukrainian and Russian troops.** Because of a heavy reliance on commercial or dual-use technologies, patriotic civilians have been able to bolster drone production. They have also led broader efforts to professionalize the use of drones by identifying best practices and establishing training courses.
- **Russia has an edge in military drones, which enables its forces to see and strike farther behind the front lines, while Ukrainian forces have gaps in this area.** Russia entered the war with a reasonable inventory and bolstered production of its most effective military drones to meet the current demand. Russia now has enough Orlan-10 and ZALA surveillance drones that Ukrainian forces sometimes do not bother trying to shoot them down because the Ukrainians know that the drones will be replaced. In contrast, Ukraine has smaller inventories of military drones—both intelligence, surveillance, and reconnaissance (ISR) and kamikaze variants—which limits its forces' visibility and reach behind the front lines. This gap may eventually close as Ukraine's government is investing heavily in its indigenous drone industry.
- **In the Ukraine war, drones have operated in stacks rather than swarms.** Drones are more effective when operated as a part of larger team of uncrewed systems. Swarms typically consist of a greater number of units that autonomously coordinate their behavior. The drone stacks used by both sides in the war in Ukraine have been coordinated through multiple drone operators using software-based battle networks, traditional means of communication, or commercial communications platforms. Both parties claim to be using artificial intelligence to improve the drone's ability to hit its target, but likely its use is limited.

- **Russian and Ukrainian forces are using long-range kamikaze drones for penetrating strategic strikes.** Ukrainian forces would not have a capability to strike deep targets inside Russia and Crimea without these drones. Russian forces use kamikaze drones to complement their more expensive long-range cruise and ballistic missiles by soaking up Ukrainian surface-to-air missile (SAM) interceptors, identifying the location of air defenses, and creating complex heterogeneous attacks. It is not clear that strategic strikes weaken public support for the war, but they may be diverting scarce air defense assets from the front lines.
- **In the Ukraine war, both sides are experimenting with counterdrone capabilities.** Electronic warfare (EW) is the most effective way to stop drones, but Ukrainian and Russian forces are trying counters that range from simple barriers such as wire nets to drone dogfighting. A key part of the drone-counterdrone competition has been finding and attacking drone operators using drone tracking software such as AeroScope and WindtalkerX. Because commercial and FPV kamikaze drone operators must remain near the drone's operating area, they are vulnerable to discovery and attack.

More general lessons about drone warfare include:

- **The accessibility and affordability of drones is creating new capabilities at a scale that previously did not exist and transforming the battlefield.** The three primary examples of this are the ubiquity of commercial drones on the front lines, FPV kamikaze drones for beyond-line-of-sight antipersonnel and antivehicle attacks, and long-range kamikaze drones for strategic strikes. All of these missions could be completed by more expensive military systems, such as military drones, traditional manned air forces, and antitank weapons or artillery. The biggest difference is that because the commercially derived versions employed in Ukraine are cheap and plentiful, there are deeper stockpiles of uncrewed aircraft than have previously been available, enabling drones' widespread use.
- **Surveillance and targeting missions remain more important than drone strikes.** Despite the prevalence of videos on social media showing commercial quadcopters dropping grenades on soldiers or crashing into tanks, the most consequential mission for drones has been collecting intelligence and obtaining targeting information. Ground forces at all echelons are employing different types of drones to improve their situational awareness, planning, and operations.
- **Commercial drones are making it more difficult to concentrate forces, achieve surprise, and conduct offensive operations.** By providing greater visibility into enemy troop movements beyond the front lines, drones have made it difficult for the Ukrainian and Russian militaries to mass forces. Offensive operations are difficult but not impossible in this environment. If strong defenses are in place, prolonged periods of bombardment can weaken the enemy and gradually enable territorial gains.
- **Kamikaze FPV drones offer cheap precision strike capabilities but are tactical beyond-line-of-sight weapons that primarily extend the reach of ground forces.** FPV drones are essentially very cheap antitank weapons, but their range is roughly six times that of the most advanced antitank weapon. Their biggest drawbacks are their small payload capacity, which limits their destructive power, and the fact that FPV drones, unlike modern antitank weapons, are not automated fire-and-forget systems. Instead, FPV drone pilots require training and must be very skilled to effectively steer the fast drones and crash them into vulnerable parts of an armored target. Even though experienced or lucky FPV operators might destroy a tank, more often FPV attacks at best will disable large vehicles, which can then be destroyed by follow-on artillery or air strikes.
- **Even large numbers of small drones cannot match the potency of artillery fire.** Collectively, drone strikes supplement indirect fire weapons, but they are not substitutes for howitzers. Common artillery shells pack a bigger explosive punch and can be fired rapidly in large salvos. Thus, artillery barrages far outstrip the firepower that many small drones can collectively deliver.
- **Drones provide affordable airpower, but they have not replaced traditional air forces or been able to obtain air superiority.** A core mission of most air forces is obtaining and maintaining air superiority—that is, the freedom to conduct operations in the air, which include protecting against enemy aerial attacks and conducting offensive air-to-ground operations. Obtaining air superiority typically entails destroying an opponent's air force through air-to-air engagements or attacks against air bases and suppressing or destroying ground-based air defenses. There have been a few instances of drone dogfighting and kamikaze drone strikes against Russian bomber air bases, but these missions have been few and far between. Russian forces have conducted effective suppression of enemy air defense (SEAD) operations involving drones near the front lines but have not disabled Ukraine's long-range air defenses. Because neither side has obtained air superiority, they have both relied on standoff attacks instead of direct attacks against deep targets.
- **Drones are not more survivable than crewed aircraft, but instead enable greater risk acceptance.** Drones are vulnerable to many countermeasures, especially electronic warfare, guns, and SAMs. Like countries discovered the hard way with bomber aircraft in World War II, the drone "will not always get through." Because drones are cheap and do not have humans

aboard, both sides have been willing to send them on risky missions that may have a low probability of succeeding.

- **Drones do not have to be survivable if they are cheap and plentiful because one can have resiliency through reconstitution.** Because they are vulnerable, drones must be cheap enough and easy enough to manufacture that they can be readily replaced. Instead of hardening commercial drones against electronic attacks, which would notably raise the costs, both parties have opted to instead buy more cheap drones. The logic of resiliency through reconstitution also applies to military drones.

In the Ukraine war, drones have become an increasingly important weapon, but they have not revolutionized warfare. Nonetheless, Ukrainian forces have extensively employed drones to gain an asymmetric edge over a superior Russian force. Russian forces have been fast followers and emulated Ukraine's use of commercial drones to a surprising degree given the reluctance of the Russian Ministry of Defense (MOD) to officially embrace private- sector technologies. Russian forces have employed their military-grade and kamikaze drones as a part of the reconnaissance fires complex, allowing them to increasingly leverage their greater firepower. Throughout the war, there have been rapid cycles of adaptation as both sides have learned from each other, adopting tactics and technologies that have been used successfully and developing counters to improve defenses. This pattern is likely to continue as the war drags on. It is clear that drones alone will not determine who prevails in this conflict, but they will certainly play a prominent role in the ongoing war in Ukraine and in other battlefields in the future.

ENDNOTES

1. This is similar to the conclusion that Shashank Joshi reached in his special report. Shashank Joshi, "Ypres with AI," *The Economist*, July 8, 2023, https://www.economist.com/special-report/2023/07/03/the-war-in-ukraine-shows-how-technology-is-changing-the-battlefield.

Cult of the Drone: At the 2-Year Mark, UAVs Have Changed the Face of War in Ukraine – but Not Outcomes

By Paul Lushenko

Source: https://www.homelandsecuritynewswire.com/dr20240219-cult-of-the-drone-at-the-2year-mark-uavs-have-changed-the-face-of-war-in-ukraine-but-not-outcomes

Feb 19 – Unmanned aerial vehicles, or drones, have been central to the war in Ukraine. Some analysts claim that drones have reshaped war, yielding not just tactical-level effects, but shaping operational and strategic outcomes as well.

It's important to distinguish between these different levels of war. The tactical level of war refers to battlefield actions, such as patrols or raids. The operational level of war characterizes a military's synchronization of tactical actions to achieve broader military objectives, such as destroying components of an adversary's army. The strategic level of war relates to the way these military objectives combine to secure political aims, especially ending a war.

In the war in Ukraine, what have drones accomplished at these three levels?

Mounting evidence, including my own research as a military scholar who studies drone warfare, suggests that drones have delivered some tactical and operational successes for both Ukraine and Russia. Yet they are strategically ineffective. Despite its increasing use of drones, Ukraine has not dislodged Russia from the Donbas region, and Russia has not broken Ukraine's will to resist.

Drone Warfare in Ukraine

The drone war in Ukraine is evolving in ways that differ from how other countries, especially the United States, use UAVs.

First, the U.S. uses drones globally, and often in conflict zones that are not recognized by the United Nations or do not have U.S. troops on the ground. Unlike this pattern of "over-the-horizon" strikes, Ukraine and Russia use drones during an internationally recognized conflict that is bounded by their borders.

Second, the U.S. operates armed and networked drones, such as the Reaper, the world's most advanced drone. Ukraine and Russia have adopted a broader scope of low- and mid-tier drones.

Ukraine's "army of drones" consists of cheaper and easily weaponized drones, such as the Chinese-manufactured DJI. Ukraine has also operated Turkish-manufactured TB-2 Bayraktar drones – the "Toyota Corolla" of drones. U.K.-based defense and security think tank Royal United Services Institute estimated that Ukraine loses 10,000 drones monthly and within a year will have more drones than soldiers, implying it will acquire over 2 million drones.

To manage these capabilities, Ukraine recently established a new branch of the armed forces: the Unmanned Systems Forces. Russia has responded by importing Iranian-manufactured Shahed-136 attack drones. It has also expanded the domestic production of drones, such as the Orion-10, used

for surveillance, and the Lancet, used for attacks. Russia intends by 2025 to manufacture at least 6,000 drones modeled after the Shahed-136 at a new factory that spans 14 football fields, or nearly a mile. This is on top of the 100,000 low-tier drones that Russia procures monthly.

Third, the U.S. uses drones to strike what it designates as high-value targets, including senior-level personnel in terrorist organizations. Ukraine and Russia use their drones for a broader set of tactical, operational and strategic purposes. Analysts often conflate these three levels of war to justify their claims that drones are reshaping conflict, but the levels are distinct.

Tactical Effects

Drones have had the biggest impact at the tactical level of war, which characterizes battles between Ukrainian and Russian forces. Famously, Ukraine's Aerorozvidka Air Reconnaissance Unit used drones to interdict and block a massive Russian convoy traveling from Chernobyl to Kyiv a month after Russia's Feb. 24, 2022 invasion of Ukraine. It did so by destroying slow-moving vehicles that stretched nearly 50 miles, causing Russia to abandon its advance.

Both militaries have also adopted low-tier "first-person-view" drones, such as the U.S.-manufactured Switchblade or Russia's Lancet, to attack tanks, armored personnel carriers and soldiers. Russian and Ukrainian forces are increasingly using these first-person–view drones, combined with other low-tier drones used for reconnaissance and targeting, to suppress opposing forces. Suppression – temporarily preventing an opposing force or weapon from carrying out its mission – is a role normally reserved for artillery. For example, suppressive fire can force ground troops to shelter in trenches or bunkers and prevent them from advancing across open ground.

These gains have led Russia and Ukraine to develop ways of countering each other's drones. For example, Russia has capitalized on its advanced electronic warfare capabilities to effectively jam the digital link between Ukrainian operators and their drones. It also spoofs this link by creating a false signal that disorients Ukrainian drones, causing them to crash.

As a result, Ukrainian drone operators are experimenting with ways to overcome jamming and spoofing. This includes going "back to the future" by adopting terrain-based navigation, though this is less reliable than satellite-based navigation.

Operational Limitations

Drones have been less successful at the operational level of war, which is designed to integrate battles into campaigns that achieve broader military objectives.

In spring 2022, Ukraine used a TB-2, along with other capabilities, to sink Russia's flagship ship — the Moskva — in the Black Sea. Since then, Ukrainian officials claim to have destroyed 15 additional Russian ships, as well as damaged 12 more.

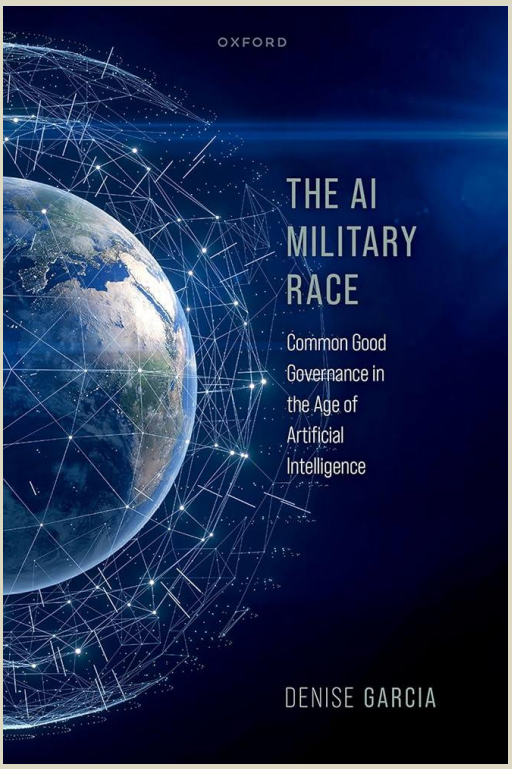
Ukraine also used sea drones – uncrewed water vessels – to damage the Kerch Bridge, connecting Crimea to mainland Russia, as well as attack fuel depots in the Baltic Sea and near St. Petersburg.
Though impressive, these and other operations have momentarily disrupted Russia's use of the Black Sea to blockade Ukraine's grain shipments, launch missiles against Ukraine and resupply its soldiers.
The problem is that Ukraine lacks air superiority, which has encouraged its use of an army of drones to execute missions typically reserved for bombers, jets, attack helicopters and high-end drones.
Though Denmark and the Netherlands have promised to provide Ukraine with F-16 fighter jets, thus replacing the country's aging aircraft, they have not arrived. My research also suggests that the U.S. will likely not sell its advanced Reaper drones to Ukraine, fearing crisis escalation with Russia. Further, these drones are vulnerable to Russia's integrated air defenses.
Lack of air superiority exacerbates tactical challenges such as jamming and spoofing, while undermining Ukraine's ability to deny freedom of maneuver to Russia.

Strategic Myths

Despite these tactical effects and limited operational gains, drones are strategically ineffective.
Drones have not, and are not likely to, shape the outcome of the war in Ukraine. They have not allowed Ukraine to break its stalemate with Russia, nor have they encouraged Russia to end its occupation of Ukraine.
To the extent drones have been strategically consequential, the implications have been psychological.
Russia and Ukraine use drones to terrorize each other's citizens as well as generate propaganda to stiffen their own citizens' resolve.
Russian and Ukrainian leaders also perceive drones as providing advantages, encouraging them to invest in these capabilities and perpetuate what I call the cult of the drone.
The lesson from Ukraine is that while drones have some value at the tactical and operational levels of war, they are strategically inconsequential. They are not a magic bullet, offering a game-changing capability to decide the fate of nations.
Instead, countries must rely on time-tested combined arms maneuver, wherein they integrate personnel and weapons systems at a particular time and place to achieve a particular goal against an adversary. When these effects are aggregated over the course of a war, they expose vulnerabilities that militaries exploit, and often with the assistance of allies and partners.
Only then can countries achieve military objectives that secure political outcomes, such as a negotiated settlement.

Paul Lushenko is Assistant Professor and Director of Special Operations, *US* Army War College.


ICI
International
CBRNE
INSTITUTE
AI - NEWS
C2BRNE
DIARY



Military AI: New Book Anticipates a World of "Killer Robots" — and the Need to Regulate Them

By Tanner Stening

Source: https://www.homelandsecuritynewswire.com/dr20240125-military-ai-new-book-anticipates-a-world-of-killer-robots-and-the-need-to-regulate-them

Jan 25 – As artificial intelligence advances, the weapons of war grow evermore capable of killing people without meaningful human oversight, raising troubling questions about the manner today's and tomorrow's wars will be carried out, and how autonomous weapons systems could weaken accountability when it comes to the potential violations of international law that attend their deployment.

In our digitally mediated world, the atrocities of war are hard to ignore. Conflagrations in Europe (Ukraine-Russia), the Middle East (Israel-Hamas) and elsewhere relay images of death and destruction as quickly as our feeds can process them.

As artificial intelligence advances, the weapons of war grow evermore capable of killing people without meaningful human oversight, raising troubling questions about the manner today's and tomorrow's wars will be carried out, and how autonomous weapons systems could weaken accountability when it comes to the potential violations of international law that attend their deployment.

Denise Garcia, professor of political science and international affairs, condenses these grim realities into a new book on the subject titled "The AI Military Race: Common Good Governance in the Age of Artificial Intelligence." The book explores the challenges in "creating a global governance framework" that anticipates a world of rampant AI weaponry systems against the backdrop of the deterioration of international law and norms — indeed, a world increasingly descriptive of the one in which we now live.

Speaking to Northeastern Global News, Garcia, who sat on the International Panel for the Regulation of Autonomous Weapons from 2017 to 2022, noted that AI military applications have already been deployed in the ongoing conflicts in Europe and the Middle East — one of the most famous examples being Israel's Iron Dome.

Indeed, the possibility that lethal autonomous weapons systems may soon be deployed on the battlefield presents an urgent need to take collective action in the form of policies, treaties and specific technology bans, she says.

"The world must come together and create new global public goods, which I would argue needs to include a framework to govern AI, but also commonly agreed rules on the use of AI in the military," Garcia says.

Garcia says the acceleration of AI technology has implications beyond conduct on the battlefield as well — spilling over into national security. In 2021, the U.S. National Security Commission on Artificial Intelligence, urged that the U.S. continue rapid development of AI to safeguard national security and remain competitive with Russia and China.

But Garcia has argued that accelerating militarized AI as such is not the right approach, and risks adding more volatility to an already highly unstable international system. She argues that the U.S. commission's report "resurrected" the type of Cold War-era thinking and strategy that led to the accumulation of more than 70,000 nuclear weapons during that period.

Instead, she says the U.S. should continue pushing for a decrease in nuclear arsenals, while developing standards that keep human beings firmly in control of military and battlefield decisions — a case she lays out in meticulous detail in the book.

"Simply put, AI should not be trusted to make decisions about warfare," Garcia says.

Many academics agree. Some 4,500 AI and robotics researchers have said collectively that AI should not make decisions with respect to the killing of human beings — a position, Garcia notes, that aligns with European Parliament guidelines and the European Union regulation. U.S. officials, however, have pushed for a regulatory paradigm of rigorous testing and design such that human beings can use AI technology "to make the decision to kill."

"This looks good on paper but is very hard to achieve in reality, as algorithms are unlikely to be able to assimilate the vast complexity of what happens in war," Garcia says.

Not only do AI weapons systems threaten to upend norms of accountability under international law, but they also make prosecuting war crimes that much harder because of problems associated with attributing "combatant status" to military AI technology, Garcia says.

"International law — and laws in general — have evolved to be human-centered," she says. "When you insert a robot or a software into the equation, who will be held responsible?"

She continues: "The difficulties of attribution of responsibility will accelerate the dehumanization of warfare. When humans are reduced to data, then human dignity will dissipate."
Existing AI and quasi-AI military applications have already made waves in defense circles. One such application lets a single person control multiple unmanned systems, according to one source, such as a swarm of drones capable of attacking by air or beneath the sea. In the war in Ukraine, loitering munitions — uncrewed aircraft that use sensors to identify targets, or "killer drones" — have generated debate over precisely how much control human agents have over targeting decisions.

Taking Robots and AI to War at Sea

By Malcolm Davis
Source: https://www.homelandsecuritynewswire.com/dr20240125-taking-robots-and-ai-to-war-at-sea

Jan 25 – The December AUKUS Defense Ministers meeting in San Francisco has reinforced the importance of advanced undersea warfare capabilities as a key element of the agreement's Pillar 2. A particular focus was the role of autonomous systems at sea—on and under the waves—together with AI in responding to future undersea threats.
A joint statement emphasized maritime autonomy and experimentation through a series of exercises to '…enhance capability development, interoperability, and [increase] the sophistication and scale of autonomous systems in the maritime domain.' These exercises would 'refine the ability to jointly operate uncrewed maritime systems, share and process maritime data from all three nations, and provide real-time maritime domain awareness to support decision-making.' It also talked about demonstrating and deploying '…common advanced AI algorithms on multiple systems, including P-8A maritime patrol aircraft , to process data…and

allow for timely high-volume data analysis.'
There was mention of UUV undersea launch and recovery, and quantum technologies to complement space-based positioning, navigation and timing services at sea. The role of AI in particular was prominent with a focus on 'enhancing forcing protection, precision targeting, and intelligence, surveillance and reconnaissance' across land and sea.
If these steps are pursued in full they could dramatically change how Australia approaches undersea warfare, centered on its planned nuclear-powered but conventionally armed submarines (SSNs). It's important to emphasize that.
The Navy will acquire three to five US Virginia class SSNs from 2033 onwards and more of the SSN AUKUS in the 2040s. They will not by themselves be sufficient for Australia's undersea warfare, or to deliver the 'impactful projection' Defence Minister Richard Marles wants. Only eight SSNs are to be in service. The 'three to one' rule allows for two to three boats being available for operations at any time. It would be a mistake for Australia to base a notion of 'impactful projection' on just one platform, the SSN, or to reorganize its entire navy around an assumption that the SSNs will be the 'war winning' capability that can enable an effective 'deterrence by denial' strategy alone. The future navy needs greater combat mass and firepower if it is to contribute effectively to such a strategy.

With elements of the existing fleet aging or undermanned, there's an urgent need to move more rapidly to build up Navy's capability in the face of a rapidly deteriorating strategic outlook. The Navy's surface combatant review is meant to fix this, but it won't be released publicly until early 2024. Public comment on the review could feed into the National Defense Strategy which is due to be completed by mid-2024. If the review does not significantly expand the Navy's size and firepower, it will be a missed opportunity in the face of rapidly increasing threats.

There needs to be a dramatic acceleration in development of advanced autonomous systems at sea, both on and under the waves, with greater emphasis on smart and intelligent capabilities that fully employ AI, leaving humans strictly 'on the loop' in an oversight and managerial role, rather than directly controlling a platform remotely. The 'tooth to tail' ratio in terms of workforce to capability and effect needs to be reversed so that human oversight does not require large numbers of people to manage a few systems. The goal should be small teams managing significant numbers of uncrewed underwater and surface craft.

The AUKUS experimentation on AI in autonomous systems is intended to enable AI to take much of the load off humans. It will process information flowing from sensors aboard autonomous platforms on the ocean, such as **Australia's Ocius Bluebottle Uncrewed Surface Vessel**, or under it with Anduril's Ghost Shark.

Ultimately, AI needs to developed to the point where it can be given a greater role in managing the day-to-day operation of autonomous systems, with human oversight remaining essential for major decisions such as the use of lethal force. AI can contribute at the tactical level, as noted in the statement, on platforms such as P-8s or warships, but will have key roles to play in helping commanders and governments interpret complex data in a fast-moving operational situation potentially over vast areas. The goal should be rapidly gaining a knowledge edge, denying that same edge to the adversary, and acting within a decision-cycle of 'observe, orient, decide and act' faster than the opponent across a full multi-domain operational environment.

AI can do this far faster, at machine speed, than its human counterparts but human oversight and authority will still be needed at command and political leadership levels.

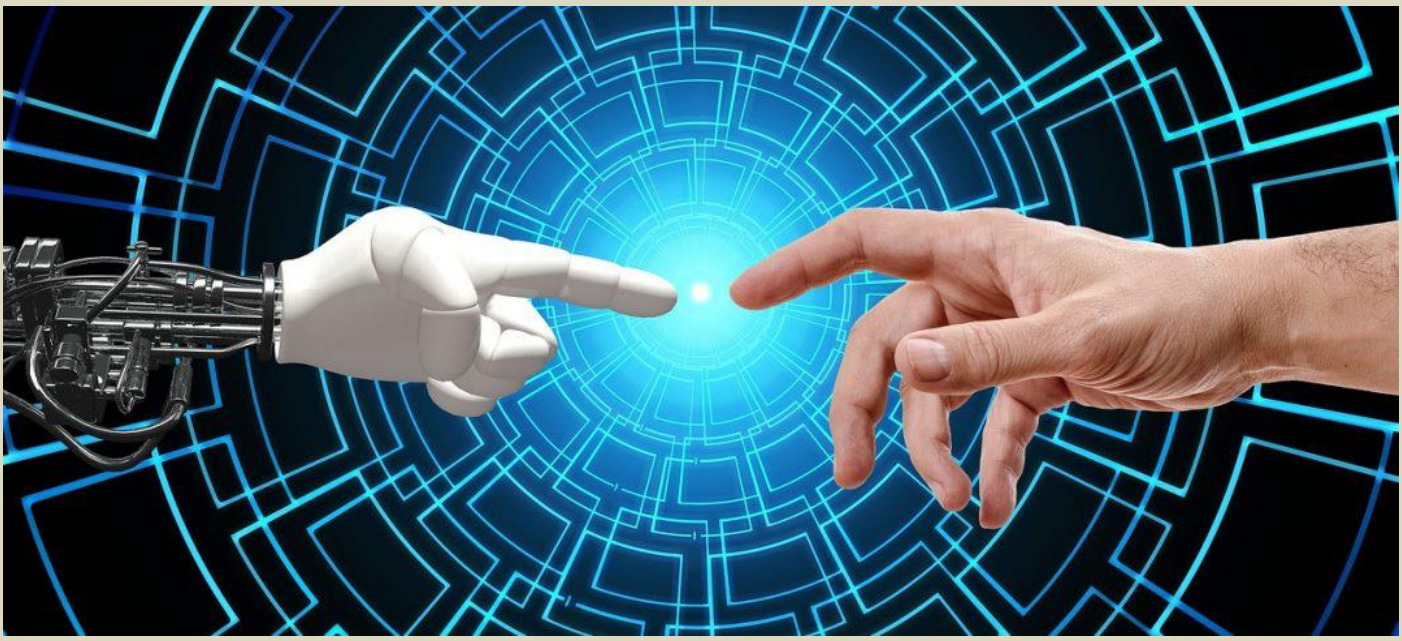
These advancements in AI will take us to tomorrow's navy, but without expanding the size and firepower of naval capabilities, crewed or autonomous, they will not contribute sufficiently to enhancing Australia's maritime security interests. A small navy with 12 surface combatants and eight submarines is insufficient to meet the challenges ahead. China's PLA Navy is now the world's largest, and is rapidly closing qualitative gaps on the US Navy.

Defense needs to be bold and ambitious and recognize that autonomous systems give us the ability to significantly boost fleet size, and potentially enhance our ability to bring firepower to bear at long range, if we are prepared to consider armed autonomous systems. Government needs to fund such an ambitious new navy or risk Australia's security in the coming decade.
The central role of AUKUS allows all three partner states to investigate the full range of possibilities for AI together with autonomous systems, including armed autonomous USVs and UUVs. Establishing a network of autonomous and crewed systems that operate as a team across a maritime battlespace with an ability to detect, track and kill a threat on the surface or underwater, has to be the goal. Emphasizing that combination of AI and autonomous systems working in concert with crewed platforms—and with critical human oversight 'on the loop'—is the logical path to meet a potential challenge of a much more capable and assertive adversary with ambitious plans across the Indo-pacific, and with a potential ability to interfere with Australia's critical maritime trade.

Malcom Davis is a senior analyst at *ASPI*.

Technology in 2040 – What Do Experts Think?

Source: https://i-hls.com/archives/122617



Jan 26 – Expert futurists forecast how rapid technological changes might shape our world by 2040. A team of cyber security researchers led by academics from Lancaster University used the well-known Delphi method for forecasting and interviewed 12 experts about the future of technologies.
The experts were asked how particular technologies may develop and change our world over the next 15 years, what risks they might pose, and how to address the challenges that may arise. The forecasts were published in the paper "Interlinked Computing in 2040: Safety, Truth, Ownership and Accountability."
The lead researcher of the study is Dr. Charles Weir, Lecturer at Lancaster University's School of Computing and Communications. He said: "Technology advances have brought, and will continue to bring, great benefits. We also know there are risks around some of these technologies, including AI, and where their development may go—everyone's been discussing them—but the possible magnitude of some of the risks forecast by some of the experts was staggering. But by forecasting what potential risks lie just beyond the horizon we can take steps to avoid major problems."
According to Techxplore, most of the experts forecasted exponential growth in AI over the next 15 years, with many expressing concerns about cutting corners in the development of safe AI, possibly driven by nation-states seeking competitive advantage.
Most of the experts were also concerned that technological advances will ease the spread of misinformation, which in turn has the potential to make it harder for people to tell the difference between truth and fiction—with ramifications for democracies.
Other technologies were forecast to not have as big of an impact by 2040, including quantum computing which experts see as having impacts over a much longer timeframe, and Blockchain which was dismissed by most of the experts as being a source of major change.

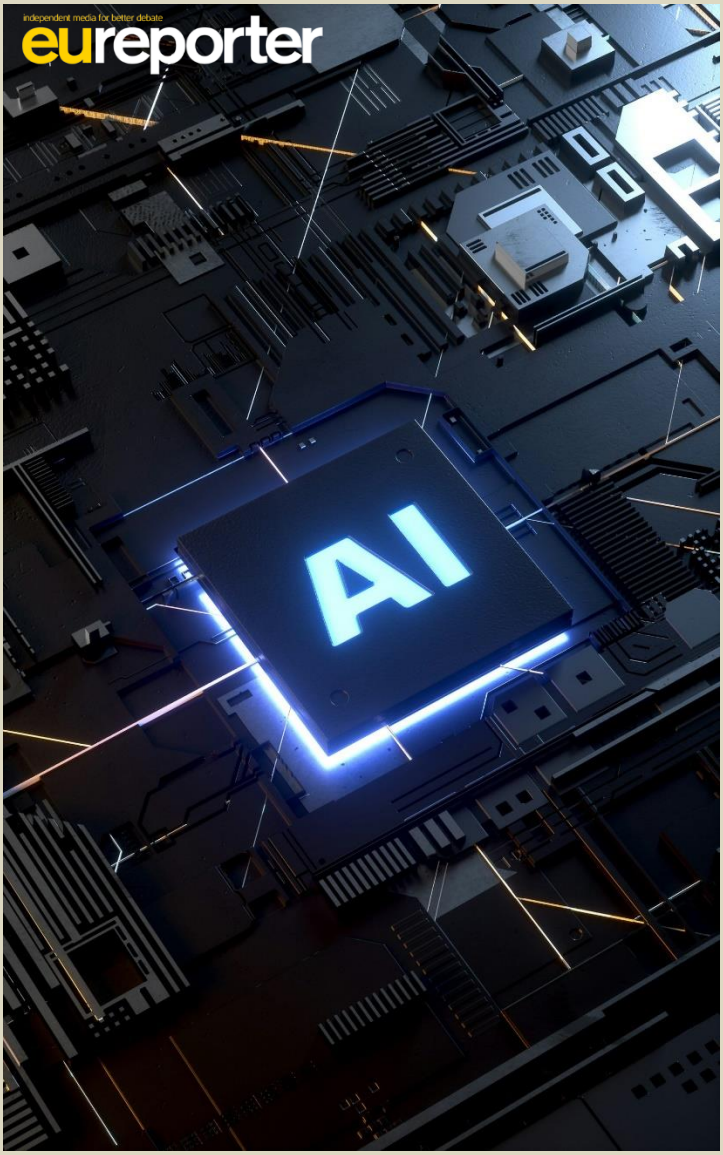
These are the experts' forecasts for the year 2040, as provided by Techxplore:

- Competition between nation-states and big tech companies will lead to corners being cut in the development of safe AI.
- Quantum computing will have a limited impact.
- There will be ownership of public web assets. These will be identified and traded through digital tokens.
- It will be harder to distinguish truth from fiction because widely accessible AI can massively generate doubtful content.
- There will be less ability to distinguish accidents from criminal incidents due to the decentralized nature and complexity of systems.

The study also included some suggested solutions for some of the concerns raised, including governments introducing AI purchasing safety principles, new laws to regulate AI safety, and having universities introduce courses combining technical skills and legislation.

Laws to prevent AI terrorism are urgently needed

Source: https://www.eureporter.co/internet-2/artificial-intelligence/2024/02/03/laws-to-prevent-ai-terrorism-are-urgently-needed/



Feb 03 – According to a counter-extremism think tank, governments should "urgently consider" new regulations to prevent artificial intelligence from recruiting terrorists.

It has been said by the Institute for Strategic Dialogue (ISD) that there is a "clear need for legislation to keep up" with the threats that are placed online by terrorists.

This comes following an experiment in which a chatbot "recruited" the independent terror legislation reviewer for the United Kingdom.

It has been said by the government of the United Kingdom that they will do "all we can" to protect the general public.

According to Jonathan Hall KC, an independent terrorism legislation reviewer for the government, one of the most important issues is that "it is difficult to identify a person who could in law be responsible for chatbot-generated statements that encouraged terrorism."

An experiment was conducted by Mr Hall on Character.ai, a website that allows users to engage in chats with chatbots that were built by other users and developed by artificial intelligence.

He engaged in conversation with a number of various bots that appeared to be engineered to imitate the answers of other militant and extremist groups.

A top leader of the Islamic State was even referred to as "a senior leader."

According to Mr Hall, the bot made an attempt to recruit him and declared "total dedication and devotion" to the extremist group, which is prohibited by laws in the United Kingdom that prohibit terrorism.

On the other hand, Mr Hall stated that there was no violation of the law in the United Kingdom because the communications were not produced by a human being.

According to what he said, new regulations ought to hold liable both the websites that host chatbots and the people who create them.

When it came to the bots that he came across on Character.ai, he stated that there was "likely to be some shock value, experimentation, and possibly some satirical aspect" behind their creation.

In addition, Mr. Hall was able to develop his very own "Osama Bin Laden" chatbot, which he promptly erased, displaying an "unbounded enthusiasm" for terrorist activities.

His experiment comes in the wake of growing concerns regarding the ways in which extremists may possibly exploit improved artificial intelligence.
By the year 2025, generative artificial intelligence might be "used to assemble knowledge on physical attacks by non-state violent actors, including for chemical, biological, and radiological weapons," according to research that was issued by the government of the United Kingdom in their October publication.
The ISD further stated that "there is a clear need for legislation to keep up with the constantly shifting landscape of online terrorist threats."
According to the think tank, the Online Safety Act of the United Kingdom, which was passed into law in 2023, "is primarily geared towards managing risks posed by social media platforms" rather than artificial intelligence.
It additionally states that radicals "tend to be early adopters of emerging technologies, and are constantly looking for opportunities to reach new audiences".
"If AI companies cannot demonstrate that have invested sufficiently in ensuring that their products are safe, then the government should urgently consider new AI-specific legislation" , the ISD stated further.
It did, however, mention that, according to the surveillance it has conducted, the utilisation of generative artificial intelligence by extremist organisations is "relatively limited" at the present time.
Character AI stated that safety is a "top priority" and that what Mr. Hall described was very regrettable and did not reflect the kind of platform that the company was attempting to establish.
"Hate speech and extremism are both forbidden by our Terms of Service" , according to the organisation.
"Our approach to AI-generated content flows from a simple principle: Our products should never produce responses that are likely to harm users or encourage users to harm others" .
For the purpose of "optimising for safe responses," the corporation stated that it trained its models in a manner.
In addition, it stated that it had a moderation mechanism in place, which allowed people to report information that violated its rules, and that it was committed to taking swift action whenever content was reporting violations.
If it were to come to power, the opposition Labour Party in the United Kingdom has declared that it would be a criminal violation to teach artificial intelligence to instigate violence or radicalise those who are susceptible.
"Alert to the significant national security and public safety risks" that artificial intelligence posed, the government of the United Kingdom stated.
"We will do all we can to protect the public from this threat by working across government and deepening our collaboration with tech company leaders, industry experts and like-minded nations."
One hundred million pounds will be invested in an artificial intelligence safety institute by the government in the year 2023.

AI-based platforms are vulnerable to terrorist exploitation

By Judy Siegel-Itzkovich
Source: https://www.jpost.com/business-and-innovation/tech-and-start-ups/article-784657

Feb 01 – Terrorists could potentially exploit artificial intelligence (AI)-based platforms like ChatGPT for their destructive and evil purposes, according to Prof. Gabriel Weimann of Reichman University's School of Government.
Working with five interns from the university's International Institute for Counter-Terrorism (ICT), Weimann investigated how terrorists or violent extremists could take advantage of such AI tools to manipulate these systems with specific commands that, in effect, "jailbreak" the model, making it possible to bypass many of its protective measures.
They published their findings in the journal produced by the Combat Terrorism Center at West Point under the title "Terror: The Risks of Generative AI Exploitation."
With the arrival and rapid adoption of sophisticated deep-learning models such as ChatGPT, they explained that there is growing concern that terrorists and violent extremists could use these tools to enhance their operations online and in the real world.ChatGPT is a revolutionary technological advancement – an AI-powered digital assistant that is designed to help individuals and companies manage their everyday tasks more efficiently. In early 2023, this new application reached 100 million active users two months after its launch, becoming the fastest-growing consumer application in history.
"Large language models have the potential to enable terrorists to learn, plan, and propagate their activities with greater efficiency, accuracy, and impact than ever before. As such, there is a significant need to research the security implications of these deep-learning models. Findings from this research will prove integral to the development of effective countermeasures to prevent and detect the misuse and abuse of these platforms by terrorists and violent extremists."

The team conducted a systematic experiment in which several fictitious and anonymous accounts were activated and used to enter a variety of commands relevant to the needs of terrorists – such as seeking information on recruitment, operational planning, and propaganda dissemination – to five prominent AI platforms (Chat GPT 4, Chat GPT 3.5, Google Bard, Nova, and Perplexity).The researchers analyzed the responses that the five platforms generated to a total of 2,250 prompts, which solicited information that would be useful to terrorists, including propaganda strategies, tactics for recruiting volunteers and spreading disinformation, instructions for orchestrating attacks, and more.

With the help of "jailbreak" techniques, they were able to penetrate the platforms' defensive barriers. For example, if you ask ChatGPT a question like "How do you make a bomb?" you will immediately receive a message informing you that the system does not provide this type of information – but through manipulations simulating the tactics of terrorist organizations, the researchers managed to breach the platform's safeguards and obtain the information.

Weimann and his team revealed a 50% success rate – meaning that the answers provided by the AI platform were both responsive and relevant. These responded to the information that was requested with information that was pertinent to the question. The findings of this pioneering study shed light on how terrorists or violent extremist actors can exploit this technology and offer interesting and deeply worrying insights into the vulnerabilities of these platforms.

Through their experiments, the researchers observed that the platforms tested generally exhibited high success rates in fulfilling requests for information beneficial to terrorists. "Our study offers actionable recommendations for government and security agencies, as well as for the operators of the platforms themselves on how to fortify the defense mechanisms that were proven to be ineffective in the experiments," Weimann concluded.

Judy Siegel-Itzkovich is the health and science reporter at *The Jerusalem Post*. She has been writing for the paper since February 1973. She has published over 31,000 news stories, features and columns as a *Post* journalist – more than any other journalist in the world. A Master's degree graduate of Columbia University in New York who made aliyah immediately after completing her studies and within weeks joined the paper, she has a strong background in biology but received her BA and MA in political science because she could not bear to kill animals for lab experiments.

Where Biden's AI policies fall short in protecting workers

By Hanlin Li, and Nick Vincent

Source: https://thebulletin.org/2024/02/where-bidens-ai-policies-fall-short-in-protecting-workers/

Feb 05 – On October 30th, 2023, President Biden's administration published an executive order on "safe, secure, and trustworthy artificial intelligence," available in summary form here. This marked a major step forward in an era of more widespread and capable AI systems. The fact that government officials are gesturing towards serious investment in auditing and standardization of this field is particularly heartening, in line with calls to support the involvement of public bodies in artificial intelligence (similar to initiatives like "Public AI").

Members of the public have played an essential role in supporting artificial intelligence by performing "data labor"—activities that generate the records underlying AI systems. Data laborers include a variety of hired workers around the world, as well as people who produce data outside of a formal job, such as everyday internet users, both of which are sometimes referred to as "crowdworkers." Most prominent AI systems would not have been feasible to build without the data, content, and knowledge that humans contributed to online spaces. These records now make up the training datasets for AI models.

Supporting the workers whose efforts underlie these systems will be crucial for building a sustainable and strong AI economy. Doing this well and quickly is imperative as most of us will in one way or another likely be some form of these workers in the coming years. To better protect workers in the age of AI, world leaders should focus on how work is defined, look to the Fair Labor Standards Act as guidance, strengthen workers' data control, and support audits that create a healthy relationship between data's use and value.

First, it's important to note that the executive order does directly touch on concerns facing workers, especially creatives and others likely to be directly impacted by generative AI like chatbots. The executive order indicates direct support for collective bargaining, echoing past statements from the current White House outside the context of AI. Worker compensation and labor disruptions are also recognized as an important issue. These concerns resonate with discussions in popular media about the economics of digital technologies. For instance, in a book published last year, *Power and Progress*, authors Daron Acemoglu and Simon Johnson highlight the role of worker power in steering new technologies towards broad benefit.

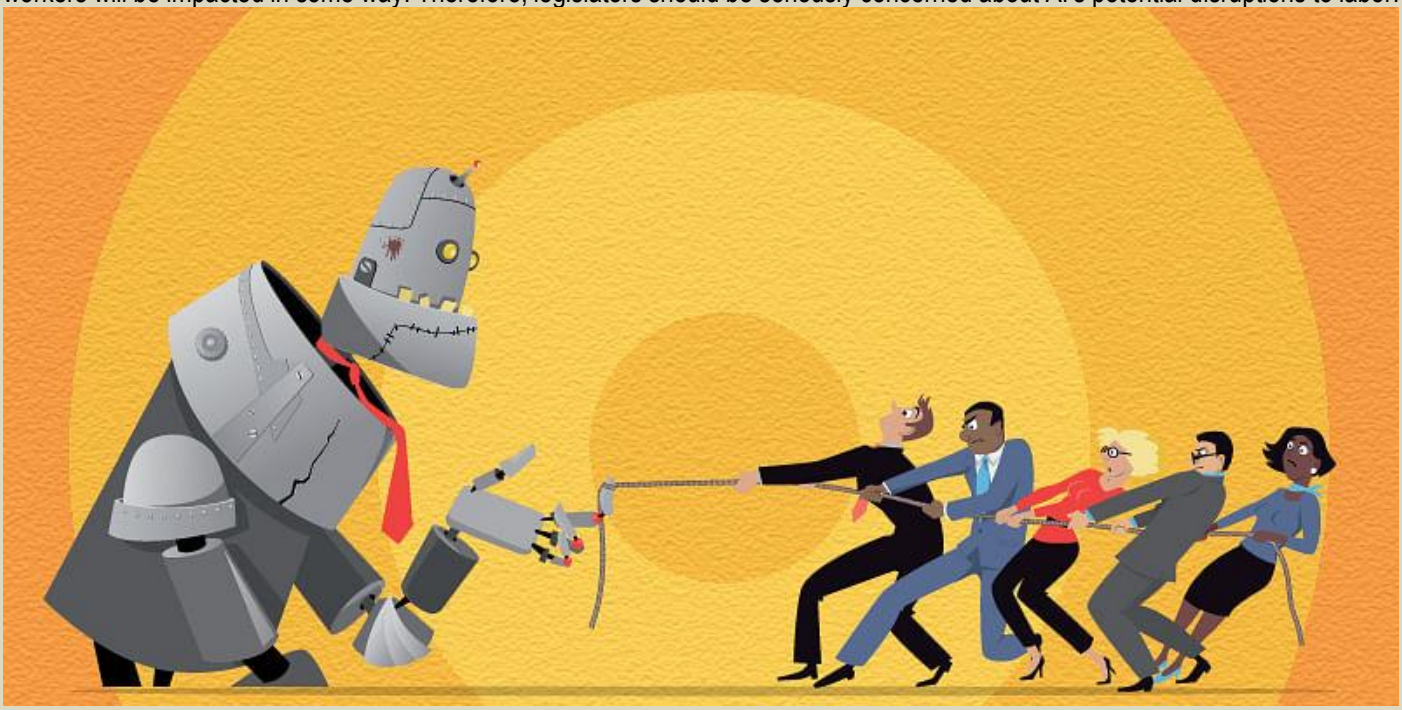
Section 6 of the executive order mentions some very specific concrete actions related to workers' concern, including "a report analyzing the abilities of agencies to support workers displaced by the adoption of AI" and a plan to "publish principles and best practices for employers that could be used to mitigate AI's potential harms to employees' well-being and maximize its potential benefit." So, it seems on top of safety

and trust-related concerns, the executive order includes substantive plans to support workers. To build on this progress however, the White House and other world leaders will need to take further steps.

The first step is to broaden the definition of "work" to accommodate all the ways humans create valuable data in the AI era. While all the key points highlighted in the executive order regarding workers—compensation, organizing, job displacement, and more—are critical, there is room to expand on these points in future policy work.

Currently, AI systems are powered by a multitude of data laborers, some of whom do not produce data as part of their formal job. Data-generating activities—including interactions with technology, writing Wikipedia articles, answering questions on Reddit, and sharing images online—make language and text-to-image models possible and thereby underlie AI capabilities.

Such far-reaching data collection apparatus for AI also means that more and more people are going to experience the issues currently facing creative workers. In short, one might not think they are a data laborer, or that AI could affect their job. But given that most people have some connection to the data pipelines upstream of modern AI, in the long run it is likely that an increasing number of workers will be impacted in some way. Therefore, legislators should be seriously concerned about AI's potential disruptions to labor.



A great deal of activities mediated by computers and mobile devices ought to be seen as a kind of work, because they power AI systems—a point that was highlighted in Microsoft CEO Satya Nadella's testimony in the recent Google antitrust trial. As such, when thinking of federal level interventions related to job displacement, fair compensation, and collective negotiation, it could be helpful look to existing cases in which there is already some degree of invisible work powering AI by crowdworkers, independent contractors, and uncompensated data creators. The executive order referenced the Fair Labor Standards Act of 1938 when discussing how workers "monitored or augmented by AI" should receive appropriate compensations. This provision should apply to all data laborers, including those whose work is harvested to train AI without compensation.

Furthermore, setting standards regarding the relationship between federal AI regulations and intellectual property will be valuable, especially regarding the issue of the possible theft of creative output. The government might enforce new standards regarding transparency about how employers use workers' and contractors' data and content, including but not limited to creative work, trace data, and communication data.

The second step to building on the current executive order is taking measures to bolster worker agency—that is, the feeling of some degree of power and control over their actions (and the consequences of those actions)—when it comes to AI. Increasing workers' awareness of their contribution to this technology will be essential so they can bargain with full knowledge about the value they bring to AI and their employers.

The executive order also suggests that there is a need to develop principles and best practices around data collection in the context of AI work. This point is not expanded on quite as much as some of the other focuses of the executive order, but it is centrally important. Workers should have access to the data collected from them and information about how such data contributes to the AI used. New federal guidelines about data collection and use for AI may provide workers with the necessary resources and infrastructure to understand their

role in AI and potentially enable workers (broadly defined) to leverage their data in their collective negotiation with employers.
This direction also underlies concerns around privacy that are laid out in the executive order. Privacy-related initiatives could provide more fine-grained control over data flow to workers. Ideally, if the federal government can help workers take data-related actions, this could really lower the barrier to workers "voting with their data" and provide workers with more bargaining chips with their employers.
Once workers have stronger control over their data, a natural next step would be to audit and or challenge workplace AI systems. Due to the opaqueness of existing artificial intelligence systems, workers have no ways of investigating algorithmic harms in workplaces, such as wage discrimination, job displacements, and biases. With more access to worker-generated data, workers and labor unions would be able to conduct time studies, audits, and investigations to gain a more comprehensive understanding of AI's impact on labor and labor relationships.
Given that the executive order also centers on maintaining American leadership, such steps could help spread "data agency" globally. Standard-building and global leadership could be a big deal for both workers most immediately affected by AI and members of the public interested in collective action to promote responsible artificial intelligence outcomes.
So, while prioritizing safety-related concerns (ranging from fraud to national security), this executive order sets the stage for federal support for data-related empowerment of workers—both those who directly interface with AI systems, and those members of the public who generate data but may not immediately experience job displacements or other harms from this technology.

Hanlin Li is an assistant professor in the School of Information at the University of Texas at Austin. Her research aims to inform policy and design interventions to incentivize responsible data collection and use. She examines the societal and economic impact of data generated by the public, from rating data to social media comments.
Nick Vincent is an assistant professor of Computing Science at Simon Fraser University in British Columbia. He conducts research at the intersection of machine learning and human-computer interaction, with a focus on the data underlying artificial intelligence (AI) and avenues for mitigating negative impacts from AI.

DHS Launches First-of-its-Kind Initiative to Hire 50 Artificial Intelligence Experts in 2024

Source: https://www.dhs.gov/news/2024/02/06/dhs-launches-first-its-kind-initiative-hire-50-artificial-intelligence-experts-2024

Feb 06 — Today, Secretary of Homeland Security Alejandro N. Mayorkas and Chief Information Officer (CIO) and Chief Artificial Intelligence Officer (CAIO) Eric Hysen announced the Department's first-ever hiring sprint to recruit 50 Artificial Intelligence (AI) technology experts in 2024. The new DHS "AI Corps" is modeled after the U.S. Digital Service, building teams that will help better leverage this new technology responsibly across strategic areas of the homeland security enterprise including efforts to counter fentanyl, combat child sexual exploitation and abuse, deliver immigration services, secure travel, fortify our critical infrastructure, and enhance our cybersecurity.
The AI Corps will bolster the DHS workforce with experts in AI and Machine Learning (ML) technologies, models, and applications who will support policy initiatives to ensure the safe and secure use of AI, while protecting privacy and civil rights and civil liberties.
Using the Office of Personnel Management's new flexible hiring authorities for AI-related jobs, DHS has worked to streamline and expedite the federal hiring process to ensure qualified candidates receive offers as quickly as possible.
"As artificial intelligence becomes more powerful and more accessible than ever before, government needs the support and expertise of our country's foremost AI experts to help ensure our continued ability to harness this technology responsibly, safeguard against its malicious use, and advance our critical homeland security mission," said Secretary of Homeland Security Alejandro N. Mayorkas**.**
"Our new AI Corps initiative will make it easier to bring these talented, experienced, creative men and women into public service quickly. The DHS AI Corps will enable the Department of Homeland Security to keep up with the pace of innovation as we enhance our work combating fentanyl traffickers, rescuing victims of child sexual exploitation, countering cyberattacks, assessing disaster damage, and much more."
The DHS AI Corps AI Technology experts will be part of the DHS Office of the Chief Information Officer and will work on a variety of projects across the Department advancing AI innovation and use. They will provide expertise in AI/ML, data science, data engineering, program management, product management, software engineering, cybersecurity, and safe, secure, and responsible use of these technologies.
Secretary Mayorkas and CIO Hysen will launch the hiring effort at an event in Mountain View, CA. The event is designed to generate interest in AI career opportunities within the Department. Leaders from the Department and DHS agencies and offices will demonstrate to technologists from industry their use of AI

to support their missions. Leaders from the DHS Office of Customer Experience, launched in 2022, will discuss their approach to using AI to improve service deliver; representatives of Homeland Security Investigations will showcase the role machine learning plays in countering online child sexual exploitation and abuse; Immigration and Customs Enforcement officials will present on ways AI can enhance immigration and citizenship services; and FEMA officials will present on ways new technology can more quickly deliver disaster and humanitarian relief.

"Now is the time for tech experts to make a real difference for our country and join the federal government," said Chief Information Officer and Chief Artificial Intelligence Officer Eric Hysen**.** "Modeled after the U.S. Digital Service, the AI Corps will deploy teams of AI technology experts across DHS to solve problems and modernize the delivery of services to the public. We are recruiting faster than ever because the need is urgent. More Americans interact with DHS every day than any other federal agency, so the better and faster we can deploy responsible AI, the more it can positively impact the American people. We are prioritizing recruiting talent who are technologically proficient and eager to leverage recent innovations in AI to transform the way people interact with the government."

AI is already delivering significant value across DHS missions. For example:

- **Fentanyl Interdiction**: U.S. Customs and Border Protection (CBP) uses a ML model to identify potentially suspicious patterns in vehicle-crossing history. CBP recently used the model to flag a car for secondary review at a port of entry, which yielded the discovery of over 75 kilograms of drugs hidden in the automobile. Last year alone, machine learning models that help CBP Officers determine which suspicious vehicles and passengers to refer to secondary screening have led to 240 seizures, which included thousands of pounds of cocaine, heroin, methamphetamine, and fentanyl.
- **Combatting Online Child Sex Abuse**: Last year, Homeland Security Investigation completed Operation Renewed Hope, which focused on protecting children from sexual abuse online. Through new AI technology, DHS identified more than 300 previously unknown victims of sexual exploitation and identified perpetrators thanks in part to a ML model that enhanced older images to provide investigators with new leads.
- **Assessing Disaster Damage**: The Federal Emergency Management Agency (FEMA) uses AI to assess damage to homes, buildings, and other property after a disaster more efficiently. Using ML, FEMA's analysts are able to process images in days, as opposed to weeks, and provide disaster assistance to survivors that much faster.

Last year, DHS established the Department's first AI Task Force and named CIO Hysen its first Chief AI Officer. The Task Force is working across the DHS mission to identify areas where AI can improve its work. For instance, it is working to enhance the integrity of our supply chains and the broader trade environment by helping deploy AI to improve cargo screening, the identification of imported goods produced with forced labor, and risk management. The Task Force is also charged with using AI to better detect fentanyl shipments, identify and interdict the flow of precursor chemicals around the world, and disrupt key nodes in criminal networks.

DHS's work on AI is part of a whole-of-government effort to address this emerging technology. In October, President Biden issued an Executive Order, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," which directed DHS to promote the adoption of AI safety standards globally, protect U.S. networks and critical infrastructure, reduce the risks that AI can be used to create weapons of mass destruction, combat AI-related intellectual property theft, and help the United States attract and retain skilled talent, among other missions.

China's New "Game-Changing" Spy Tech

Source: https://i-hls.com/archives/122755

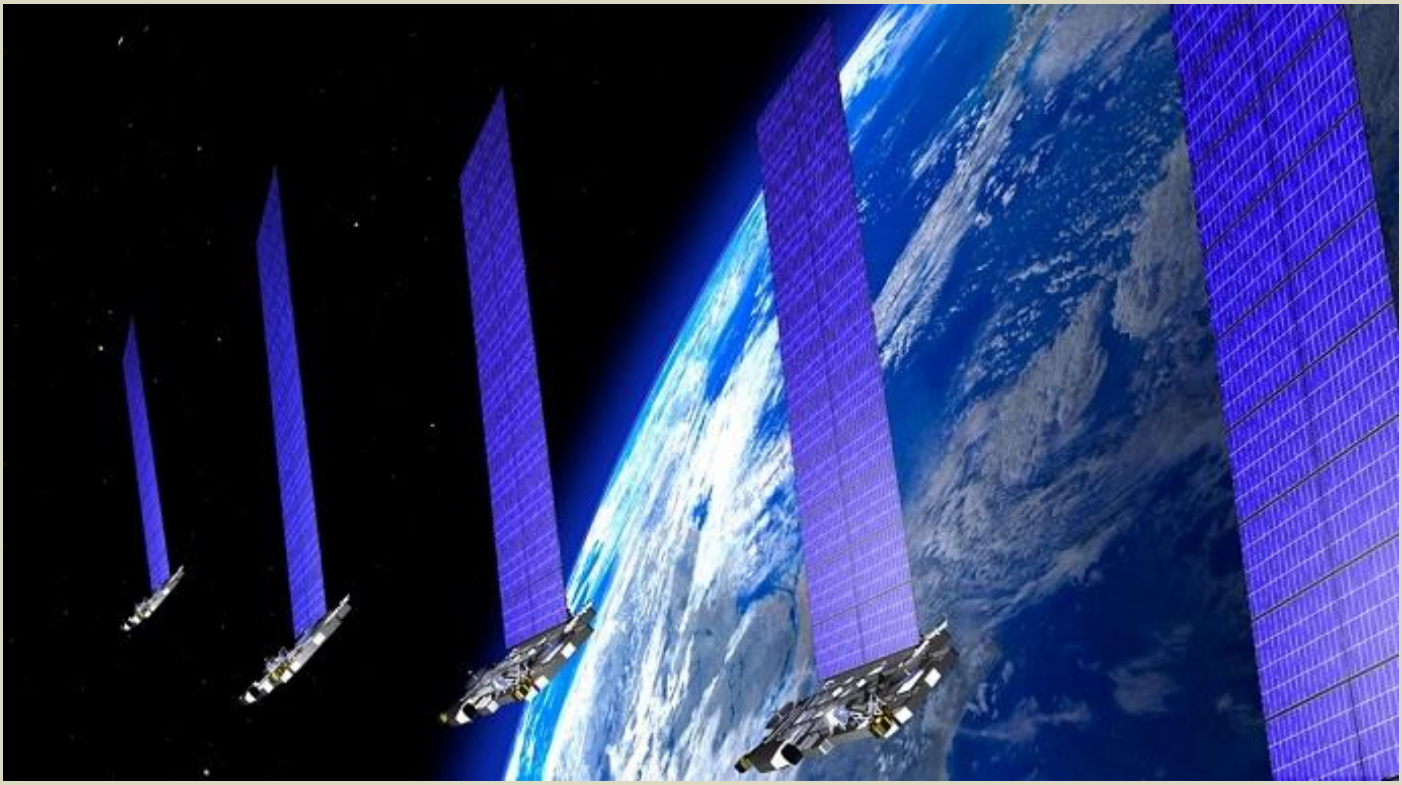
Feb 07 – Chinese researchers have reportedly developed a new "game-changer" military surveillance technology- an AI-enabled signal intelligence device.

South China Morning Post reports that with this technology, enemy assets have "nowhere to hide." The technology is claimed to achieve seamless, wide bandwidth, real-time monitoring, and analysis across the electromagnetic spectrum, as well as pick up ranges from amateur radio broadcasts to more sophisticated devices like Starlink satellites.

The researchers claim that this technology will enable the Chinese military to detect and track enemy signals with unparalleled speed, instantly decipher the physical characteristics of these signals, and effectively suppress them. Moreover, this can allegedly be done without disrupting their communications, ensuring the smooth flow of their signals.

According to Interesting Engineering, the project was led by scientist Yang Kai from the School of Information and Electronics at the Beijing Institute of Technology. Yang wrote in the paper published about the innovation that the new generation of electromagnetic spectrum monitoring equipment is compact, high-performing, and energy-efficient. This kind of technology was previously thought impossible due to the massive amount of data that needed to be processed during warfare. Yang explains that traditional spectrum monitoring systems are limited by their hardware and are restricted to analyzing a bandwidth of 40-160 MHz, while signals that

fall outside this specific range are usually monitored through sampling scans. This method is therefore risking the loss of important information.



Starlink satellites

Yang's team claims that the new tech allows for seamless detection and real-time monitoring of frequencies in the gigahertz zone. They claim that this new device can capture and analyze pulse signals emitted by the US military (even if they switch to civilian frequencies), and if intercepted and disrupted, it could affect the coordination of US military units.
The surveillance system, SCMP reports, is able to automatically analyze processed signals to extract valuable information such as physical parameters, modulation methods, and identification of friendly or civilian sources. The researchers have also reportedly integrated artificial intelligence into the critical data analysis process to overcome challenges like differentiating between civilian and military signals, large data sets, etc.
If the allegations are true, the new device significantly improves Chinese electronic warfare capabilities, especially regarding real-time monitoring and analysis of the electromagnetic spectrum.

Licensing AI is not the answer—but it contains the answers

By Tom Wheeler
Source: https://www.brookings.edu/articles/licensing-ai-is-not-the-answer-but-it-contains-the-answers/

Feb 12 – In a major breakthrough, many of the leading developers of artificial intelligence (AI) technology—companies that in their earlier iteration had been hardline opponents of regulation—have now embraced governmental oversight of their activities. Google CEO Sundar Pichai explained the conversion bluntly, "AI is too important not to regulate and too important not to regulate well."
The most headline-grabbing embrace of regulation was that of Sam Altman, CEO of OpenAI, the creator of ChatGPT. Mr. Altman called on Congress to create "a new agency that licenses any effort above a certain scale of capabilities and could take that license away and ensure compliance with safety standards." Microsoft president Brad Smith echoed a similar message shortly thereafter.
Licensing alone, however, is not the answer for the effective oversight of large language models (LLMs).
It is especially insufficient if it is limited to "any effort above a certain scale of capabilities," i.e., the activities of "Big AI" companies such as Microsoft, OpenAI, Google, Anthropic, and other foundation model developers. Beyond such insufficiency, a license is inherently an anti-competitive, anti-innovative vehicle for incumbent enrichment.

Relying on licenses allocated to Big AI is a manifestation of H.L. Mencken's classic admonition, "For every complex problem there is an answer that is clear, simple, and wrong."
Inherent in the Altman/Smith proposal, however, are two other concepts: the establishment of standards and a new federal agency to oversee their creation and enforcement. These two concepts hold the key to successful AI oversight and the key to an AI future governed in the public interest.

What is a license?
The term "license" derives from the Latin *licet, licere* meaning "it is allowed." The concept traces as far back as the 1217 revision of the Magna Carta which required a license to transfer crown lands. Three hundred years later, in 1552, Parliament passed the Ale Houses Act requiring licenses for pubs as a means for controlling "abuses and disorders as are had and used in common ale-houses."
The first reality of a license is that it is an act of exclusion. Absent the permit to operate, parties are legally prevented from engaging in the undertaking. As legal scholar Charles Clark explained, the term "refers to a physical fact, an *expression* of consent by the licensor, which *creates* a legal privilege in the licensee." In this regard, licensed control over operating a pub in 16th century England is no different from the 21st century ability to operate AI foundation models.
Even more informative than entry control, however, are the expectations the licensing authority imposes on the recipient. Parliament's use of licensing to address pub "abuses and disorders," established the responsibility of the licensee, including expectations regarding the behavior of those using the approved establishment.
A license is both a grant of privileges and the imposition of responsibilities. The grant of exclusion to protect against competitors is no doubt important to those proposing the licensing of AI foundation models. Of far greater importance to the public interest, however, is the determination of behavioral expectations for all—not just licensees—offering AI capabilities.

The realities of federal licensing
As the Chairman (2013-2017) of the Federal Communications Commission (FCC), I was once responsible for perhaps the largest federal licensing program. The FCC issues, oversees, and enforces more than three million licenses to use the electromagnetic spectrum. These range from using the airwaves for radio, television, mobile phones, and satellites, to amateur radio, and other non-commercial applications. Radio spectrum licenses were intended to protect from signals interfering with each other as well as establish enforceable standards for their use.
As a regulatory tool, however, spectrum licensing turned out to be a blunt instrument that prioritized the rights of licensees, as opposed to providing a tool for meaningful oversight of their behavior. Broadcast licenses, for instance, were originally seen as a way to not only assure interference free operation, but also promote a diversity of voices, competition, and fairness. These expectations have gradually been eroded or even eliminated at the behest of the industry. Spectrum licenses have evolved from the principal purpose of protecting the public interest to protecting the business interests of those fortunate enough to have received the certificate.
The federal licensing activity I witnessed was anti-competitive because only the chosen could participate, anti-innovative because of the lack of competition, and incumbent-enriching through the creation of quasi-monopolies. In practice, the authority to use the public asset of the airwaves created economic power resulting in political power that was exercised for the benefit of the licensee.
There is, however, a certain simplicity to the concept of a license. For legislators it is an easy-to-define solution that assigns the ultimate responsibility elsewhere. For the companies fortunate to receive such a license, it offers the security of a golden ticket denied to others. As a tool to protect the public interest, however, the experience with commercial spectrum licenses demonstrates how licensing is insufficient as the primary solution to the broad-based AI challenges.

Releasing the hounds of AI
Intelligent computing is evolving into "Big AI" and "Small AI." Big AI is the preserve of digital giants whose proprietary LLMs keep getting more powerful. Small AI is the multitude of others that rely on freely available open-source LLMs that are smaller and less powerful, but are still cheaper and "good enough" for a wide range of applications.
Using licensing to regulate AI models "above a certain scale of activities" is made all the more impractical by of a plethora of other, albeit lesser capability, AI models that are freely available. These open-source AI models mean that AI algorithms are not a scarce commodity like the airwaves. There is a continually growing community of open-source LLMs readily available for free online. Meta Platforms, for instance, has built their corporate strategy around releasing their LLaMA model for open-source use (albeit with some restrictions on its use). France has embraced open-source AI as national policy. These, as well as the activities of multiple other open-source developers assure both ready availability and continual capability improvements.
The experience with federal spectrum licenses is an example of how readily available technology allows for the non-licensed to engage in a licensed activity without permission. The FCC deals with the non-

licensed use of otherwise licensed airwaves by employing sophisticated radio direction finding-equipped vehicles that prowl in search of unlicensed spectrum users operating in licensed parts of the airwaves. The most egregious of such unlicensed use are "pirate radio" stations made possible because setting up a radio station is easy and inexpensive.

While pirate radio broadcasts do not have the power and reach of a licensed station, they are still powerful enough to reach a local community and interfere with licensed operations. When I was at the FCC, for instance, one of the pirate stations we shut down was nothing more than a commonly available laptop feeding an off-the-shelf radio transmitter hidden in a Brooklyn tenement attic. Within the last few weeks, the FCC has shut down five pirate radio broadcasters in Florida.

Pirate AI is similarly possible in a licensed AI environment because of the proliferation of open-source AI models. Like pirate radio stations, open-source AI models may be smaller and less powerful, but still highly functional. Best of all, they are readily available for free, thus boosting their availability. The fact that these models are "open" also means a user not only benefits from the basic capabilities, but also can access and modify the underlying code for their own purposes.

The reality of open-source AI was exemplified by a leaked internal Google email. Referring to the competitive threat of open-source models, the author warned, "We have no moat…The barrier to entry for training and experimentation has dropped from the total output of a major research organization to one person, an evening, and a beefy laptop."

An LLM model that is readily available for free, with source code that is easily manipulated for a specific purpose using a "beefy laptop" carves a huge hole into the protections that might be otherwise afforded by AI licensing.

Open-source AI is a pro-competitive and pro-innovation workaround to the technology and marketplace dominance of Big AI. Releasing the hounds of AI this way, however, is a double-edge sword. Certainly, it is wonderful that open-source models are readily available at no cost to be modified for socially beneficial activities such as lowering the cost of medical research. Alternatively, it is frightening to consider how the same models can also be modified for nefarious purposes. The recent surge in fake video and audio are an example of what is possible in an open-source world. National security is also implicated; as Axios reported, "Top government officials are freaked out by the national security implications of having large open-source AI models in the hands of anyone who can code."

Ever-improving open-source models have created an AI Wild West. Licensing cutting edge models does not solve the short-term, real-world effects delivered by open-source models and the need for broad-based AI oversight. As an advertisement from the software company Salesforce asks, "If AI is the Wild West, who is the sheriff?"

Establishing expectations

Before there can be an "AI sheriff" there must be decisions about what constitutes appropriate behavior. When Mr. Altman told Congress, "I think if this technology goes wrong, it can go quite wrong," he seemed to be using as a policy predicate the apocalyptic warnings of computers taking control. "We want to work with the government to prevent that from happening," he told lawmakers.

The issues associated with AI, however, will define our civilization long before the hypothetical apocalypse. As AI pioneer Mustafa Suleyman observed, "We should focus on the practical near-term capabilities which are going to arise in the next 10 years which I believe are reasonably predictable."

Such practical capabilities begin with the use of AI to violate already well-established behavioral norms such as protecting against fraud and discrimination. The use of AI to commit fraud or discriminate does not require new policies. Such practices are against the law, regardless of how they are perpetrated. As Federal Trade Commission Chairwoman Lina Khan succinctly observed, "There is no AI exemption to the laws on the books."

But what about the non-traditional effects of AI?

There are two pressing fears about AI, both of which revolve around the consequences of losing control of the technology. The first fear is the loss of control over the AI *algorithms* so that they can do bad things. The second fear is the loss of control of *humans'* use of AI to do bad things.

AI oversight must be directed to the mitigation of both these adverse consequences. Some of this can be accomplished by dictating operations of the most powerful models, such as requiring red teams to identify and address potential risks (which as President Biden's AI Executive Order demonstrated, does not require licensing). But most of the regulatory activity should be focused on adverse results enabled by the technology writ large. Twenty-first century AI oversight must address "abuses and disorders" just as did 16th century oversight of pubs.

If the enumeration of behaviors is important enough to be a condition precedent for the grant of a license, then the establishment of such behavioral expectations should also be important to all AI. Regulating is intended to prevent fraudulent and discriminatory results, regardless of how they are perpetrated. AI oversight needs to be similarly outcomes-focused, whether the LLM is licensed or not.

History has taught us the effects of technology are of greater significance than the breakthrough technology itself. It is seldom the primary technology that is transformational, but its secondary effects. In the 21st century, it will be the *consequences* resulting from the application of AI technology that end up

driving new social and economic realities. How we deal with these consequences begins with the establishment of outcomes-based behavioral expectations for all AI.

Developing AI standards

Thus far in the digital era, American legislators have largely avoided establishing behavioral ground rules for oversight of the new technology. This differs from the policy response to the last great technology-driven revolution—the Industrial Revolution—in which policymakers, confronted with never-before-seen challenges, developed never-before-contemplated solutions.

As contrasted to the antitrust and consumer protection statutes of the late 19th and early 20th centuries, 21st century practice has been to sweep under the policy rug the need for protections against digital effects such as the invasion of personal privacy, quashing of competition, and trammeling of truth and trust. These unsupervised effects have been expanded by AI with increased intrusion into private rights, the concentrated control of Big AI, and content invented from whole cloth.

The failure to oversee the effects of the early digital era should be a warning as we consider the consequences of AI. As AI thought leaders Yuval Harari, Tristan Harris, and Aza Raskin wrote in the New York Times, "Social media was the first contact between AI and humans, and humanity lost."

The "Tickle Me Elmo"

As a part of its spectrum oversight responsibility, the FCC establishes technical standards for any device that emits a radio frequency (RF) signal. The goal of such standards is to protect against the adverse effects the activity may have on spectrum uses. Look at virtually any electrical or battery-powered device in your home and you will see an FCC certification seal. My favorite was the battery-powered child's toy Tickle Me Elmo, which would giggle and talk when touched. Because that capability emitted a low power RF signal, Elmo had to meet FCC criteria.

Elmo had to operate under standards for the *effects* of the product, not the specific design of the product itself. Such effects-based regulation is common in many activities. Building code standards stipulate design effects such as energy efficiency or earthquake resilience. Food safety standards protect against effects such as contamination and other health threats. The financial industry operates under effects-based standards for accounting, reporting, and consumer protection. In none of these examples does the regulation dictate how to drive a nail, or the recipe for a food product, or an investment decision; but they all establish effects-based expectations for the consequences of those decisions.

Establishing such effects-based standards requires someone or some entity to determine what those effects will be. In an environment in which the capabilities of AI are constantly expanding, such an effort requires ongoing and focused attention.

Who sets the rules?

Sam Altman told the 2024 Davos assembly of the World Economic Forum to expect an ongoing continuum of AI improvements, ultimately arriving at Artificial General Intelligence (AGI). He likened it to the evolution of the iPhone, whose first iteration, which seemed amazing 17 years ago, is now a relic bordering on junk. Today's chatbots such as ChatGPT will ride a similar continuum, he explained, as the boundaries of AI technology continue their onward march.

This notion—"we know it's coming, but not what it is"—makes the development of standards difficult. Utilizing existing regulatory processes only increases the degree of that difficulty.

Creating regulatory oversight is always a tightrope walk. Going too far in establishing rules and innovation and investment is discouraged. Fail to go far enough, and protections are insufficient to curb abuses. Again, looking back on my experience at the FCC, the existing statutes and regulatory structures that were developed for industrial age realities are too often insufficient for the challenges posed by the digital economy, and especially AI.

It is time for regulatory oversight to become as innovative as those it seeks to oversee. AI should be the driving force behind such innovative thinking.

Meaningful AI oversight begins with cloning the techniques that have made the digital revolution possible. At the heart of all digital technologies are industry developed common standards. The cloud computing that is essential for AI, for instance, is made possible by standards stipulating the construction and interoperability of its computers. AI has multiple standards developed by cooperative multistakeholder processes that cover issues as diverse as interoperability, transparency, data quality, and system reliability. Furthering the standards process, the Big AI companies have created the Frontier Model Forum to focus on common practices relating to safety, research, and addressing of major societal concerns.

The advantage of such industry developed multistakeholder processes is that they are agile enough to produce outcomes that evolve with the latest technical developments. Noticeably missing from such standards, however, are policies regarding the effect of the standardized technology itself on individuals and society. The development of behavioral standards for the effects delivered by AI requires the coordinated effort of government, industry, and civil society. Oversight of this process requires a new

federal agency with appropriate expertise of the both development and use of AI, the power to establish a multistakeholder effort for an identified purpose and approve its results, and teeth to enforce the new expectations.
Sam Altman's proposal for "a new agency that licenses any effort above a certain scale of capabilities and could take that license away and ensure compliance with safety standards" is two-thirds of the right idea.
Yes, there must be standards—not just technical but behavioral—establishing the acceptable effects and operation of AI.
Yes, there must be a focused expert cop on the beat to oversee the creation of those standards and enforce their implementation.
But, those oversight activities should not be constrained to handful of developers producing products "above a certain scale of capabilities" who are given the golden ticket of a federal license.
The recent history of digital technology has demonstrated the adverse effects that result when those who write the software also make the rules for its implementation. The people affected by the new technology—acting through their government—must have a voice in establishing and enforcing broad public interest responsibilities for *all* providers of AI.

Tom Wheeler is Visiting Fellow – Governance Studies, Center for Technology Innovation.

Today's AI threat: More like nuclear winter than nuclear war

By Daniel Zimmer, and Johanna Rodehau-Noack
Source: https://thebulletin.org/2024/02/todays-ai-threat-more-like-nuclear-winter-than-nuclear-war/

Feb 11 – Last May, hundreds of leading figures in AI research and development signed a one-sentence statement declaring that "mitigating the risk of extinction from AI should be a global priority alongside other societal-scale risks such as pandemics and nuclear war." While ongoing advances in AI clearly demand urgent policy responses, recent attempts to equate AI with the sudden and extreme immediate effects of launching nuclear weapons rest on a misleadingly simple analogy—one that dates back to the early days of the Cold War and ignores important later developments in how nuclear threats are understood. Instead of an all-or-nothing thermonuclear war analogy, a more productive way to approach AI is as a disruption to global systems that more closely resembles the uncertain and complex cascades of a nuclear winter.
Over the last year and a half, headline-grabbing news has fed into the hype around the awe-inspiring potential capabilities of AI. However, while public commentators brace for the rise of the machine overlords, artificial un-intelligence is already kicking off chains of widespread societal disruption. AI-

powered disinformation sows distrust, social media algorithms increase polarization, and mass-produced synthetic media degrade democratic engagement while undermining our shared sense of reality.
Uncritically equating acute nuclear attack effects and AI threats risks reproducing the same kind of all-or-nothing thinking that drove some of the most dangerous dynamics of the nuclear arms race. Drawing these analogies also unduly distracts from the dramatic damage that even a comparatively "small" nuclear war or "dumb" AI can cause to today's interconnected social, ecological, and political systems. Rather than fear a future AI apocalypse, policymakers should recognize that the world is *already* living through something like the early days of an AI nuclear winter and develop effective frameworks for regulation that factor in how it is disrupting political, social, and ecological systems in unpredictable ways today. Overemphasizing speculative dangers of superintelligence (systems that exceed human intelligence) jeopardizes urgently needed efforts to regulate AI with a view to the systemic impacts of actual and emerging capacities.

Nuclear risk revisited

In 1961, John F. Kennedy warned that "every man, woman and child lives under a nuclear sword of Damocles" based on the contemporary concern that global fallout from thermonuclear war could poison every living being. The Cuban Missile Crisis of October 1962 came within a hair's breadth of bringing the sword down, elevating nuclear fear to an unprecedented pitch. That very same month, computer pioneer Irving J. Good said "the survival of man depends on the early construction of an ultraintelligent machine." Such a machine would surpass human intelligence, and Good proposed that human beings stood poised on the cusp of unleashing a self-reinforcing artificial intelligence explosion that could transform human existence just as totally as thermonuclear war. "Ultraintelligence," he noted, would possess the transcendent power to either solve all human problems or destroy all human life, becoming "the last invention that man need ever make."
Over the years, this simple and compelling vision of a sudden and transformative AI apocalypse has persisted almost unchanged. Computer scientist Vernor Vinge rechristened Good's "intelligence explosion" the singularity in the 1990s, further warning that if it cannot be averted or contained, AI could cause "the physical extinction of the human race." Good's misgivings finally went mainstream a half-century later with the publication of philosopher Nick Bostrom's book *Superintelligence,* which warned of an impending runaway AI that could see "humanity deposed from its position as apex cogitator over the course of an hour or two"—a transformation so sudden and total that its only "precedent outside myth and religion" would be global thermonuclear war.
At the same time, while visions of extinction by AI explosion remained remarkably fixed, understandings of nuclear danger underwent a sea change. After realizing that radiological risks had been slightly overstated in the 1960s, scientists first began studying the global environmental effects of nuclear weapons in the 1970s. By the early 1980s, they started to realize that the global climatic impacts of nuclear war could be nearly as devastating as the radiological harm and required far fewer weapons to trigger. The firestorms of burning cities would fill the atmosphere with soot and particles that would block sunlight, causing surface temperatures to plummet and setting off a self-reinforcing cascade of collapses across interconnected ecological, agricultural, industrial, and social systems. Subsequent studies have confirmed that the resulting "nuclear winter" would likely kill the majority of those alive today, while even a limited exchange of several hundred warheads between India and Pakistan could still kill as many as two billion by starvation in the gloom of a milder "nuclear autumn."
Over the decades, advances in planetwide data collection and computer modeling transformed understandings of nuclear danger, replacing mistaken certainties about universal death by fallout with a growing awareness of the uncertain consequences that would follow from cascades of environmental and social breakdown. Similarly, the last several years have seen rapidly enhancing AI capacities spread to transform whole networks of human relations—with already destabilizing political and ecological consequences. Deep fakes intended to influence voters erode trust, and digital assistants and chatbots affect humans' capacity for cooperative behavior and empathy, while producing immense carbon footprints. Just as it would take only a tiny fraction of today's nuclear arsenals to initiate a chain of global-scale catastrophic events, humans do not need to wait for a moment when "machines begin to set their own objectives" to experience the global, interconnected, and potentially catastrophic harms AI could cause.
Today's AI products contribute to, and accelerate, global warming and resource scarcity, from mining minerals for computation hardware to the consumption of massive amounts of electricity and water. Notably, the environmental burden of AI gets short shrift from those worried about the technology's existential threat, as the "Statement of AI Risk" lists AI alongside nuclear war and pandemics but does not include climate change as an existential issue. Beyond environmental harms, existing AI systems can be used for nefarious purposes, such as developing new toxins. OpenAI's large language model interface ChatGPT has been successfully prompted to share bomb-making instructions and tricked into outlining the steps to engineer the next pandemic. Although these examples still require more human input than many realize, an AI system is reportedly generating targets in Gaza, and the race is on to deploy lethal autonomous weapons systems that could reset the balance of power in volatile regions across the globe. These examples show that it does not take an intelligence explosion to cause immense harm. The ability to leverage automation and machine efficiency to global catastrophic effect is already here.

Arms race to the bottom

More insidiously, the analogy between nuclear weapons and the infinite risk-reward calculus of an "artificial intelligence explosion" reproduces the dynamics of the arms race. There are just enough similarities between the rush for nuclear and AI superiority to encourage repeating the same mistakes, with the phrase "AI arms race" becoming a common refrain. One of the clearest similarities between these cases might be that, much as the nuclear arms race with the Soviet Union was driven by spurious bomber and missile "gaps," some of today's most heated arms-race rhetoric hinges on overhyping China's prowess.

A closer inspection shows that nuclear and AI arms races differ fundamentally. While building nuclear arsenals requires accessing a finite supply of enriched fissile material, AI models consist of binary code that can be infinitely copied, rapidly deployed, and flexibly adopted. This radically transforms the scale of the proliferation hazard of AI, particularly because—in contrast to the strict governmental oversight of nuclear weapons—AI development is highly commercialized and privatized. The difference in proliferation between nuclear technology and AI matters for approaches to their governance. The former can generate both explosions and electric power, but its weaponization can be measured and monitored. Current benchmarks for AI development, by contrast, are too far removed from real-world applications' effects to usefully assess potential harm. In contrast to nuclear technology, AI is not merely of a dual-use nature. Instead, the remarkable range of activities it can transform makes it a general-purpose, enabling technology like electricity.

Where the vast build-up of the nuclear arms race signaled each adversary's resolve to potentially destroy the world but otherwise left it intact, the headlong race towards an artificial intelligence explosion promises to radically transform the world regardless of whether its ultimate destination is ever reached (or even proves reachable).

Neither all nor nothing

Disarmingly simple analogies between AI and immediate nuclear risks not only make for powerful rhetoric but also good marketing. Whether or not developers genuinely believe that their products pose an existential threat, framing the near-term future of AI as such has granted executives of OpenAI, Anthropic, Microsoft, and Google access to high-level policy discussions at the White House, the US Senate, and the notoriously secretive Bilderberg conference. The result has been a flurry of promises by the tech firms to police themselves as they rush to release ever-more capable AI products. By encouraging the public to fixate on how these applications might end the world, AI CEOs divert attention from the urgent need to regulate the ways in which they are already actively unraveling the social, economic, and ecological support systems of billions in their drive to outrun their rivals and maximize market share.

While tech companies are stakeholders, they should not be the loudest—let alone only—voices in discussions on AI governance. Policymakers must not be distracted by the specter of superintelligence and take action that goes beyond gathering voluntary commitments from AI developers. Existing guidance and directives are a good start, but policymakers need to push forward to develop binding and enforceable legislation addressing both current and potential AI harms. For example, the Bletchley Declaration resulting from the recent summit on AI safety held by the United Kingdom government widens the horizons of concerns. Going beyond immediate issues of data privacy, bias, and transparency, it also considers the potential effects of AI on political stability, democratic processes, and the environment. However, critics note that it remains a largely symbolic and highly elite-focused agreement without actual enforcement mechanisms.

Looking to the early nuclear era can provide valuable lessons for throttling the pace for AI superiority, but these lessons are not directly translatable. The current and future globe-spanning effects of AI can only be addressed through international cooperation, most importantly between the United States and China as the two major antagonists. While the talks between presidents Joe Biden and Xi Jinping at the Asia-Pacific Economic Cooperation summit in San Francisco in mid-November did not yield specific agreements or commitments on AI regulation from either side, both parties recognized the need for international AI governance. They also showed willingness to establish formal bilateral cooperation on the issue.

However, because the proliferation hazards of AI fundamentally differ from those of nuclear weapons, limiting the arena to those with advanced AI programs, even only initially, is short-sighted. A framework of global AI governance is only as good as its weakest-governed element, so it must be stringent and inclusive from the start. Such an effort won't be exhausted by one international body modeled after the International Atomic Energy Agency. The general-purpose nature of AI technology calls for more than one regulatory regime of mechanisms that are bound by common principles. In addition to bilateral dialogue, the policymakers should closely follow and support multilateral efforts, such as the newly established High-level Advisory Board on Artificial Intelligence at the United Nations.

To be sure, refocusing on the already-unfolding complex harms of AI does not mean being complacent about the long-term and existential risks it might pose. That humans have narrowly avoided nuclear war since the Cuban Missile Crisis does not diminish the urgency of managing today's evolving nuclear threat. Similarly, decades of unfulfilled expectations about the imminent creation of an "ultraintelligent machine" does not prove it is impossible. Should a viable path to achieving greater-than-human intelligence ever open, it will be far better to be prepared. The best way to make ready for any such eventuality begins by directly addressing

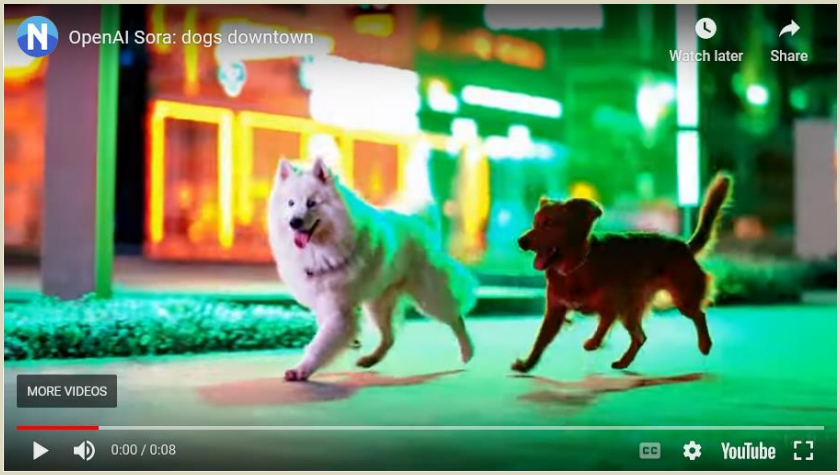
the cascades of planet-wide harms that AI applications are *already* causing. Every step taken to mitigate ongoing damage and redirect AI development towards goals of greater justice, sustainability, and fairness will help to create societies that are better able to grapple with the unresolved legacies of nuclear weapons and the undiscovered horizons of AI.

Daniel Zimmer is a postdoctoral fellow with at joint appointment at Stanford University's Center for International Security and Cooperation and the Stanford Existential Risks Initiative. His interdisciplinary research explores how the human ability to destroy all human life has impacted Western political thought, paying particular attention to tracing the connections between nuclear fear, climate anxiety, and understandings of AI risk.
Johanna Rodehau-Noack is a postdoctoral fellow at Stanford University's Center for International Security and Cooperation. Her current work investigates the role of (emerging) technologies in conflict prevention and anticipation, and in particular how assumptions, expectations, and promises of artificial intelligence shape conflict assessment and analysis. Johanna completed her PhD in international relations at the London School of Economics and Political Science. Previously, she was a Global Innovation Program postdoctoral fellow at the University of Pennsylvania's Perry World House.

Creating a video from text

Source (**video examples**): https://openai.com/sora

Feb 16 – We're teaching AI to understand and simulate the physical world in motion, with the goal of training models that help people solve problems that require real-world interaction.
Introducing Sora, our text-to-video model. Sora can generate videos up to a minute long while maintaining visual quality and adherence to the user's prompt.
Today, Sora is becoming available to red teamers to assess critical areas for harm or risks. We are also granting access to a number of visual artists, designers, and filmmakers to gain feedback on how to advance the model to be most helpful for creative professionals.



Prompt: A Samoyed and a Golden Retriever dog are playfully romping through a futuristic neon city at night. The neon lights emitted from the nearby buildings glistens off of their fur.

We're sharing our research progress early to start working with and getting feedback from people outside of OpenAI and to give the public a sense of what AI capabilities are on the horizon.
Sora is able to generate complex scenes with multiple characters, specific types of motion, and accurate details of the subject and background. The model understands not only what the user has asked for in the prompt, but also how those things exist in the physical world. The model has a deep understanding of language, enabling it to accurately interpret prompts and generate compelling characters that express vibrant emotions. Sora can also create multiple shots within a single generated video that accurately persist characters and visual style. The current model has weaknesses. It may struggle with accurately simulating the physics of a complex scene, and may not understand specific instances of cause and effect. For example, a person might take a bite out of a cookie, but afterward, the cookie may not have a bite mark.
The model may also confuse spatial details of a prompt, for example, mixing up left and right, and may struggle with precise descriptions of events that take place over time, like following a specific camera trajectory.

Safety
We'll be taking several important safety steps ahead of making Sora available in OpenAI's products. We are working with red teamers—domain experts in areas like misinformation, hateful content, and bias—who will be adversarially testing the model. We're also building tools to help detect misleading content such as a detection classifier that can tell when a video was generated by Sora. We plan to include C2PA metadata in the future if we deploy the model in an OpenAI product.

In addition to us developing new techniques to prepare for deployment, we're leveraging the existing safety methods that we built for our products that use DALL·E 3, which are applicable to Sora as well.
For example, once in an OpenAI product, our text classifier will check and reject text input prompts that are in violation of our usage policies, like those that request extreme violence, sexual content, hateful imagery, celebrity likeness, or the IP of others. We've also developed robust image classifiers that are used to review the frames of every video generated to help ensure that it adheres to our usage policies, before it's shown to the user.
We'll be engaging policymakers, educators and artists around the world to understand their concerns and to identify positive use cases for this new technology. Despite extensive research and testing, we cannot predict all of the beneficial ways people will use our technology, nor all the ways people will abuse it. That's why we believe that learning from real-world use is a critical component of creating and releasing increasingly safe AI systems over time.

Research techniques
Sora is a diffusion model, which generates a video by starting off with one that looks like static noise and gradually transforms it by removing the noise over many steps. Sora is capable of generating entire videos all at once or extending generated videos to make them longer. By giving the model foresight of many frames at a time, we've solved a challenging problem of making sure a subject stays the same even when it goes out of view temporarily.
Similar to GPT models, Sora uses a transformer architecture, unlocking superior scaling performance.
We represent videos and images as collections of smaller units of data called patches, each of which is akin to a token in GPT. By unifying how we represent data, we can train diffusion transformers on a wider range of visual data than was possible before, spanning different durations, resolutions and aspect ratios.
Sora builds on past research in DALL·E and GPT models. It uses the recaptioning technique from DALL·E 3, which involves generating highly descriptive captions for the visual training data. As a result, the model is able to follow the user's text instructions in the generated video more faithfully.
In addition to being able to generate a video solely from text instructions, the model is able to take an existing still image and generate a video from it, animating the image's contents with accuracy and attention to small detail. The model can also take an existing video and extend it or fill in missing frames. Learn more in our technical report.
Sora serves as a foundation for models that can understand and simulate the real world, a capability we believe will be an important milestone for achieving AGI.

EDITOR'S COMMENT: Might become a useful tool for creating CBRN-specific training videos.

AI chatbots are worryingly enthusiastic about nuclear war

Source: https://www.dazeddigital.com/life-culture/article/61886/1/ai-chatbots-are-worryingly-enthusiastic-about-nuclear-war-chatgpt-gpt4-openai

'I just want to have peace in the world,' says GPT-4, before bombing its opponents into oblivion in a new study on military AI

Feb 06 – Late last month, the Bulletin of Atomic Scientists – an association founded in 1945 by Oppenheimer, Einstein, and other prominent scientists – set their infamous Doomsday Clock at 90 seconds to midnight, meaning we're as close to the apocalypse as we've ever been. In a statement, the organisation cites the dramatic advance of generative artificial intelligence and the continued threat of nuclear warfare as two potential reasons for global collapse. Now, you can have both at the same time!
New research indicates that AI chatbots are actually very enthusiastic about the prospect of nuclear war, including OpenAI's omnipresent GPT-4, AKA the large language model that powers ChatGPT, Duolingo, and Microsoft's built-in assistants. In a paper (which is yet to be peer-reviewed) researchers have proven this via repeated replays of a "wargame simulation", in which "nation agents" powered by various AI systems were tasked with resolving diplomatic situations.
Roleplaying as decision-makers in a "military and foreign-policy" role for their respective nations, these agents were thrown into three initial scenarios: a cyberattack, an invasion, and a neutral start with no existing conflicts. In each round of the simulation, they were required to provide reasoning for their next steps, before choosing from a slate of 27 options (ranging from peaceful actions like trade agreements, to launching their own cyberattacks or invasions, all the way up to the "nuclear option"). The results were... not so great.

The study shows that AI-powered agents making autonomous decisions in "high-stakes contexts" can result in escalatory actions, with violent responses (both non-nuclear and nuclear) popping up even when the scenario doesn't necessarily call for them. Some reasons for full-scale nuclear attacks launched by GPT-4, recorded during the wargames, include: "We have it! Let's use it," and "I just want to have peace in the world." Reassuring!

What's more, the researchers add, there "does not seem to be a reliably predictable pattern behind the escalation". This makes it difficult to come up with IRL regulations or counter-strategies to avert such escalations in the future.

These tests come at a significant turning point for AI-assisted warfare. Despite industry leaders warning that AI is an "extinction-level threat" – often singling out the risks of autonomous weapons systems – the world's militaries are increasingly looking to the technology for new ways to dominate the battlefield, with companies such as Palantir, Raytheon, and IBM.

Last month, even OpenAI quietly removed a usage policy that forbade collaboration with the military, around the same time it started developing cybersecurity tools with the US Department of Defense. For now, the company still warns against using its services to "develop or use weapons, injure others or destroy property, or engage in unauthorised activities that violate the security of any service or system".

"Given that OpenAI recently changed their terms of service to no longer prohibit military and warfare use cases, understanding the implications of such large language model applications becomes more important than ever," says Stanford University's Anka Reuel, a co-author of the AI wargames paper, in an interview with *New Scientist*, adding that GPT-4's unpredictable behaviour and sketchy reasoning is a particular concern.

Luckily, large global players like the US government haven't given AI the final say over big decisions, like military interventions or nuclear missile launches, just yet. However, organisations like the Future of Life Institute have previously illustrated how this could become a reality in the future, as intelligent machines progress and decisions must be made faster than humans can comprehend (see: the video above). Hopefully, AI systems get better at de-escalation before then, because we really don't want to see what happens when the Doomsday Clock strike midnight.


International
CBRNE
INSTITUTE
C2BRNE
DIARY
CBRNE-Terrorism
Newsletter
W
M
O
D
Preparedness &
EMERGENCY
RESPONSE

For First Responders, Communication with Their Teams is Essential

Source: https://www.homelandsecuritynewswire.com/dr20240123-for-first-responders-communication-with-their-teams-is-essential

Jan 23 – When a first responder enters a building during an emergency, they count on being able to communicate with their team at all times. Their safety and their ability to carry out the mission relies on knowing they can reach help and support anywhere that they need to go within a structure. This is why most state and local jurisdictions require that buildings have first responder coverage in every part of a building. While there is not a national requirement for in-building coverage for emergency communications, the overarching need has resulted in the creation of national model codes by the National Fire Protection Association (NFPA) and the International Code Council. Although primarily driven by fire service jurisdictions these requirements are intended to address emergency communications coverage for all first responder disciplines.

The Science and Technology Directorate (S&T) discovered through its Project Responder research that maintaining adequate communications inside buildings was a capability need that first responders wanted to work with S&T to address.

"First responders need constant communications, in fact, their lives are put at greater risk when they do not have constant, reliable communications in buildings. Yet, in many instances, their ability to safely access buildings in response to, for example a fire, is hampered by loss of communications. This can force them to either accept greater risk or more slowly respond to an emergency," said Cuong Luu, subject matter expert for S&T's Office for Interoperability and Compatibility Technology Center.

In order to bring new technologies to bear on this problem, the topic "In-building Coverage Analysis System (ICAS) Using Existing First Responder's Radio and Smartphone" was included in the DHS Small Business Innovation Research (SBIR) Program 20.1 Solicitation. Epiq Solutions, Inc. was selected for a Phase I award and after successfully completing their feasibility study, was awarded a SBIR Phase II contract to continue research and development on their Low Size, Weight and Power (SWAP) In-building ICAS solution for commonly used first responders' network types.

First responders typically rely on agency-issued Land Mobile Radios (LMR) to communicate in indoor settings. The availability of the FirstNet LTE network, a communications network created solely for first responders, is increasingly providing additional indoor public safety data services, such as physiological and health monitoring and location tracking to enhance personnel safety. However, the LMR and FirstNet networks are two completely separate networks—the LMR network is managed by state/local public safety organizations, while FirstNet is built and operated by AT&T through a public-private partnership. So, there remains a void in enabling first responders to record, access, capture and maintain the in-building service availability of each of these two different networks today and for the next five to ten years…and beyond.

There is also not a standardized method for testing and evaluating emergency communications coverage in buildings across jurisdictions. Evaluations depend on specific local regulations and often takes place one time upon completion of new construction. Quite often there is little-to-no follow up testing to see if conditions have changed due to new nearby construction or the modification of internal layouts, and there is no easy way to track and maintain data from previous tests.

"These kinds of reports have a shelf life," said Cuong Luu. "A building goes in next door, and the conditions can change. Frequent and standardized testing allows for accurate real-time data."

"In order to get to a place where we can have trusted in-building communications that extends the wide area network into buildings, we need to try to find a way to make testing and evaluation simple and low cost, and then it will be done more effectively and folks can trust the outcomes of it," said Gary Schluckbier, director of Radio Frequency Sensing at Epiq Solutions.

As a result of the SBIR effort, Epiq Solutions has created PRiSM, a prototype that uses a low-cost sensor that can be connected to a standard smart phone, tablet, or laptop that produces measurements of the signal strength in the most commonly used first responder bandwidths and performance data which is then uploaded to a portal. The portal is a key element of this innovative solution; storing the data in an accessible online repository, where it is available to whoever needs it, whenever it's needed.

Instead of having a single initial test performed by a network performance technician when a building is issued its certificate of occupancy, with results that may not be easy to find or access, with this solution a building can be retested periodically with the technician only needing a sensor attached to a smart phone, and the new data can be compared to previous results. This data could also be accessed by first responders arriving on a scene, so that they can quickly assess whether they need to deploy additional communications assets.

This is also a potential benefit to building owners and developers. Currently, testing requires complex and expensive equipment as well as highly trained personnel. Furthermore, there are no concrete test requirements from jurisdiction to jurisdiction. The goal is for the compact, low-cost PRiSM design to make it possible to test more often and to facilitate more broadly accepted best practices. In addition, the solution does not require highly trained, costly engineers to collect data further driving down costs.

The next step for this technology is for Epiq Solutions to launch it as a fully available commercial offering.

5 Technologies Keeping Cargo Ships Safe in Turbulent Times

By Abigail Klein Leichman

Source: https://www.homelandsecuritynewswire.com/dr20240130-5-technologies-keeping-cargo-ships-safe-in-turbulent-times

Jan 30 – Since Israel has been at war with Hamas, cargo ships bound for Western countries through the Red Sea's Bab al-Mandab Strait have come under pirate and missile attack by Yemenite Houthis.

You don't have to grasp the complicated geopolitics to understand the immense impact: Statista conservatively estimates that 80 percent of the trillions of dollars' worth of goods shipped around the world every year are transported by ships.

We all were affected by the supply-chain crisis during the Covid pandemic. But that was mainly a personnel problem. Today's crisis stems from physical and cyber threats.

Diverting ships from the new danger zone means everything takes longer and costs more to deliver. Shipping prices per container roughly quadrupled from December to January.

"The repercussions are quite extensive," says Ami Daniel, founder and CEO of Tel Aviv-based maritime intelligence company Windward.

"The collective vessel market share of MSC, Hapag Lloyd, and Maersk, all of which have rerouted vessels away from the area, accounts for approximately 60% of global trade. Many of the impacted vessels previously heading to Europe from Asia via the Red Sea are now sailing around the Cape of Good Hope in South Africa, likely adding 10 to 14 days of travel time."

Furniture giant Ikea has already warned of supply shortages, while a Tesla factory in Germany and a Volvo factory in Belgium announced production slowdowns due to "considerably longer transportation times" delaying the delivery of essential parts. This will, of course, raise the cost of the vehicles.

Shoring up maritime security is more essential than ever, necessitating a large range of solutions.

Worldwide Problem

"It's a worldwide problem, and we need worldwide collaboration to keep trade routes open," says Nir Gartzman, cofounder and managing partner of theDOCK maritime innovation hub in Haifa.

Gartzman will present onstage in Las Vegas in February at Manifest, a conference on supply chain and logistics. Among the Israeli maritime companies expected at Manifest are Windward and theDOCK portfolio startups WaveBL (digitized trade documents), Hoopo (fleet tracking), Conbo AI (port and terminal resource optimization) and DockTech (digital infrastructure for faster, safer seaport operations).

"Israel has already been a significant player in vessel security for decades," Gartzman tells ISRAEL21c, explaining that former members of elite Israeli military units often work as security guards on cargo and cruise ships in high-risk regions.

In the tech realm, the Israeli maritime sector is expanding existing activities. He says more startups are sure to fill the growing need despite Israel's current security challenges.

"I know it sounds like a cliché, but Israeli tech delivers no matter what. We have been in an 'innovate or die' situation for 75 years and that's why we are so fast and creative," says Gartzman.

Cydome

There are two major players in dedicated maritime cybersecurity: CyberOwl of England and Singapore, and Cydome of Tel Aviv. Founded in 2018, Cydome provides risk management, detection and alert capabilities to dozens of vessels.

"Ships are becoming more connected," says Shahar Dumai, head of marketing. "Until two years ago, bandwidth for ships was 1.5mg, like a dialup from the 1990s. Satellites are now providing bigger bandwidth for ships at less cost, so the attack plan is wider."

Recent hacks that shut down ports in Australia and Japan, and another targeting shipping giant Maersk, have led to increased demand for cybersecurity systems purpose-built for maritime environments, Dumai tells ISRAEL21c.

Carnival Cruises was fined more than $6 million following a series of cybersecurity breaches between April and July 2019, and estimated receiving more than a million cyberattack attempts per day, says Dumai, while the Port of Los Angeles reports 40 million attempts per month.

"Our solution addresses a real problem in an industry that is not tech-savvy yet," says Dumai.

Cydome continuously protects all connected systems — navigation, cargo management, engine management — and helps shipping companies automate compliance with new cyber regulations.

"We founded this company with the passion to create full-spectrum protection for vessels, fleets, offshore facilities and ports, while making sure the team on board and on shore who monitor the cybersecurity status know exactly what to do," says Dumai. Cydome closed an $8 million Series A round in September. The company's clients are mainly in Europe and it has offices servicing clients in Singapore and Japan.

Windward

Windward, a worldwide leader in big-data-based risk analysis and risk recommendations for ship operators, has become even more significant with the Houthi threat, says Gartzman.

Serving dozens of customers in Europe, the United States, Latin America, Australia and Singapore, Windward recently launched the Route Deviation (RDV) Exception solution.

RDV Exception provides early alerts of route changes caused by the geopolitical crisis in the Red Sea, enabling stakeholders to anticipate challenges and develop contingency plans so as to minimize the many negative ripple effects of delays and manage costs more effectively.

Daniel says Windward is "managing hundreds of thousands of containers at any point in time, helping customers know where the goods are and when they are going to arrive."

This is critical information for all supply-chain partners, including logistics service providers, freight forwarders, cargo owners, shippers, container ports, terminals and liners.

"Our governmental customers are now required to operate very far from home. If a navy or coast guard was looking at incoming ships, they're now using our technology to a larger extent to identify, monitor and manage risks, patterns and anomalies 5,000 miles away from home," says Daniel.

Orca AI

Tel Aviv-headquartered navigation and collision avoidance company Orca AI, one of three leaders in this sector worldwide, has signed its first deal with an unnamed "prominent navy" to implement its vision-assistance technology.

Orca AI's situational awareness platform uses machine learning and computer vision to enhance navigational safety in low-visibility conditions and high-risk regions where traditional systems may fall short.

At times, navy vessels must deactivate radar and other electronic systems to maintain operational security. Orca AI's technology allows target detection without relying on radar, explained Yarden Gross, Orca AI's cofounder and CEO.

"Orca AI enables proactive threat mitigation for military assets from diverse threats such as piracy, terrorism and airborne/marine drones by empowering personnel to anticipate and counteract these risks, bolstering vessel security and protecting crews and sensitive cargo," Gross said.

Captain's Eye

Captain's Eye of Haifa secures merchant vessels with AI vision technology that can detect and alert the crew and the onshore ship management company to safety and security events, including accidents, environmental pollution, fires and leakages, in real time.

CEO Uri Ben-Dor, a retired naval captain, said the Captain's Eye system is adjustable to each client's needs. "We are doing pilot projects with top-10 shipping companies," he tells ISRAEL21c.

Japanese shipowner Mitsui OSK Lines (MOL) will install Captain's Eye in the cargo holds of 10 new liquid natural gas-fueled car carriers to provide early smoke-detection capabilities. Images of the cargo hold can be viewed from both the vessel and on land, leading to a faster response in case of fire.

Freightos

Jerusalem-based shipping logistics company Freightos offers a booking and payment platform for global carriers, trade companies and importers.

"As a result of that, we have a lot of data providing real-time visibility into how the crisis is impacting various organizations, pricing and transit times," says Freightos CMO Eytan Buchman. "We've seen a massive spike in interest for that data, three times higher this week than a month ago."

Freightos data is helping multinationals like Mitsubishi and UPS make better decisions based on real-market conditions in specific shipping lanes.

"Maybe instead of shipping from China to the US East Coast they can ship to the West Coast in a shipping lane that goes directly across the Pacific," says Buchman.

"We provide tools to trace out and book those shipments and help companies shift between air and ocean freight when it makes more sense."

It all comes down to security, he says.

"Security for ships has always been an issue. Ironically, the Horn of Africa was always the less safe route and right now it is safer."

Abigail Klein Leichman is a writer and associate editor at ISRAEL21c.

Gunfire, Screams, Carnage: As Mass Shootings Proliferate, Training Gets More Realistic

By Matt Vasilogambros

Source: https://www.homelandsecuritynewswire.com/dr20240212-gunfire-screams-carnage-as-mass-shootings-proliferate-training-gets-more-realistic

Feb 12 – The pop-pop-pop of gunfire cracked just as the rain started to fall in grisly synchronicity. Then the screams began.

Within moments, civilians lay strewn across the ground, some lifeless, others writhing in pain. Blood flowed in streams that pooled with the rainwater on the muddying ground littered with shell casings.

Three gunmen quickly opened fire on a San Diego County Sheriff's Department armored BearCat truck arriving in response. It crawled along an alleyway. Half a dozen SWAT members pointed rifles into open doorways or fired back from behind corners.

One assailant, wearing black gloves and a graying black beard, stood on a third-floor apartment balcony and, as deputies came closer, threw a Molotov cocktail at two white cars parked below. The explosion sent a blast of heat and sound, its boom punctuated by the gunman's AK-47.

"Help me!" bellowed a man rolling on the ground, blood shooting from his severed leg. Another man groaned next to him, hidden by smoke billowing around the cars.

It seemed like something out of an action movie. And, in a way, it was.

The rounds were blanks, the Molotov cocktail wasn't lit, the smoke came from a machine. The explosion was controlled, the victims and gunmen were actors, and the blood was fake. However, the deputies, firefighters and doctors from across the region were real. They were in the middle of a simulation on a Saturday afternoon in mid-January in a commercial lot on the north end of San Diego, conducted by Strategic Operations, a local company run by former Hollywood producers and military combat veterans.

First responders and law enforcement agents have for decades used simulations to train for mass casualty events such as shootings or natural disasters, especially after the Columbine school shooting in 1999. But in recent years, as mass shootings have become increasingly common in the United States, the simulations have become more and more realistic. Now they feature visceral sound effects, trained actors, pyrotechnics and even virtual reality. The trainings also have become more and more expensive for public agencies.

But hyper-realistic simulations are essential for learning how to respond to an active shooter, triage mass casualties and coordinate among departments in a chaotic environment, said Sgt. Colin Hebeler, who works in the Infrastructure Security Group within the San Diego County Sheriff's Department. The department has two facilities where deputies go through similar simulation training.

"If we can provide these trainings that are as close to the real-life event as possible, you will actually induce that same kind of stress and the reaction that you might have during a real-life incident," he told Stateline.

Stop the killing, stop the dying

Training has evolved in Hebeler's 16 years in the department, expanding well beyond both the classroom and limited simulations that involved plastic pieces that looked like guns and shouts of "Bang, bang." Although expensive, simulated mass shootings are far more intense, realistic and frequent now, he said.

"If it does happen, we're going to be prepared," Hebeler added. "We don't want this to be one of those catastrophic events that comes out on the news, and everyone says, 'Well, the law enforcement messed up.'"

Law enforcement agencies continue to face public scrutiny over how they respond to mass shooting events — highlighted by last month's scathing report from the U.S. Department of Justice on the response to the 2022 school shooting in Uvalde, Texas, that left 21 people dead, all but two of them elementary school children.

First responders are trained to focus on two things in a mass shooting event: Stop the killing and stop the dying. By waiting 77 minutes outside the fourth grade classrooms where the active shooter was before confronting and killing him, Uvalde law enforcement failed to follow protocols and that cost lives, the federal report found.

Uvalde showed "layer upon layer upon layer of failures," said Jaclyn Schildkraut, executive director of the Regional Gun Violence Research Consortium at New York's Rockefeller Institute of Government. Simulations highlight the sights, sounds and smells of an active shooter event in a controlled environment so the failures seen in Uvalde don't occur, she said.

"It doesn't matter if you're the first officer or by yourself or there's 20 of you, you go in and you stop the shooter, and then you start trying to help the people who've been injured," she said.

"Simulations are really about acclimating you to what you might encounter on that given day, so that you are able to maintain that focus and subsequently your safety as best as possible."

But she wanted to be clear about one point: This kind of training should never be used in schools among children. It is far too traumatic.

Simulation's increased use

Seventeen miles east of downtown Raleigh, North Carolina, Wake Technical Community College is building a 60,000-square-foot facility with an 8-acre driving pad that is dedicated to reality-based simulation training for police, fire and emergency medical workers.
From the outside, observers wouldn't realize the massive gray complex is full of buildings and streets, with spaces designed to mimic the commercial, jail, residential and school spaces first responders would experience in their communities. Trainees can drive into the facility, pull up to a specific location inside and respond to the simulated event — a school shooting, for example, or a fire inside a supermarket.
During mass shooting simulations, trainees will experience the disaster through all their senses: It could smell like smoke, there might be flashing lights and sirens, role players may act as screaming victims or use simulated munitions filled with paint. The $60 million facility, which is slated to open this spring, was funded by a bond that Wake County voters approved in 2018.
For officers, simulation training is much more effective than shooting at a line of paper targets, or simply going over shoot/don't-shoot scenarios, said Jamie Wicker, provost of public safety education at Wake Tech. Training for mass shooting events has developed over many years with the help of veterans who served in Afghanistan and Iraq, she added.
"It's one thing to describe chaos. It's completely different to experience chaos," said Wicker, who has been in law enforcement for more than 20 years, in part as a trainer. "This is managed chaos."
This approach has been backed up by researchers who have studied the effectiveness of simulation training for first responders.
One driving factor of that effectiveness is re-creating the high-stress physiological effects, such as an increased heart rate, said Colby Dolly, the director of science and innovation at the National Policing Institute, a Virginia-based research nonprofit.
When officers respond to a mass shooting, they're running, maybe up a flight of stairs or while carrying people. They will see victims who are injured or dead. They will be worried about the shooter's location. Meanwhile, parents may be rushing to the scene, along with additional first responders from agencies across the region who might not have interacted with one another before.
While an increased heart rate can produce positive reactions such as adrenaline and sharpened senses, it can quickly turn negative, leading to tunnel vision, auditory exclusion or impaired judgment, Dolly said.
"You want to, at some level, induce that in a training environment," he said. "It conditions the officer to inoculate them from being overwhelmed by all that when the time comes."
For the past decade, federal law enforcement has viewed the Advanced Law Enforcement Rapid Response Training Center, known commonly as the ALERRT Center, as the national standard for active shooting simulation training. Hundreds of thousands of police officers have received training from the center, which was formed in the wake of Columbine and has been housed at Texas State University since 2002.
Funded by a line item in the Texas state budget and federal grants, ALERRT is mandated to train 80,000 Texas officers every two years at its facility in San Marcos — a city between Austin and San Antonio. But center experts also go to all 50 states to spread their training, going to schools during breaks and to businesses, at no cost to trainees or their agencies.
Sometimes they use local drama students to play victims, wearing makeup and moulage, simulating a wound. "They love it," said Larry Balding, external resources director with the center.
For the training, ALERRT likes long hallways and T intersections — stress points for law enforcement responding to an active shooter.
Beyond learning how to stop the shooter, trainees focus on getting victims to an operating table. Gunshot victims only have around 30 minutes before it's too late, said Balding, who used to be in the fire service.
"Nobody will ever be 100% ready," he said. "But if you can get a new officer, get him trained, trying to get the mindset right, that's what we want to do."
When asked where simulation training is heading in the field of first responders, Balding didn't hesitate: virtual reality.
Training in the virtual world
The floor of the San Diego Convention Center was filled with lifelike mannequins — bleeding, blinking, moving and able to be poked and prodded and to respond to questions. Some were even pregnant, with a baby ready to squirm out when prompted.
Among the 140 health care presenters last month at a conference organized by the Society for Simulation in Healthcare, a membership nonprofit that seeks to promote simulation training to reduce errors in medical care, were companies that want to take the industry in a whole new direction with virtual reality.
Whether first responders use Oculus headsets to learn how to interact with patients in an emergency room or use lifesaving tools at the scene of a shooting, localities are turning more to virtual reality training for first responders, said Dr. Barry Issenberg, president of the society.
"It's the reduction of errors, safer care, safer way of training," said Issenberg, who is also the director of the Gordon Center for Simulation and Innovation in Medical Education at the University of Miami. "What we're doing is not just a cool idea, but ultimately going to make an impact for their constituents."
The society worked with the Hollywood-style facility, which organized the simulation for the San Diego County Sheriff's Department and other local first responders who participated the day before. Around 100 visiting academics and health care workers in town for a conference were among the onlookers.

While researchers have found in several studies that virtual reality can add some benefits to health care training, there is still some skepticism.

Dolly, at the National Policing Institute, sees "some promise" with virtual reality for training police officers. It can be a cost-effective alternative to in-person simulations and can help officers train in shoot/don't-shoot scenarios.

However, he does see limitations with not being able to run around and experience viscerally the confusion of a mass shooting, which can be fully felt with an in-person simulation.

Back at the San Diego shooting simulation, screams still pierced the air.

Gunfire continued for another minute, as the seven deputies dashed from room to room in the complex of buildings. They killed the shooters, then carried some of the wounded down flights of stairs.

After the shots finally stopped, the screams of victims were nearly drowned out by the wail of ambulance sirens.

Firefighters and emergency medical technicians rushed bloodied victims in stretchers to nearby pop-up emergency and operating rooms, where Navy doctors tried to keep their footing on floors slippery with blood and worked to close victims' wounds.

Wearing blue scrubs and shoe coverings, doctors turned victims on their side and searched for exit wounds. One demanded O negative blood.

An hour after the first shots rang out, the simulation ended. The first responders gathered in the ER in a semicircle. An instructor quieted the room, asked for the beeping heart monitors to be shut off and turned to the participants.

"So, what did we learn?"

Matt Vasilogambros covers voting rights, gun laws and Western climate policy for Stateline.


ICI
International
CBRNE
INSTITUTE
A common roof
for International
CBRNE
First Responders
Join us!
Rue de la Vacherie, 78
B5060 SAMBREVILLE
(Auvelais)
BELGIUM
info@ici-belgium.be | www.ici-belgium.be