C²BRNE DIARY

Dedicated to Global First Responders

ICI International CBRNE INSTITUTE

10\23

October 2023

PART B

From lone wolves to terrorist pogrom

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

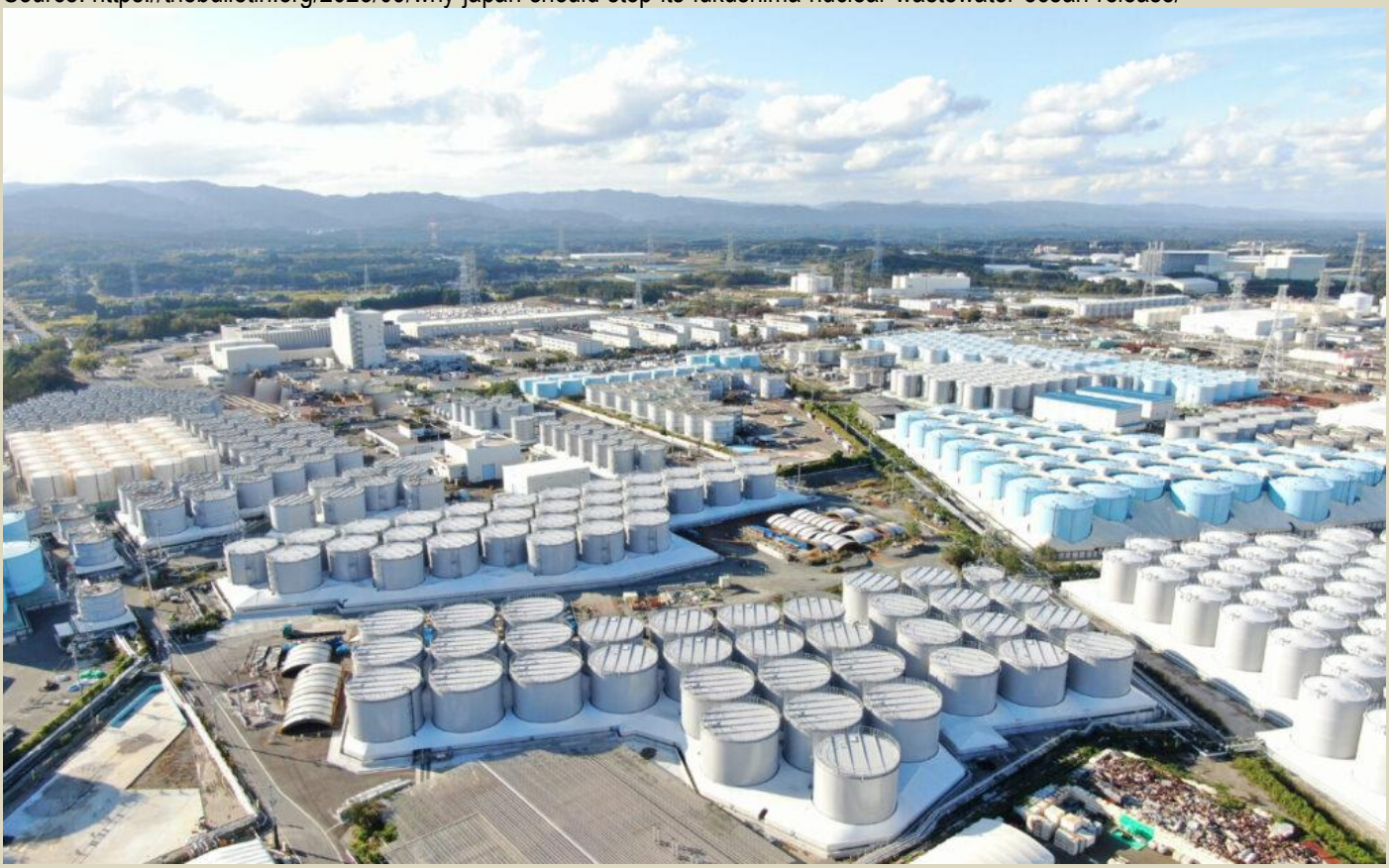
DIRTY R-NEWS

C2BRNE DIARY

Why Japan should stop its Fukushima nuclear wastewater ocean release

By Tatsujiro Suzuki

Source: https://thebulletin.org/2023/09/why-japan-should-stop-its-fukushima-nuclear-wastewater-ocean-release/



Water tanks holding contaminated water at Fukushima Daiichi nuclear power plant in Japan. (Credit: IAEA)

On August 24, 2023, Japanese electric utility holding company Tokyo Electric Power Co. (TEPCO) announced that it has started discharging so-called "treated" and "diluted" water from the damaged Fukushima Daiichi nuclear power plant into the Pacific Ocean.

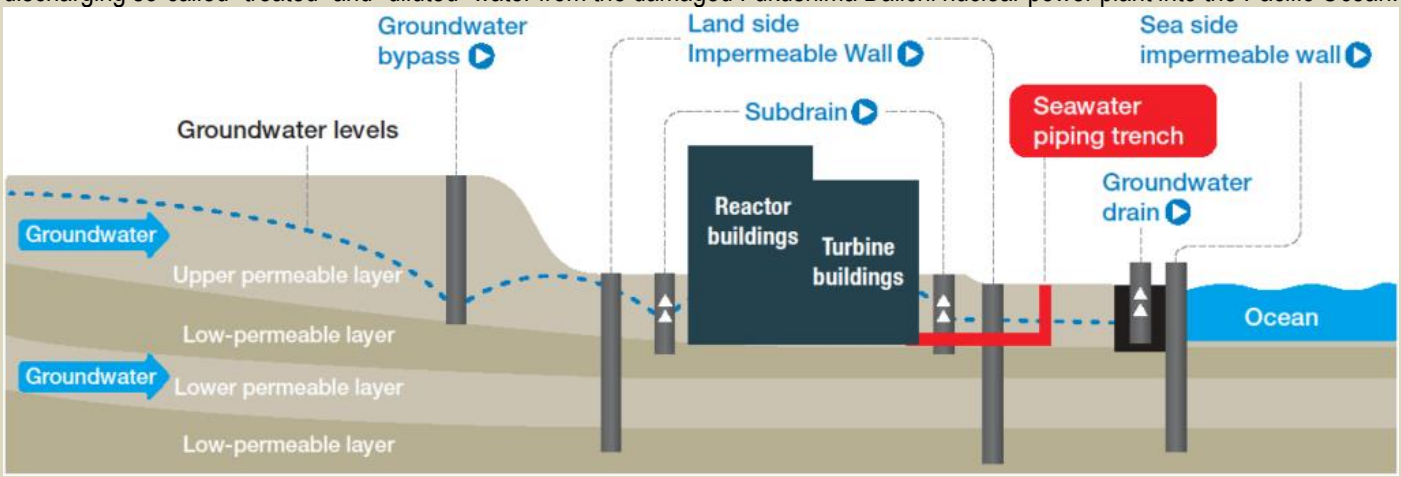


Figure 1. Groundwater flow through the Fukushima Daichi nuclear power plant before treatment. (Credit: IAEA)

This is not the end of controversy over the release of "treated water." Rather, it may be the beginning of what might be a long-lasting struggle where science meets politics and lack of public trust, both inside and outside of Japan. To understand TEPCO's decision and why this operation caused such a big controversy, one must explain what this "treated water" being released is, the scientific debates over this operation, and the underlying social and political issues.

"Treated" or "contaminated" water?

When underground water, including rainfall, passes through the damaged Fukushima Daiichi reactor site and is used to cool the melted fuel debris inside the reactors, it becomes contaminated with oil as well as many harmful radioactive nuclides, including cesium and strontium. Generation of "contaminated water" has been gradually declining due to various measures, such as pumping up water by sub-drains and the construction of impermeable, land-side frozen walls (see Figure 1). According to TEPCO, contaminated water generation declined from 540 cubic meters (m^3) per day in 2014 to 90 m^3 per day in 2022.

Part of the radioactive substances that contaminate the water is now being removed by multi-nuclide removal equipment called "advanced liquid processing systems" (ALPS)—an unfortunate name given that the Alps mountain range in Europe is home to some of the cleanest freshwater in the world. After the removal of most radioactive substances—except for tritium, which cannot be removed by the Alps system—treated water is then stored in tanks (see Figure 2). The Alps process is supposed to reduce the concentration of radionuclides, except tritium, to levels below regulatory standards. However, according to TEPCO's data, as of March 31, 2023, of the total of about 1.3 million m^3 of treated water, only about a third satisfied regulatory standards and the other two-thirds needed to be re-purified.

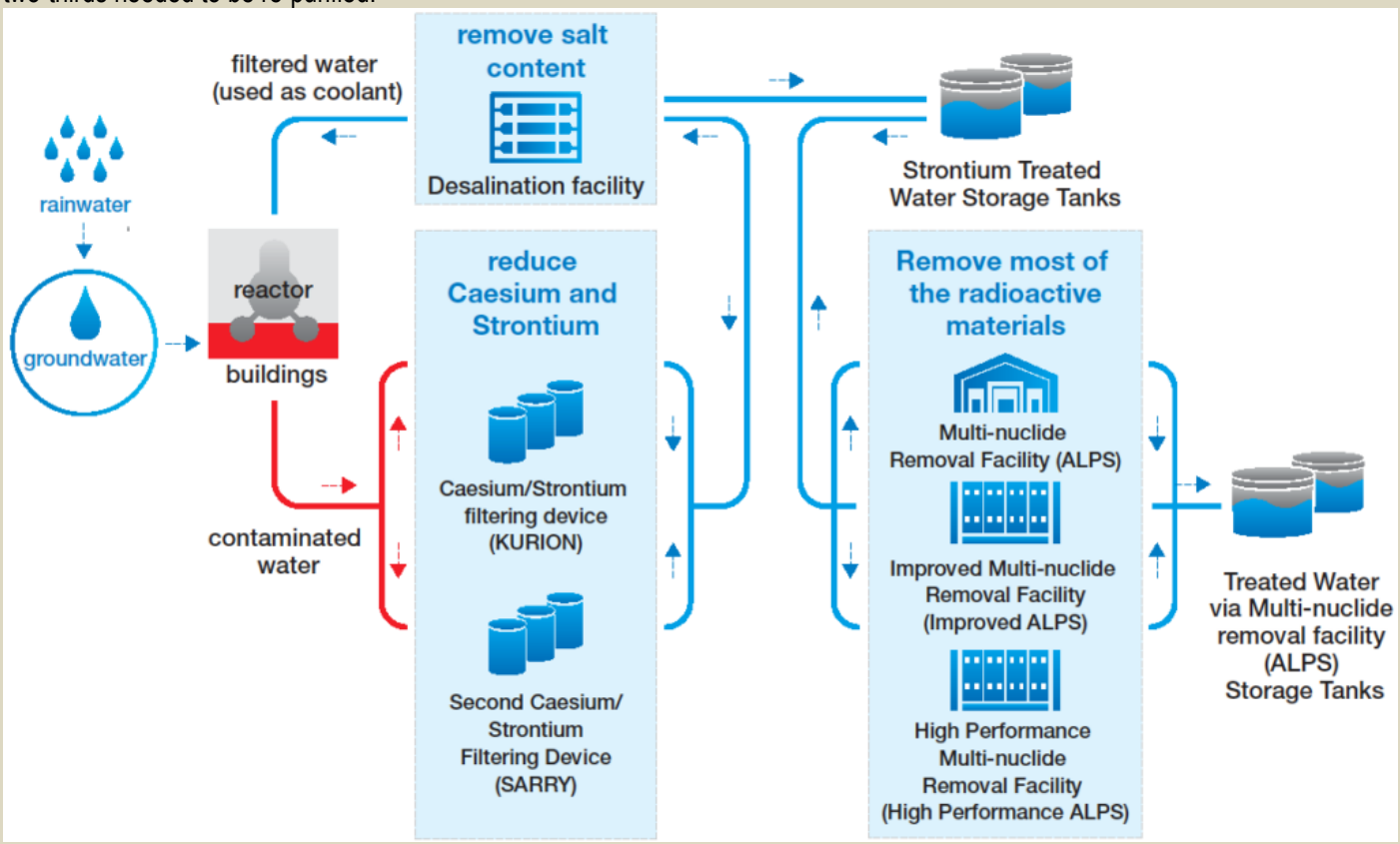


Figure 2. Depiction of the so-called Alps process treating contaminated water at the Fukushima Daichi nuclear power plant. (Credit: IAEA)

It can't be denied that "treated water" is not as pure as "tritiated water" because treated water may still contain other radioactive nuclides, albeit in small proportions. But the comparison of Fukushima's "treated water" with other "tritiated water" released during the normal operation of other nuclear power plants can be misleading because the latter is not contaminated with other radioactive nuclides.

TEPCO says it re-purifies the "treated water" to make sure the water satisfies regulatory standards before it is released to the sea. To do that, the company's plan is to dilute "treated water" with large amounts of sea water to reach a concentration of tritium of 190 Becquerel (Bq) per liter, which is much lower than the allowed concentration of 1,500 Bq per liter.

The first discharge happened over a period of 17 days and involved a total of 7,800 tons of treated water being released to the sea. TEPCO plans to discharge treated water three more times in 2023, and the total tritium discharge by the end of March 2024 is expected to reach about 5 trillion Bq. This is much lower than the annual discharge target of 22 trillion Bq set before the Fukushima accident.

In addition to tritium, TEPCO must report that the concentration of all other radionuclides is below regulatory standards. To do this, TEPCO uses a simplified index, which corresponds to the sum of ratios of the concentration of each radioactive nuclides (excluding tritium) compared to regulatory standards. If this ratio is below one, it means the concentration of other radionuclides is below regulatory standards. TEPCO reported that the water being discharged during the first period was measured to have an index of 0.28, therefore satisfying regulatory standards. TEPCO said the operation may last at least 30 years to discharge all "treated water."

Scientific debate

The Japanese government and TEPCO argue that the whole operation satisfies both Japanese regulatory standards and international safety standards. Besides, the Japanese government officially asked the International Atomic Energy Agency (IAEA) to conduct an independent review of the safety of the ALPS treated water release. On July 4, 2023, the IAEA published its "comprehensive report," which concluded that the ALPS process is "consistent with relevant international safety standards" and that "the discharge of the treated water [into the sea], as currently planned by Tepco, will have a negligible radiological impact on people and the environment." But there are scientific arguments against TEPCO's release plan.

The Pacific Island Forum expressed its concern in a statement in January 2023 about whether current international standards are adequate to handle the unprecedented case of the Fukushima Daiichi tritiated water release. Based on a report from an independent expert panel established by the forum, TEPCO's guideline compliance plan does not appear to include the transboundary implications of IAEA's guidance in its General Safety Guide No. 8 (GSG-8), which requires that the benefits of a given process outweigh the harms for individuals and societies.

The experts also recommended the alternative method of using the treated water to manufacture concrete for the construction industry instead of releasing it to the sea. By immobilizing the radionuclides in a material, this alternative would imply a lower potential for human contact and would avoid transboundary impacts. Quoted in a *National Geographic* article, one of the panel members, Robert Richmond, director of the Kewalo Marine Laboratory of the University of Hawaii, summarizes well the uncertainty surrounding the impacts of TEPCO's water release plan on the ocean environment: "It is a trans-boundary and trans-generational event" and that he does not believe "the release would irreparably destroy the Pacific Ocean but it does not mean we should not be concerned."

Lack of public trust

In addition to scientific debate, TEPCO's ALPS treated water issue has become more of a social and political controversy. The origin of this debate was the speech given by then-Prime Minister Shinzo Abe before the International Olympic Committee on September 7, 2013, in which he referred to the city where the 2020 Summer Olympics were to be held by saying: "Some may have concerns about Fukushima. Let me assure you, the situation is under control. It has never done and will never do any damage to Tokyo." After Abe's speech, the government took over the responsibility for the management of the contaminated water, while TEPCO is still responsible for all decommissioning operations at the Fukushima Daiichi nuclear power plant. Since then, all policy decisions about the treated water have been made by the Japanese government, with TEPCO simply following the government, which has complicated the decision-making process.

In August 2015, the Japanese government and TEPCO promised to the local fishermen that they "will not implement any disposal without understanding of interested parties." The government even established a committee consisting of experts from a local university to discuss technical options and held meetings with local citizens for several years to build trust with the local communities. So, when the decision was made by former Prime Minister Yoshihide Suga in August 2021 to release the "treated water" to the sea, this felt like a treachery for the local fishermen and many other interested parties. In a June 2023 statement opposing the planned discharge of treated water, the head of Japan's national fisheries cooperatives Masanobu Sakamoto said: "We cannot support the government's stance that an ocean release is the only solution. … Whether to release the water into the sea or not is a government decision, and in that case we want the government to fully take responsibility."

The subsequent lack of public trust in TEPCO and Japan's Ministry of Economy, Trade and Industry has been one of the major reasons for this continued controversy. In August 2018, a news investigation revealed that the "tritiated water" still contained other radioactive nuclides after treatment, which were above regulatory standards—a result that was not consistent with the explanation given by TEPCO. The justification then advanced by the ministry and TEPCO on the need and timing for the water discharge was no more convincing: They claimed that there would be a need for storage space once the melted fuel debris would be taken out of the reactors and that, without discharge now, the plant's storage area would be filled soon. But, the timing—and even the feasibility—of removing the fuel debris is not known at all. Besides, there are potential storage space available at the nearby Fukushima Daini nuclear power plant.

Concerns have also spread to neighboring countries despite the Japanese government's efforts to explain its plan. For instance, the South Korean government even sent some of its experts, including senior officials of the South Korean Nuclear Safety and Security Commission. Seemingly reassured after the visit, Yoo Guk-hee, the chairperson of South Korean commission, declared: "[I]f the water release is carried out

as planned, the discharge standard and target level (of radiation) would be consistent with international standards". Still, both fishermen and consumers in South Korea are worried about the impacts of water release from the Fukushima nuclear plant, which led the largest fisheries market to start monitoring the fish's radioactivity to allay those concerns.
Building upon the South Korean experts' visit, the Japanese government called for a science-based dialogue with the Chinese government, complaining that it continued to describe the Fukushima treated water as "contaminated" water. But the Japanese government's effort seems not to have been successful, with a spokesperson of the Chinese Foreign Ministry saying that Japan has yet to prove that its planned water discharge is safe and harmless. In August, China decided to ban imports of all seafood products from Japan shortly after Japan started discharging treated water from Fukushima that month. And there seems to be no prospect of reducing tensions between the two countries over this issue.

How to improve the situation?
Several options exist that could help restore public trust in TEPCO's and the Japanese government's treated water plan at Fukushima.
First, the Japanese government and TEPCO should realize that the management of radioactive wastewater is not a purely scientific and technical issue. Public controversies of this sort cannot be resolved by "science-based" dialogues only. Yes, a scientific dialogue is essential, but it's not enough. Rather, Fukushima's treated water is a typical case of "trans-science" using Alvin Weinberg's term, meaning an issue where "questions which can be asked of science and yet *which cannot be answered by science*" (Weinberg's emphasis). TEPCO's and the Japanese government's plan also needs a non-scientific approach to the issue and provide additional measures, including an improved decision-making process and a sincere dialogue (not persuasion) with stakeholders.
Second, to restore public trust and confidence, the government should first stop the water release and task an independent oversight organization which can be trusted by stakeholders. The IAEA review of TEPCO's plan was helpful at best, but it was not enough, as it only verifies the samples provided by TEPCO for the first discharge but does not review the entire plan which could continue for the next 30 years. In fact, IAEA Director General Rafael Mariano Grossi clarified in the foreword of the agency's "comprehensive report" that the review was "neither a recommendation nor an endorsement of that (government) policy." Complete transparency over the entire decision-making process and disclosure of supporting data and information are essential conditions to improve public trust.
Third, TEPCO and the Japanese government should designate the current release operations as part of a "demonstration" program and declare that they will make a final decision about the plan after studies confirm that the release has had no significant impacts on the ocean environment and fish. This would imply that the government stops the release of the treated water, and asks the scientific community to conduct such studies. At the same time, the government could also continue to explore technical alternatives to its plan that may be more attractive to both domestic and international stakeholders. In addition to provide a face-saving opportunity to the Japanese government and TEPCO to justify that they "temporarily" halt the release, it would show that they have sincerely listened to the concerns expressed by the stakeholders.
The Japanese government and TEPCO clearly have the ability to improve public trust in their handling of the treated water at Fukushima, but this requires them to go beyond their "scientific logic" only.

Tatsujiro Suzuki is vice director and professor at the Research Center for Nuclear Weapons Abolition at Nagasaki University, Japan. He is former vice chairman of Japan's Atomic Energy Commission, and now a member of the Advisory Board of Parliament's Special Committee on Nuclear Energy since June 2017. Dr. Suzuki has a PhD in nuclear engineering from Tokyo University (1988).

●▶ **Read also: Fukushima Water Discharge: The Science Behind the Decision**

Is Myanmar About to Go Nuclear?

By Andrew Selth
Source: https://www.homelandsecuritynewswire.com/dr20230927-is-myanmar-about-to-go-nuclear?page=0,1

Sep 27 – A front-page story in the *Sydney Morning Herald* in 2009 confidently predicted that within five years Myanmar would have its own nuclear weapon and be capable of producing one atom bomb every year thereafter, if all went according to plan. The story, by two respected Myanmar watchers, was based on the claims of a military 'defector', but followed years of rumours, gossip and speculation.
As history has shown, this prediction was spectacularly wrong. If Myanmar's military government was ever contemplating a nuclear weapons program—and some observers still argue that it wasn't—the scheme

had barely reached the experimental stage. Following the *Herald* story, the International Institute for Strategic Studies wrote that Myanmar 'has no known capabilities that would lend themselves to a nuclear weapons program'.

Two years later, the US government said that, despite concerns that North Korea might be willing to transfer sensitive nuclear technologies to Myanmar's military regime, it saw no signs of a major nuclear weapons program. Other governments agreed, and there the matter seemed to rest. International concerns, where they existed, were assuaged further in 2011 by the transfer of power to an unexpectedly reformist quasi-civilian government.

Between 2015 and 2020, Aung San Suu Kyi's government took important steps in this field. In 2016, Myanmar ratified the Comprehensive Nuclear-Test-Ban Treaty, which it had signed in 1996. The same year, it acceded to the Convention on Nuclear Safety and the Convention on the Physical Protection of Nuclear Material. In 2018, it signed the Treaty on the Prohibition of Nuclear Weapons. All these instruments made clear the National League for Democracy's opposition to the manufacture, testing and use of nuclear weapons.

Despite all these measures, however, the specter of the world's first 'Buddhist bomb' still hangs over Myanmar. It has been given impetus by the coup in February 2021 and the military regime's increasingly close relations with Russia. More to the point, perhaps, fears of a new clandestine nuclear weapons program are being stoked by pro-democracy activists, who are keen to blacken the junta's name and garner additional international support. Once again, the situation in Myanmar demands careful analysis of the available information and sober judgements.

Myanmar's military leadership has long been attracted to the idea of nuclear energy. In 2000, for example, it was announced that Myanmar planned to purchase a small reactor from Russia 'for peaceful research'. The deal collapsed in 2002, but in 2007 Russia signed an agreement with the ruling State Peace and Development Council to build a nuclear studies center comprising a 10-megawatt reactor and two laboratories. It would also provide training in Russia for Myanmar technicians.

A memorandum of understanding to this effect was signed in 2015, but no reactor was ever built, contrary to the claims of activists that as early as 2010 construction had actually been completed on three reactors in Myanmar's north.

From 2003, however, it was Myanmar's shadowy relationship with North Korea that raised the most concerns regarding the transfer of nuclear technology. These fears were fueled by claims made by a few 'defectors', some ambiguous 'evidence' and a flood of tendentious reporting on the subject. Despite signs suggesting that any nuclear program was in its early stages, and was being badly mismanaged, some observers were prepared to believe the worst. This led to the dramatic *Herald* story in 2009.

Since the 2021 military coup, the junta has clearly considered its nuclear options. When Commander-in-Chief Min Aung Hlaing was in Russia in July 2022, he reportedly discussed 'the peaceful use of nuclear energy' with his Russian interlocutors. In February, the junta signed an agreement for Russia's Rosatom State Atomic Energy Corporation to build a small modular reactor in Myanmar. In June, the two countries signed a preliminary agreement to cooperate in the peaceful use of nuclear energy.

Interestingly, the junta has called upon China to share its advanced nuclear technology. This was reportedly to assist in various civil fields. The junta has also re-established ties with North Korea, which were downgraded by Aung San Suu Kyi's government, probably in response to US pressure. Inevitably, both moves have been seen by some as nuclear-weapons-related, but so far no credible evidence has been offered to sustain such a view.

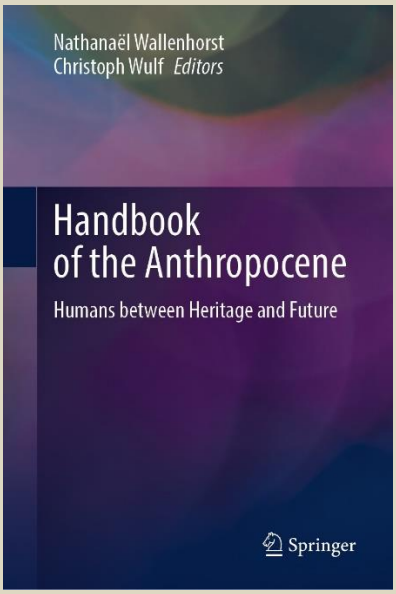
While the goal of Myanmar's nuclear program has never been clear, there have always been public references to Myanmar's increasing energy consumption and need for more reliable power generation. Given the country's ample gas reserves and potential for hydroelectricity, that rationale has never been persuasive. References to the use of nuclear technology in the agricultural and health sectors have been equally vague. The lack of an adequate explanation for a nuclear plant has left the field open to accusations that the junta has more nefarious plans.

Indeed, a recent news story reported that 'Myanmar's political opposition and military analysts have expressed concern that the [Russian nuclear] technology could be leveraged militarily'. Such warnings need to be kept in perspective. How nuclear technology might be used in such a fashion has not been spelt out, and already the imagination of some commentators is running well ahead of the situation on the ground.

It is not enough to say, as some activists have, that the junta is inherently evil and has already demonstrated a readiness to do anything to stay in power, and then leap to the conclusion that it plans to build a nuclear weapon. Also, it has yet to be explained how a nuclear weapon could possibly assist the

junta to defeat its enemies, almost all of whom are based in Myanmar itself, and pose the kind of threats that can't be removed by possession of such a device.
It has been suggested that a nuclear weapon would help the military regime keep its foreign enemies at bay and win various concessions, as North Korea has done for many years. Yet, the junta doesn't face a significant threat from the international community. Most of the sanctions imposed to date are largely symbolic, and no country is going to invade or use military force to support the opposition movement. In any case, if pressed, the junta could always turn to Russia and China for support.
Having said all that, the question must still be asked: why is the junta expending precious resources on a nuclear reactor of arguable utility when it is already struggling with a costly civil war, an economy in dire straits, the collapse of government services and widespread poverty and hardship? Status and a wish to strengthen relations with Russia may be elements in the mix, but they alone are unlikely to account for the measures taken to date.
International responses to the junta's nuclear deal with Russia have been relatively muted. The US has expressed its concerns, but they are more about the support being provided to the regime than about the nuclear aspects. The attitudes of other countries aren't known but most seem to be watching and waiting to see what, if anything, eventuates. The International Atomic Energy Agency has yet to reveal whether the proposed new reactor will be built under its customary safeguards.
Significantly, no government or international organization has raised the bogey of a Myanmar nuclear weapon. They have doubtless learned the lessons of the past, and are reluctant to leap to any conclusions, particularly when evidence for such a program is lacking. That hasn't stopped activists and popular pundits, however, from sounding warnings which, from an analytical viewpoint, must be seen as premature, at least.

Andrew Selth is an adjunct professor at the Griffith Asia Institute at Griffith University. His latest major work is Intelligence and intelligence agencies in Myanmar since the 2021 coup.



Nuclear Waste

By Christine Eriksen and Stephen Herzog
Handbook of the Anthropocene pp 1521–1525 (Chapter)
Source: https://link.springer.com/chapter/10.1007/978-3-031-25910-4_247

Abstract
Nuclear waste epitomizes the Anthropocene. Scientific discovery of nuclear fission in the 1930s ushered in the atomic age. The onset of nuclear weapons and nuclear energy production in the 1940s and 1950s then created a uniquely human problem with planetary implications. Today, 33 countries operate 442 nuclear power reactors, and nine countries possess nearly 13,000 nuclear arms. The result is high-level waste that is dangerously radioactive for millennia to come. Yet, there has *never* been a permanent waste solution in place. Technically feasible long-term nuclear waste storage options exist, but nearly all governments prefer riskier interim plans hidden from public view and debate. This chapter considers the likelihood of societies addressing the contentious environmental and economic politics of deep geological repositories; and it asks, how long will obfuscation of the risks of this unique Anthropocene challenge continue?

US report: Iran can make a nuclear weapon in less than two weeks

Source: https://www.israelnationalnews.com/news/377748

Oct 02 – Iran is not pursuing nuclear weapons at this time but has the infrastructure in place and the know-how to make a nuclear weapon in less than two weeks, a new US report finds.
"It is assessed that Iran is not pursuing a nuclear weapons program at this time, but has the capacity to produce enough fissile material for a nuclear device in less than two weeks," said the US Department of Defense's 2023 Strategy for Countering Weapons of Mass Destruction report, as quoted by *JNS*.
"Further, the United States assesses Iran to be noncompliant with its CWC [Chemical Weapons Convention] obligations. For example, Iran has not submitted a complete chemical weapons production facility declaration to comply with CWC processes. The United States is also concerned that Iran is pursuing dual-use central nervous system-acting chemicals for offensive purposes," added the report.

In August, it was reported that Iran has significantly slowed the pace at which it is accumulating near-weapons-grade enriched uranium and has diluted some of its stockpile. The International Atomic Energy Agency (IAEA) confirmed those assessments in a report published last month.
In February, CIA Director William Burns acknowledged that Iran has advanced in its uranium enrichment, but also said there's no evidence it decided to resume its weaponization program.
Iran recently caused an uproar among Western nations after it decided to ban several IAEA inspectors from the country.
The IAEA was responsible for verifying Iran's compliance with the 2015 Iran nuclear deal, under which Tehran curbed its nuclear program in return for the easing of US, European Union and UN sanctions.
In 2018, then-US President Donald Trump withdrew from the agreement and reimposed sanctions on Tehran.
Iran responded to Trump's withdrawal from the 2015 nuclear deal by scaling back its compliance with the agreement.
The Biden administration sought to return to the deal and held indirect talks with Iran on a return to compliance, but the negotiations reached a stalemate last September, after Iran submitted a response to a European Union proposal to revive the deal. A senior Biden administration official said the Iranian response "is not at all encouraging."
A US official later said that the efforts to revive the 2015 Iran nuclear deal have "hit a wall" because of Iran's insistence on the closure of the UN nuclear watchdog's investigations.
Last week, US State Department spokesman Matthew Miller said Iran must take "de-escalatory" steps on its nuclear program if it wants to make space for diplomacy with the United States.

EDITOR'S COMMENT: No surprise! But it could be a good excuse for countermeasures. Let's hope that logic will prevail in all parts interested or threaten.

Putin's "bluff": a cautionary note about underestimating the possibility of nuclear escalation in Ukraine

By Stephen J. Cimbala, and Lawrence J. Korb
Source: https://thebulletin.org/2023/10/putins-bluff-a-cautionary-note-about-underestimating-the-possibility-of-nuclear-escalation-in-ukraine/

Oct 02 – Timothy Snyder, the widely acclaimed Yale University historian and expert on conflict in the bloodlands of Central and Eastern Europe, recently wrote an important essay on the status of the war in Ukraine. It offers an insightful analysis of the reasons why the United States and NATO must continue to support Ukraine in its resistance to Russian aggression. He contends that calls for a negotiated settlement of the conflict are premature, and that only a decisive victory for Ukraine will provide a lasting peace and deter Russia from further aggression. As he points out:
The Ukrainians are defending the legal order established after the Second World War. They have performed the entire NATO mission of absorbing and reversing an attack by Russia with a tiny percentage of NATO military budgets and zero losses from NATO members. Ukrainians are making a war in the Pacific much less likely by demonstrating to China that offensive operations are harder than they seem.
Snyder has become a leading Western interpreter of the Russian invasion and Russian President Vladimir Putin's psyche, writing and speaking widely, including to the United Nations. Despite the soundness of his analysis of the current situation with respect to fighting the conventional war in Ukraine, however, Snyder dismisses too abruptly the possibility of Russian escalation to nuclear weapons use. In his judgment, the "nuclear bluff" from Moscow "has largely worn itself out," and the argument that Russia could escalate is a triumph of Russian propaganda; he contends that a more robust Ukrainian conventional military offensive will actually make nuclear war less likely by "demonstrating that nuclear blackmail need not work."
The arguments of Snyder (and others) assume that the United States and NATO have fallen victim to "analysis paralysis" that has created unnecessary concern about escalation, thereby forestalling timely increases in weapons such as longer range missiles, combat aircraft, and other requirements for a more robust counteroffensive against Russian defenses in eastern and southern Ukraine.[1] From this perspective, the United States and NATO should provide as much additional support as quickly as possible to enable a decisive Ukrainian military victory, notwithstanding Russian nuclear coercive diplomacy. Deep-strike systems and information networks provided by Ukrainian allies should, this argument suggests, enable Kiev to strike critical targets inside Russia, including command-control systems, logistics, and military bases and installations, bringing home to Russians some of the costs that Russia has inflicted on Ukrainian forces and civilian infrastructure.[2]

This screen shot from a US Defense Department video clip shows a Russian Su-27 fighter jet flying near an American Reaper drone in March, over the Black Sea near Crimea, spraying what the Defense Department says is jet fuel.

We have three major concerns about this optimism in regard to nuclear risk—concerns that should be loudly raised by policy makers, analysts, and media commentators. First, the United States and NATO cannot and should not assume that Russian reasoning about nuclear deterrence and escalation will follow a logic similar to that of their Western counterparts.[3] Second, escalation need not be the outcome of deliberate forethought: Inadvertent escalation could lead to a crossing of the nuclear threshold under circumstances that were not planned for or foreseen. And third, no one should underestimate what Ukraine and NATO have already accomplished in this war, both in terms of strategy and in policy—significant accomplishments won without provoking nuclear escalation.

The **first concern** is that Vladimir Putin's risk assessment might be different than what NATO observers predict. As US Army Lt. Col. Brandon Colas has noted, from the perspective of what behavioral psychologists call prospect theory, decision makers are more likely to take larger risks to avoid a significant loss than they would to achieve a gain of similar proportions.[4] In this regard, some US and NATO messaging since the beginning of Russia's invasion of Ukraine may have the unintended effect of lowering Russia's threshold for the first use of non-strategic nuclear weapons. Examples include messaging that: conveys ambiguity about a US or NATO response to Russian nuclear first use; implies that a Russian loss in the war against Ukraine will cause the end of Putin's regime; or suggests that Russia will lose great power status in the aftermath of a conventional military defeat. From Putin's perspective, the use of nonstrategic nuclear weapons could restore the deterrent credibility lost from the failure of Russia's conventional military power, remind the world that Russia is still a great power, and shake up expectations about Russia relative to the existing international order.[5]

The **second concern** involves the possibility of inadvertent escalation that results from the fracas of conventional war and the behavior of military forces in conflict zones. For example, US leaders have complained that Russian military aircraft are repeatedly taking "batting practice" against American military airplanes near the conflict zone in and around Ukraine. This includes dangerous fly-bys, jinking and spoofing the opposition with provocative aeronautics and near-miss collisions.

Also, there's an interesting feature of Russia's nonstrategic nuclear weapons inventory: The majority of their so-called tactical nuclear weapons are actually assigned to the Russian navy instead of the ground or air forces. Therefore, the possibility of incidents at sea involving one or more nuclear-armed combatants cannot be ruled out. Russia's recent escalation of its war against civilian shipping in the Black Sea, aiming to deprive Ukraine of its grain exports, creates additional risks of a Russia–Ukraine or NATO–Russia contretemps at sea. Presumably Russian (and NATO) nuclear weapons are kept under positive controls even after having been deployed with forward forces. But sometimes navy admirals and captains are not as easily tethered to higher-echelon micromanagement as are leaders in other branches of the armed services. It is important to remember that, during the Cuban missile crisis of 1962, a Soviet submarine

commander almost fired a nuclear armed torpedo in response to US depth charges; he was stopped by the executive officer on the boat, whose concurrence was required.

A **third factor** weighing against demands for an absolute Ukrainian military victory lies in the recognition that Russia has already suffered a strategic political defeat. Instead of dividing and weakening NATO, Russia's invasion of Ukraine has had the opposite effect. NATO is stronger than any time since the end of the Cold War and has added to its membership the formerly neutral states of Finland and Sweden. Putin has also been branded as an international war criminal and is reluctant to travel anywhere outside of Russia. Following the debacle of the Wagner group uprising, Russia's internal solidarity is full of question marks (notwithstanding the brutal demise of former Putin crony Yevgeny Prigozhin). Admittedly, China and North Korea still support Russia with military aid and political expressions of solidarity, and Russia sees the BRICS forum as an opening for increasing its global influence. Nonetheless, in a best case for Russia in Ukraine, it will have to settle for a negotiated cease fire and a peace agreement that leaves it with less territory in Ukraine than it has occupied—or, even worse, to continue with an extended war that drains its economic resources and military power.

US and NATO aspirations for a Ukrainian military victory are understandable and laudable. But concerns about the possibility of nuclear escalation are not to be dismissed, and they go beyond accepting any obviously tendentious Russian propaganda. In addition to high-end conventional military performance by Ukraine and NATO political unity, another requirement for success in defending Ukraine is escalation control. Russian nuclear threats should not paralyze Ukrainian or NATO determination to persevere in the conventional war, which has existential stakes for Western democracy. But Western leaders should also remember that war is the least predictable of human activities, and nuclear war has unacceptable and irreversible consequences for all of humanity.

Notes

[1] See, for example: Anne Applebaum, "Fear of Nuclear War Has Warped the West's Ukraine Strategy," *The Atlantic*, November 7, 2022, https://www.theatlantic.com/

[2] See, for example: "Ukraine Strikes Headquarters of Russia's Black Sea Fleet," *New York Times*, September 13, 2023, https://www.nytimes.com/live/2023/09/13/world-russia-ukraine-news

[3] Stephen Blank, "Nuclear Weapons in Russia's War Against Ukraine," *Naval War College Review*, v. 75, no. 4 (Autumn 2022), pp. 53-78.

[4] Brandon Colas, "A Rational Choice? Russia's Potential Use of Nonstrategic Nuclear Weapons," *Aether*, V. 2, no. 2 (Summer, 2023), pp. 18-30.

[5] Ibid.

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.

North Korea halts nuclear reactor, likely to extract bomb fuel: Report

Source: https://english.alarabiya.net/News/world/2023/10/05/North-Korea-halts-nuclear-reactor-likely-to-extract-bomb-fuel-Report

Oct 05 – North Korea has halted the nuclear reactor at its main atomic complex, probably to extract plutonium that could be used for weapons by reprocessing spent fuel rods, a South Korean news report said on Thursday, citing a government source.

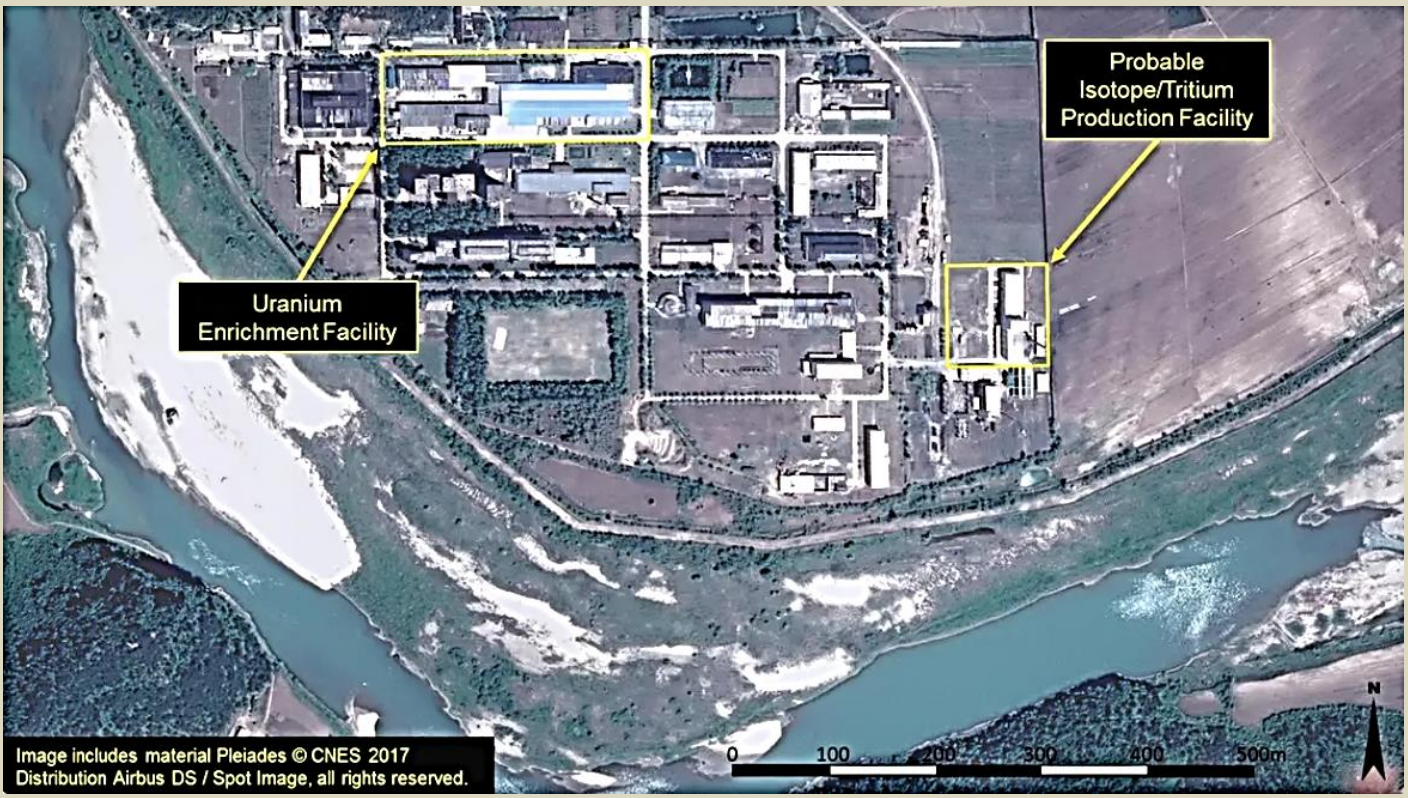
The operation of the five megawatt nuclear reactor at the Yongbyon nuclear complex has been suspended since late September, according to intelligence assessment by US and South Korean authorities, the report said.

"South Korea and the US believe this could be a sign of reprocessing work being done to obtain weapons-grade plutonium," the Donga Ilbo newspaper quoted a government source as saying.

Reprocessing of spent fuel rods removed from a nuclear reactor is a step taken before plutonium is extracted. The Yongbyon nuclear complex is the North's main source of plutonium that it likely has used to build nuclear weapons.

North Korea has also operated uranium enrichment facilities, which is a separate source of material that could be used for nuclear weapons. "The possibility of a nuclear test by North Korea is not ruled out," Donga Ilbo quoted a senior government official as saying, without elaborating on what analysis pointed to the assessment the move may be related to a nuclear test. South Korea defense ministry spokesman Jeon Ha-gyu declined to comment on the details of the report but said US and South Korean intelligence

authorities are closely monitoring related developments. North Korea has previously halted the operation of the reactor before restarting it and public confirmation of the purpose of such a move, whether it is for maintenance or for fuel extraction, is usually unavailable. North Korea claims itself a nuclear state but has kept how many nuclear weapons it may have built or deployed a secret. Independent estimates of the North's plutonium range as high as 70 kg, which could be enough to build 20 or more weapons.



A satellite image of the radiochemical laboratory at the Yongbyon nuclear plant in North Korea by Airbus Defense & Space and 38 North released on July 14, 2017. (Reuters)

US nuclear scientist Siegfried Hecker, who visited the Yongbyon complex in 2010, said despite the time North Korea has spent on the project, its capacity for producing plutonium and also the stock of fissile material itself are still limited.

Russia President Vladimir Putin, who recently hosted North Korean leader Kim Jong Un for a summit and pledged closer military cooperation with Pyongyang, could offer the North much needed help with all aspects of its nuclear program, Hecker said.

"For the shorter term, what concerns me most is Russia clandestinely supplying plutonium directly," Hecker, a former director of the Los Alamos National Laboratory, said in comments published on the 38 North project.

North Korea has conducted six underground nuclear tests and there have been concerns since last year that it may be about to conduct another test as part of efforts to develop miniaturized nuclear warheads.

North Korea's parliament adopted a constitutional amendment last week on its policy of nuclear force. Kim has also ordered the production of nuclear arms to increase "exponentially" and to diversify its nuclear capabilities.

Should Nuclear Weapons Be Made Less Lethal?

By Frank N. von Hippel

Source: https://www.armscontrol.org/act/2023-09/features/should-nuclear-weapons-made-less-lethal

Sept 2023 – In the new film *Oppenheimer*, the protagonist, J. Robert Oppenheimer, directs the secret U.S. Manhattan Project, to design, build, and test a new weapon of mass destruction. The ethical issues are obvious, but the fear that the Nazis have a nuclear bomb project swamps those concerns until it becomes clear, after the Allied forces crossed the Rhine into Germany in the spring of 1945, that the Nazi initiative never got off the ground.

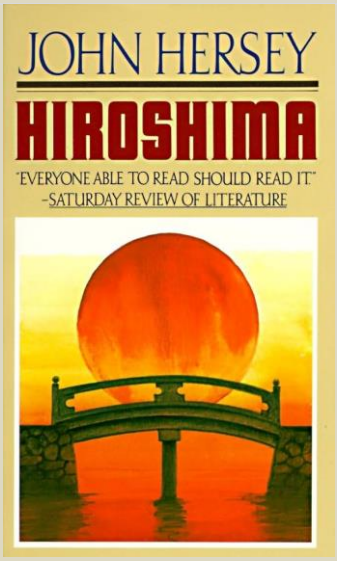
In the movie, some Manhattan Project scientists petition against using nuclear weapons against Japan, but they are too late. Before Japan surrenders, two atomic bombs with explosive powers equal to 15 kilotons and 20 kilotons of chemical explosive, respectively, kill an estimated 220,000 civilians in the

Japanese cities of Hiroshima and Nagasaki. Later, Oppenheimer says to President Harry S Truman, "Mr. President, I feel I have blood on my hands."

The problem of using explosives as weapons on military targets in urban areas was made clear by the bombings of Hiroshima and Nagasaki which killed an estimated 220,000 civilians by the end of 1945. This 1948 photo shows the devastation in Hiroshima three years after the United States dropped the bomb. (Photo by STF/AFP via Getty Images)

The ability of nuclear weapons to kill catastrophic numbers of living beings still haunts people of conscience. **Today, the explosive yield of the average U.S. nuclear warhead is equivalent to 200,000 tons (200 kilotons) of chemical explosive, or about 100,000 times the yield of the improvised explosive that, in 1995, destroyed the front one-third of the Alfred P. Murrah federal building in Oklahoma City, killing 168 people, incinerating dozens of cars, and damaging more than 300 buildings.**[1] Those 200 kilotons are vastly in excess of what would be required to destroy most military targets of the major U.S. adversaries. A single such explosion in an urban area could kill hundreds of thousands of civilians, dwarfing Russian President Vladimir Putin's war crimes in Ukraine. This colossal lethality is not the only choice available to U.S. war planners. U.S. bombs and cruise missile warheads have a "dial-a-yield" feature that allows their explosive yields to be reduced to as little as 300 tons, but this low-yield option has not been added to the U.S. ballistic missile warheads that, in a contemporary conflict, would be used to attack hundreds of command-and-control targets in Russian and Chinese urban areas. Only a couple of dozen of U.S. ballistic missile warheads have had their yields reduced to about 10 kilotons, and the rationale for that move was not to reduce civilian casualties, but to make it more credible that the United States would retaliate with nuclear weapons if Russia struck first with low-yield tactical nuclear weapons. It is time for the U.S. Congress to consider whether this nuclear stockpile is consistent with the international laws of war and whether, at a minimum, it should require that low-yield options be installed in all U.S. ballistic missile warheads.

The Lesson of Hiroshima



The problem with using nuclear explosives as weapons on military targets in urban areas was made clear by the bombing of Hiroshima, which was described initially by Truman as "an important Japanese Army base." He soon learned that a city and a large fraction of its civilian inhabitants had been destroyed along with the base. On August 10, the day after the Nagasaki bombing, he refused to authorize the dropping of a third bomb on a third Japanese city, explaining that he did not like the idea of "killing all those kids." The impact of nuclear weapons on civilians became more widely understood in 1946 after *The New Yorker* published John Hersey's stories of six survivors of the Hiroshima bombing: a young female clerk, a physician, a mother, a German priest, a surgeon, and a pastor. The article subsequently became a book, ***Hiroshima***, that sold millions of copies.

The Advent of Higher-Yield Thermonuclear Warheads

Three years later, after the United States detected radioactivity in the atmosphere from the first Soviet test of a fission bomb, the Truman administration asked the Atomic Energy Commission's General Advisory Committee to consider a proposal to develop much more powerful thermonuclear, or hydrogen bombs (H-bombs), as urged by the nuclear physicist-veterans of the World War II nuclear weapons project: Edward Teller, Ernest Lawrence, and Louis Alvarez. The committee was chaired by Oppenheimer, and its membership included James Conant, the president of Harvard University, who oversaw all U.S. wartime military research programs; Enrico Fermi, the legendary Italian physicist who led the effort to design the reactors that produced the plutonium for the Nagasaki bomb and tens of thousands more warheads during the Cold War; and I.I. Rabi, who later served as President Dwight D. Eisenhower's first science adviser.

The committee's conclusion was that the hydrogen bomb "is not a weapon which can be used exclusively for the destruction of material installations of military or semi-military purposes. Its use therefore carries much further than the atomic bomb itself the policy of exterminating civilian populations.... We are all agreed that it would be wrong at the present moment to commit ourselves to an all-out effort toward its development."[2] That advice was swamped, however, by the panic created by the Soviet test and by the possibility that Moscow might get the H-bomb first. About five years later, the United States and Soviet Union tested deliverable thermonuclear weapons.

The average explosive yield of U.S. nuclear weapons peaked in 1957.[3] Thereafter, the focus of the U.S.-Soviet nuclear arms race shifted to the development of lightweight but still very powerful nuclear explosives that would enable a single bomber carrying cruise missiles or a ballistic missile carrying multiple independently targetable reentry vehicles to attack simultaneously multiple targets separated by hundreds of kilometers.

In the 1970s, the average yield of U.S. nuclear weapons stabilized at about 200 kilotons of chemical explosive, about 10 times more powerful than the bombs used on Hiroshima and Nagasaki. The average yield of Russia's warheads was similar.

Areas of Destruction

Scaled from the five square miles flattened and burned by the Hiroshima bomb, **the destructive blast area of a 200-kiloton warhead would be about 30 square miles, roughly the size of San Francisco**. The area burned by fire could be twice as large, and the area in which the radioactive fallout from a ground burst would be lethal to unsheltered people could be two to three times larger still.[4] Initially, such large areas of destruction were seen as beneficial to nuclear stability. Robert McNamara, President John Kennedy's secretary of defense, was told in 1963 that, irrespective of whether the United States or the Soviet Union struck first, both countries would suffer tens of millions of deaths.[5] This concept soon came to be known as mutually assured destruction. Some nuclear strategists, including James Schlesinger, who eventually became defense secretary, advocated an alternative counterforce strategy in which the United States would attack the locations of Soviet nuclear and conventional weapons and related scientific and industrial support infrastructure. This seemed more legitimate than attacking the other country's population. Leadership and military command and control, however, were targeted as well, and those targets are mostly in cities.

Consider, for example, Russia's counterpart to the Pentagon, the complex that houses Russia's General Staff, which is located near the Kremlin and is one of the highest-priority nuclear command-and-control facilities on the U.S. target list. Central Moscow has a population density of about 30,000 persons per square mile. **A rough estimate of the consequences of a 200-kiloton airburst over the General Staff complex finds that more than a quarter million civilians would be killed and 1 million others seriously injured**.[6]

This example is far from unique. Bruce Blair, who discussed such questions at length with former commanders-in-chief of the U.S. Strategic Command, commented in 2020, in his last article, "It takes a herculean sleight of mind to reconcile the law of armed conflict with a U.S. nuclear target plan that includes around 1,500 aimpoints, many hundreds located inside large cities in Russia and China."[7]

Originally, the justification for large warhead yields was as compensation for uncertainties in the locations of targets and the poor delivery accuracy of early U.S. bombers and ballistic missiles. Yet, reconnaissance satellites revealed the precise locations of most targets 50 years ago. The accuracy of modern cruise missiles has become well known as a result of the U.S. use of about 2,000 sea-launched Tomahawk cruise missiles with conventional explosive warheads for attacks on Iraq in 1993, 1996, and 2003; Serbia and Montenegro in 1999; Afghanistan in 2001; Libya in 2011; and Syria in 2017.[8] U.S. long-range ballistic missiles also have become more accurate.

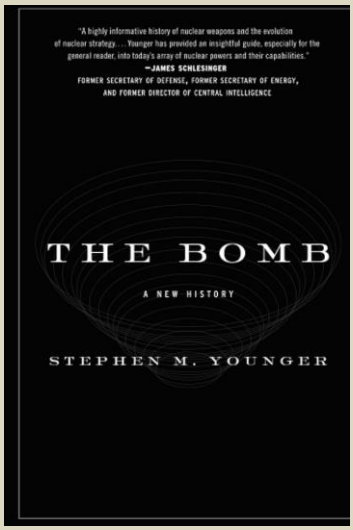
Nuclear Weapons and the Law of War

The 1977 Additional Protocols to the 1949 Geneva Conventions made "indiscriminate" killing of civilians a war crime. **For more than three decades, the United States insisted that this law of war did not apply to nuclear weapons.** In 2013, however, the Obama administration announced that nuclear targeting "must also be consistent with the fundamental principles of the Law of Armed Conflict. Accordingly, plans will, for example, apply the principles of distinction and proportionality and seek to minimize collateral damage to civilian populations and civilian objects."[9]

A former commander-in-chief of Strategic Command has reported, however, that in practical applications the translation of this presidential guidance became "minimize civilian damage to the extent possible consistent with achieving objectives."[10] Giving priority to "achieving objectives" resulted in command and control and other nuclear-related targets in urban areas being kept on the U.S. nuclear target list. Blair reported in 2018 that "100 [U.S. nuclear] aimpoints dot the greater Moscow landscape alone."[11] This is consistent with a detailed 2001 nongovernmental effort to reproduce the U.S. nuclear war plan for Russia, which identified 362 "leadership command, control and communication" targets in Russia, of which 87 were located in Moscow.[12]

In 2022, in response to reports of too many civilians being mistakenly targeted and killed by U.S. drone attacks, the U.S. Department of Defense issued a Civilian Harm Mitigation and Response Action Plan.[13] In his cover letter, Secretary of Defense Lloyd Austin stated, "We will ensure that we are well prepared to prevent, mitigate, and respond to civilian harm in current and future conflicts, including by integrating civilian protection into our mission objectives from the start." Eleven combatant commands were required to "incorporate [Civilian Harm Mitigation and Response] lessons learned and recommendations into current joint targeting processes to reduce the risk of civilian harm in future operations." It specifically required "scalable yields" to be considered for future weapon systems. One of those 11 commands was Strategic Command, which is responsible for planning potential nuclear attacks against nuclear-armed adversary nations, Russia and China in particular.

The secrecy of Strategic Command's target-selection process conceals it from congressional and public view, even from the civilians in the Pentagon. When Defense Secretary Dick Cheney finally forced a review by a civilian in 1989-1991, he learned that the targeting process was driven by interservice competition for targets. Adjacent facilities of adversaries, even parts of the same facility, were targeted separately to justify larger U.S. nuclear forces; and artifices were contrived to work around strictures against targeting densely populated areas, such as considering only where people live at night and not where they work during the day.[14] This review facilitated the dramatic post-Cold War reduction of the number of deployed U.S. nuclear warheads. There is no indication, however, that it reduced the focus on targeting leadership and command-and-control sites in urban areas.



A Proposal to Reduce U.S. Warhead Yields

In 2009, Steven Younger, a nuclear weapons designer who later served as director of Sandia National Laboratories, where the electronic controls for U.S. nuclear warheads are designed, published a book, ***The Bomb***, in which he observed, "Missile accuracies have greatly improved since the last nuclear weapon was introduced into the U.S. stockpile in the 1980s, but there has been no political support to follow through with a reduction in the yields of our nuclear weapons."[15] Younger proposed that, for many targets, nuclear warheads could be replaced by non-nuclear weapons such as accurate conventional explosive warheads, explosion-powered electromagnetic pulse generators, and cyberattack systems.

For targets whose destruction still would require the use of nuclear weapons, he argued that 90 percent could be destroyed by warheads with a yield of about 10 kilotons, 5 percent of the current average 200-kiloton yield of U.S. warheads, and most of the rest can be destroyed with 500-kiloton earth-penetrating weapons. Russia's General Staff complex, which is reportedly underlain by bunkers and tunnels "beneath a thick layer of concrete,"[16] might be a candidate for one of Younger's 500-kiloton warheads but at enormous cost in civilian casualties.

Shifting from hundreds of kilotons to 10-kiloton warheads would be a step back from H-bomb levels of destruction, but would still be at Hiroshima levels. Much better would be to replace the warheads with precision-guided conventional weapons.

The yields of U.S. warheads could be reduced to about 10 kiloton by replacing their fission-fusion second-stage explosives with inert objects of equal weight, as reportedly has been done for about 25 U.S. submarine-launched warheads. Yields could be reduced further without removing the secondary explosive by turning off the injection of deuterium-tritium fusion gas that boosts the yield of the fission "primary" explosive. Indeed, U.S. nuclear bombs and the warheads of U.S. nuclear-armed cruise missiles already have a dial-a-yield feature that reportedly allows a reduction of their explosive power from about 100 kilotons to as low as 0.3 kiloton.[17]
This feature may have been added when the warheads were designed around 1980 so that they could be used as either tactical or strategic weapons. The bombs could be used by fighter-bombers against a Soviet tank force invading West Germany. The cruise missiles could be launched at the same targets from offshore ships and submarines. The United States was concerned about minimizing civilian casualties in its NATO ally, West Germany.
Yet, more than 98 percent of U.S. ballistic missile warheads on strategic missiles targeted on Russia and China still have fixed yields reportedly ranging from 90 to 455 kilotons. These warheads would be used to target nuclear command-and-control installations in urban areas. Bombers and cruise missiles would be too slow.

The Debate Over Yield Reduction

The Trump administration's 2018 Nuclear Posture Review expressed concern about "Moscow's perception that its greater number and variety of non-strategic nuclear systems provide a coercive advantage in crises and at lower levels of conflict." The United States already had about 1,000 bombs and air-launched cruise missile warheads with low-yield options, but the Trump administration ultimately decided to close the "variety" gap by altering a few tens of the several hundred 100-kiloton W76 warheads deployed on U.S. submarine-launched ballistic missiles to produce yields of about 10 kilotons[18] and developing a new nuclear-armed submarine-launched cruise missile.
As with earlier proposals for low-yield warheads, the Trump administration's proposal was controversial. It would reduce the casualties from the use of small numbers of nuclear weapons, but their reduced yield might make easier the transition from conventional to nuclear weapons in a conflict.
As one critic pointed out, however, if Russia threatened to use nuclear weapons, it would be because it was losing a conventional war.[19] During the Cold War, when the Soviet Union had numerical superiority in conventional weaponry, the same logic drove NATO to place nuclear artillery units in the path Warsaw Pact forces were expected take if they crossed the inter-German border. About one-quarter of U.S. deployed warheads already have low-yield options. Having such options for ballistic missile warheads as well would not lower the threshold for nuclear war. As President Joe Biden said in 2022, "I don't think there's any such thing as the ability to easily [use] a tactical nuclear weapon and not end up with Armageddon." To limit NATO's support of Ukraine, Russian President Vladimir Putin keeps reminding that he has nuclear weapons, but he also declared in December 2022, "[W]e have not lost our minds; we are well aware of what nuclear weapons are.… [W]e are not going to wield these weapons like a razor running around the globe."
All nuclear-weapon states understand that there is a clear line between conventional and nuclear war but that, beyond that, there is no clear line this side of Armageddon. Some have expressed concerns that a nuclear-armed target country would not know that incoming conventionally armed long-range ballistic missiles were not nuclear until they arrived and thus might launch its nuclear missiles on warning. This is a legitimate disincentive for launching missiles of any type against a nuclear-armed country. Yet, if that decision has been made and a conventional warhead could accomplish the goal of incapacitating a communications tower in an urban area without killing 100,000 civilians, for example, that would be the choice required by the laws of war.
An alternate justification for not targeting leadership and command-and-control targets in urban areas is because such a decapitation strategy has such a low likelihood of success. There are too many fallback routes for sending out the launch command. Also, in Russia's case, the leadership has devised a "Dead Hand" strategy, in which if the leadership receives a warning on its early-warning sensors of an incoming attack, it can activate the so-called Perimeter system. That means, if seismic, light-flash, and other sensors agree that they have detected nuclear explosions and communications with the leadership in Moscow go dead at the same time, a crew in a central superhardened launch control center would send out the signal to launch a nuclear retaliatory strike.[20]

Other Policy Options

As with others who lived through the Cold War, Biden knows viscerally the fear of nuclear annihilation. Nearly four decades after the fall of the Berlin Wall, however, the danger of nuclear war has become an abstract concept to most people. The necessity to maintain nuclear deterrence at an adequate level is invoked regularly to assure funding for modernizing U.S. nuclear warheads and their delivery vehicles. Yet even with Putin's threats, it is difficult to imagine that nuclear weapons could be used deliberately. Few people are aware of the launch-on-warning postures that bring with them the possibility of a nuclear war by accident.
The ultimate goal must be to eliminate these weapons. That was recognized in the conferences on the humanitarian consequences of nuclear weapons use that led to the 2017 Treaty on the Prohibition of Nuclear Weapons. Despite the danger to their own citizens and to global civilization, the nuclear-armed

states are resisting the pressure for disarmament. The ability to threaten nuclear destruction has become an integral part of their security strategies.

A first step could be to follow Younger's advice and substitute conventional weapons for nuclear weapons wherever possible. Jeffry Lewis and Scott Sagan have proposed that the United States remove from its nuclear target list any structure that can be destroyed by a conventional weapon.[21] The United States has large numbers of air- and sea-launched cruise missiles with conventional warheads for just such purposes.

There also has been a continuing interest in deploying long-range conventionally armed ballistic missiles. In 2005, General James Cartwright, commander-in-chief of Strategic Command, proposed a study of whether, with accuracy improvements, some fraction of the targets in the U.S. nuclear war plan could be destroyed by conventional warheads mounted on long-range ballistic missiles. Cartwright's successor, Kevin Chilton, rejected the idea, arguing that conventional warheads would not have the same psychological impact as nuclear warheads.[22] This suggests that the strategy of nuclear deterrence through assured destruction may live on under the cover of the nuclear targeting of command-and-control facilities in urban areas.

A second step would be to add the low-yield option to U.S. ballistic missile warheads and to call for other nuclear-armed states to do the same. The purported added deterrence value of having the higher yield would remain because it could be restored with the flip of a switch, but the lowest yield should be the default setting. That would confront decision-makers considering using higher-yield options and the lawyers advising them on the requirements of the law of war with the tradeoff of tens to hundreds of thousands of additional civilian deaths per urban target.

The low-yield option would fit naturally into the Defense Department's new policy focus on civilian harm mitigation. Installation of a low-yield option in U.S. ballistic missile warheads could be included in the National Nuclear Security Administration's ongoing campaigns to life-extend and improve nuclear warhead safety and security.

The fundamental ethical problem posed by nuclear weapons would remain, however. As was learned from Hiroshima and Nagasaki, the civilian consequences of using even low-yield warheads in urban areas are unacceptable.

ENDNOTES

1. U.S. Federal Bureau of Investigation, "Oklahoma City Bombing," n.d., https://www.fbi.gov/history/famous-cases/oklahoma-city-bombing (accessed August 15, 2023).
2. Atomic Archive, "General Advisory Committee's Majority and Minority Reports on Building the H-Bomb, October 30, 1949," n.d., https://www.atomicarchive.com/resources/documents/hydrogen/gac-report.html (accessed August 15, 2023).
3. Office of Scientific and Technical Information, U.S. Department of Energy, "Summary of Declassified Nuclear Stockpile Information," n.d., https://www.osti.gov/opennet/forms?formurl=https://www.osti.gov/includes/opennet/document/press/pc26tab1.html (accessed August 15, 2023).
4. Samuel Glasstone and Philip J. Dolan, eds., "The Effects of Nuclear Weapons," U.S. Department of Defense and U.S. Department of Energy, 1977, https://www.osti.gov/servlets/purl/6852629. The maximum radius from ground zero for a given blast overpressure scales as yield Y1/3. If the atmosphere is clear, the slant radius from the center of the fireball for a given amount of radiant heat measured in calories per square centimeter scales as Y1/2. For fallout, the height of the cloud for a 200-kiloton surface burst is about 35,000 feet. Ibid., p. 431. From that height, the average fallout time is about six hours. Ibid., p. 458. The multiplier to get a two-week dose from a six-hour dose-rate/hour is about 20. Ibid., p. 403. A 600 rem two-week dose would correspond to a 30 rem/hour dose at six hours, which would extrapolate back to a theoretical one-hour dose rate of 260 rems/hour if all the radioactivity had fallen out immediately. Ibid., p. 392. For a 200-kiloton explosion with 50 percent of the yield coming from fission, the downwind distance of the one-hour dose rate contour of 300 rem/hour is 50 miles, and the maximum width is four miles. Ibid., p. 430. I multiply by a factor of π/4 to get the area of the corresponding oval.
5. Fred Kaplan, T*he Bomb: Presidents, Generals, and the Secret History of Nuclear War* (New York: Simon & Schuster, 2020), p. 91.
6. Alex Wellerstein, "Nukemap," n.d., https://nuclearsecrecy.com/nukemap/ (accessed August 15, 2023). Airburst altitude chosen to maximize area subject to 200 pounds per square inch overpressure.
7. Bruce G. Blair, "Loose Cannons: The President and US Nuclear Posture," Bulletin of the Atomic Scientists, January 1, 2020, n.3, https://thebulletin.org/premium/2020-01/loose-cannons-the-president-and-us-nuclear-posture/.
8. Niall McCarthy, "Countries Hit by U.S. Tomahawk Cruise Missiles Since Desert Storm," *Forbes*, April 7, 2017.
9. U.S. Department of Defense, "Report on Nuclear Employment Strategy of the United States Specified in Section 491 of 10 U.S.C.," June 12, 2013, https://apps.dtic.mil/sti/pdfs/ADA590745.pdf.
10. Gen. Robert Kehler (ret.), "Commanding Nuclear Forces," in *Managing U.S. Nuclear Operations in the 21st Century*, ed. Charles Glaser, Austin Long, and Brian Radzinsky (Washington: Brookings Institution Press, 2022), p. 149.
11. Bruce G. Blair, Jessica Sleight, and Emma Claire Foley, "The End of Nuclear Warfighting: Moving to a Deterrence-Only Posture," Princeton University and Global Zero, September 2018, p. 36, https://www.globalzero.org/wp-content/uploads/2018/09/ANPR-Final.pdf.
12. Matthew G. McKinzie et al., "The U.S. Nuclear War Plan: A Time for Change," Natural Resources Defense Council, June 2001, p. 103, https://www.nrdc.org/sites/default/files/us-nuclear-war-plan-report.pdf.
13. U.S. Department of Defense, "Civilian Harm Mitigation and Response Action Plan (CHMR-AP)," August 25, 2022, https://media.defense.gov/2022/Aug/25/2003064740/-1/-1/1/CIVILIAN-HARM-MITIGATION-AND-RESPONSE-ACTION-PLAN.PDF.

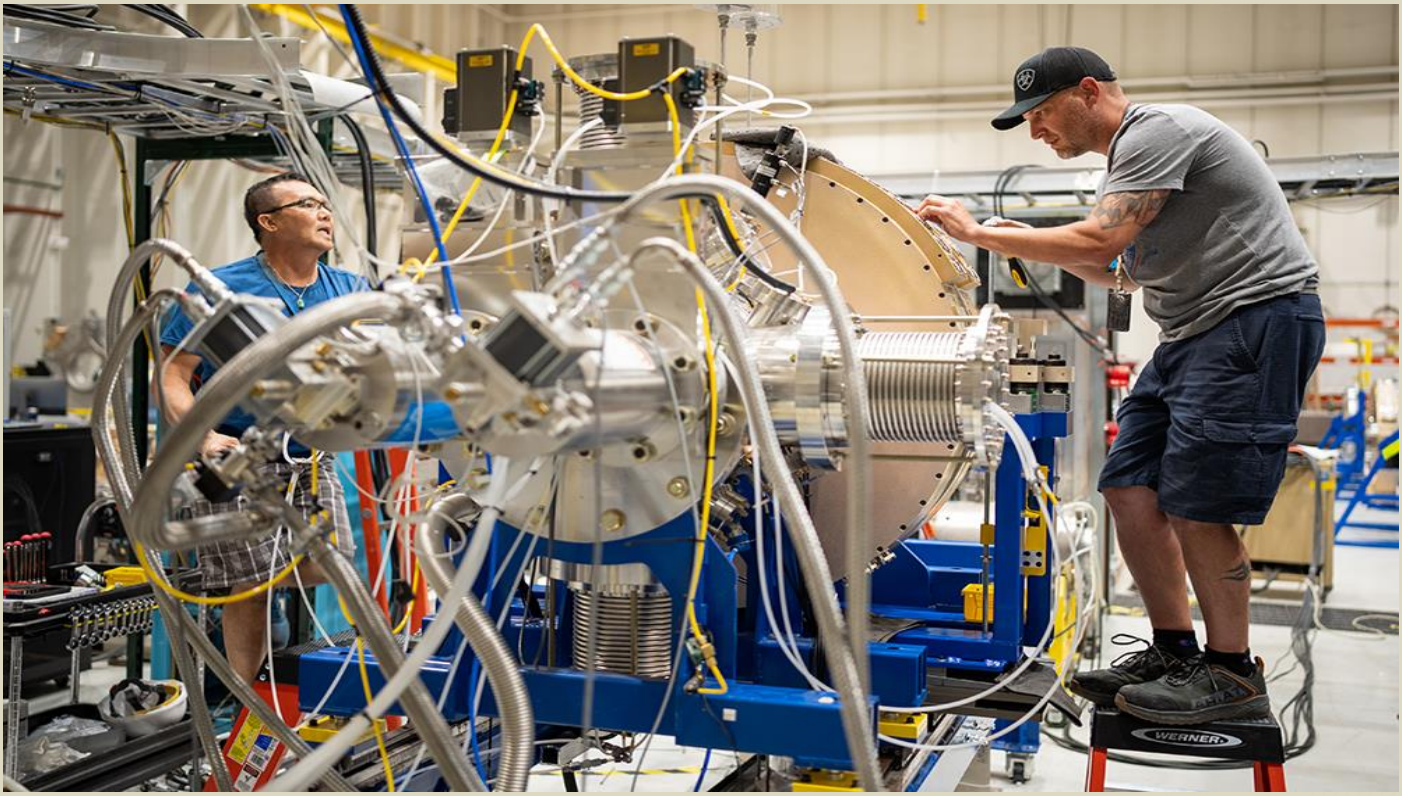
14. Franklin C. Miller, "Establishing the Ground Rules for Civilian Oversight," in *Managing U.S. Nuclear Operations in the 21st Century*, ed. Charles Glaser, Austin Long, and Brian Radzinsky (Washington: Brookings Institution Press, 2022), pp. 53-70.
15. Stephen M. Younger, *The Bomb: A New History* (New York: Ecco, 2009), p. 41.
16. Alexander Vershinin, "Russia's Military Command Center: Sending Orders From the Heart of Moscow," Russia Beyond, January 4, 2018, https://www.rbth.com/defence/2016/01/04/russias-military-command-center-sending-orders-from-the-heart-of-moscow_555889.
17. Hans Kristensen, "The Flawed Push for New Nuclear Weapons Capabilities," Federation of American Scientists, June 29, 2017, https://fas.org/publication/new-nukes/.
18. Amy F. Woolf, "A Low-Yield, Submarine-Launched Nuclear Warhead: Overview of the Expert Debate," *CRS In Focus*, IF11143, January 5, 2021, https://crsreports.congress.gov/product/pdf/IF/IF11143/5.
19. Jon Wolfsthal, "Say No to New, Smaller Nuclear Weapons," War on the Rocks, November 22, 2017, https://warontherocks.com/2017/11/say-no-new-smaller-nuclear-weapons/.
20. "Lieutenant General Sergei Karakaev: 'Vladimir Vladimirovich was right - we can destroy the United States in less than half an hour,'" interview with the commander of the Russian Strategic Missile Forces, *Komsomolckaya* Pravda, Dec. 16, 2011, http://www.kp.ru/daily/25805/2785953.
21. Jeffry G. Lewis and Scott D. Sagan, "The Nuclear Necessity Principle: Making U.S. Targeting Policy Conform With Ethics and the Laws of War," *Daedalus*, Vol. 145, No. 4 (Fall 2016): 62.
22. Amy F. Woolf, "Conventional Prompt Global Strike and Long-Range Ballistic Missiles: Background and Issues," *CRS Report*, R41464, July 16, 2021, pp. 8-9, https://crsreports.congress.gov/product/pdf/R/R41464/52.

Frank N. von Hippel is a senior research physicist and professor of public and international affairs emeritus with the Program on Science and Global Security at Princeton University.

EDITOR'S COMMENT: This a hilarious title along with some very useful information. Either you quit smoking or reducing it to 5-10 cigarettes per day will not help you escape lung cancer or COPD.

Scorpius Images to Test Nuclear Stockpile Simulations

Source: https://www.homelandsecuritynewswire.com/dr20231009-scorpius-images-to-test-nuclear-stockpile-simulations



Oct 09 – One thousand feet below the ground, three national defense labs and a remote test site are building Scorpius — a machine as long as a football field — to create images of plutonium as it is compressed with high explosives, creating conditions that exist just prior to a nuclear explosion.

These nanosecond portraits will be compared with visuals of the same events generated by supercomputer codes to check how accurately the computed images replicate the real thing.

"It's clear we need to know that the stockpile will work if required," said Jon Custer, Sandia National Laboratories project lead. "Before President Bush's testing moratorium in 1992, we knew it did since we were physically testing. Now we have computer codes. How well do they predict what really happens? Do we have accurate data we put into the codes? To answer these questions with higher fidelity, we need better experimental tools, and Scorpius is a major new experimental tool."

The $1.8 billion project, combining the expertise of researchers from Sandia, Los Alamos and Lawrence Livermore national labs with support from the Nevada National Security Site — a test area bigger than the state of Rhode Island — is expected to be up and running by late 2027.

Tickling the dragon's tail

"We intend to use Scorpius' actual images, gained from what we call 'tickling the dragon's tail,' to check our computer simulations," Custer said. "These simulations theoretically describe the hydrodynamics of plutonium in its various states, and we want to see how closely they match."

Hydrodynamics here refers to material compressed and heated with such intensity that it begins to flow and mix like a fluid.

Tickling the dragon's tail in this case means designing experiments that approach but stay below the threshold of criticality — that is, always subcritical, involving less than the mass needed for an explosion — while enabling a study of plutonium in that highly compressed and thermally heated state.

Above-ground facilities have tested the explosive behaviors of surrogate materials, but the inherent differences with plutonium cannot be accurately accounted for. While Scorpius will produce X-ray images during full-scale testing of plutonium, facilities that are equivalent but above-ground, including the Dual-Axis Radiographic Hydrodynamic Test Dual-Axis Radiographic Hydrodynamic Test machine at Los Alamos, instead must use implosionlike episodes to test the behaviors of surrogate materials.

"Plutonium is a very strange element," Custer said. "There is no true surrogate. Nothing else behaves like it.

"So, the question to us is, are we feeding accurate data into our codes about plutonium's behavior?" he said.

To find out, Scorpius, the buried interrogating machine, will produce X-ray images of plutonium as it implodes, with experiments specially designed to remain subcritical.

Three questions for Scorpius

First, researchers want to evaluate the effect of aging on plutonium to continue to validate that the U.S. deterrent will be effective if called upon. Plutonium, which transmutes from uranium, ages through a process called radioactive decay. Many nuclear weapons have been in service for 30 to 50 years.

"If you had a car in a garage for 30 to 50 years and one day you insert the ignition key, how confident are you that it will start?" Custer asks. "That's how old our nuclear deterrent is. It has been more than 30 years since we conducted an underground nuclear explosive test. And cars are mass-produced by the millions, with every problem well exposed. Our deterrent is built individually, one at a time. So, we want every assurance of reliability to warn potential adversaries that the U.S. stockpile remains a credible deterrent, now and into the future."

Second, he says, consider weapons built since the underground nuclear explosive testing moratorium declared by President George Bush in 1992. The issue here is to show that changes in designs from 1992 to the present that were linked to physical tests of the past are just as potent, if not more so, than their underground-tested ancestors.

Finally, the congruence of theoretical and physical processes in both these test series, providing theoretical validation with Scorpius data, will help remove doubt about future simulations. These subcritical tests with Scorpius are expected to show that newly designed weapons of the future will function if called upon, even though constructed mainly from supercomputer designs and potentially significantly altered to overcome the changes in overall environments expected from the use of new materials and unanticipated electronic advances.

Daniel Sinars, director of Sandia's Pulsed Power Center, said, "We are entering an era where our modernization programs are going to start making significant changes to the nuclear explosive packages, even if the performance characteristics of the weapons don't change. That is, they are not 'new' weapons, but they may have a lot of new technology."

"Having Scorpius is part of what will be needed to have an agile and responsive stockpile for weapon design that can qualify such changes in the absence of underground testing," Sinars said.

Programs to modernize the U.S. stockpile currently can take up to 15 years to execute.

"If instead we wanted to develop a new weapon or modernize them in more like five years, we will need capabilities to quickly assess design changes and risks for new hardware options," Sinars said. "Scorpius is part of a suite of capabilities that the weapon science folks envision as critical to going faster."

Sandia researcher Josh Leckbee, who led the injector development and design for Scorpius, confirmed that requirement.

"One of the key benefits and drivers for needing the Scorpius capability is to give confidence in existing and new designs," Leckbee said.

"All the existing weapons in the stockpile have traceability to underground testing. It will be difficult to put weapons with new designs that are not directly tied to underground testing into the future stockpile," he said. "To do this, we'll need extreme confidence in our predictive modeling capability. Scorpius allows diagnosing of subcritical tests to build that confidence."

In short, said Dave Funk, vice-president for Enhanced Capabilities for Subcritical Experiments at the Nevada National Security Site, "The specific goal of ECSE is to understand the hydrodynamics of plutonium and validate current models of plutonium behavior with the goal of certifying the changes to the nuclear stockpile without the need to return to underground testing."

"We are looking forward to establishing this capability in 2027, conducting the first subcritical experiments using these new capabilities to support our nuclear deterrent and demonstrate once again our technical prowess as a nation," Funk said.

The most complex part

Sandia's role in the Scorpius project is to design and construct the electron beam injector that will occupy the first 45 feet of the big machine, Custer said. "Much of the rest is to accelerate our electron pulses up to their final energy before slamming them into a heavy metal target to create the very bright X-ray flashes that will take the pictures."

Stainless steel tubes able to maintain high vacuum levels inside the machine will transport electrons, aluminum will be used where possible for its lower weight and lack of magnetic susceptibility and magnets will focus the electron beam. "Lots of vacuum pumps, sensors, wiring for power and signals, water lines for cooling, et cetera," Custer said.

The machine will be able to produce four separate 80-nanosecond pulses of electrons at 1,400 amps per pulse. Those four pulses can be produced anywhere the experimenters want over a three-microsecond window.

Demonstrating that the injector is capable of four independent pulses was a key part of the technology maturation that the team has been doing for the last several years to be ready for this phase of the project.

"Being able to see multiple images in time as the device implodes really puts the computer codes to the test," Custer said.

Sandia's resumé fits the job because of the Labs' long-standing expertise in pulsed power. Its Z machine, Saturn and Hermes-III comprise three of the five largest pulsed power machines in the world. Sandia has made pulsed electron beam machines and done novel experiments in radiography with its series of Radiographic Integrated Test Stand accelerators, an ancestor of the current project and jointly developed by Sandia and Nevada.

Los Alamos is responsible for post-pulse acceleration — taking the beam from 1.7 megavolts up to 22 megavolts — and for turning the electrons into X-rays downstream, as well as for the X-ray camera system. Los Alamos also oversees integration of all the components into a functioning system ready for experiments, Custer said.

Lawrence Livermore will provide the pulsed power for both the injector and the accelerator. They also have responsibility for several of the injector subsystems.

"It is worth noting that Scorpius is based on 'solid state' pulsed power promoted by Lawrence Livermore," Sinars said. "That means that the initial pulses of electrical energy are coming from large numbers of circuit boards rather than the big banks of massive capacitors, or Marx banks used by Sandia's Saturn and Z, and that was Lawrence Livermore's primary contribution to the injector."

Personnel at the Nevada National Security Site have helped all parties with design and testing, will assist with assembly and ultimately will be the owner and operator of the system in the underground U1a Complex. They are also doing extensive construction to prepare the space where Scorpius will be installed.

Plans for the complicated project were the focus of nearly 10 years of proposals modified, discarded and accepted through a multistage Department of Energy critical decision vetting process that finds and removes conceptual and technical errors before funding can be committed to the project. Final approval came late last year.

To design the injector responsible for creating the images was an engineering challenge.

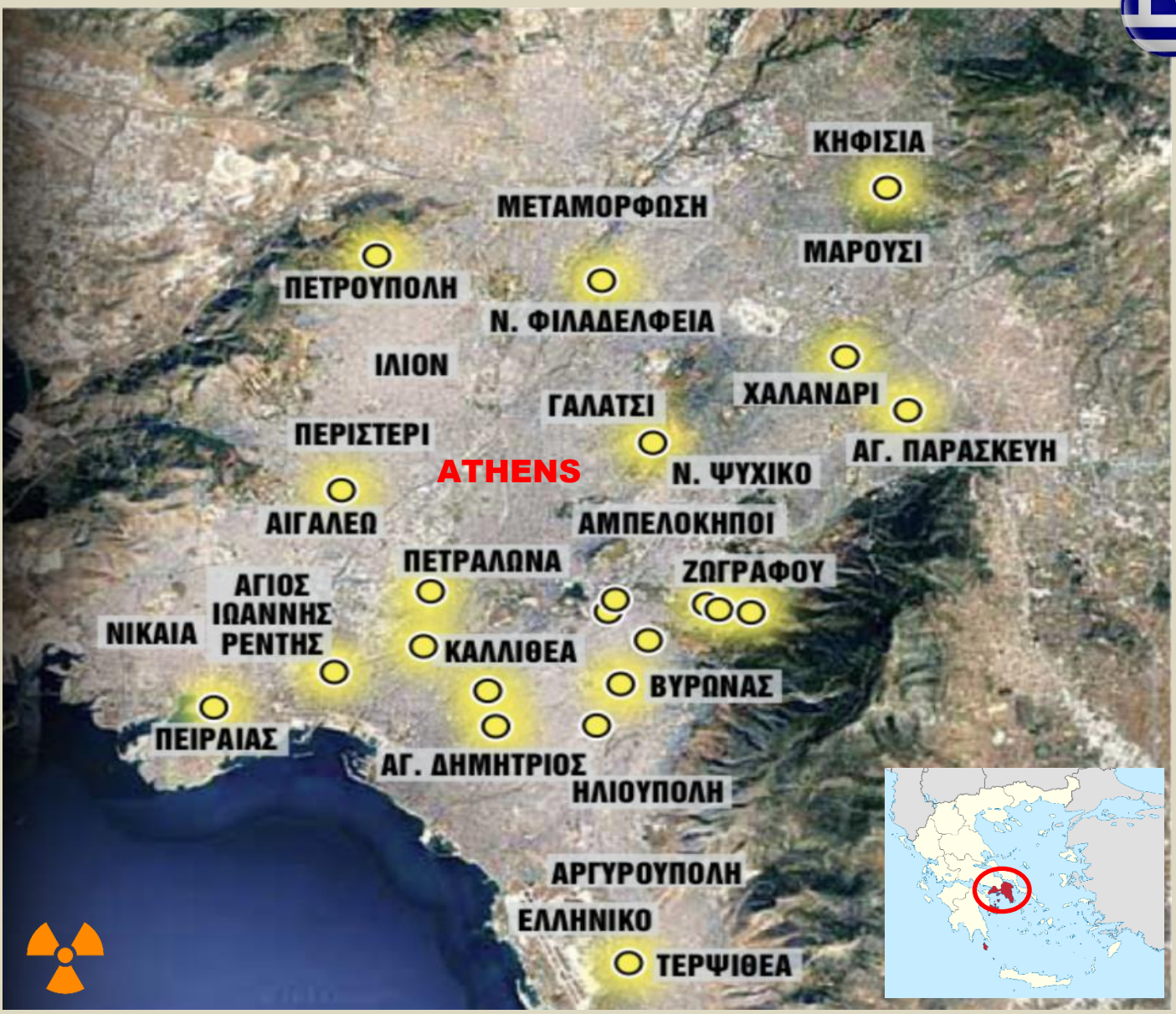
"No data existed to guide multipulse high-voltage design and no multipulse high-voltage test capability existed to conduct experiments," Leckbee said. "We teamed with the beam physics group at LLNL, who led electron beam optics design and simulation for the injector."

The Sandia mechanical engineering team dedicated more than 30 individuals to developing creative solutions to manage competing requirements in high voltage, thermal, structural, alignment, vacuum and space constraints, Leckbee said. "The resulting injector design is an assembly with over 1,000 unique part drawings."

"Our first shipment of injector components is slated to be sent out in March of 2024 when our assembly space in Nevada is ready, with the last shipment by early 2025," Custer said. "Assembly and testing will take until the fall of 2025 when we will turn the injector over to Nevada. They will then move it underground into the U1a facility at the Nevada Test Site in 2026 or 2027."

"I think I'm biased," Custer said, "but, yes, I think the injector is the most complex part of the whole system."

37 years after the Chernobyl disaster



Cs-137 traces in 23 areas of Attika prefecture, Greece

An alternative to the proliferation of uranium enrichment in the Middle East

By Seyed Hossein Mousavian and Frank N. von Hippel

Source: https://thebulletin.org/2023/10/an-alternative-to-the-proliferation-of-uranium-enrichment-in-the-middle-east/

Oct 10 – During recent negotiations, Saudi Arabia reportedly has asked for three big concessions in exchange for normalizing relations with Israel: recognition of Saudi Arabia's right to uranium enrichment; a US security guarantee for Saudi Arabia; and Israel's recognition of an "independent Palestinian state."

With regard to enrichment, Saudi Arabia has proposed that the United States partner with it in building a "nuclear Aramco" that would enrich and presumably export nuclear fuel. Israel, which has its own unacknowledged nuclear weapon program, correctly sees uranium enrichment as a route to nuclear weapons and has long opposed it in Iran and other Middle Eastern countries. At the United Nations on September 23, Prime Minister Netanyahu stated, "As long as I'm prime minister of Israel, I will do everything in my power to prevent Iran from getting nuclear weapons."

US State Secretary Antony J. Blinken meets with Saudi Foreign Minister Faisal bin Farhan in Riyadh, Saudi Arabia on June 7, 2023. Despite Blinken's visit, differences remain over Saudi Arabia's ambitions to develop its own civilian nuclear power industry and Washington seeing it as a potential proliferation risk. (Photo by Hisham Mousa / US State Department, via Flickr)

EDITOR'S COMMENT: Why it is OK for US to develop nuclear power/energy but a potential proliferation risk for everybody else (except Turkey)?

Paradoxically, however, he may be working with the Biden administration on a deal that would allow uranium enrichment in Saudi Arabia, under US supervision.

A Saudi enrichment program—even in partnership with the United States—would likely prompt other nations, including the United Arab Emirates (UAE), Turkey, and Egypt, to launch their own enrichment programs. But a multinational consortium could supply the nuclear power plants of Middle Eastern countries while assuring the world that the enriched uranium it produced is used only for peaceful purposes. The Hamas attack on Israel last week will certainly complicate and likely delay any agreement among Israel, the Saudis, and the United States. Eventually, however, the nuclear fuel needs of the Middle East will have to be addressed, and a multinational uranium enrichment enterprise seems a practical possibility for containing nuclear weapons proliferation in the region.

The enrichment landscape

Under Article 4 of the Treaty on the Non-Proliferation of Nuclear Weapons (NPT), every member state has the right to access nuclear technology for peaceful purposes. Since the 1970s, however—when India used reprocessing technology provided by the United States to launch its nuclear weapons program and Pakistan responded by launching its own nuclear weapons program using uranium enrichment technology obtained illicitly from the Netherlands—the spread of the capabilities to separate plutonium and enrich uranium have been central to the international debate over nuclear weapons nonproliferation policy. The motivations for Saudi Arabia (or any other Middle Eastern country) to create a uranium-enrichment program would not be economic. No small enrichment program, including those of Brazil, Iran, and Japan, makes economic sense. Smaller programs simply cannot compete with the major suppliers of enrichment services: Russia, France, China, and URENCO. URENCO, with the second largest enrichment capacity

after Russia, is owned jointly by Germany, the Netherlands, and the United Kingdom. Even the United States abandoned its efforts to subsidize a private enrichment program in the face of this international competition. The only enrichment capacity in the United States today is owned by URENCO.

If it is impossible to prevent the spread of enrichment capabilities to the Middle East, however, the best alternative to a dangerous proliferation of national programs would be a multinational consortium such as a URENCO for the Middle East. A multinational would be more economically viable. It also would provide greater assurance to the world that the enrichment is strictly for peaceful purposes and would be a great confidence-building measure among the member states in the region. Indeed, one motivation for the founding of URENCO in 1970 was the Soviet Union's concern about Germany having a national enrichment program. A Middle East enrichment consortium could include protections against technology leakage and foreign partners that have enrichment expertise, including the United States. All the Middle Eastern partners in such a consortium would have to forego national enrichment programs and use the enriched uranium produced by the consortium to fuel their nuclear power plants. Both moderate and hardline Iranian presidents floated a related idea in 2005. That spring, one of us (Mousavian) accompanied Iran's future president, Hassan Rouhani, then secretary of Iran's Supreme National Security Council, to separate meetings with the heads of the other Persian Gulf States with whom he offered to share Iran's enrichment technology. That September Iran's new hardline President Ahmadinejad, in a speech at the UN, stated, "The Islamic Republic of Iran is prepared to engage in serious partnership with private and public sectors of other countries in the implementation of uranium enrichment program in Iran … as a further confidence-building measure."

A Saudi-Iranian enrichment partnership?

The location of a multinational Middle East enrichment program would of course be a contentious issue. But if this issue could be dealt with, Saudi Arabia and Iran could be founding partners of a Middle East enrichment consortium. In the first step, building on the recent efforts at détente between Iran and Saudi Arabia, a regional security and cooperation system could be established in the Persian Gulf. This regional cooperation system could contain a multilateral enrichment mechanism coupled with a pledge by consortium members not to acquire nuclear weapons or national enrichment or plutonium separation programs in the context of wider political, security, economic and cultural cooperation. Other Middle Eastern countries could join in a subsequent phase. That could provide a long-term solution to concerns about Iran's national program.

Israel, the only country currently possessing nuclear weapons in the Middle East too could join and monitor the facility if it abandoned its nuclear weapons program and dismantled its nuclear weapons. That would realize the dream of a Middle East nuclear-weapons-free zone that has been on the international agenda for 50 years. Given the deep wells of distrust in the Middle East—deepened today by Hamas' attack on Israel—our proposal may be dismissed as politically infeasible. If political leaders cannot imagine a more peaceful, secure, and stable future for the region, however, no progress will be possible. A Saudi-Iranian uranium-enrichment consortium could be a step on a path toward reduced nuclear risk for the entire region.

Ambassador Seyed Hossein Mousavian is a Middle East Security and Nuclear Policy Specialist at Princeton University and a former chief of Iran's National Security Foreign Relations Committee. His book, *A Middle East Free of Weapons of Mass Destruction,* was published in May 2020 by Routledge. His latest book, *A New Structure for Security, Peace, and Cooperation in the Persian Gulf,* was published in December 2020 by Rowman & Littlefield Publishers.

Frank N. von Hippel is a Professor of Public and International Affairs emeritus, Princeton University, a co-founder of the Program on Science and Global Security at Princeton University's School of Public and International Affairs, a founding co-chair of the International Panel on Fissile Materials, and a member of the *Bulletin*'s Board of Sponsors. A former assistant director for national security in the White House Office of Science and Technology, von Hippel's areas of policy research include nuclear arms control and nonproliferation, energy, and checks and balances in policy making for technology.

Iran Should Worry: How Many Nuclear Weapons Does Israel Actually Have?

By Maya Carlin

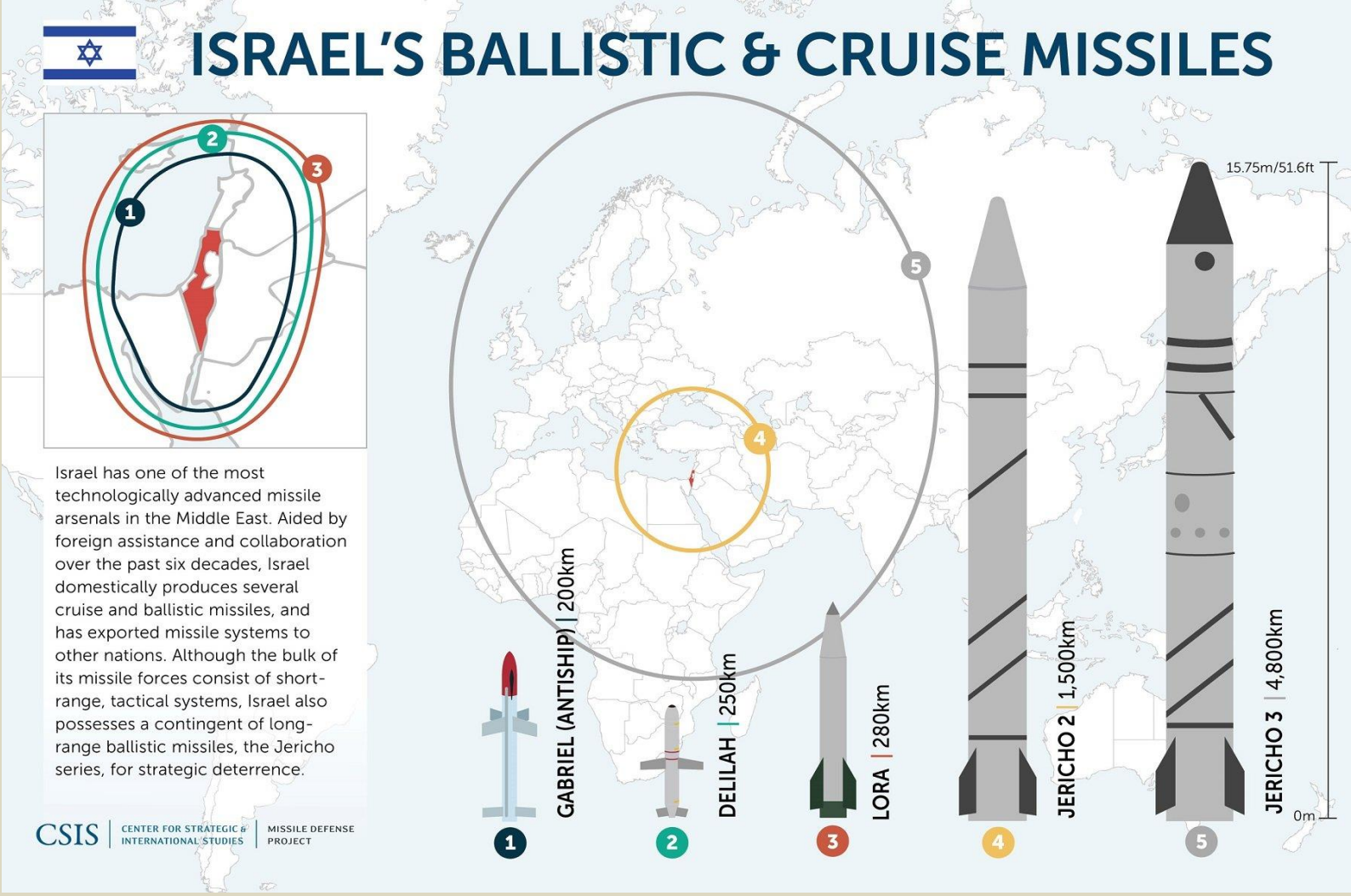
Source: https://www.19fortyfive.com/2023/10/how-many-nuclear-weapons-does-israel-actually-have/

.

Oct 13 – Israel and Iran have engaged in a shadow war for more than four decades, and Israel views its top adversary's nuclear program as a red line. While Israel keeps its own suspected nuclear program under wraps, it is widely believed to possess weapons of mass destruction.

Nuclear Development

When Israel was founded in 1948, Prime Minister David Ben-Gurion was adamant about protecting the country's new borders from hostile neighbors.



Around this time, a unit within the Israel Defense Forces (IDF) Science Corps dubbed HEMED GIMMEL began initial geological surveys of the Negev. Over the next decade or so, the unit would continue to pursue atomic energy studies. In the 1960s, Israel teamed up with the French aerospace company Dassault to create the Jericho ballistic missile program.

Ultimately, France withdrew from the program, but Israel powered on and produced the two-stage solid-fuel Jericho-1 missile on its own. During the 1973 Yom Kippur War, the Jericho missile was reportedly put on high alert.

Many experts assert that nuclear weapons were loaded onto these missiles when the IDF was unable to thwart incoming surprise attacks in the Sinai Desert and at the Golan Heights. As the conflict progressed, however, Israel was able to successfully combat enemy forces through combat.

The Jericho Missile Specs & Capabilities

With a range of around 500 kilometers, the Jericho-1 could hit Egypt and Syria from the Negev. As detailed by the Center for Strategic and International Studies, the first Jericho variant was "13.4 m long, with a 0.8 m diameter, and a total launch weight of 6,700 kg.8 The missile used a two-stage solid propellant engine and could be launched from a railroad flat truck or a TEL vehicle. The Jericho could carry a payload of up to 650 kg, reportedly equipped with a 450 kg high explosive warhead, a 20 kT nuclear warhead, or potentially a chemical warhead."

Over the years, a second Jericho variant was developed, with an even longer range. Although Israel maintains its official status of nuclear ambiguity, it is widely believed that the Jewish state has a newer Jericho-3 ballistic missile with even more enhanced capabilities.

What Drives Israel's Nuclear Ambiguity?

If Iran or any other country in the Middle East were to acquire nuclear weapons, Israel's longstanding policy of ambiguity could change.

According to the country's Begin Doctrine, the Israeli government is tasked with maintaining a preventative strike policy to ensure that no hostile country could develop these weapons.

Considering Iran's proximity to the nuclear threshold, Israel's policy of opacity could change in the near future.

Maya Carlin is a Senior Editor for 19FortyFive, is an analyst with the Center for Security Policy and a former Anna Sobol Levy Fellow at IDC Herzliya in Israel. She has by-lines in many publications, including The National Interest, Jerusalem Post, and Times of Israel.

Fukushima wastewater issue will further divide a nation, split families, and cause 'atomic divorce'

By Maxime Polleri

Source: https://thebulletin.org/2023/10/fukushima-wastewater-issue-will-further-divide-a-nation-split-families-and-cause-atomic-divorce/

Mothers march in Tokyo against radiation exposure risks five years after the Fukushima nuclear disaster on March 5, 2016. (Photo by Maxime Polleri)

Oct 17 – In a bid to dispel seafood worries around the release of Fukushima nuclear wastewater into the ocean, Japan's Prime Minister Fumio Kishida ate an array of sashimi late in August; the raw fish ranged from flounder to sea bass caught in the Fukushima area. It is "safe and delicious," he joyfully declared during a public relations effort to revitalize the fishing industry, which has been affected by a Chinese seafood ban and consumer anxieties over the wastewater release.

Many applauded Kishida's comment, which echoes the same government narrative around post-Fukushima food safety, as well as his firm support for the release of tritium-contaminated water—a discharge process that the International Atomic Energy Agency stated complies with operational safety limits for radiation.

But as someone who studied the aftermath of the Fukushima nuclear disaster for more than a decade, I believe that this decision will irreversibly erode public trust and create irreparable long-lasting tensions. During my years of research in Japan as an anthropologist, I witnessed first-hand how state policies around Fukushima's economic recovery are fragmenting communities, which constitutes an enduring catastrophe of its own.

Since 2011, in the hope of recovering from the worst nuclear disaster since Chernobyl, Japan has embraced an official policy of revitalization at Fukushima. The policy has different features, which all converge into a discourse of minimizing radiation risk, promoting Fukushima's food products, and repatriating former evacuees. While this government's policies have given the population some sense

of normalcy, they have also been harshly opposed, which is at the root of the discord now caused by the government's release of nuclear wastewater.

Minimizing radiation risk

Since March 2011, Japan's government and state-mandated experts have repeatedly told the population that the levels of radiation released during the nuclear disaster at Fukushima were too low to pose any significant health risks, preferring to highlight their impacts on mental well-being instead.

Since March 2011, Japan's government, state-mandated experts, and international organizations have repeatedly told the population that the levels of radiation released during the nuclear disaster at Fukushima were too low to expect any increase in cancers and other health effects in the future. But for many, fear and stigma related to the perceived risk of exposure to ionizing radiation are in fact perceived as the real risk. Throughout the years, these public relations efforts failed to convince parts of the population, especially after a survey conducted by the Environment Ministry revealed that children in Fukushima developed thyroid abnormalities. While some experts linked this increase in thyroid cancer among the youth to the radiation exposure at Fukushima, the government embraced another narrative, in which a "screening effect" led to the detection of thyroid cysts and nodules that would not otherwise have been discovered.

In this context of competing narratives, voicing concerns about the radiation safety at Fukushima has created internal community divisions, especially as the government's discourse has been adopted by certain segments of the population. For instance, mothers who evacuated their children from Fukushima for fear of adverse health effects have faced backlashes from their own parents—who often refused to be evacuated—worrying about not seeing their grandchildren. In interviews I conducted in 2016, parents blamed their daughters' decision to leave, often saying that: "The country's leaders are saying that it's safe, so why do you contradict them?"

Promoting food safety

Following the disaster, food safety became a contentious issue. Wary of contamination, many people stopped consuming food from Fukushima, which led to a drastic reduction in sales of food products. To revitalize Fukushima's agriculture and fishery industries, the government established regulatory criteria and encouraged food consumption through public relations activities, saying, much like Kishida, that food was "safe and delicious." In doing so, the government sought to fight what it calls "harmful rumors" around radiation risks, which lead people to avoid food products. But as with radiation safety generally, it is hard for citizens to voice concerns about food safety, despite independent testing showed cases of localized radiation contamination. As one mother explained to me: "Other

members of the community will tell you to stop spreading rumors. So, it's quite hard to express oneself directly."

In Fukushima, mothers complained that neighbors watch their shopping practices. When the mothers do not buy products from Fukushima, they are accused of being un-patriotic and hampering the region's revitalization. Such incidents inside local communities reminds us of the traditional practice of *murahachibu*—the shame-based social ostracism that was widespread in Japan during the Edo pe riod of the 17th to 19th century and reemerged after the Fukushima nuclear disaster and, most recently, the COVID-19 pandemic. The Japan government's plan to release radioactive wastewater into the ocean will likely exacerbate social ostracism within local communities even further.

Entangled between the social pressures to support their community and the need to protect their families as they see fit, mothers feel forced to make impossible choices. The mothers' decisions to evacuate their children from Fukushima severely affect their family ties, even creating disagreements within couples in a new phenomenon called "atomic divorce." To make things worse, in a country where the government declares Fukushima as being safe, evacuation is depicted as unnecessary. In line with its policy, the government announced in 2017 the termination of financial support for people who decided not to return to Fukushima. Masahiro Imamura, the Reconstruction Agency Minister, illustrated this decision by saying that, from now on, voluntary evacuees would be "self-accountable" for their choice.

Demands for evacuation are harder to justify now, and mothers who evacuated spoke of backlashes from their community, accusing them of living on state subsidies. "More and more we are being depicted as 'annoying' people," one mother told me in 2016. Being a critic of the government's policies at Fukushima is often kept secret, as individuals fear reprisals from their community. Mothers spoke of *migoroshi*—literally, "letting someone die"—to describe their situation as victims of community tensions created by post-disaster policies.

Nuclear wastewater's social cost

Tragically, catastrophes and crises are often followed by severe social tensions and crises. Japan's 2011 triple disaster—earthquake, tsunami, and nuclear meltdowns—is no exception. In Japan, such community breakdowns add a fourth disaster, which painfully lingers to this day.

The controversy surrounding the release of nuclear wastewater is already creating tensions very reminiscent of 2011. Currently, Japan is aggressively defending its position through a series of public relations messages exhorting citizens to eat Japanese marine products and stop spreading harmful rumors. Some citizens have answered this call, and the number of donations supporting Fukushima's products have increased drastically. However, social media posts promoting food consumption are already derided or called out, ironically, for being "tasteless." Fukushima's mothers also worry that anxiety and divisions among residents will increase as they've done in the past. Even fishermen are divided about state supports, with 151 plaintiffs filing a lawsuit against the government to stop the wastewater release.

No science-based narratives will bridge these gaps. These are not issues of science, but concerns about how recovery is conceptualized, as well as who is expendable in post-disaster politics. For now, in a few delicious bites of fatty flounder, all these palatable tensions have vanished under an array of camera shutters and television crews. Until they resurface.

Maxime Polleri is an assistant professor in the Department of Anthropology at Université Laval, in Quebec City, Canada. As an anthropologist, he studies the governance of nuclear catastrophes, with a focus on the 2011 Fukushima nuclear disaster. Polleri is also a Network Affiliate at the Center for International Security and Cooperation at Stanford University, where he was previously a MacArthur Nuclear Security fellow. He is also a member of MITATE Lab, an international research program on Fukushima issues.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

An explosion following a lightning strike in the Uzbek capital kills 1 person and injures 162

Source: https://apnews.com/article/uzbekistan-tashkent-explosion-1c507c460b4863bbb18fd2002a3ffc2d

Sep 28 – A powerful explosion in the Uzbek capital, Tashkent, killed a teenage boy Thursday and injured at least 162 people following a **fire caused by a lightning strike**, Uzbekistan's Ministry of Health said.

The Ministry of Emergency Situations said the explosion happened early in the morning at a warehouse in southern Tashkent but did not say what was inside it to cause the powerful blast which it said was attended by 16 fire crews.

Russian state media Tass later reported that the warehouse contained several dozen electric vehicles and batteries. It said that the explosion also caused minor damage to the nearby Quruvchilar subway station.

Video and photos posted on social media showed a fire and cloud of smoke that was visible across Tashkent, as well as apartments that had reportedly been damaged by the force of the blast.

Twenty-four people were hospitalized after the explosion and the remaining 138 were treated for their injuries and sent home according to the health ministry which added that Uzbekistan's leading medical specialists were treating the casualties.

Swiss approve CHF 100 million package to demine Ukraine

Source: https://www.reuters.com/world/europe/swiss-approve-chf-100-million-package-demine-ukraine-2023-09-29/

Sep 29 – Switzerland's Federal Council has approved a 100 million Swiss franc ($109.57 million) package to demine parts of Ukraine, the government said on Friday. "A total of CHF 100 million will be earmarked for humanitarian demining between 2024 and 2027, funded in equal parts by the Department of Defence, Civil Protection, and Sport (DDPS) and the Federal Department of Foreign Affairs (FDFA)," the government said. Switzerland is already involved in demining work in Ukraine and allocated 15.2 million Swiss francs in 2022 and 2023.

The additional amount announced on Friday will enable Switzerland to provide equipment and training for Ukrainian deminers and support the government in its efforts to coordinate the "herculean undertaking," the Swiss government said.
($1 = 0.9127 Swiss francs)

The few and the Brave!

Searching for mines in Ukraine!

Liverpool Women's Hospital bomber had asylum grievance, police say

Source: https://www.bbc.com/news/uk-england-merseyside-66986590

Oct 03 – A man who died when his homemade bomb went off outside a hospital had a grievance against the British state because his asylum claim was rejected, a police investigation has found.
Emad Al Swealmeen's device exploded in a taxi outside Liverpool Women's Hospital on 14 November 2021.
The 32-year-old was killed, but driver David Perry escaped the blast.
Counter Terrorism Policing North West said his grievance "combined with mental ill health" led to the attack.
The force's report into the bombing said it was "most likely" that Al Swealmeen's grievance against the British state for failing to accept his asylum claim had "compounded his mental ill health, which, in turn, fed that grievance and ultimately a combination of those factors led him to undertake the attack".
Det Supt Andy Meeks said it was believed Al Swealmeen intended to go into the hospital and detonate his device, but it was likely that it had exploded earlier than planned.

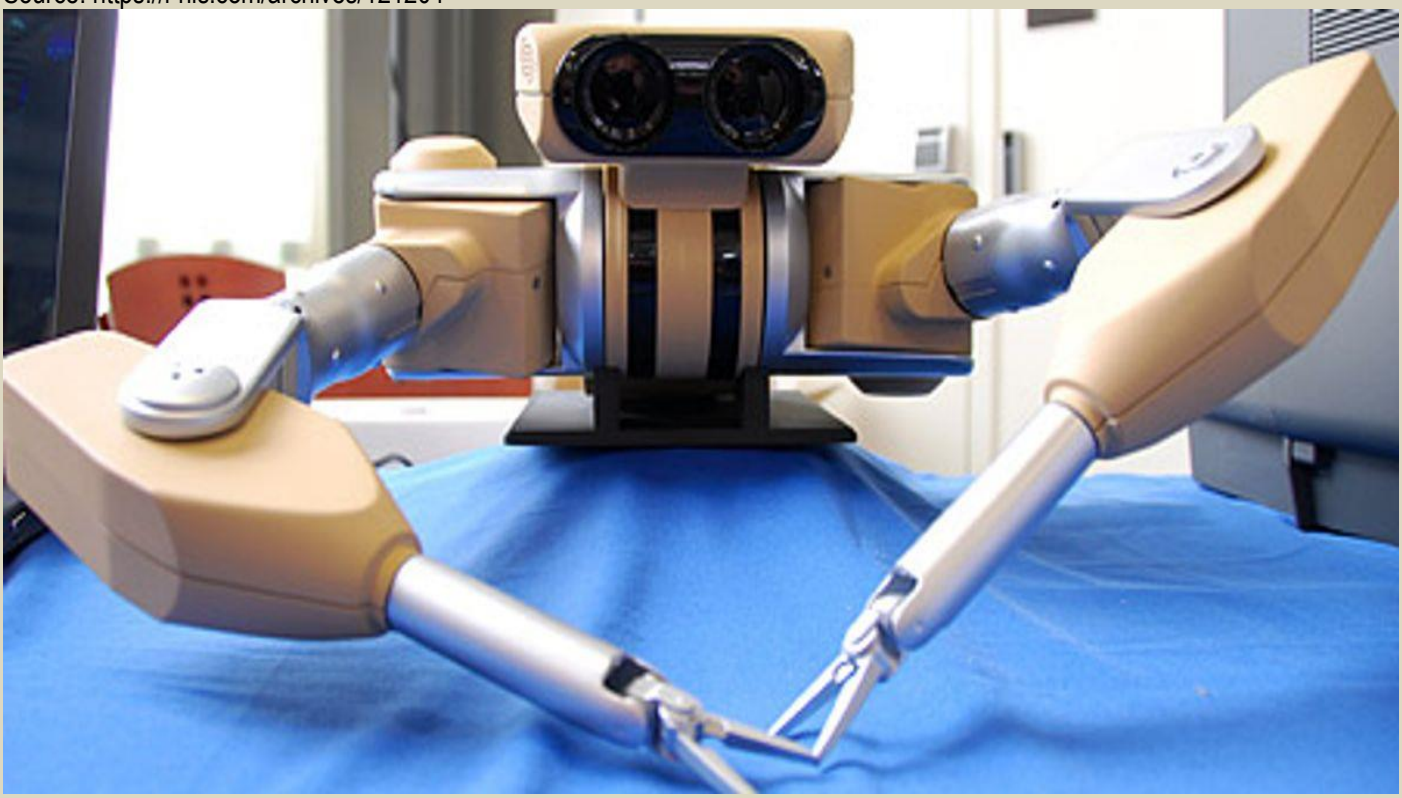
He said there was no evidence anyone else was involved in the attack.
The explosion, which was captured on the hospital's CCTV, propelled ball bearings through the taxi, blowing out its front windscreen.
The glass hit a tree 52ft (16m) away and damage was caused to the hospital's windows.

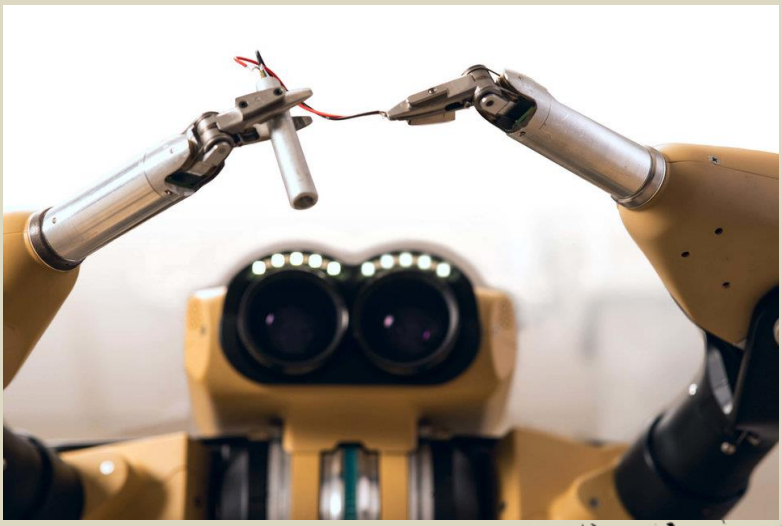
Det Supt Meeks said Al Swealmeen, who was born in Iraq, had gone to considerable lengths to stay in the country, including converting to Christianity, although the authenticity of his conversion was in doubt.
A previously confidential 2015 asylum judgment, released to the BBC in 2022, also revealed his claim of being a Syrian refugee had lacked basic facts.
The force said Al Swealmeen came to the UK in 2014, having applied for a visa in Abu Dhabi claiming he wanted to travel for a holiday and to watch the filming of Britain's Got Talent in Belfast.
He falsely claimed to be a Syrian national when interviewed by Home Office officials and his asylum claim was rejected.
Det Supt Meeks said Al Swealmeen began a conversion to Christianity in 2015, when his asylum appeal rights were exhausted, and was baptised at Liverpool Cathedral in November that year.
He forwarded letters of support from members of the church community to the Home Office to support his asylum claim in 2017.
In January 2020, a further asylum claim was rejected on the basis he had not truly accepted the Christian faith and rejected others.
Det Supt Meeks said Al Swealmeen's deterioration in mental health coincided with developments in his asylum case.
He said he was detained by police under the Mental Health Act in 2015 and was later sectioned.
The investigation into the attack found Al Swealmeen rented a flat in Rutland Avenue, about 1.5 miles (2.4km) from the hospital, with the "sole purpose" of building the bomb.
Officers found mixing bowls and bags of chemicals inside the flat, along with a mobile phone containing instructions on how to make explosives.
A search of his other address, which he shared with other asylum claimants in Sutcliffe Street, uncovered two unfinished improvised firearms.

A subsequent search of his mobile phones found they had been largely erased and he had taken precautions to conceal his intentions.
As a result, the report said officers would "never truly know why Al Swealmeen took the actions that he did that led to the explosion".
Following the report's publication, Merseyside Police's Assistant Chief Constable Jon Roy said the public's reaction to the attack had been "unbelievable", adding: "In the face of adversity, they were strong and determined and unbowed."
"Ultimately, the aim of terrorists is to create conflict, distrust and fear, but that didn't happen here and people across Liverpool stood shoulder to shoulder," he added.

Bomb Detection by Robots and AI

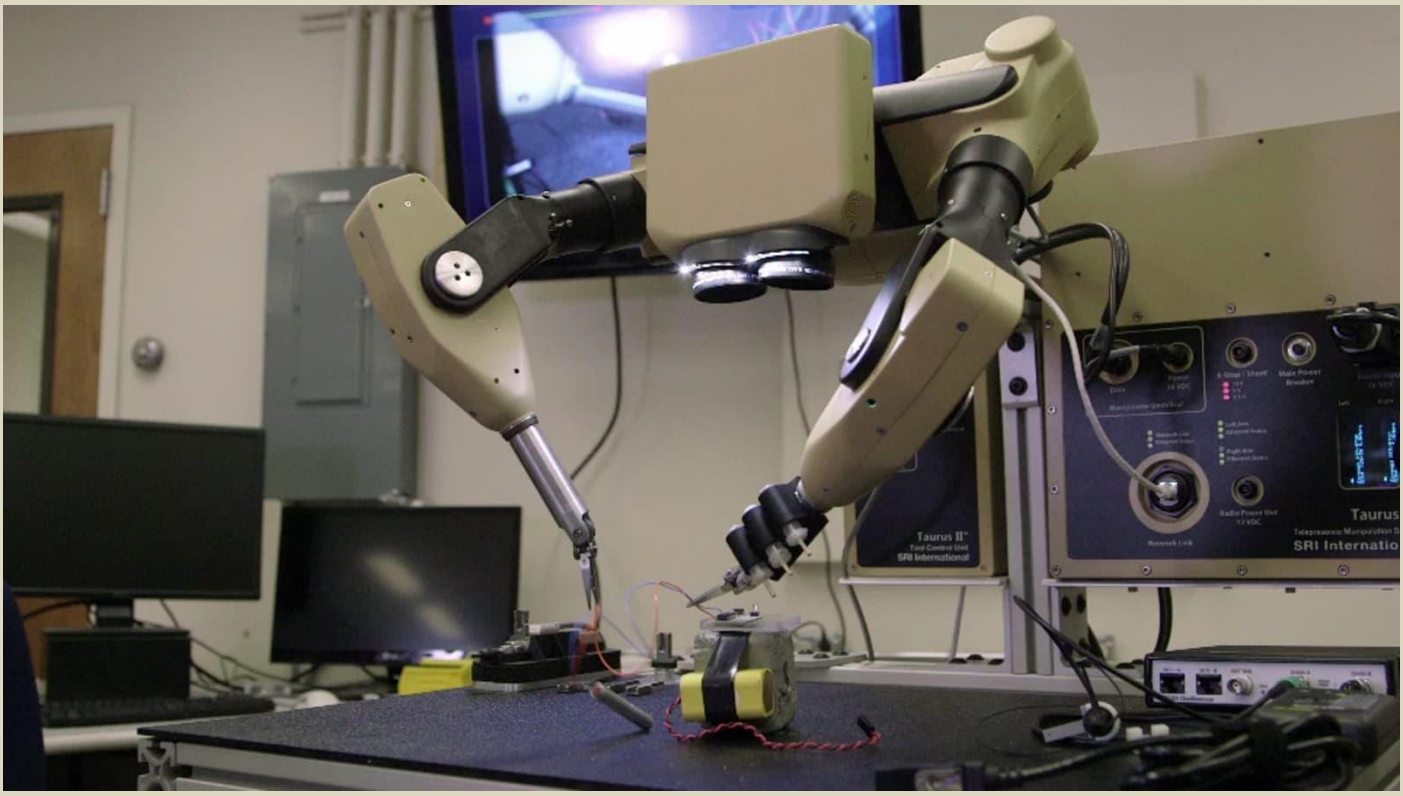
Source: https://i-hls.com/archives/121204





Oct 08 – The European Defense Agency (EDA) has successfully demonstrated how artificial intelligence and unmanned systems can work together to detect explosives and improvised explosive devices (IEDs) in different scenarios, which is a major breakthrough for defense research.
According to Interesting Engineering, the demonstration involved one UAV and two UGVs, each equipped with different sensors, which coordinated autonomously to search for mock-ups of explosives and IEDs, including unexploded ordnance, in rural and urban areas. The demonstration showed that the system can perform complex tasks with minimal human intervention and was part of AIDED- "Artificial Intelligence for Detection of Explosive Devices".
The system uses various sensors for detection, like the EMI (metal detector that can locate metallic objects underground or inside objects), the ground penetrating radar (that can provide more accuracy but is sensitive to the movements of the carrier), the Laser-Induced

Breakdown Spectroscopy (which uses a powerful laser beam to create a small plasma of the area to be analyzed by a spectrometer, and a bigger sensor that is used to identify the explosive device.



The system also reportedly uses neural networks and AI algorithms that can learn from data for each type of sensor signal processing, while the neural networks were trained on labeled data sets acquired during the project.
Other sensors are used for localization and mapping algorithms for robot navigation, and to cope with situations like when there is no GPS available. The system faced challenges and demonstrated the 'detect and avoid' system for avoiding collision between the UAV flying at very low altitudes for good detection and the UGVs.
This demonstration is a significant milestone for the AIDED project, showing that AI can be effectively used in several aspects of an unmanned systems operational environment, like mission planning, self-navigation, teamwork, and explosive device detection.

A 'certain kind of courage' needed: A look at SAF's selection process, training for its bomb disposal experts

Source: https://www.channelnewsasia.com/singapore/bomb-disposal-explosive-ordnance-saf-unit-training-selection-3843341

Oct 16 – When the Singapore Armed Forces (SAF) was alerted to a World War II aerial bomb last month, the experts sent to assess the situation had never been involved in such a disposal.
But the team of first timers, comprising regular servicemen from the SAF's Explosive Ordnance Disposal (EOD) unit, had been training for this day.
They assessed on Sep 20 that the unexploded bomb was unsafe to be moved from the Upper Bukit Timah construction site. Then, others from the unit – also known as the 36th Battalion of the Singapore Combat Engineers (36SCE) – were roped in to dispose of it on-site.
The unit is the national responder to any explosive incidents and also responds when war relics are discovered.
Full-time national servicemen (NSFs) were among the 45 SAF personnel involved in the disposal operations that spanned six ensuing days. They helped construct the protective works, which included cement blocks and sandbags, to prevent the blast from affecting nearby homes.
One of the NSFs involved told journalists that he wasn't fazed, despite it being his first time. Third Sergeant (3SG) Teo Jin Kay is serving his National Service as an EOD specialist and has been undergoing training since April. So, when the call came to serve, he was ready to answer.

"Once you join, you know you are preparing to be (called up) … Even though you don't know if you'll be activated, you're preparing for the chance that you will be," the 19-year-old said, matter-of-fact.
"We have to be ready. It's part of being in 36SCE."

"Consistently logical", able to work under stress
3SG Teo's unflappable demeanour is among the traits that EOD unit looks for through its "rigorous selection process" that includes physical and psychometric tests.
"Generally, we're looking for someone who is logical – consistently logical. We need people who work (well) under stress … and along the way, through their training, demonstrate a certain kind of courage and bravery," said Lieutenant Colonel (LTC) Ng Tee Yang.
"For example, the team commanders (who) were moving the bomb at Upper Bukit Timah on that day had to be beside the bomb, ready to move it. Knowing the risks that are involved, they still had to do (it)."
While some of these traits can be picked up on psychometric tests, others may require "a bit more time to assess", the commanding officer in 36SCE said.

Part of the assessment requires soldiers in the Explosive Ordnance Disposal unit to don a bomb suit. (Photo: CNA/Gaya Chandramohan)

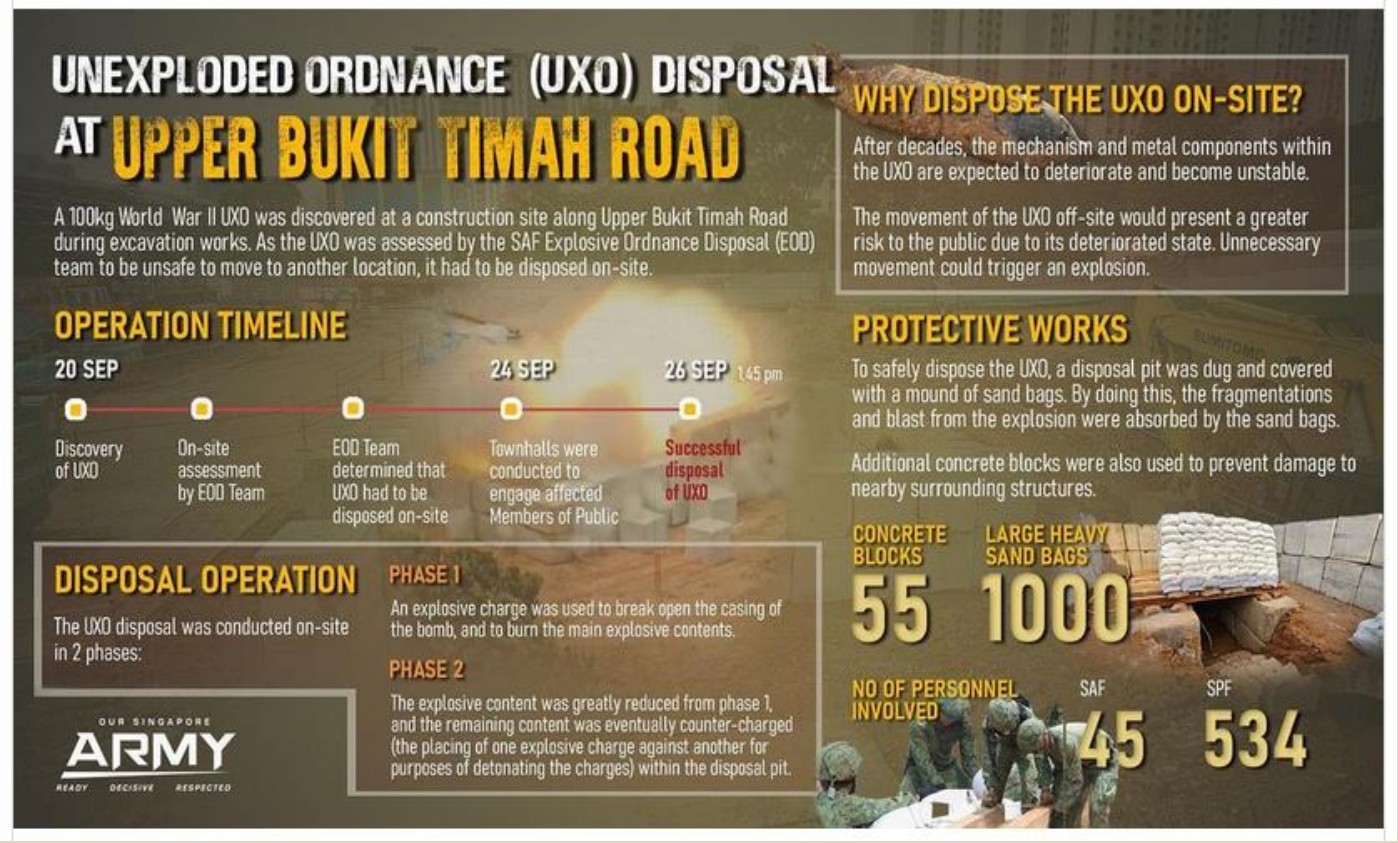
In the physical test, EOD hopefuls are required to don a bomb suit – which some have reported makes them feel claustrophobic as it is "a very closed environment", said LTC Ng.
They would then need to perform "required skills", such as being nimble in completing their tasks in an obstacle course.
The bomb suit weighs around 34kg including the helmet, and is typically worn in an improvised explosive device (IED) disposal. It wasn't used in the Upper Bukit Timah EOD disposal.
The weight of the suit is not the only issue, added First Warrant Officer (1WO) Peter Chong. "As you wear it for a prolonged period of time, the heat build-up in the suit is tremendous. Every time the operator dons the suit, you see the sweat dripping (after five to 10 minutes)."
1WO Chong, a regimental sergeant major in 36SCE, pointed out that the heat "sometimes gets unbearable". But the men are "trained to withstand it" – often, for hours at a go.
"In our type of operations, you cannot say (you will) only wear half an hour then take a rest. Because (there) is still a threat that is there," added LTC Ng. After going through a series of physical challenges,

trainees are tasked to complete a puzzle. At the same time, trainers would distract them with questions to assess their ability to multitask and whether they are still “able to perform” and complete the puzzle, he said.
Upon successfully completing the course, NSFs like 3SG Teo take on the role of Third In-Command (3IC), which allows them to be trained in "their fundamental skills and (preparations) beyond peacetime operations”, he added.

Part of the EOD unit's training is learning to identify unexploded ordnances. (Photo: CNA/Gaya Chandramohan)

One aspect of EOD training, as demonstrated by 3SG Teo, involves using an Explosive Ordnance Reconnaissance kit to identify an unexploded ordnance.
The kit comes with measuring tools, including a measuring tape and vernier calliper, and other equipment to brush off sand or mud from the ordnance.
Before approaching, however, EOD operators will ask witnesses who discovered the bomb for as many details as possible to eliminate certain hazards before heading in.
Another aspect of training in the unit involves navigating a remotely operated vehicle (ROV) to disrupt an IED. The cameras on the ROV allow operators to manoeuvre the vehicle from a safe distance by assessing the threat via a screen on their end.
In the Upper Bukit Timah disposal, NSFs made up the team that “supported the plan on ground”, such as by building the protective works, added LTC Ng.
They take “minimally one year to train for both their roles as 3IC in peacetime and their respective roles in hot war (situations)” during NS, and eventually rise up the ranks during their NS cycle.
On the other hand, regulars in the unit will fill the roles of team commander and the Second In-Command (2IC) with “key responsibilities to assess the unexploded ordnance disposal and assess the situation to neutralise any improvised explosive device”, he said.
Such regulars were in the first team sent to assess the Upper Bukit Timah site once the SAF was alerted to the war relic.
When team commanders approach a site, they first look for the fuse of the unexploded ordnance (UXO). This is the firing mechanism or “the brain of the UXO”, and without it, the ordnance is “quite safe”, explained 1WO Chong.
After assessing the possible hazards involved in the ordnance, the team then makes a call: Conduct an on-site disposal or, if it’s safe enough, transport the unexploded bomb elsewhere for disposal.
Regulars take about three to five years to gain experience and go through the necessary training before being assessed to take on the role of team commander, LTC Ng pointed out.
They are selected to undergo a series of assessments to “assess their competency” and “analytical abilities to see if (they) can remain calm and think logically under pressure”.

"Ultimately, we need each operator to make logical and sound decisions to ensure that he and his team move out and come back safely," he said.



Tight communication, teamwork

Rigorous training, significant as it is, must be complemented with teamwork, LTC Ng stressed. The heroic lone ranger singlehandedly detonating an IED that's often glamorised in Hollywood movies doesn't happen in reality.

3SG Teo Jin Kay is serving his National Service in the SAF's Explosive Ordnance Disposal unit. (Photo: CNA/Gaya Chandramohan)

While the Upper Bukit Timah disposal was challenging, it was "not uncommon", he said, highlighting a similar disposal in 2019.

That year, a 50kg aerial bomb was found in River Valley, also during excavation works at a construction site. It was similarly assessed to be unsafe to move and had to be disposed of on-site.

What made the recent disposal most challenging, however, was its proximity to surrounding residential areas, he said.

As the unexploded war relic had deteriorated after decades, it could trigger an explosion "due to instability", he added. "We have zero room for errors and we must get it right."

LTC Ng outlined the "close and tight communication" needed with various agencies to make the mission a success.

The Singapore Police Force managed public safety and communication by helping to evacuate nearby residents, while the Singapore Civil Defence Force was on standby to provide medical assistance for EOD responders and the public.

The Building and Construction Authority was also called in to assess the potential impact on the structural integrity of the surrounding buildings, and SAF worked with the Land Transport Authority to enforce road closures on the day.

SAF also worked with the nearby secondary school to ensure minimal disruption to their examination timetable and the Infocomm Media Development Authority in light of potential telecommunication cables underground.

"It was a complicated operation. But everybody came together with a lot of synergy," added LTC Ng, noting that the coordination between agencies made the recent operation surprisingly smooth.

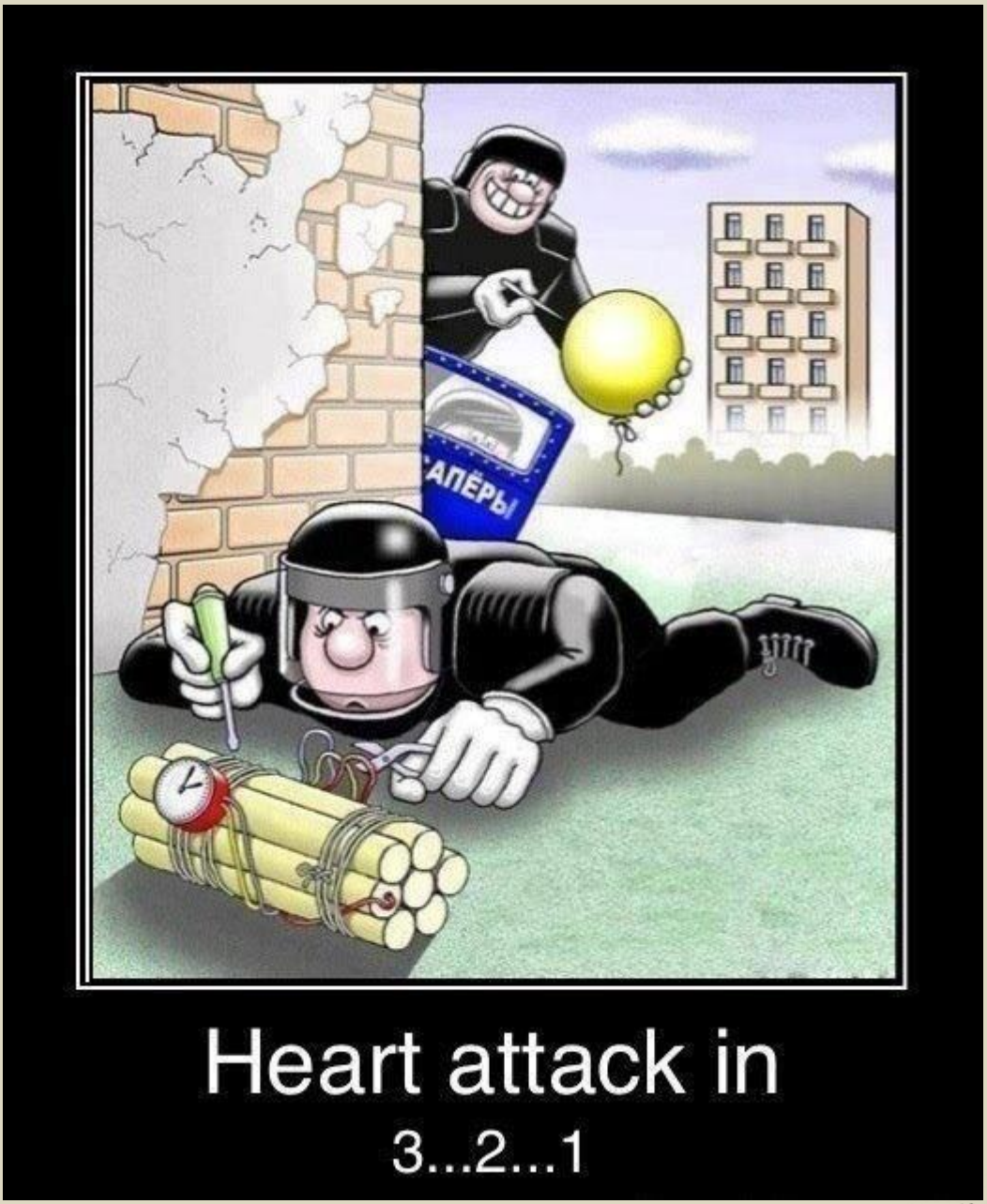
The two controlled detonations took place at about 12.30pm and 1.45pm on the day, after which the authorities carried out safety checks in the area until about 5pm. Shortly after, residents were notified through WhatsApp channels set up for their respective estates that safety checks had been completed and they could return home.

Although some Hazel Park residents spotted damage in certain common areas of their condominium, most were relieved to find no damage to their homes.

As for 3SG Teo, the Upper Bukit Timah disposal will go down in his books as a "fulfilling experience" – especially since he saw his training "being put into practice" to impact the public, he said.

The 19-year-old NSF had to reassure his parents who were initially concerned when they found out he would be involved in the disposal. But he pointed out that the training "makes sure we perfect all these

aspects of an operation, so that in situations like this, we can rely on our training to make sure everything goes smoothly and safely".
In fact, after conducting their assessment at the site, LTC Ng said the team of first responders – which hadn't attended to such a disposal previously – reflected on how they could "infuse" the experience into their future training.
"The key is to induce stress during training as much as possible … (So that) we go through it during training, such that we don't have to go through it for the first time during a real activation."
Staying abreast with the latest threat landscape and keeping their skills fresh is a necessity, he added.
"The terrorists only need to get it right once, but we need to get it right all the time."



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

The Biggest Hack of 2023 Keeps Getting Bigger

Lily Hay Newman and Matt Burgess

Source: https://www.wired.com/story/moveit-breach-victims/

Oct 02 – In a field of shocking, opportunistic espionage campaigns and high-profile digital attacks on popular businesses, the biggest hack of 2023 isn't a single incident, but a juggernaut of related attacks that keeps adding victims to its score. In the coming months, more people, as many as tens of millions, could find out that their sensitive information has been compromised. But more still will likely never learn of the situation or its impact on them.

Since May, mass exploitation of a vulnerability in the widely-used file transfer software MOVEit has allowed cybercriminals to steal data from a dizzying array of businesses and governments, including Shell, British Airways, and the United States Department of Energy. Progress Software, which owns MOVEit, patched the flaw at the end of May, and broad adoption of the fix ultimately halted the rampage. But the "Clop" data extortion gang had already orchestrated a far-reaching smash and grab. And months later, the full extent of the damage is still coming into view.

Last week, Ontario's government birth registry, BORN Ontario, said that it suffered a MOVEit-related attack earlier this year in which hackers stole sensitive personal data from 3.4 million people, including 2 million babies as well as expectant parents and those seeking fertility care. The compromised health data dates from January 2010 to May 2023. While organizations like BORN continue to disclose a slow trickle of MOVEit incidents, researchers say that the number of suspected attacks—and the total number of people whose data has already been stolen in these incidents—far exceeds what has come to light.

"I don't think we're done hearing about this by any means. We're going to keep seeing that rolling disclosure over probably the next few months," says Emily Austin, security research manager and senior researcher at the threat intelligence firm Censys. "These companies are completing their investigations—they're starting to notify customers who might have been affected."

Austin points out that one of the nuances of the MOVEit situation is that it is a true software supply chain security issue. The vulnerabilities existed in two versions of the MOVEit service: the cloud service known as MOVEit Cloud, and the local version that institutions run themselves on their premises, known as MOVEit Transfer. The latter is where most of the exploitation occurred. But many organizations that had data stolen in MOVEit exploitation attacks weren't directly using it. Instead, they'd collaborated with a third party or contracted with a vendor that does. Attackers were able to steal whatever data they could grab from vulnerable MOVEit systems, whether the information was from one institution or many.

"An advanced and persistent threat actor used a sophisticated, multi-stage attack to exploit this zero-day vulnerability, and we are committed to playing a collaborative role in the industry-wide effort to combat cybercriminals intent on maliciously exploiting vulnerabilities in widely used software products," Progress Software said in a statement.

Centralized data repositories like MOVEit have been particularly appealing targets to Clop, which is known for strategically exploiting systems embedded in the software supply chain, including multiple file transfer tools. Earlier this year, Clop claimed it breached more than 100 organizations by abusing the GoAnywhere file transfer tool. The gang also mounted a massive data extortion campaign at the end of 2020 by exploiting flaws in Accellion networking equipment.

The MOVEit incident eclipses them, though, both in the number of victim organizations and individuals whose data was compromised. Antivirus company Emsisoft has been tracking the number of MOVEit victim organizations that have publicly declared they were impacted since May. The researchers have combed individual US state breach notifications, filings with the US Securities and Exchange Commission, public disclosures, and Clop's own disclosure website to tabulate and reconcile the true toll of the attacks.

To date, Emsisoft has concluded that 2,167 organizations have been impacted by the sprawling campaign. The number had been hovering around 1,000 in recent months, but it jumped significantly when the National Student Clearinghouse revealed 890 colleges and universities across the US—including Harvard University and Stanford University—had been impacted by MOVEit breaches. Organizations in the US account for 88.8 percent of known victims, according to Emsisoft, while a smattering of other organizations in Germany, Canada, and the UK have also been exposed by Clop and come forward.

According to Emsisoft's analysis, around 1,841 organizations have disclosed breaches, but only 189 of them have specified how many individuals were impacted by the incident. From these detailed disclosures, Emsisoft has found that more than 62 million individuals had their data breached as part of Clop's MOVEit spree. But since there are estimated to be nearly 2,000 organizations that have not revealed how many individuals had personal data affected in their breaches—and since researchers have concluded that there are other impacted organizations that haven't come forward at all—the true total of people whose data was compromised is likely even larger, possibly on the scale of hundreds of millions of individuals, according to Emsisoft.

"It's inevitable that there are corporate victims that don't yet know they're victims and there are individuals out there who don't yet know they've been impacted," says Brett Callow, a threat analyst at Emsisoft. "MOVEit is especially significant simply because of the number of victims, who those victims are, the sensitivity of the data that was obtained, and the multitude of ways that data can be used."

Censys' Austin says file transfer tools are by their nature a "fantastic target" for cybercriminals. The whole purpose of the tools is to manage and share data, so these services are often trusted with large volumes of sensitive information. BORN Ontario said in a statement last week that the data taken in the breach was from those "seeking pregnancy care and newborns." This included lab test results, pregnancy risk factors, and procedures. Names, dates of birth, government ID numbers like Social Security numbers, addresses, and more have all been compromised in other MOVEit incidents.

While cybercriminal groups often make headlines for attention-grabbing ransomware or extortion attacks, such as those against casinos, persistent and unrelenting theft, publication, extortion, and trade of people's sensitive data from sprees like the MOVEit rampage can ruin lives—a cumulative reality that is often overshadowed by individual incidents where profits are on the line. Hacks on schools have revealed details of sexual assaults, child abuse allegations, and suicide attempts, with the Associated Press reporting individuals often don't know the details have been published. Meanwhile, breaches of mental health service providers have exposed patients' records. Callows says that he suspects the slow drip of MOVEit-related disclosures "will rumble on for years." More broadly, he and Austin emphasize that defenders should prepare for cybercriminals to continue targeting widely-used data management software. As Callow puts it, "MOVEIt isn't the first file transfer application to be exploited and it likely will not be the last." Just last week, MOVEit developer Progress Software disclosed a new set of vulnerabilities in one of its file transfer tools for servers, known as WS_FTP Server, along with patches for the flaws. The company says that it has not "currently" seen evidence that the bugs are being actively exploited.

Lily Hay Newman is a senior writer at WIRED focused on information security, digital privacy, and hacking. She previously worked as a technology reporter at Slate magazine and was the staff writer for Future Tense, a publication and project of Slate, the New America Foundation, and Arizona State University.

Matt Burgess is a senior writer at WIRED focused on information security, privacy, and data regulation in Europe. He graduated from the University of Sheffield with a degree in journalism and now lives in London.

New Cyber Algorithm Shuts Down Malicious Robotic Attack

Source: https://www.homelandsecuritynewswire.com/dr20231017-new-cyber-algorithm-shuts-down-malicious-robotic-attack

Oct 17 – Australian researchers have designed an algorithm that can intercept a **man-in-the-middle (MitM) cyberattack** on an unmanned military robot and shut it down in seconds. In an experiment using deep learning neural networks to simulate the behavior of the human brain, artificial intelligence experts from Charles Sturt University and the University of South Australia (UniSA) trained the robot's operating system to learn the signature of a MitM eavesdropping cyberattack. This is where attackers interrupt an existing conversation or data transfer. The algorithm, tested in real time on a replica of a United States army combat ground vehicle, was 99% successful in preventing a malicious attack. False positive rates of less than 2% validated the system, demonstrating its effectiveness. The results have been published in *IEEE Transactions on Dependable and Secure Computing*.

UniSA autonomous systems researcher, Professor Anthony Finn, says the proposed algorithm performs better than other recognition techniques used around the world to detect cyberattacks. Professor Finn and Dr Fendy Santoso from Charles Sturt Artificial Intelligence and Cyber Futures Institute collaborated with the US Army Futures Command to replicate a man-in-the-middle cyberattack on a GVT-BOT ground vehicle and trained its operating system to recognize an attack. "The robot operating system (ROS) is extremely susceptible to data breaches and electronic hijacking because it is so highly networked," Prof Finn says.

"The advent of Industry 4, marked by the evolution in robotics, automation, and the Internet of Things, has demanded that robots work collaboratively, where sensors, actuators and controllers need to communicate and exchange information with one another via cloud services. "The downside of this is that it makes them highly vulnerable to cyberattacks.

"The good news, however, is that the speed of computing doubles every couple of years, and it is now possible to develop and implement sophisticated AI algorithms to guard systems against digital attacks."

Dr Santoso says despite its tremendous benefits and widespread usage, the robot operating system largely ignores security issues in its coding scheme due to encrypted network traffic data and limited integrity-checking capability.

"Owing to the benefits of deep learning, our intrusion detection framework is robust and highly accurate," Dr Santoso says. "The system can handle large datasets suitable to safeguard large-scale and real-time data-driven systems such as ROS."

Prof Finn and Dr Santoso plan to test their intrusion detection algorithm on different robotic platforms, such as drones, whose dynamics are faster and more complex compared to a ground robot.

October is Cyber Security Awareness Month. According to Statista, the **robotics market is projected to reach US$37 billion in 2023. Service robots dominate the market and others are increasingly used worldwide – including in military, civilian, agricultural, industrial, search and rescue, and medical sectors.**

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS

Iran parades new 'longest-range' drone on Iraq war anniversary, state media report

Source: https://www.reuters.com/world/middle-east/iran-parades-new-longest-range-drone-iraq-war-anniversary-state-media-2023-09-22/

Sep 22 – Iran on Friday paraded its military hardware on the anniversary of its 1980s war with Iraq, including "the longest-range drone in the world" along with ballistic and hypersonic missiles, Iranian state media said.

They said the drone "was unveiled" in the parade, which was broadcast live, and that drones displayed in the event were named Mohajer, Shahed and Arash.

The Islamic Republic said last month that it had built an advanced drone named Mohajer-10 with an enhanced flight range and duration as well as a larger payload.

It has an operational range of 2,000 km (1,240 miles) and can fly for up to 24 hours, state media reported then, adding that its payload could reach 300 kg (661 pounds), double the capacity of the Mohajer-6 drone.

The United States has accused Iran of providing Mohajer-6 drones, among other unmanned aerial vehicles (UAVs), to Russia for its war against Ukraine. On Tuesday, Washington expanded Iran-related sanctions, citing Tehran's "continued, deliberate proliferation of UAVs" enabling Russia, its proxies in the Middle East and other destabilising actors".

Iran denies providing drones to Russia for the conflict in Ukraine.

"Our forces ensure security in the region and the Persian Gulf," President Ebrahim Raisi said at Friday's parade in the capital Tehran. "We can teach the people of the region that resistance is today's way. What forces the enemy to retreat is not submission and wavering, but resistance."

A video released last month by Iranian media showed the Mohajer-6 among other military hardware, with a text reading "prepare your shelters" in both Persian and Hebrew, the latter an allusion to Iran's arch-regional enemy, Israel.
The United States issued fresh Iran-related sanctions on Tuesday, targeting multiple people and entities in Iran, Russia, China and Turkey over Tehran's drone and military aircraft development.
The Iran-Iraq war erupted on Sept. 22, 1980 when the forces of then-Iraqi President Saddam Hussein invaded Iran. The conflict, which was economically devastating and left at least half a million dead, ended in stalemate in August 1988.

AtlasNEST aims to make airports safer, by deploying drones

Source: https://newatlas.com/drones/atlasnest-airports-drones/

Multiple AtlasNEST stations can be installed around one airport, if needed – Atlas Aerospace

Sep 22 – Ordinarily, drones flying around airports are thought of as a hazard. The AtlasNEST system, however, utilizes drones to fly over landing areas where problems may be occurring, in order to give control tower workers a bird's eye view.

Developed by Latvian firm Atlas Aerospace, AtlasNEST consists of an outdoor docking station which houses one of the company's AtlasPRO tricopter drones. Multiple stations can be set up around one airport, depending on how large and/or busy that airport is.

The AtlasPRO drone's battery is swapped for fresh one every time it returns to the station – Atlas Aerospace

All that's required for each station is an electrical outlet. If someone in the control tower wishes to check out a suspicious vehicle, monitor the landing of a plane that's in trouble, see if a certain runway really *is* clear – or otherwise get a good look at something that's far from the tower – they remotely trigger

the AtlasNEST. It responds by launching its drone, which autonomously flies to the provided coordinates to transmit a real-time aerial view from its 10x-optical-zoom thermal camera.
The AtlasPRO has a claimed runtime of 32 minutes, a communications range of up to 10 km (6 miles) via LTE, and it autonomously returns to the station when its job is done. A freshly charged battery is then robotically swapped into the aircraft, so it's ready to go out again at a moment's notice.
Atlas Aerospace is offering the AtlasNEST via leasing programs that start at €4,200 (about US$4,479) per month.

In a world-first, T-600 heavy lift drone launches anti-sub torpedo

Source: https://newatlas.com/military/t-600-heavy-lift-drone-anti-sub-torpedo/

The T-600 with its Sting Ray torpedo – BAE Systems

Sep 29 – A recent NATO exercise in the waters off the coast of Portugal saw naval drones reach a new level. As part of the exercise, a BAE Systems/Malloy Aeronautics T-600 heavy lift Uncrewed Air System (UAS) air launched an inert Sting Ray training torpedo.
The major navies of the world have a keen interest in aerial drones of all shapes and sizes. As these become more sophisticated, they've moved into more niches, freeing up humans for more important tasks.
Though at first glance it looks like the sort of quadcopter drones used to make videos, the T-600 is about the size of a compact car. It's an electric-powered demonstrator craft that is easily broken down for transport, has a payload of 200 kg (441 lb), top speed of 140 km/h (87 mph) and a range of 80 km (50 miles).
As part of NATO's Robotic Experimentation and Prototyping with Maritime Uncrewed Systems (REPMUS) 2023 exercise, the T-600 went through a series of demonstrations for representatives from NATO countries as well as Ireland and Sweden.
The highlight of these demos was the drop of a Sting Ray training variant anti-submarine torpedo. It was the first time such a weapon had been deployed by a drone as part of a sea mission. The purpose was not only to show off the T600's anti-submarine warfare capabilities, but also its potential for automated logistics, resupply, casualty evacuation and other tasks, with a relatively light environmental footprint but without the need for human pilots.

According to BAE Systems, the T-600 will be the basis for an all-new T-650 all-electric heavy lift UAS with rapid reconfiguration capabilities for military, commercial and humanitarian markets.
"In just two years since we launched our collaboration with Malloy, we've developed a heavy lift UAS and working with the UK Royal Navy and Portuguese Navy, have taken part in the latest NATO REPMUS exercise," said Neil Appleton, Head of Sustainable Electric Products, BAE Systems Air. "The demonstration showcased the capability of our T-600 technology demonstrator, carrying an inert Sting Ray torpedo in front of the world's premier naval forces."

AI and the Future of Drone Warfare: Risks and Recommendations

By Brianna Rosen
Source: https://www.justsecurity.org/89033/ai-and-the-future-of-drone-warfare-risks-and-recommendations/

Oct 03 – The next phase of drone warfare is here. On Sep. 6, 2023, U.S. Deputy Defense Secretary Kathleen Hicks touted the acceleration of the Pentagon's Replicator initiative – an effort to dramatically scale up the United States' use of artificial intelligence on the battlefield. She rightfully called it a "game-changing shift" in national security. Under Replicator, the U.S. military aims to field thousands of autonomous weapons systems across multiple domains in the next 18 to 24 months.
Yet Replicator is only the tip of the iceberg. Rapid advances in AI are giving rise to a new generation of lethal autonomous weapons systems (LAWS) that can identify, track, and attack targets without human intervention. Drones with autonomous capabilities and AI-enabled munitions are already being used on the battlefield, notably in the Russia-Ukraine War. From "killer algorithms" that select targets based on certain characteristics to autonomous drone swarms, the future of warfare looks increasingly apocalyptic.
Amidst the specter of "warbot" armies, it is easy to miss the AI revolution that is underway. Human-centered or "responsible AI," as the Pentagon refers to it, is designed to keep a human "in the loop" in decision-making to ensure that AI is used in "lawful, ethical, responsible, and accountable ways." But even with human oversight and strict compliance with the law, there is a growing risk that AI will be used in ways which fundamentally violate international humanitarian law (IHL) and international human rights law (IHRL).
The most immediate threat is not the "AI apocalypse" – where machines take over the world – but humans leveraging AI to establish new patterns of violence and domination over each other.

Drone Wars 2.0
Dubbed the "first full-scale drone war," the Russia-Ukraine War marks an inflection point where states are testing and fielding LAWS on an increasingly networked battlefield. While autonomous drones reportedly have been used in Libya and Gaza, the war in Ukraine represents an acceleration of the integration of this technology into conventional military operations, with unpredictable and potentially catastrophic results. Those risks are even more pronounced with belligerents who may field drones without the highest level of safeguards due to lack of technological capacity or lack of will.
The lessons from the war in Ukraine include that relatively inexpensive drones can deny adversaries air superiority and provide a decisive military advantage in peer and near-peer conflicts, as well as against non-state actors.
The United States and other countries are taking these lessons seriously. Mass and speed will apparently dominate the future drone wars, as the United States – through Replicator and other initiatives – seeks to develop the capacity to deploy large amounts of cheap, reusable drones that can be put at risk to keep pace with adversaries such as China. Increasingly, discrete drone strikes against non-state actors will be displaced by AI-enabled drone swarms that communicate with each other and work together (and with humans) to destroy critical infrastructure and other targets. This emerging technology poses even greater risks to civilians than the drone wars of the past. Unlike conventional drone warfare, which is vetted and controlled by human operators, the new drone

wars will be more automated. Human-machine collaboration will pervade nearly every stage of the targeting cycle – from the selection and identification of targets to surveillance and attack. The largest shift will be the least visible, as proprietary algorithms sift through reams of intelligence data and drone feeds to compile target lists for human approval.

While humans may continue to sign off on the use of lethal force, AI will play a more pervasive role in shaping underlying choices about who lives and dies and what stands or is destroyed. As AI reduces human involvement in killing, drone warfare will most likely become less explainable and transparent than it is now. This is true not only for the public – which is already kept in the dark – but also for government officials charged with implementing and overseeing the drone program.

The problem of explainability, where humans cannot fully understand or explain AI-generated outcomes, is a broader issue with AI that is not limited to drone strikes. Computational systems that rely on AI tend to be opaque because they involve proprietary information, evolve as they learn from new data, and are too complex to be understood by any single actor.

But the problem of explainability is particularly acute when it comes to drone warfare.

In the sprawling U.S. interagency process, military and intelligence agencies rely on different information streams, technology, and bureaucratic procedures to support the drone program. These agencies are developing their own AI tools which are highly classified and based on algorithms and assumptions that are not shared with key policymakers or the public. Add to this mix AI systems producing outcomes that cannot be fully understood and it will be impossible for government officials to explain why an individual, for example, was mistakenly targeted and killed.

The problem of explainability will foster a lack of accountability in the coming drone wars – something that is already in short supply. When civilians are mistakenly killed in AI-enabled drone strikes, Pentagon officials will also be able to blame machines for these "tragic mistakes." This is especially the case for drone swarms, where drones from different manufacturers may fail to communicate properly, despite the Pentagon spending millions of dollars on the technology. As drones begin to talk to each other as well as to humans, the accountability and legitimacy gap between the human decision to kill and the machines performing the lethal act is likely to grow.

Minding the Gap

These challenges are well known, and the Pentagon has long touted a policy of "responsible AI" that aims to address them through a labyrinth of laws and regulations. This sounds good on paper, but the conventional drone program, too, was promoted as being "legal, ethical, and wise" before serious concerns about civilian harm surfaced. If the past drone wars are any indication, truly responsible AI drone warfare similarly may prove elusive, particularly where gaps in protection arise in the various legal, ethical, and policy frameworks that govern AI use. For this reason, several states and the International Committee of the Red Cross (ICRC) have proposed banning weapons systems that lack meaningful human control and are too complex to understand or explain. In the first United Nations Security Council meeting on AI in July, U.N. Secretary-General António Guterres proposed that states adopt within three years a "legally-binding instrument to prohibit lethal autonomous weapons systems that function without human control or oversight, which cannot be used in compliance with international humanitarian law."

But even if states agree to such a ban in principle, significant questions remain. What legal limits must be placed on autonomous weapons systems to ensure compliance with IHL? What type and degree of human control is needed to ensure that future drone strikes meet the IHL principles of necessity, proportionality, and discrimination, as well as precaution? Is compliance with IHL sufficient or is a new treaty required? While many states have called for such a treaty, the United States, Russia, and India maintain that LAWS should be regulated under existing IHL. As the new drone wars become more ubiquitous, the exceptional rules that are said to apply in war – notably the lower levels of protections afforded by IHL – risk becoming the default regime. In the long term, the practical effects of this are the continued erosion of the prohibition on the use of force and the adoption of increasingly permissive interpretations of international law. The full costs and consequences of these developments are still emerging, but the precedents set now are likely to undermine individual rights in pernicious and irreversible ways. To counter this trend, states at a minimum should reaffirm the application of IHRL within and outside of armed conflict. The individualisation and automation of war has prompted a turn toward principles enshrined in IHRL, such as a stricter interpretation of the necessity criterion under certain conditions and similarly the provision that force should be used only if bystanders are unlikely to be harmed. Yet while IHRL offers additional protections beyond IHL, the precise interaction between IHL and IHRL is disputed and varies according to state practice. Fundamentally, these legal regimes were not designed to regulate non-traditional conflicts and non-traditional means of using lethal force, and gaps in legal protections are likely to grow wider in the coming drone wars. These gaps have prompted the ICRC to emphasize "the need to clarify and strengthen legal protections in line with ethical considerations for humanity." In cases not covered by existing treaties, Article 1(2) of Additional Protocol I and the preamble of Additional Protocol II to the Geneva Conventions, commonly referred to as the "Martens Clause," provide that individuals should be protected by customary IHL, as well as the "principles of humanity and the dictates of public conscience." But ethical considerations may diverge substantially from the law. The relationship between morality and law is a longstanding scholarly debate beyond the scope of this article. Briefly, the law serves a different

purpose from morality insofar as it must consider the effect that conventions will have on behavior, degrees of epistemic uncertainty in the real world, and anarchy in the international system. Under these circumstances, the morally optimal *laws* may be, in the words of Henry Shue, just those that "can produce relatively few mistakes in moral judgment – relatively few wrongs – by angry and frightened mortals wielding awesomely powerful weapons." The unpredictable and complex nature of AI, however, complicates efforts to discern, *ex ante*, the right course of action. Even when humans follow all the legal and policy guidelines, the gap between human decision-making and machine action implies that outcomes may not be moral. Far from it. What is moral may not be legal or wise – and vice versa.Policy guidance, meanwhile, is not a substitute for the protections that the law affords. The newly crafted U.S. Presidential Policy Memorandum (PPM), for example, is supposed to provide additional protections above what the laws of war require for direct action, that is, drone strikes and special operations raids. But the policy guidance is not legally binding, can secretly be suspended at any time, contains numerous exemptions for collective and unit self-defense, and applies to only a fraction of U.S. drone strikes outside of "areas of active hostilities," notably in Iraq and Syria. Moreover, the policy guidance was written with conventional drone strikes in mind. As the world stands at the precipice of a new phase in AI-driven drone warfare, it is time to rethink the rules.

Walking Back from the Precipice

There have been a number of proposals for regulating lethal autonomous weapons systems, including AI-enabled drones. But if the past drone wars are any indication, these regulations are still likely to fall short. Human oversight and compliance with existing laws and standards is essential, but not sufficient.

To more fully protect civilians in the coming drone wars, U.S. policymakers should take the following steps as a matter of urgency:

1. ***Develop a U.S. government-wide policy on the use of AI in drone warfare.*** While the Department of Defense has published numerous guidelines on AI and autonomous weapons systems, these directives do not necessarily apply to other agencies, such as those in the U.S. Intelligence Community. This oversight is deeply concerning given the crucial role that these other agencies may play in identifying, vetting, and attacking targets on a routine basis.
2. ***Follow the "two-person rule."*** During the Cold War, the two-person rule required two or more authorized individuals to be present when nuclear weapons or material were being repaired, moved, or used. This rule was designed to prevent nuclear accidents or misuse that could pose significant risks to human life. AI-enabled weapons have similar potential for catastrophic results and should follow the same rule for all drone operations.
3. ***Reduce the accountability gap.*** Increasing autonomy in drone warfare will make strikes more unpredictable, resulting in mistakes that cannot be attributed to any particular individual. To reduce this risk, the timeframe between when humans approve a target for lethal action and when drones take that action should be minimized to mere seconds or minutes, not days or months. Under no circumstances should drones be allowed to independently target individuals who are on a pre-approved (human approved) "kill list."
4. ***Conduct and publish routine AI health audits.*** To mitigate the problem of explainability, humans must check AI and AI must check itself. "Checking AI" can be a powerful tool in ethical audits, helping humans test AI systems and identify flaws or underlying biases in algorithms. AI health checks must be performed at regular intervals, and the results should be briefed to members of Congress (e.g., the Gang of Eight), and a redacted version should be made available to the public.

Pandora's box has been opened, but policymakers can still place necessary guardrails on the AI revolution in drone warfare. In the words of Martin Luther King, the United States is "confronted with the fierce urgency of now" and there is "such a thing as being too late."

Brianna Rosen is a Senior Fellow at Just Security and a Strategy and Policy Fellow at Oxford University's Blavatnik School of Government. She previously served for a decade in the U.S. government, including at the White House National Security Council and Office of the Vice President.

Cheap drones rigged with explosives have become the leading anti-tank weapon against Russian forces, Ukrainian commander says

Source: https://uk.sports.yahoo.com/news/cheap-drones-rigged-explosives-become-184708410.html

Oct 04 – Cheap drones rigged with explosive devices have become extremely prominent and have emerged as the leading anti-tank weapon for the Ukrainian military in Russia's war against it. A Ukrainian officer told The Washington Post in a report published on Wednesday that first-person-view (FPV) drones,

which are operated remotely with the use of a controller and headset, "have become the main anti-tank weapon" against Russian forces, compared to alternatives like anti-tank missiles.

A Ukrainian drone operator from the 24th Separate Mechanized Brigade holds a drone during the testing of new military equipment including FPV drones on the training area amid the Russia-Ukraine war in Donetsk Oblast, Ukraine on August 03, 2023.Wojciech Grzedzinski/Anadolu Agency via Getty Images

The inexpensive homemade explosive-laden one-way attack drones have been destroying Russia's more advanced T-90M tanks, worth millions of dollars, and other armored vehicles on the battlefield, Senior Lt. Yuri Filatov, drone systems chief commander for Ukraine's 3rd Separate Assault Brigade, told the Post. In a single day, Filatov recalled, Ukrainian forces used the exploding drones to wreck four Russian tanks, all while keeping Ukrainian troops a safe distance from the destruction. "As we use more drones," the officer told The Washington Post, "we are losing fewer people." In recent months, these low-budget attack drones, which cost between **$400 and $500**, have wreaked havoc on the battlefields in Ukraine. They're being used by both the Ukrainians and the Russians. "It's a revolution in terms of placing this precision guided capacity in the hands of regular people for a tiny fraction of the cost of the destroyed target," drone expert Samuel Bendett of the Center for Naval Analyses told the Post.

"We're seeing FPV drones strike a very precise spot, which before was really the domain of very expensive, high precision guided weapons. And now it's a $400 drone piloted by a teenager," he added.

The expert explained that the use of the unmanned aerial vehicles could have a "tremendous psychological effect" on would-be targets. "You almost never know where an FPV drone is coming from," said Bendett.

A deputy company commander in Ukraine's 80th Separate Assault Brigade told the Post that Russian troops use FPV drones the same way as Ukrainian soldiers but noted that it appears Moscow has more equipment. "It's like a chess game," said the commander who goes by the call sign Swift. "They're winning it. Just in terms of quantity." While that may be the case, experts previously told Insider Ukraine has demonstrated better top-level support for the production of these systems than Russia. Ukraine's Minister of Digital Transformation Mykhailo Fedorov, for example, has said that the country is dedicated to building up a cutting-edge "army of drones," and that project has seen the introduction of thousands of unmanned platforms into combat. The Associated Press recently reported Ukraine has already trained more than 10,000 new drone pilots this year.

US Army scrambles to catch up to rising drone threat

By Sam Skove (Staff Writer)

Source: https://www.defenseone.com/threats/2023/10/us-army-scrambles-catch-rising-drone-threat/391014/

Oct 06—Dangling from the ceiling and laid flat on display stands, sleek drones of every shape and size were ubiquitous at last month's sprawling DSEI arms show. Far less common were weapons to stop them. The same is true on the battlefields of Ukraine—and in the arsenals and training grounds of the U.S. Army.

Paratroopers with the Army's 82nd Airborne Division train on Dronebuster counter unmanned aircraft systems at Fort Liberty, North Carolina, July 28, 2023. U.S.Army / Pvt. Jayreliz Batista Prado

Army officials say NATO's largest land force is making progress when it comes to defending troops from drones. But service leaders have yet to make definitive plans for their future counter-drone force, even as they field far fewer defenses than analysts suggest will be needed.

Drones are ubiquitous on Ukrainian battlefields, where they have been used for everything from artillery coordination to strikes on civilian infrastructure. Russian loitering munition drones, for example, are the leading cause of destruction of Ukraine's Polish-supplied artillery, Polish Land Forces' Lt. Gen. Wieslaw Kukuła told *Defense One*.

Consequently, Ukraine and Russia both field a wide array of drone-killing tech, from hand-held jammers to vehicle-mounted autocannons. Ukrainians say Russian electronic warfare is particularly potent against their drones.

But both sides' drones regularly slip through air defenses, mounting strikes on Moscow and on Ukrainian power stations. The latter concerns Ukrainian Air Force Command, said spokesman Yuriy Ihnat, who added that Ukraine lacks sufficient short-range air defenses to fend off this winter's expected attacks by Russia on electrical plants.

Ukraine isn't alone. If anything, the U.S. Army may be even more behind when it comes to drone-killing solutions.

About two decades ago, the Army radically cut spending on short-range anti-air systems, under the belief that the Air Force could control the sky. In 2005, the Army reduced its short-range air defense, SHORAD, units to two active duty battalions and seven National Guard battalions, both operating the 1980s-era Avenger.

"Army SHORAD by 2014 was, for all intents and purposes, extinct," wrote Army Capt. Peter Mitchell in an essay for West Point's Modern War Institute.

The Army has since made moves to address the drone threat. The Army leads the Pentagon office tasked with combating small drones, and will launch a counter-drone training academy at Fort Sill in 2024. It's testing various types of defenses, including microwave weapons from Epirus.

In 2021, the first Army unit took delivery of the M-SHORAD, a Stryker-mounted short range air defense system that sports four Stinger missiles and an autocannon. The Army plans to field 144 M-SHORADS, enough for four battalions.

The Army has also approved the purchase of three types of hand-held drone-jamming systems. It's unclear how many are fielded. The maker of one approved system, the DroneBuster, reports having sold 2,000 to "military and law enforcement customers around the globe."

The Army also has the Mobile-Low, Slow, Small Unmanned Aircraft System Integrated Defeat System (M-LIDS), which is currently deployed to the Middle East. In April, Aaron Hankins of Leonardo DRS Land Systems said that the Army wanted to equip nine divisions with five sets of MLIDS each, and would start fielding systems next year. Leonardo Land Systems is the developer and integrator of the air defense systems on the MLIDS.

Spurred in part by reports from the Ukraine war, Army leaders say that they are working on a new counter-drone strategy. "We're going to need to probably have organic air defense with our maneuver units so that they can protect against drones," said Army Secretary Christine Wormuth at think tank CSIS.

"The Army is very much watching the kinds of drone/counter-drone war in Ukraine and doing the best we can to incorporate those lessons into our future plans," said Doug Bush, assistant Army secretary for acquisition at a September press briefing in the Pentagon.
Some in the Army want to add anti-drone strategies at every level of command. The drone threat is "going to be so prevalent," said Lt. Col. Richard Brennan, who participated in an Army-led counter-drone tabletop training event in September. "It has to be something you're accounting for at the lowest level."
But despite active debate, the Army has yet to figure out just who needs counter-drone systems and how many to buy.
The problem of how many counter-drone systems the U.S. need is a "key question" for the Army, said Chris Pernin, a senior physical scientist at the RAND Corporation who also participated in the September counter-drone training event.
Meanwhile, the number of weapons fielded are likely far under what's required. Past air defense plans gave each Army division its own dedicated short-range air defense battalions. With plans to field just four M-SHORAD battalions, that means that 15 Army divisions will have to do without.
The problem, in fact, may be even worse. Nick Reynolds, a research fellow for land warfare at RUSI who has written extensively on the Russo-Ukrainian war, believes that Western armies should have "some sort of counter-drone capability at every echelon from company-level and above."
The Army fields a collective 19 active duty and National Guard divisions, with a minimum of 950 companies. With the Army planning just 144 M-SHORAD systems and 45 M-LIDS sets, most of those companies will therefore go without a dedicated anti-drone system.
Nor, even, is it obvious which anti-drone system the U.S. will use. The U.S. has tested microwave weapons, lasers, auto-cannons, and jammers against drones, but has not chosen one single system to invest in. "The Army is going to have to face reality," on counter-drone policy, said Peter Wilson, a senior defense policy analyst at RAND Corporation."How do you protect your mechanized armored forces? How do you maneuver under the threat of surveillance?"
Other nations, meanwhile, are plowing ahead with anti-drone acquisition, representatives of two companies that produce anti-drone weapons told *Defense One* at DSEI.
Multiple countries have purchased MSI Defense Systems's jammer-and-gun combination, and the weapon is currently in serial production in several variants, said product manager Robert Gordon. APS is even refining its jammers based on data collected from sending them to Ukraine's frontline around Bakhmut, said Maciej Klemm, CEO of APS.
Still, despite a rise in demand related to Ukraine, industrial manufacturers see every country as being one step behind. "Yes, there is a lot of investment; yes, there are a lot of requests for information; but it's an education process so far," said Silje Jahr, head of sales at anti-drone company MARSS.
MSI's Gordon agreed: "The drone threat has moved so much quicker than both industry and the military's ability to find solutions. Everyone is behind the curve."

AI drone swarms that choose their own kill targets are the next 'weapons of mass destruction', scientists warn

Source: https://www.the-sun.com/tech/9342885/ai-drone-swarms-kill-targets-weapons-mass-destruction/

Oct 16 – Scientists have warned that autonomous drones powered by artificial intelligence could cause harm to civilians.
In a recent study, researchers have claimed that AI-powered instruments are the new weapons of mass destruction (WMD).
"Technological progress has brought about the emergence of machines that have the capacity to take human lives without human control," the paper reads.
"These represent an unprecedented threat to humankind," it continued.
These autonomous weapon systems (AWS) include AI drones that are already being developed by countries like the United States and China.
Drones are aerial devices that initially were controlled remotely by a person, however, now they work autonomously without human control.
Insect-sized drones that are "reduced to undetectable devices capable of administering lethal biochemical substances through their stings" are also of concern to the researchers.
They note that science and society are challenged by such unprecedented technologies because they might not always be developed responsibly.
"The potential consequences of a deployment of AWS for citizen stakeholders are incommensurable, and it is time to raise awareness in the public domain of the kind of potential threats identified and to encourage legal policies ensuring that these threats will not materialize," the paper reads.

Drone tech

Today's AI drones use machine learning and sensors to gather data, assess their environment, and even fire an attack on their own.
The paper notes that these armed, fully autonomous drone swarms are deemed to become future weapons of mass destruction.
This is because they combine "two properties unique to traditional weapons of mass destruction."
The first is the ability to cause mass harm and the second is the lack of human control to ensure the weapons do not harm civilians.
"Experts doubt that any single autonomous weapon could ever be capable of adequately discriminating between civilian and military targets, and with thousands or tens of thousands of drones in a swarm, this risk becomes incommensurable," the paper reads.
In conclusion, the paper deems that AWS are deadly devices that can identify potential targets and independently choose to attack them based on algorithms.
In response to this growing threat, the researchers propose that experts increase multidisciplinary research and dialogue around the topic.
Specifically, they call for public discussions on ethical and moral responsibility at AWS.

New tech can guide drones without relying on GPS

Source: https://i-hls.com/archives/121323

Oct 18 – Researchers at The University of Tokyo and telecommunications company NTT in Japan developed an RFID-based guidance system for autonomous drones.
Drones conventionally rely on imaging to determine their location, but as more and more piloting is being done by machines it is becoming increasingly difficult to make a drone aware of its location, which makes tools like GPS and image recognition increasingly necessary. Furthermore, changes in weather conditions impact the quality of the images generated from onboard sensors. The Japanese collaboration has found the solution in RFIDs.
According to Interesting Engineering, RFID (radio-frequency identification) tags are battery-less tags that are temporarily powered up by the radio signal emitted by an RFID reader. The tag then uses this energy to relay the information it contains back to the reader using an integrated antenna.

The Japanese research team deployed a similar system on the autonomous drone. Since the communication occurs using millimeter wave frequency, the signals can travel a few miles and the drone can communicate with the RFID tag, even if it isn't within visual range.
Since conventional RFID tags are made to work over extremely short ranges, the researchers have worked on improving the reflective capabilities of the RFID tags by adding corner reflectors to the tags so that they could receive and send back signals over a wider three-dimensional angle.
In order for them to also function in highly congested environments (like urban landscapes) the research team had to develop a new signal-processing pipeline that could work with greater accuracy and overcome the narrow reading range of millimeter-wave RFID technology.
All this begs the question, why not simply use GPS? The researchers explained that for the GPS-based tech to function, there need to be two GPS modules, one on the drone and the other on the landing point. This would not only increase the cost of installation and maintenance of these modules, it would also require that the landing port maintain a source of power to keep the GPS module working.
While all this is not very feasible in extremely remote locations, a battery-less RFID tag on the other hand can work anywhere in the world without the need to generate power for its operation. Moreover, it can be relied upon for long periods of time, as long as it remains undamaged in the remote location.
This solution could reportedly be deployed to deliver healthcare needs in remote areas or even disaster response without waiting for infrastructure to be made ready.

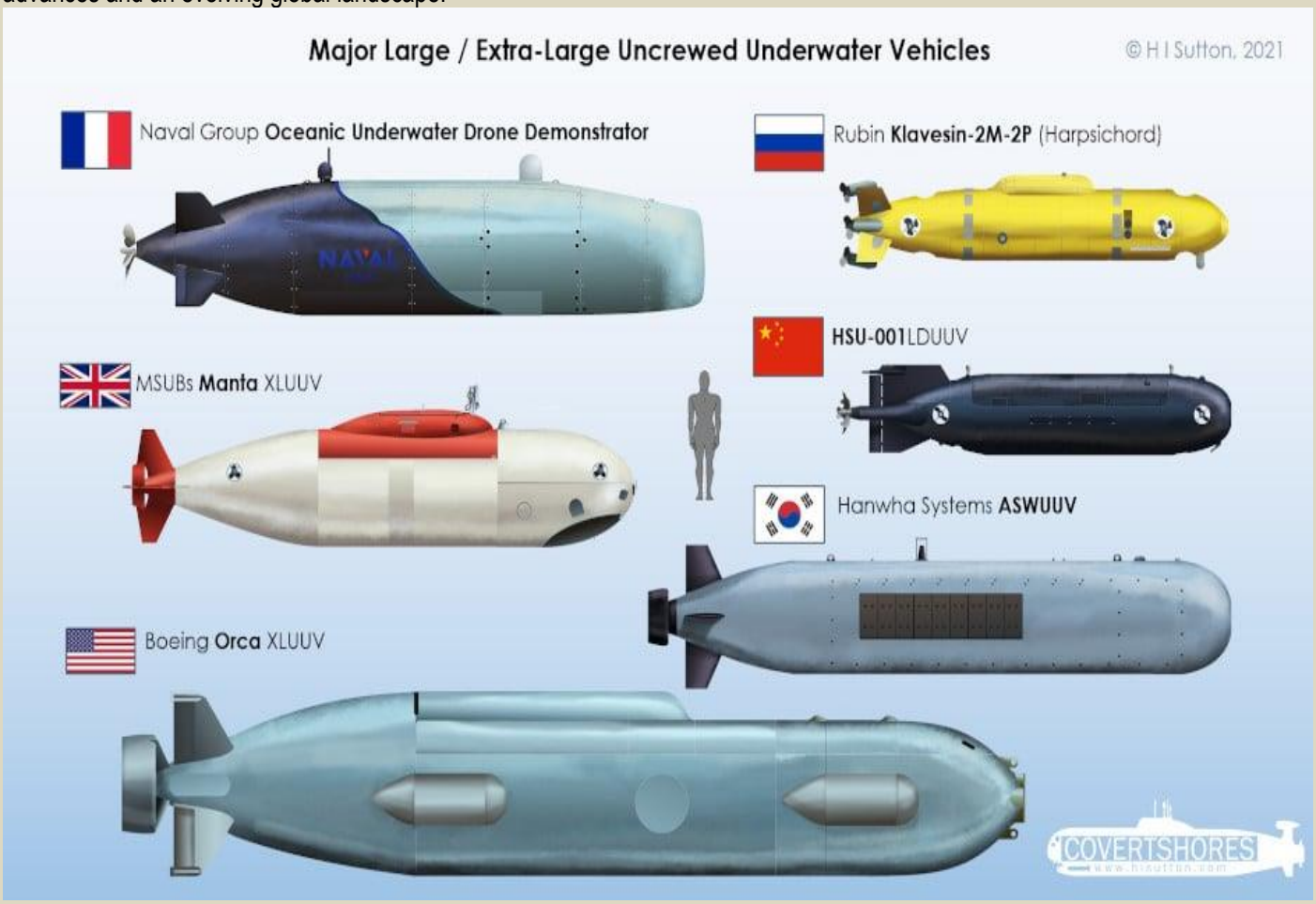
Uncrewed Submarines – the Future of Naval Warfare

Source: https://i-hls.com/archives/121303

Oct 17 – There is a worldwide growing significance in modern maritime security of drone submarines, also called "uncrewed underwater vehicles" (UUVs). These UUVs are becoming increasingly affordable, widespread, and sophisticated.

Maritime defense and security are extremely important, and the potential consequence of a disruptive event, be it a blockage, an accident, or an explosion in a critical location, has not escaped the attention of nations worldwide, who know the strategic importance of safeguarding these vulnerable undersea assets.

One pressing example is the ongoing war in Ukraine, where the use of underwater drones proved their multifaceted applications in intelligence, surveillance, reconnaissance, mine countermeasures, antisubmarine warfare, electronic warfare, underwater sensor grid development, and special operations. The potential of these underwater drones is set to expand, driven by technological advances and an evolving global landscape.



According to Interesting Engineering, nations worldwide are also working on broader initiatives to gain control over underwater sea domains, like the proposed US Advanced Undersea Warfare System, which envisions a network of fixed submarine stations capable of deploying defensive and offensive drones. Another example is the South China Sea, in which China is reportedly developing an expansive "Underwater Great Wall" composed of ships, bases, and drones, both on the surface and beneath the waves, to closely monitor the region and make it challenging for foreign navies to operate in international waters.

Some analysts claim that these developments signify the advent of a "new age of naval warfare," which is characterized by an increasing reliance on autonomous maritime systems. Moreover, the increased number of sea drones may induce the growth of hybrid or "grey zone" approaches to conflict- tactics that avoid full-scale warfare, keep casualties to a minimum and impose significant costs on adversaries.

It is clear that underwater drone submarines are poised to play a pivotal role in the security and stability of coastal nations and global trade routes, and with the potential for disruptive threats and innovative defensive capabilities, countries must adapt and integrate these technologies into their long-term planning to ensure a secure and resilient maritime future.

Emerging Technologies, Part 2 – Uncrewed Vehicles

By Ian Pleet

Source: https://domesticpreparedness.com/articles/emerging-technologies-part-2-uncrewed-vehicles

Oct 18 – Uncrewed vehicles have many forms: uncrewed aerial vehicles (UAVs), uncrewed ground vehicles (UGVs), and uncrewed maritime vehicles (UMVs). They are autonomous or remotely controlled machines designed to perform tasks without human operators' direct involvement. They have evolved rapidly in emergency management, humanitarian relief, and disaster response. These vehicles offer advantages such as enhanced data collection, accessibility to remote or hazardous areas, and increased operational efficiency, making them valuable assets in addressing all hazards and managing emergencies.

Benefits During Disaster Response

Search-and-rescue operations widely use UAVs for earthquake responses, floods, and other natural disasters. UAVs with cameras and thermal sensors can quickly survey disaster-stricken areas, locate survivors, and identify hazards or blocked pathways for rescue teams. UAVs create high-resolution maps of disaster-affected regions, providing real-time data on the damage extent and helping authorities plan and allocate resources more effectively. Drones can function as flying communication relays in areas with a disrupted conventional communication infrastructure, facilitating coordination among rescue teams and affected communities.

Uncrewed vehicles provide humanitarian relief in remote or inaccessible regions to transport medical supplies, vaccines, and essential medications to disaster-stricken areas, ensuring timely aid to those in need. UAVs can assess the structural integrity of critical infrastructure, such as bridges and buildings, following disasters, guiding engineers and responders in prioritizing repair and reconstruction efforts. For disaster response, UGVs can navigate challenging terrains to deliver food and clean water to affected populations in disaster zones, especially where traditional transportation is unavailable. With specialized sensors and manipulators, these vehicles can manage hazardous materials in chemical spills or nuclear accidents, minimizing human exposure to danger. Uncrewed vehicles can collect data on environmental conditions, air quality, and pollutant levels, aiding in disaster impact assessment and response planning.

Examples of Uncrewed Vehicle Applications

These are four examples of successful implementation of uncrewed vehicles being used to respond to natural disasters:

- Following the devastating earthquake in Nepal in 2015, UAVs surveyed the affected areas, assessed the damage, and created detailed maps to assist rescue and recovery efforts.
- In response to Hurricane Harvey's aftermath in 2017, the Federal Aviation Administration authorized UAVs to support damage assessment, search-and-rescue operations, and infrastructure inspection.
- During the 2018 Kerala floods in India, UAVs aided in locating stranded individuals, assessing flood levels, and mapping areas to distribute relief materials effectively.
- Australia has extensively used UAVs equipped with infrared cameras to monitor the spread of wildfires, track hotspots, and assess fire damage.

In conclusion, uncrewed vehicles have become valuable tools in emergency management, humanitarian relief, and disaster response efforts. With their ability to collect real-time data, navigate challenging terrains, and perform tasks that might be dangerous for human responders, these vehicles significantly enhance the efficiency and effectiveness of hazardous emergency operations. As technology advances and regulations evolve, integrating uncrewed vehicles in disaster management will save lives and improve response capabilities.

Links to other articles in this series:

Part 1 – Information and Communication

Part 2 – Uncrewed Vehicles

Part 3 – Artificial Intelligence and Machine Learning

Part 4 – Robotics and Automation

Part 5 – Legal and Privacy Concerns

Ian Pleet is a veteran U.S. Navy Hospital Corpsman and has worked as a contractor in U.S. Northern Command (USNORTHCOM), U.S. Indo-Pacific Command (USINDOPACOM), and U.S. Central Command (CENTCOM). He is a Change Management Advanced Practitioner, FEMA Professional Continuity Practitioner, and Nationally Registered EMT.


ICI
International
CBRNE
INSTITUTE
AI - NEWS
C2BRNE
DIARY

Inventor ponders ethics of wiring human brain tissue into computers

Source: https://newatlas.com/computers/cortical-labs-dishbrain-ethics/

Cortical Labs has prototyped computing modules built around human brain cells, and is looking to commercialize this hybrid learning intelligence – Cortical Labs

Sep 22 – When you take 800,000 human brain cells, wire them into a biological hybrid computer chip, and demonstrate that it can learn faster than neural networks, people have questions. We speak to Dr. Brett Kagan, Chief Scientific Officer at Cortical Labs.

Cortical Labs is an Australian company doing some mind-boggling work integrating human brain tissue, grown from stem cells, into silicon electronics, where they can talk to computer components using the same electrical signals they send and receive in the body, and exhibit learning behaviors by constantly rewiring themselves, growing and shrinking connections as they do when we learn.

The company says its "human neurons raised in a simulation... grow, learn and adapt as we do." That they consume vastly less power, and appear to learn much faster, and generalize learned knowledge more effectively, than the building blocks of today's reinforcement learning supercomputers, while showing "more intuition, insight and creativity."

Living neurons continually rewire themselves on the silicon substrate, forming, strengthening and weakening connections in response to stimuli – Cortical Labs

Indeed, the company hit the world stage in 2022 with a paper titled "*In vitro neurons learn and exhibit sentience when embodied in a simulated game-world*."

Sentience – the capability to experience sensations or feelings – in this case referred to the neurons' apparent preference for ordered and predictable electrical stimulation when wired into a computer chip, as opposed to random and unpredictable stimulation.

The Cortical team effectively used this preference as a reward/punishment scheme while feeding the cells information about a video game – Pong – and allowing them to move the paddle, and found that both human and mouse brain cells were quickly able to figure out how the game worked, keeping the ball in play significantly longer after just 20 minutes in the system. Human neurons, perhaps unsurprisingly, showed a significantly greater learning rate than the mouse ones.

A ridiculously exciting moment for science, and a potential revolution in computing – but the concept of sentience implies that there's an entity there experiencing something. This raises ethical questions; does a collection of human brain cells, grown in a petri dish, bathed in cerebro-spinal fluid and fed an electrical picture of a simulated world, have moral rights?

If you eventually give it control over a robotic body, thus giving it a similar electrical picture of the real world to the one our senses give us – and that certainly seems to be a stretch goal here, judging again by the company's website – what on Earth do you call that thing? And as the company moves to commercialize this technology, is the whole shebang remotely OK?

While the company has clearly leaned in to the whole sentience idea in some of its advertising, Cortical Labs is keen to get out in front of these questions, put a lid on the idea that these things might be conscious or self-aware, and build an ethics framework into its work at this early stage. As such, it's teamed up with some of its more vocal early critics and presented a framing study to begin illuminating the path forward, putting forth the idea that these living computer chips have plenty of potential to do moral good.

We caught up with Cortical Labs Chief Scientist Dr. Brett Kagan, to learn where things are at with this controversial and groundbreaking technology. What follows is an edited transcript.

Loz: I think I first encountered your work earlier this year when Monash announced military funding for development of the DishBrain.

Dr. Brett Kagan: Yeah. We'll leave it at that, Monash put out a media release on that. Yes, they're involved in that and we're doing a collaboration with them, as well as University of Melbourne on that. But the DishBrain, and the synthetic biological intelligence paradigm, have been developed pretty much in-house, with some involvement of just a few collaborators looking at some of the stuff around the edges.

So where are things at at the moment with the technology itself, and in which directions are you pushing?

The technology is still very much at the early stages. You know, we often compare our work now to the early transistors. They're kind of ugly. They're kind of big, and ungainly, but they could do some useful stuff. And decades of innovation and refinement led to some remarkable technology that now pervades our entire world. We see ourselves as being at that early stage.

We often compare our work now to the early transistors. They're kind of ugly. They're kind of big, and ungainly, but they could do some useful stuff.

But the difference between this and transistors is that at the end of the day, we're working with human biological tissue, which reflects to us – so there are immediate applications that become useful now. You don't have to wait for the technology to get to that very mature stage that could end up in everyone's home. In fact, if you can figure out how brains are working, you can design better drugs, or understand diseases better, or even just understand *us* better, which from a research perspective is highly impactful.

Can you describe DishBrain in simple terms?

We've already moved on from that moniker, but DishBrain was the initial prototype we developed to really ask the question, can you interact with living biological brain cells in such a way as to get an intelligent process out of them? And we did that by playing the game Pong.

So essentially, DishBrain is a system that takes information from neurons when they're active – which you can see through electricity – places that information into a world – in this case, the Pong game – and allows them to actually impact the Pong game by moving a paddle. And then as they move the paddle that changes the way the world looks, and you then take that information for how the world looks and feed it back into the neurons through electrical information. And if you do that in a tight enough loop, it's almost like you can embody them inside this world.

That's what the DishBrain prototype was designed to do. And what we saw, to our excitement, was actually yeah, not only can you get meaningful learning, you get that meaningful learning incredibly rapidly, sort of in line with what you might expect for biological intelligence.

Not only can you get meaningful learning, you get that meaningful learning incredibly rapidly, sort of in line with what you might expect for biological intelligence.

So from the Pong construct, where have you taken it since then?

Essentially, we've been trying to take that technology to the next level. The initial work we did was very cool in an academic sense. You know, we had a question, we developed a new technology to answer the question, and we got a pretty nice answer that people seem to be interested in.

But actually for us, it's no good having this technology if others can't access it. So we've been putting a huge amount of effort into actually building more accessible technologies for people. We've been building a full stack – hardware, software, user interface, as well as all the wetware, which we call the biology, so that people can actually have access to this and start exploring ways to apply it, that might appeal to them.

We get all sorts of requests – can they play music? Can you use it to test for epilepsy? Can you mine Bitcoin with it? Some of these we provide more support to than others! But the bottom line is like, even if it's an idea we think is a bit out there, we want to make it available for other people to investigate it. So

that's where we've been focusing on taking the technology: just making it accessible. And we've made some great strides in that.

So what, you've got a box that you can now ship to to people?

It's still in the prototype stage, but yeah, we have some boxes.

How long do these cells live?

We're able to keep cells alive for up to a year. **Six months is very standard,** but that's actually just using traditional cell culture methods. If you're going to ask how long do human neurons survive for, I mean, you can look at people. We have neurons, and while some new ones are born throughout our lives, for the most part, the ones you're born with are the ones you die with. Probably slightly fewer for most of us! So neurons can last 100, 120 years in theory.

In practice, we don't think we'll necessarily get neurons in a dish to do that, but we do have confidence that we will be able to get to a state where we can keep them alive and functioning well for 5 to 10 years. We're not there yet, but theoretically, it's very possible.

Right, and which applications are you seeing them shine in? What's looking most promising?

We see the immediate short term focus being stuff like drug discovery, disease modeling, and understanding how intelligence arises. Now that can sound kind of pedestrian, some might say, but if you look at, let's say, clinical trials for neurological diseases, for new drugs, you're talking about 1-2% success rates. For iterations on things already shown to work for another disease, you're looking at only a 6-7% success rate, maybe 8%, depending on what you're looking at. It's abysmally low. And so that means there's all this money being poured into drugs that in theory should help people, but are wasted.

The MaxOne chip – Cortical Labs

So, yeah, we can improve that by actually testing drugs on the true function of neurons, right? The true function of a neuron is not just to sit in a dish, or to even have activity. The true purpose of a neuron is to process information. So we've been doing testing on drugs and finding that you can get massively different responses if you're testing them on neurons while they're actually playing a game, versus just sitting there doing nothing.

Right, you're giving these neurons a job to do, and then assessing the effects of various drug interventions?

Yeah, exactly. And it gives you a very different perspective, that could really change the field of pharmacology for neuro-related diseases.

Fascinating. So as a computer component, outside the context of drug testing, are there particular tasks that this thing is likely to excel in?

Yeah, the answer is something like, anything that we humans might do better than machine learning. That might sound weird, because these days people love to hype up the machine learning angle, ChatGPT and whatnot. And they're really cool devices. And they do some stuff really, really well. But there are also things they just don't do well at all.

For example, we still use Guide Dogs for the visually impaired, instead of some sort of machine learning protocol. That's because dogs are great at going into a new environment, inferring what's around them, and what that is, even if they've never seen it before. You and I can see any trash can and generally immediately identify it as a trash can pretty quickly. Machine learning can't necessarily do that.

So that's what we've seen. We've done tests against reinforcement learning, and we find that in terms of how quickly the number of samples the system has to see before it starts to show meaningful learning, it's chalk and cheese. The biological systems, even as basic and janky as they are right now, are still outperforming the best deep learning algorithms that people have generated. That's pretty wild.

The biological systems, even as basic and janky as they are right now, are still outperforming the best deep learning algorithms that people have generated. That's pretty wild.

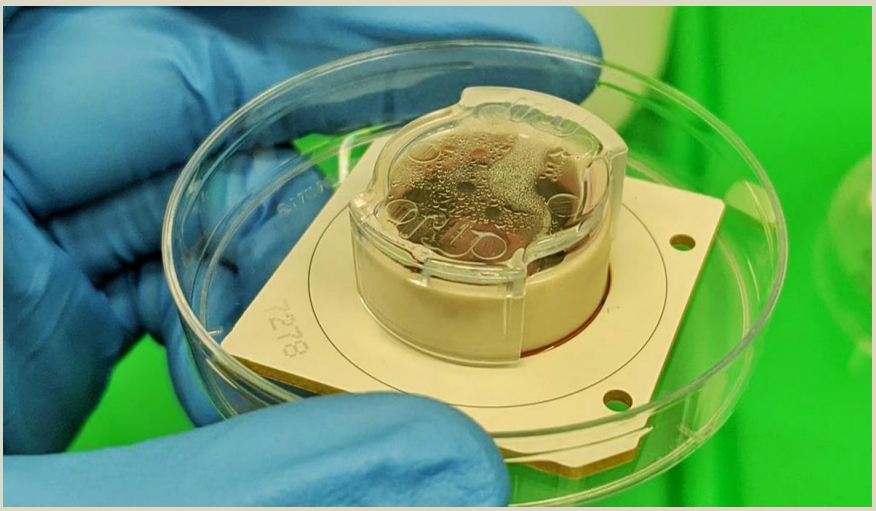
We published a paper through NeurIPS last year, if you're familiar with that conference, and we have another one under peer review at the moment. So yeah, it's been validated, it's not just an anecdote!

I guess the ethics side of things comes in when you start actually trying to figure out like, what are we dealing with here? Is this a life form? I mean, it is a life form! The cells are alive. It's biological. So I guess the question is, how do you draw a distinction between between what you guys are working with here and an animal? How is it fair to picture and to treat these things?

Everyone has a slightly different intuitive feeling about what that should be, and what we're really focused on in this work is anticipating what those might be, so that we can actually help educate people better as to the reality of the situation. Because it's all too easy for people to form an idea in their head that doesn't reflect that reality.

So we almost view it actually as a kind of different form of life to let's say, animal or human. So we think of it as a mechanical and engineering approach to intelligence. We're using the substrate of intelligence, which is biological neurons, but we're assembling them in a new way.

Let's compare an octopus to a human, they both show an intelligence, in some ways remarkable intelligences. But they're incredibly different, right? Because their architecture is so different. We're trying to build another architecture that yet again is different. And it can use some of the abilities that these things



have, without necessarily capturing, let's say, the conscious, emotional aspect. So in some ways, it's a totally different source of life, but then how do you treat that? And that's the questions we start to discuss in this paper.

The "wetware," looking particularly wet after a test session – Cortical Labs

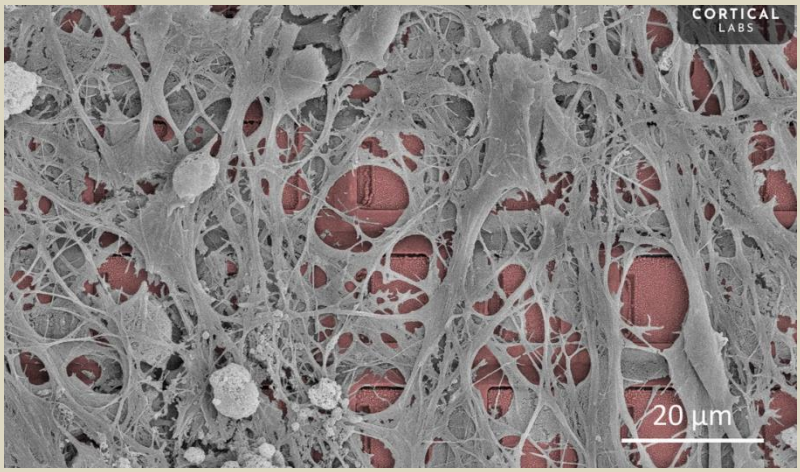
Yeah, obviously consciousness itself is still pretty mysterious. What's your intuition on, like, is there a number of cells, is there a level of interconnectivity... At what point does it go from being a pile of cells to getting a social security number?

Exactly, and people have been trying for even longer than neuroscience research has been around to answer these questions – like what is consciousness? What makes us *us*? What makes our feelings different to someone else's feelings? Or is it all the same? Or is it all an illusion?

We can't answer those questions now. But what we can do with these systems is actually start to pull apart, at a more nuanced level, what leads to certain patterns of activities and patterns of behavior that one might see. So the other work that we published in *Nature Communications*, about the same time as this one, was actually pulling apart something that happens in humans, that people had proposed was a marker for consciousness.

And we found that when you put these cells in a environment, like the Pong environment, they started to show this metric really, really strongly. But when we dove deeper into it we realized really clearly, like no question of a doubt about it, that what the cells are showing is not a marker of consciousness; it's simply what happens to a complex system in a structured information environment.

And so what we've done here is actually say look, some people – not many, but some – would propose that this is a marker of consciousness. But actually, it's so much more basic than that. And the initial proposals were very erroneous, based on a lack of information about how some things are working.



Human neurons growing on a Cortical Labs silicon chip – Cortical Labs

Briefly, what metric was this that you're talking about?

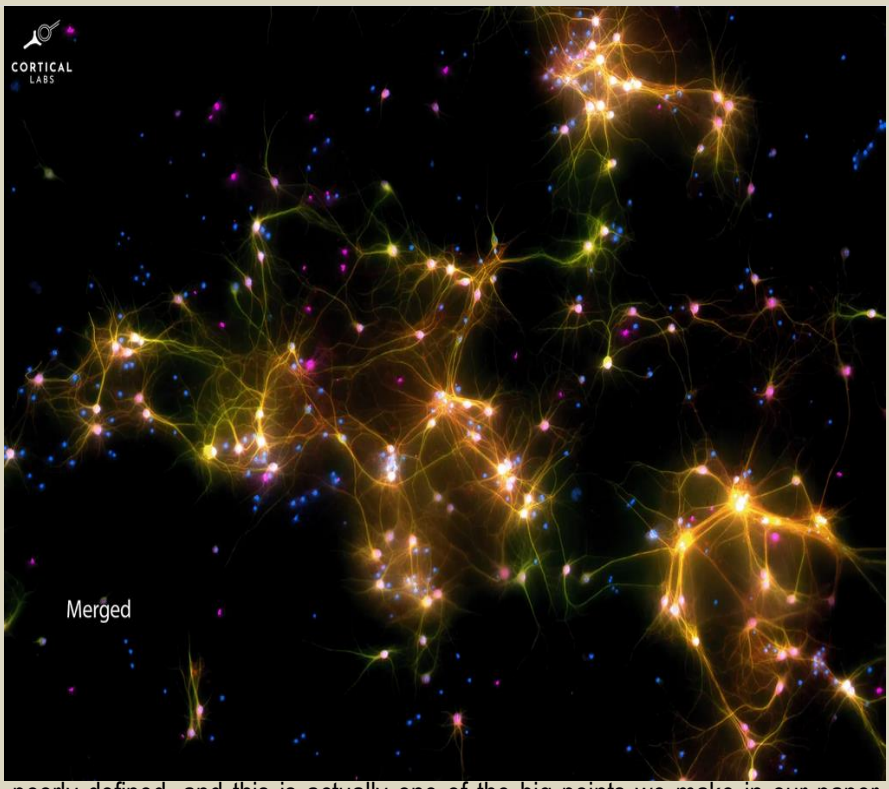
It's called criticality. It's a bit mathy. But in short term, you can imagine that there's a system, let's say water, and it could either freeze or stay liquid, and it's like right on the edge point. If it gets a bit cold, it'll freeze. If it gets a bit warmer, it won't. It's like right on the edge point. And brains can do similar things with activity. They can sit right on the edge point between chaos and order.

And that's been proposed to be really useful for a bunch of things. And this is where it all comes together, right? Like, you've got this hardcore math concept. And you have these discussions and ethics. But actually, by building out these systems, what we can start to do is be like, what is the right way ethically to think of this math concept and how it actually reflects something that's more meaningful to the average person. Which is, let's say, how they relate to the world and experience the world.

And you can see very clearly, in a way that people couldn't describe before, that that metric is useful to describe someone who's in a structured world... It's hard to make this simpler, right? But it's not a good marker for say, someone experiencing something unique.

And so by using the system, not only is there an ethics of the system, but the systems can help to answer ethics of the world, in a way that you can't do in a human, because a human has so much complexity going on. You can't just isolate and be like, what causes this thing to happen or not happen? Because there's everything else going on internally, externally, you can't remove a human from the world. But with a system you can. So you can start to pull apart and find that these things are far more fundamental, and that helps us ethically to

understand that actually, these things don't show any markers of consciousness. What they do show is markers of structural organization, you know, which one might call intelligence.



The beautiful efficiency of biological neural connections – Cortical Labs

It's almost like you're approaching this question from the opposite side as the people trying to figure out whether AIs are conscious. Like, GPT has passed all the Turing tests, there are very few tests on which language models don't appear to exhibit sentience, but intuitively, people know that it's not a sentient thing at the moment, it's a matrix of probabilities and they're trying to clarify the distinction at that end. But you guys are going from the opposite direction, which is like, we've got a group of living cells here. At what point does this become conscious or sentient?

Exactly. And I mean, even those words are so poorly defined, and this is actually one of the big points we make in our paper. Scientifically, ethically, socially, whatever, to discuss this technology right now is almost impossible, because nobody can agree on what these words mean.

Scientifically, ethically, socially, whatever, to discuss this technology right now is almost impossible, because nobody can agree on what these words mean.

And so we say to people, look, this technology seems to have huge potential. But because it's biological, and particularly using human cells, people start to feel unsure about it. So we're trying to say, hey, look, you can do this in a highly ethical way. Not only can you do it in a highly ethical way, doing this technology is really the only way we can start to understand the ethics of other things. That's why we've engaged with these amazing bioethicists, who have no vested interest in anything other than working out how to approach this technology responsibly, so it can be sustainable and have longevity.

What are the practical considerations for you guys? Like, if at some point you determine that you're dealing with something conscious, how does this affect what you do? Or are there kind of grades of sentience that can be treated differently?

100%. So for us, it needs to be a very tiered approach, and the one thing we're very against is people dropping into slippery slope arguments now.

For us, the very first thing we need to establish is the language that we're using, so we can all be on the same page. In theory, that should not be an impossible task, In practice, well, we'll see. Then we need to start to figure out how do we even define when these problems pop up? So we looked at criticality, maybe that was one option? It's absolutely, clearly not. We've looked at other things, again, absolutely, clearly not good markers. So it's like, first we need to find the markers that we can work with.

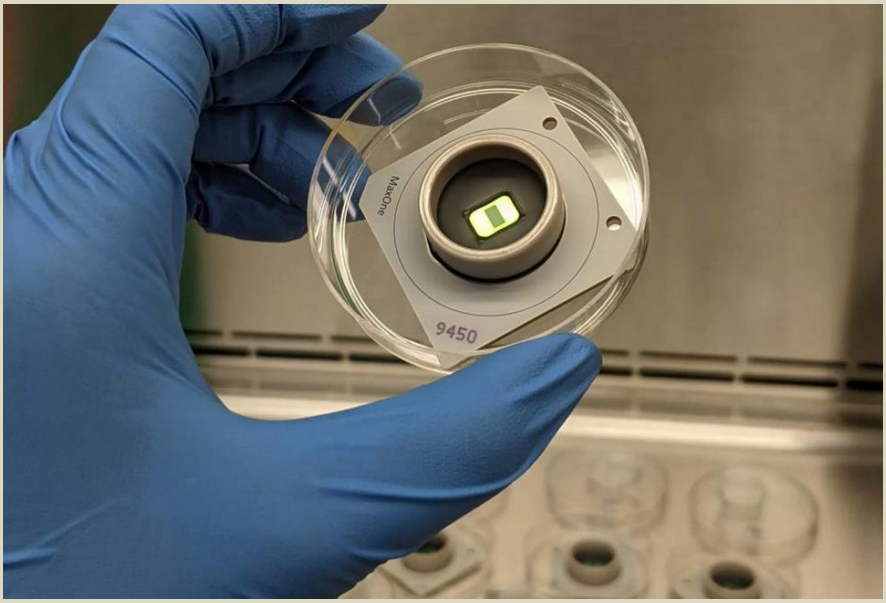
Bio-computers will require a little more attention than your standard desktop PC – Cortical Labs

And as I said, that's got this great benefit where it has this very organic interaction with the existing work people are doing, in trying to understand what consciousness even is, and how to define it. And that has implications not just for this work, but arguably for the way we live as people, how we treat animals, how we treat plants.

If we can understand at the level where consciousness is arising, it really just redefines how we relate to the world in general and to other people and to ourselves. And that's a really exciting perspective.

And then beyond that, let's say that these systems do develop consciousness – in my opinion, very unlikely, but let's say it does happen. Then you need to decide, well, is it actually ethically right to test with them or not? Because we do test on conscious creatures. You know, we test on animals, which I think have a level of consciousness, without any worry... We eat animals, many of us, with very little worry, but it's justifiable.

Is it actually ethically right to test with them or not? Because we do test on conscious creatures. You know, we test on animals, which I think have a level of consciousness, without any worry.



The MaxOne chip – Cortical Labs

So even if they do display this, let's say that you have to test on these partially conscious blobs in a dish. And let's not oversell it – little blobs of tissue in a dish that show some degree of awareness in the far future when we've improved it. It still could be worthwhile testing on it if you can develop, let's say, a cure for dementia. Right? I'm not sure where it would go. Obviously, these are very speculative. But even at that case, there could still be very strong arguments that this is still the best way to solve a much bigger problem.

You're playing in a strange and magical kind of world, invoking these concepts.

Yeah, a lot of people tell us what we're working on is like science fiction. But my response to that is that the difference between science and science fiction is once you start working on the problem, and we're very fortunate to have an amazing team of people, both with Cortical Labs, and with our collaborators who are working on these problems right now.

So where do you go from this paper?

So for us, this really is a framing paper. It's sort of saying: Here's what the technology looks like, because that's still very unclear to many people. Here's some applications, and here's our thinking around some of those applications and here's how to step forwards. And the key pathway is that we're adopting this idea called anticipatory governance, which is really about identifying where are the benefits, where are the potential issues, and how do we maximize those benefits while minimizing the issues. We'll really be diving into this area deeper to make sure that the work can, as I say, be progressed and applied responsibly.

The one thing we don't want is for people to see this and think, oh, science is running amok, no one's regulating this. Well, no one can regulate this yet because we don't understand it well enough.

The one thing we don't want is for people to see this and think, oh, science is running amok, no one's regulating this. Well, no one *can* regulate this yet because we don't understand it well enough. So our goal is to understand it, so we can all move forward and give people the confidence that this research has been done in the right way. You know, I'm not aware of many research fields, or perhaps any, where this sort of approach has been taken, where people have integrated ethics into the foundation of this type of research. But I think for the work we're doing, it's necessary.

Some of the people on this paper that we just did, the way we initially made contact was in opposition, they'd written a paper basically calling for prohibition of research down this line. And we wrote in saying, look, there's a bunch of errors we think that you've made in how you've done some of this work. And these folks actually turned around and went, yeah, actually, we agree with you. Why don't we work together on the next paper? So they ended up putting a piece in *The Conversation*.

And so we reached out to them saying, you know, we appreciate your openness, let's work together. So some of these people have gone from, you know, 'we need to decide what's not permissible,' to quote their paper, 'and actually start regulating it,' to 'this stuff has huge ethical potential if we do it right.' Let's work together. So I think it's been a great sort of 180 in quite a lot of the community simply by engaging and bringing all these different people together.

I was wondering what kind of external pushback you'd been getting. But those are the people you're now working with on ethics?

Yeah. You're always going to get a few people who are just negative, right? There's always gonna be people who are just naysayers. But what's been really awesome for us to see is that as soon as the

international community realized that we want to work with people to make this right and do the right thing, the welcome and the engagement we've had has been amazing.
And I think the problem really highlights that most scientists have a bit of disdain for that side. You know, they want to sit in their ivory towers and lob things off. But we're not like that, right? We want to bring the international community along. And so that's why we've gone out and engaged with them.

So, where you say there's huge ethical potential, you're talking about the ability to test drugs on complex neuron configurations doing some kind of intelligent work, before you go to clinical trials in humans?

That's just one of them. They're captured in the paper, so I'll be super brief. But one is reducing testing on animals. Two is improving the chance for clinical outcomes for people. Three is like equity and access; it's like a personalized medicine approach if you can test on a person's own DNA – which we can do, because we can generate cells from a consenting donor, so you actually improve equity and access. And because we're making the technology affordable, that has a socioeconomic benefit to it as well.
There's also the whole power consumption issue, as I said. If this could lead to more efficient use of power, it's less damaging to the environment, which is generally agreed upon as an ethical good.
And then once you get to this consciousness debate, the chance to actually identify what may or may not lead to consciousness, so we can figure out how to just be better in general is huge. It's further out there, but if it's attained, a huge ethical benefit, so these are sort of the core ones, but as I said, they're discussed in more detail in the in the paper.
Visiting The Cortical Lab

Right. Where does your company go commercial? What sort of product do you end up selling?

We're building up a cloud-based system. There's two options basically, the earliest one will be a cloud-based system, so you could log in from anywhere in the world, and you could test your environments that you might want to build, or you could work with us, and we'll help build them for you.
It'd be like, what happens to a neuron or collection of neurons if you do this, or if you put this drug in, or if you use this type of disease, cell line, whatever. So that's the first one, basically a cloud-based service. You can think of it like AWS, but for biology, right, and very much focused on on biological interventions and their effect on problem solving.
And in some ways, it could be computation, so we have a lot of neuromorphic people wanting to figure out how these things work so they can try and reproduce it in hardware. Or machine learning people looking at maybe, you know, could I build a better algorithm designed closer to the way the biology works? So there's a computing angle even now. It's just more of a deep research question so far. So that's the immediate short term commercialization options. Longer term, we obviously can't give any clear promises because it's more speculative, but as I said, the preliminary work suggests that for autonomous, self-learning systems, this is incredibly supportive. And on the ethical angle, for an autonomous, self-learning system, because it's contained to the biology, it's also arguably a hell of a lot safer than something that could, you know, presumably get out there and just replicate itself through software alone.
Not to mention the whole power consumption angle – machine learning, LLMs and all of that are hugely power-hungry during training, but human brains run on 20 watts.

They've been around for millions and millions of years. They've had a bit of time to optimize!

Use of AI to create bioweapons, weapons of mass destruction concerns the UK

Source: https://www.theweek.in/news/world/2023/09/25/use-of-ai-to-create-bioweapons-weapons-of-mass-destruction-concerns-the-uk.html

Sep 25 – As the United Kingdom prepares for the global artificial intelligence safety summit, discussions on use of the technology to create weapons of mass destruction and bioweapons by terrorists are said to dominate the summit attended by world leaders. Britain has been airing concerns about the ability of technology to evade human control altogether.
According to reports, the UK is sending representatives across the globe to build a consensus and to issue a joint statement about the dangers of using the technology to cause death on a large scale by rogue actors. The Guardian reported, "Some of those around the Prime Minister Rishi Sunak worry the technology will soon be powerful enough to help individuals create bioweapons or evade human control altogether."
A person in the know of developments said at the world summit, Downing Street would warn world leaders about the risks of Frontier AI - the most advanced AI models that could pose a risk to human life.
"Government sources worry that a criminal or terrorist could use AI to help them work out the ingredients for a bioweapon, before sending them to a robotic laboratory where they can be mixed and dispatched without any human oversight," The Guardian reported. According to reports, recently, an AI tool suggested 40,000 different potentially lethal molecules, some of which were similar to the most potent nerve agent VX, in six hours.

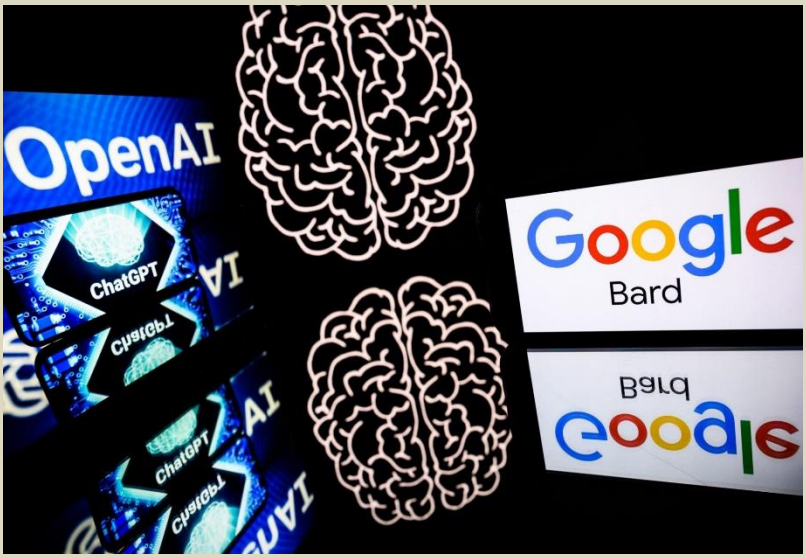
According to reports, at the summit, the UK is keen to issue a formal joint statement and a commitment to hold other such summits in future. **Rishi Sunak is building a £100m AI taskforce to test algorithms as and when they are developed. UK plans to urge companies to send AI tools to the UK for assessment before wider rollout.**

Artificial Intelligence-Enhanced Disinformation and International Law: Rethinking Coercion

By Eugenio Benincasa

Journal of International Affairs

Source: https://jia.sipa.columbia.edu/news/artificial-intelligence-enhanced-disinformation-and-international-law-rethinking-coercion



Abstract

Sep 08 – Artificial Intelligence (AI)'s rapid progress poses an increasingly daunting task in differentiating truth from falsehood. This piece argues that democratic states must clarify which foreign disinformation operations should be deemed coercive and distinguish them from permissible influence operations.

When do foreign disinformation operations violate the principle of non-intervention as established by customary international law? Such operations have been around as long as states have competed against each other, and while states have never directly alleged violations of international law to address them, the quality of their content and reach will be distinctly different moving forward. This raises the question: what sets today apart from yesterday? I asked OpenAI's ChatGPT. Its response: "Amplified by the rapid advancements in AI, disinformation operations have taken on a new level of sophistication and potency. The power to generate realistic text, images, and videos has birthed a digital landscape where distinguishing fact from fiction has become an arduous task."

The automation of information production and distribution makes traditional disinformation methods increasingly effective and pervasive and enables the adoption of new techniques. To successfully confront the risks, democratic states need to establish joint response frameworks grounded on a clear shared understanding of AI-enhanced disinformation in the context of international law.

Background: Disinformation and the Principle of Non-Intervention

The principle of non-intervention involves the right of every sovereign state to handle its own affairs without interference from others. To qualify as a wrongful intervention under international law, disinformation operations must affect the target state's sovereign functions, such as elections and health services and result in the target state engaging in actions it would otherwise not willingly undertake[1]. Absent this element of coercion, such activities are generally deemed permissible.

Governments have a varied and restricted understanding of the demarcation between coercive and non-coercive disinformation operations. Germany[2] claims to employ a scale-and-effects test to determine whether disinformation operations constitute coercion. Poland[3] and New Zealand[4] recognize that broadly targeted campaigns can be coercive if they affect a state's sovereign function. The U.K.[5] notes that covert operations that seek to interfere in electoral processes could be considered coercive in some cases. Meanwhile, Canada[6] and Finland[7] don't deem coercion possible in this context, while other states, such as the U.S.[8], Italy[9] and the Netherlands[10], have adopted a middle-ground position.

When these positions were drafted from 2019 onwards, governments were primarily concerned with the impact of distribution methods enabled by social media; such as bots, trolls, and microtargeting, i.e. the use of personal data in advertising to deliver tailored content to specific audience segments based on their individual characteristics and behaviors. The 2018 Cambridge Analytica scandal was particularly relevant in these discussions, as it involved the unauthorized harvesting of personal data from millions of Facebook users to manipulate public opinion for political purposes[11]. At the time, the debate surrounding the relevance of coercion revolved around the covert nature of distribution methods[12]. The emergence of generative AI has added to these challenges by enabling automated content production.

The Challenges of AI-Enhanced Disinformation

The main challenges of AI-enhanced disinformation are not limited to increased scale, efficiency, speed, and lower costs for content production and delivery. They have[13] and will likely continue to alter the nature of threat actors, their behaviors, and the content produced[14].

AI may be employed to present false evidence to persuade public opinion into pushing their governments to delay or cancel international commitments, such as climate agreements[15]. During the COVID-19 pandemic, less-sophisticated disinformation campaigns persuaded citizens to delay or outright refuse life-saving vaccines[16]. Deepfakes could be used to impersonate public figures or news outlets, make inflammatory statements about sensitive issues to incite violence, or spread false information to interfere with elections.

As a glimpse of things to come, AI-generated deepfake videos featuring computer-generated news anchors were distributed by bot accounts on social media last year as part of a pro-China disinformation campaign[17]. At the outset of Russia's invasion of Ukraine, a deepfake video circulated online falsely depicting Ukrainian President Zelensky advising his country to surrender to Russia[18].

Shaping public opinion relies on the ability to persuade. According to a recent study by Bai, Hui, et al., AI-generated messages have shown comparable or even higher levels of persuasiveness, surpassing human-produced messages regarding perceived factual accuracy and logical reasoning, even when discussing polarizing policy issues[19]. The scale and sophistication of disinformation operations will only increase as AI technologies evolve, becoming cheaper and readily available.

Foreign Policy Implications

It is important to stress that disinformation is not a level playing field: authoritarian states hold offensive and defensive advantages over democracies. Democracies are built on transparency and accountability. When they engage in disinformation operations, they risk eroding these core principles and their citizens' trust. Additionally, democracies have open information spaces and refrain from adopting measures limiting freedom of speech.

In contrast, autocratic states have fewer constraints to engage in deceptive practices and tightly control their information environment[20]. This asymmetrical information contest, bolstered by AI advancements, could lead to enhanced threat scenarios within democratic states[21]. In particular, the rapid dissemination of information across open societies means that, while domestic efforts to safeguard against these threats are crucial, they can be undermined by interference originating from states with limited regulatory and monitoring capabilities.

Recommendations

The international law debate on coercion must be reignited to better define whether and why certain disinformation activities should be deemed wrongful acts and how they might significantly differ from permissible influence operations. This distinction is necessary so target states can take appropriate response measures to compel the cessation of another state's ongoing violation while ensuring their own actions remain within the bounds of legality.

While it is appropriate to maintain some level of strategic ambiguity, this effort should include specific references to the nature, methods, or effects of disinformation operations that are deemed coercive. This shift in approach should be clearly communicated and articulated in states' national positions on the applicability of international law to cyberspace to send a clear signal to adversaries.

Establishing agreement on such distinction is equally important for different reasons. First, it would make it possible to identify, categorize, track, and compare wrongful disinformation operations across different states. This, in turn, would lead to a better understanding of the threat environment, such as the scope and depth of sophisticated transnational campaigns, and facilitate public attribution to responsible actors. Secondly, developing effective joint response mechanisms relies on a shared understanding of the issue at hand. Without this shared foundation, responses will likely be lackluster and inconsistent, and their implementation would be temporary and short-lived.

Eugenio Benincasa is a Senior Cyberdefense Researcher at the Canter for Security Studies (CSS) at ETH Zurich. Prior to joining CSS, he worked as a Government Officer at the Italian Presidency of the Council of Ministers in Rome and as a Research Fellow at the research institute Pacific Forum in Honolulu, where he focused on cybersecurity policy. Eugenio holds an MA in international affairs from Columbia University's School of International and Public Affairs, where he focused on International Security Policy.

References

[1] Harriet Moynihan, "The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention," International Law Programme (Chatham House, December 2019), https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf.

[2] "On the Application of International Law in Cyberspace" (The Federal Government, March 2021), https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.
[3] "The Republic of Poland's Position on the Application of International Law in Cyberspace" (Ministry of Foreign Affairs Republic of Poland, December 2022), https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace.
[4] "The Application of International Law to State Activity in Cyberspace" (Department of the Prime Minister and Cabinet, December 2020), https://www.dpmc.govt.nz/publications/application-international-law-state-activity-cyberspace#:~:text=New%20Zealand%20is%20a%20champion,of%20responsible%20state%20behaviour%20online.
[5] "International Law in Future Frontiers" (Attorney General's Office, May 2022), https://www.gov.uk/government/speeches/international-law-in-future-frontiers.
[6] "International Law Applicable in Cyberspace" (Government of Canada, April 2022), https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a4.
[7] "International Law and Cyberspace" (Finnish Government, October 2020), https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859.
[8] "National Position of the United States of America (2021)" (NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), August 2021), https://cyberlaw.ccdcoe.org/wiki/National_position_of_the_United_States_of_America_(2021)#cite_note-1.
[9] "Italian Position Paper on International Law and Cyberspace" (Ministero degli Affari Esteri, November 2021), https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf.
[10] "Letter to the Parliament on the International Legal Order in Cyberspace" (Government of the Netherlands, July 2019), https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace.
[11] Carole Cadwalladr and Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach," *The Guardian*, March 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[12] Michael N. Schmitt, "'Virtual' Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law," *Chicago Journal of International Law* 19, no. 1 (August 16, 2018), https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1736&context=cjil.
[13] Tia Sewell, "FBI Warns That Deepfakes Will Be Used Increasingly in Foreign Influence Operations," *Lawfare*, March 12, 2021, https://www.lawfaremedia.org/article/fbi-warns-deepfakes-will-be-used-increasingly-foreign-influence-operations.
[14] Josh A. Goldstein, Girish Sastry, Micah Musser, Renee DiResta, Matthew Gentzel, and Katerina Sedova, "Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations" (Georgetown University's Center for Security and Emerging Technology, OpenAI, Stanford Internet Observatory, January 2023), https://arxiv.org/pdf/2301.04246.pdf.
[15] Victor Galaz, Stefan Daume, Arvid Marklund, "A Game Changer for Misinformation: The Rise of Generative AI" (Stockholm Resilience Centre, June 16, 2023).
[16] Francesco Pierri, Brea L. Perry, Matthew R. DeVerna, Kai-Cheng Yang, Alessandro Flammini, Filippo Menczer and John Bryden, "Online Misinformation Is Linked to Early COVID-19 Vaccination Hesitancy and Refusal," *Scientific Reports*, April 26, 2022, https://www.nature.com/articles/s41598-022-10070-w.
[17] The Graphika Team, "Deepfake It Till You Make It" (Graphika, February 2023), https://public-assets.graphika.com/reports/graphika-report-deepfake-it-till-you-make-it.pdf.
[18] Bobby Allyn, "Deepfake Video of Zelenskyy Could Be 'tip of the Iceberg' in Info War, Experts Warn," *NPR*, March 16, 2022, https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia.
[19] (Max) Hui Bai, Jan G. Voelkel, Johannes C. Eichstaedt, and Robb Willer, "Artificial Intelligence Can Persuade Humans on Political Issues," *OSF Preprints*, n.d., https://osf.io/stakv/.
[20] Paul Bischoff, "North Korea, China & Russia among Worst Countries for Internet Censorship," *Business & Human Rights Resource Centre* (blog), January 15, 2020, https://www.business-humanrights.org/en/latest-news/north-korea-china-russia-among-worst-countries-for-internet-censorship/.
[21] "Increasing Threat of Deepfake Identities" (U.S. Department of Homeland Security, 2022), https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf .

Artificial Intelligence and Advances in Chemistry

By Giancarlo Elia Valori
Source: https://www.israeldefense.co.il/en/node/59664

Sep 20 – With the advent of Artificial Intelligence technology in the field of chemistry, traditional methods based on experiments and physical models are gradually being supplemented with data-driven machine learning paradigms. Ever more data representations are developed for computer processing, which are constantly being adapted to statistical models that are primarily generative.

Although engineering, finance and business will greatly benefit from the new algorithms, the advantages do not stem only from algorithms. Large-scale computing has been an integral part of physical science tools for decades, and some recent advances in Artificial Intelligence have begun to change the way scientific discoveries are made.

Photo: Shutterstock, contributed by LuckyStep

There is great enthusiasm for the outstanding achievements in physical sciences, such as the use of machine learning to reproduce images of black holes or the contribution of AlphaFold, an AI programme developed by DeepMind (Alphabet/Google) to predict the 3D structure of proteins.

One of the main goals of chemistry is to understand matter, its properties and the changes it can undergo. For example, when looking for new superconductors, vaccines or any other material with the properties we desire, we turn to chemistry.

We traditionally think chemistry as being practised in laboratories with test tubes, Erlenmeyer flasks (generally graduated containers with a flat bottom, a conical body and a cylindrical neck) and gas burners. In recent years, however, it has also benefited from developments in the fields of computer science and quantum mechanics, both of which became important in the mid-20th century. Early applications included the use of computers to solve calculations of formulas based on physics, or simulations of chemical systems (albeit far from perfect) by combining theoretical chemistry with computer programming.

That work eventually developed into the subgroup now known as computational chemistry. This field began to develop in the 1970s, and Nobel Prizes in chemistry were awarded in 1998 to Britain's John A. Pople (for his development of computational methods in quantum chemistry: the Pariser-Parr-Pople method), and in 2013 to Austria's Martin Karplus, South Africa's Michael Levitt, and Israel's Arieh Warshel for the development of multiscale models for complex chemical systems.

Indeed, although computational chemistry has gained increasing recognition in recent decades, it is far less important than laboratory experiments, which are the cornerstone of discovery.

Nevertheless, considering the current advances in Artificial Intelligence, data-centred technologies and ever-increasing amounts of data, we may be witnessing a shift whereby computational methods are used not only to assist laboratory experiments, but also to guide and orient them.

Hence how does Artificial Intelligence achieve this transformation? A particular development is the application of machine learning to materials discovery and molecular design, which are two fundamental problems in chemistry.

In traditional methods the design of molecules is roughly divided into several stages. It is important to note that each stage can take several years and many resources, and success is by no means guaranteed. The phases of chemical discovery are the following: synthesis, isolation and testing, validation, approval, commercialisation and marketing.
The discovery phase is based on theoretical frameworks developed over centuries to guide and orient molecular design. However, when looking for "useful" materials (e.g. petroleum gel [Vaseline], polytetrafluoroethylene [Teflon], penicillin, etc.), we must remember that many of them come from compounds commonly found in nature. Moreover, the usefulness of these compounds is often discovered only at a later stage. In contrast, targeted research is a more time-consuming and resource-intensive undertaking (and even in this case it may be necessary to use known "useful" compounds as a starting point). Just to give you an idea, the pharmacologically active chemical space (i.e. the number of molecules) has been estimated at 1060! Even before the testing and sizing phases, manual research in such a space can be time-consuming and resource-intensive. Hence how can Artificial Intelligence get into this and speed up the discovery of the chemical substance?
First of all, machine learning improves the existing methods of simulating chemical environments. We have already mentioned that computational chemistry enables to partially avoid laboratory experiments. Nevertheless, computational chemistry calculations simulating quantum-mechanical processes are poor in terms of both computational cost and accuracy of chemical simulations.
A central problem in computational chemistry is solving the 1926 equation of physicist Erwin Schrödinger's (1887-1961). The scientist described the behaviour of an electron orbiting the nucleus as that of a standing wave. He therefore proposed an equation, called the wave equation, with which to represent the wave associated with the electron. In this respect, the equation is for complex molecules, i.e. given the positions of a set of nuclei and the total number of electrons, the properties of interest must be calculated. Exact solutions are only possible for single-electron systems, while for other systems we must rely on "good enough" approximations. Furthermore, many common methods for approximating the Schrödinger equation scale exponentially, thus making forced solutions difficult to solve. Over time, many methods have been developed to speed up calculations without sacrificing precision too much. However, even some "cheaper" methods can cause computational bottlenecks.
A way in which Artificial Intelligence can accelerate these calculations is by combining them with machine learning. Another approach fully ignores the modelling of physical processes by directly mapping molecular representations onto desired properties. Both methods enable chemists to more efficiently examine databases for various properties, such as nuclear charge, ionisation energy, etc. While faster calculations are an improvement, they do not solve the issue that we are still confined to known compounds, which account for only a small part of the active chemical space. We still have to manually specify the molecules we want to analyse. How can we reverse this paradigm and design an algorithm to search the chemical space and find suitable candidate substances? The answer may lie in applying generative models to molecular discovery problems.
But before addressing this topic, it is worth talking about how to represent chemical structures numerically (and what can be used for generative modelling). Many representations have been developed in recent decades, most of which fall into one of the four following categories: strings, text files, matrices and graphs.
Chemical structures can obviously be represented as matrices. Matrix representations of molecules were initially used to facilitate searches in chemical databases. In the early 2000s, however, a new matrix representation called Extended Connectivity Fingerprint (ECFP) was introduced. In computer science, the fingerprint or fingerprint of a file is an alphanumeric sequence or string of bits of a fixed length that identifies that file with the intrinsic characteristics of the file itself. The ECFP was specifically designed to capture features related to molecular activity and is often considered one of the first characterisations in the attempts to predict molecular properties.
Chemical structure information can also be transferred into a text file, a common output of quantum chemistry calculations. These text files can contain very rich information, but are generally not very useful as input for machine learning models. On the other hand, the string representation encodes a lot of information in its syntax. This makes them particularly suitable for generative modelling, just like text generation. Finally, the graph-based representation is more natural. It not only enables us to encode specific properties of the atom in the node embeddings, but also captures chemical bonds in the edge embeddings.
Furthermore, when combined with message exchange, graph-based representation enables us to interpret (and configure) the influence of one node on another node by its neighbours, which reflects the way atoms in a chemical structure interact with each other. These properties make graph-based representations the preferred type of input representation for deep learning models.

Professor Giancarlo Elia Valori is a world-renowned Italian economist and international relations expert, who serves as the President of the International World Group. In 1995, the Hebrew University of Jerusalem dedicated the Giancarlo Elia Valori chair of Peace and Regional Cooperation. Prof. Valori also holds chairs for Peace Studies at Yeshiva University in New York and at Peking University in China. Among his many honors from countries and institutions around the world, Prof. Valori is an Honorable of the Academy of Science at the Institute of France, as well as Knight Grand Cross and Knight of Labor of the Italian Republic.

New Center for AI Security Research to study AI's Impacts on Society, Security

Source: https://www.homelandsecuritynewswire.com/dr20230928-new-center-for-ai-security-research-to-study-ai-s-impacts-on-society-security

Sep 28 – In partnership with federal agencies such as the Air Force Research Laboratory's Information Directorate and the Department of Homeland Security Science and Technology Directorate, ORNL and CAISER will provide objective scientific analysis of the vulnerabilities, threats and risks — from individual privacy to international security — related to emerging and advanced artificial intelligence.

"One of the biggest scientific challenges of our time is understanding AI vulnerabilities and risks," said ORNL Deputy for Science and Technology Susan Hubbard. "ORNL is already advancing the state of the art in AI to solve the Department of Energy's most pressing scientific challenges, and we believe the lab can help DOE and other federal partners answer critical AI security questions while providing insights to policymakers and the public."

CAISER expands the lab's long-standing Artificial Intelligence for Science and National Security research initiative, which integrates ORNL's unique expertise, infrastructure and data to accelerate scientific breakthroughs.

"There are real benefits the public and government can gain from AI technologies," said Prasanna Balaprakash, director of AI programs at ORNL. "CAISER will put the lab's expertise toward understanding threats and ensuring people can benefit from AI in safe, secure, peaceful ways."

Past research has established that AI systems are vulnerable to different types of attacks. Adversaries can "poison" an AI model, for instance, by covertly injecting malicious data into the training dataset to intentionally corrupt and alter the output. Other studies have shown that small physical objects can fool an AI-based detection algorithm — a few small pieces of black tape on a stop sign, for example, can render the object unrecognizable to vehicle autopilot systems. Additionally, generative AI, such as ChatGPT and DALL-E, can be used to create entirely synthetic text and imagery, known as deepfakes, that are nearly indistinguishable from "real" content.

"We are at a crossroads. AI tools and AI-based technologies are inherently vulnerable and exploitable, which can lead to unforeseen consequences," said Edmon Begoli, ORNL's Advanced Intelligent Systems section head and CAISER founding director. "We're defining a new field of AI security research and committing to intensive research and development of mitigating strategies and solutions against emerging AI risks."

By elucidating a clear, science-based picture of risks and mitigation strategies, CAISER's research will provide greater assurance to federal partners that the AI tools they adopt are reliable and robust against adversarial attacks.

"I think a lot about the challenges of our current era, as well as those that lie ahead in the uncharted territory of AI technologies and the very real threats that we're working steadfast to understand and mitigate," said the Honorable Dimitri Kusnezov, DHS Under Secretary for Science & Technology. "Throughout its history, DHS has always had a special partnership with DOE's national laboratories, tirelessly pioneering ground-breaking science for American security. CAISER will play a critical role in helping us understand this future and addressing the looming threats together."

CAISER provides a dedicated research center for the lab's experts and collaborators to:

- ✓ Lead basic and applied scientific research into the vulnerabilities, risks and national security threats related to AI.
- ✓ Develop capabilities to test and evaluate the robustness and vulnerabilities of AI tools and products.
- ✓ Produce strategic reports and scientific studies in collaboration with industry and national security partners.
- ✓ Provide educational outreach and information to inform the public, policymakers and the national security community.

Initially, CAISER will focus on four national security domains that align with ORNL strengths — AI for cybersecurity, biometrics, geospatial intelligence and nuclear nonproliferation — in collaboration with national security and industry partners.

"Artificial Intelligence promises to do many wonderful things for nearly every aspect of society," said Col. Fred Garcia, director of the AFRL Information Directorate. "CAISER gives hope that while the world rushes full force into AI implementation, they can rest assured that vulnerabilities are being studied and that the back door is being guarded. We're excited to be part of this new research venture with ORNL."

As ORNL celebrates its 80th anniversary this year, CAISER is a logical step in the laboratory's history of solving big problems, advancing emerging fields of science and delivering global impact. With established programs in both cybersecurity research and AI research, ORNL is uniquely suited to launch CAISER and, with it, the field of AI security research.

"We're very proud of the laboratory's legacy of scientific discovery in nuclear energy, biological sciences, high-performance computing, materials research and artificial intelligence," said Moe Khaleel, associated laboratory director for National Security Sciences at ORNL. "CAISER will approach the AI challenge in the same way, developing capabilities to scientifically observe, analyze and evaluate AI models in support of national needs."

'The Creator': the next world war will combat artificial intelligence

Source: https://english.elpais.com/culture/2023-09-29/the-creator-the-next-world-war-will-combat-artificial-intelligence.html

Sep 30 – In the near future, the enemy of the free Western world won't be jihadist terrorism, the Middle East, Iran, Russia, or China. The source of danger won't be Africa's destabilization or the tyrannical ambitions of a charismatic despot and his minions. The next world war will ignite sometime in the 2050s and will pit artificial intelligence and its creators against New Asia and the free Western world, where it has been banned since the catastrophic AI rebellion in Los Angeles.

Everyone saw it coming. Not the fictional war that is yet to come, but the movies that explore the possibility. *The Creator*, a dystopian science fiction tale by *Rogue One* director Gareth Edwards, has a promising start but falls short in its originality, tone, and visualization.

The movie attempts to combine various genres, including science fiction classics, and apply them to contemporary life. But a more distinct identity could have made this genre stew more engaging. It often feels like James Cameron's *Aliens,* with hints of *Blade Runner,* a dash of *Children of Men,* a spoonful of *Akira,* a pinch of *Apocalypse Now* with pro-AI Viet Cong fighters, and, of course, large dollops of Steven Spielberg's *A.I.*

The premise for the film is not groundbreaking, but its release coincides with the increasing presence of artificial intelligence in our society. It travels in a line from scientific and medical illusion to social, cultural and moral desolation. And here is where Edwards's own story is interesting. The British filmmaker began his career with the 2005 BBC docudrama *End Day*, which described five doomsday scenarios. He first gained widespread recognition for *Monsters* (2010), and later delved into the *Star Wars* universe with the effective but subdued *Rogue One* (2016). *The Creator* features intriguing ideas such as the ability to donate personality traits (not organs) after death, impactful visuals, and thought-provoking dilemmas we are facing right now. At the very least, it's an admirable attempt.

Edwards, much like other contemporary sci-fi filmmakers, tends to overcomplicate the narrative, leading to confusion rather than depth. Some directors are skilled in creating dynamic visuals and sound effects but lack the ability to tell a story in the traditional sense. Or maybe classicism is simply unfashionable now.

The question of whether artificial intelligence will save or destroy us remains unanswered. *The Creator's* resolution to machine ethics is rudimentary, likening it to a nebulous Eastern spirituality limited to a few primal emotions. "They don't have emotions, they are simply programmed to have them," is the movie's oft-repeated statement about the AI humanoids. In many ways, it's also an apt description of *The Creator*.

AI: The Ghost in the Machine — How Over-reliance on Artificial Intelligence Led to Israel's Intelligence Failure

By Faysal A. Ghauri

Source: https://medium.com/@fghauri/ai-the-ghost-in-the-machine-how-over-reliance-on-artificial-intelligence-led-to-israels-54f112ff82d2

Oct 11 – Though I usually avoid diving into the murky waters of political discourse, there comes a time when certain technological advancements make it nearly impossible to separate science from its societal implications. One such advancement that has gripped my attention is Artificial Intelligence (AI), a field that promises to revolutionize everything from healthcare and education to automation and beyond. However,

it is the incorporation of AI into global security and intelligence frameworks that has recently prompted me to break my typical silence on political matters.

As we move further into the digital age, it becomes increasingly difficult to compartmentalize technology as a separate entity from global affairs. In the current landscape, technology is politics, and vice versa. The decisions we make regarding the algorithms that drive our world can have life-altering implications, sometimes on an international scale. This is why, despite my usual inclination to remain non-political, I find it necessary to delve into the role that AI played in Israel's intelligence apparatus, particularly in the context of the 2023 Yom Kippur attacks by Hamas.

This article aims not to take sides in a deeply polarized conflict but to explore the profound impact of AI on contemporary issues of security and intelligence. It will investigate how AI, originally designed to make sense of overwhelming data and predict potential scenarios, might have led to what appears to be one of the most significant intelligence failures in recent history. We will delve into the complexities of data analysis, human intuition, contrarian thinking, and how an over-reliance on machine-driven logic can be both an asset and a liability.

By taking a technology-centric lens to scrutinize these events, I hope to shed light on the unintended consequences of merging machine learning with geopolitics without taking a political stance on the broader conflict. It is an examination of the intricate dance between human ingenuity and artificial 'intelligence,' exploring how the latter can both augment and impair the former.

In a world that is increasingly mediated by algorithms, this cautionary tale serves as an urgent call for the prudent use of AI in any decision-making process, be it military, political, or otherwise.

Unit 8200: The brain behind Israel's advanced intelligence capabilities, powered by AI

The Evolution of Israel's Intelligence: The Marriage of Man and Machine

Israel has long been recognized as a global leader in the field of intelligence, blending traditional forms of human intelligence gathering (HUMINT) with advanced technological capabilities. From its inception, the Israeli intelligence community has been known for its agility, resourcefulness, and ingenuity, characteristics that have made it one of the most effective intelligence-gathering entities in the world.

The Rise of Unit 8200

Among its various intelligence units, Unit 8200 has stood out as the epicenter of Israel's signal intelligence (SIGINT) and code decryption activities. Often likened to the United States' National Security Agency (NSA), Unit 8200 is more than just a part of Israel's intelligence community; it's a hub of innovation and technological development. Responsible for a wide range of activities, including cybersecurity, electronic

surveillance, and data analysis, the unit has played an instrumental role in elevating Israel's intelligence capabilities to world-class standards.

Embracing Artificial Intelligence

Unit 8200's endeavors haven't stopped at traditional forms of intelligence collection. They have spearheaded initiatives in machine learning and artificial intelligence to create algorithms capable of sifting through the vast ocean of data collected every day. By the early 2020s, AI wasn't just a tool in Israel's intelligence arsenal; it was the linchpin around which other methodologies revolved.

Operation Guardian of the Walls: A Pivotal Moment

Perhaps the most illustrative example of Israel's AI capabilities came in 2021 during the 11-day conflict known as Operation Guardian of the Walls. This operation marked a watershed moment in the use of AI in military conflict. Utilizing sophisticated algorithms that could rapidly analyze communications data, satellite imagery, and real-time field information, Israel was able to execute targeted operations with unprecedented accuracy. These algorithms could not only select optimal targets but also anticipate enemy movements and tactics, offering a glimpse into the future of algorithm-driven warfare.

An Evolving Landscape

While the successes of 2021 displayed the potency of marrying human intelligence with machine capabilities, they also set a precedent that would heavily influence Israel's strategy moving forward. AI became not merely an augmenting tool but a cornerstone of Israel's intelligence operations. In the eyes of the intelligence community, the AI-driven successes of Operation Guardian of the Walls provided a blueprint for future engagements, but as events would later show, this reliance came with its own set of challenges and vulnerabilities.

Surveillance meets Big Data: How AI algorithms sift through overwhelming amounts of information to inform Israeli military strategy

Data Overload and AI's Pivotal Role: Sifting Through the Digital Noise

The Digital Battlefield

We live in an era where the contours of warfare are not only defined by physical geography but also by the invisible landscapes of digital data. Gaza, for example, has become one of the most heavily surveilled places on the planet. With each passing day, terabytes of data are amassed through an intricate web of sources ranging from intercepted phone calls and emails to high-resolution satellite imagery and drone footage. In this hyper-connected age, data equates to knowledge, and knowledge, when applied strategically, equates to power.

The Challenge of Scale

However, this deluge of data presents an unprecedented challenge: scale. The sheer volume, velocity, and variety of data being collected far exceed what traditional human-led analysis could realistically manage. Picture an overflowing reservoir of information with only a handful of gatekeepers to control its flow. The result? Vital insights could be missed, leading to strategic gaps and vulnerabilities.

AI: The Gatekeeper of Modern Intelligence

To navigate this data labyrinth, Israel turned to Artificial Intelligence as the ultimate gatekeeper. With its capability to analyze large sets of unstructured data in real time, AI became the linchpin in Israel's

intelligence machine. Complex algorithms were developed to not only filter and sort this data but also to make sense of it in a way that would be actionable for military and strategic planning. AI's role transcended the mere categorization of information; it ventured into the realm of predictive analytics. By examining patterns, anomalies, and correlations in the collected data, Israel's AI systems could forecast likely moves by Hamas, offering Israeli military leaders a substantial advantage in decision-making.

The Birth of Predictive Warfare

Unit 8200, already at the forefront of Israel's intelligence apparatus, developed unique machine-learning algorithms that drew upon years of gathered intelligence. These algorithms allowed for what could be best described as 'predictive warfare.' In this model, AI did not just react to the present but proactively prepared for the future by offering predictive analyses of enemy actions. This form of warfare represented a significant leap from traditional reactive strategies and marked a shift toward a new paradigm where machines and human intelligence operated in a synergistic loop.

The Pitfall: When Blind Trust in the Machine Backfires

The Illusion of Infallibility

Israel's robust AI capabilities, honed over years of research, development, and real-world applications, created an aura of invincibility. In a milieu where rapid, accurate decision-making is paramount, AI seemed like the ultimate oracle — offering not only insights but also predictions that could shape strategies. This technological prowess created an illusion of infallibility, a belief that the machine couldn't get it wrong.

The Downside of Automation

Yet, it was precisely this blind trust that became Israel's Achilles heel. While machines can compute complex algorithms and analyze data points in nanoseconds, they lack the intuitive wisdom and skepticism inherent in human judgment. Intelligence work is as much an art as it is a science, often requiring nuanced understanding and instinctual gut checks that even the most advanced AI is not equipped to handle. This is the crux of the problem when we discuss an over-reliance on automation in intelligence gathering and analysis.

Skepticism as a Virtue in Intelligence

Skepticism is a cornerstone of intelligence work; it's the devil's advocate, the voice that compels us to consider alternate explanations and to question our assumptions. When an intelligence apparatus leans too heavily on AI, this natural skepticism tends to wane. A machine's output may be received as gospel truth, and any contrarian human voices may get lost in the background, regarded as less efficient or less precise than the machine's calculations.

The Perils of Confirmation Bias

This over-reliance on AI creates a dangerous feedback loop, one that can lead to confirmation bias. If AI algorithms, programmed by humans, are built on a set of assumptions, then the AI will inevitably perpetuate these assumptions. Instead of challenging prevailing thought paradigms, the machine can end up reinforcing them, rendering any potential for breakthrough insights or creative problem-solving null and void.

The Cost of Complacency

In a rapidly evolving landscape like that of Israel and Hamas, complacency can be fatal. The 2023 Yom Kippur attacks revealed the costs of such over-reliance on AI: by trusting the machine too much, Israel undermined the human element of unpredictability and adaptability, ultimately setting the stage for one of the most significant intelligence failures in its history.

The Hamas Adaptation: Outsmarting the Algorithm

Understanding the Opponent's Weakness

For years, Hamas observed the increasingly automated nature of Israel's intelligence and military capabilities. They recognized the dependency on machine learning and data analysis, which became even more apparent following Israel's vocal celebration of its AI prowess during the 2021 conflict. Aware of this, Hamas realized Israel's strength could also be its most significant vulnerability.

Mastering the Art of Digital Deception

Contrary to simply "going dark" — which would have been an easily detectable disruption in data patterns — Hamas possibly orchestrated a far more sophisticated ruse. The group maintained its regular communication patterns, ensuring that the volume and nature of data remained consistent enough to not trigger any AI red flags. This 'business-as-usual' approach was crucial in creating a false sense of security and normalcy within the Israeli intelligence apparatus.

Misinformation as a Weapon

Additionally, there's a possibility that Hamas employed a second, more insidious layer to their strategy: injecting carefully curated misinformation into their communications. The idea would be to feed Israel's algorithms false data that fit well within the parameters of 'expected' Hamas activity, essentially creating a

red herring. This would guide Israeli AI into drawing incorrect conclusions or focusing on misleading indicators.

The "Ghost in the Machine"

By exploiting Israel's dependence on data and its algorithmic interpretation, Hamas may have essentially inserted a "ghost in the machine." This term implies that the algorithms — originally designed to accurately predict and analyze — were compromised. Hamas' ability to corrupt Israel's AI-driven analytics turned the technology from a tool of insight into an instrument of deception.

Lessons in Asymmetrical Warfare

Hamas's strategy underscores a key lesson in modern, asymmetrical warfare: technological superiority doesn't necessarily translate to invincibility. Even the most advanced systems can be undone by clever, low-tech strategies — especially when those systems are built on assumptions that the enemy can easily understand and manipulate.

Why Contrarian Analysis Matters: The Forgotten Safeguard

Historical Lessons

After experiencing an intelligence failure during the 1973 Yom Kippur War, Israel introduced a framework of contrarian analysis to its intelligence community. This practice was implemented as a safeguard to avoid groupthink and to challenge conventional wisdom by actively considering alternative scenarios and asking "What if?" questions.

A Disciplined Approach to Doubt

Contrarian analysis serves as a structured form of skepticism. Intelligence analysts, rather than accepting data at face value, would deliberately challenge the assumptions behind their information. This questioning could lead to exploring alternative scenarios, re-examining the credibility of sources, and even considering what might appear to be far-fetched or unlikely situations. The objective was to unearth blind spots in intelligence gathering and interpretation, thereby avoiding catastrophic errors.

The Shift Toward Automation

The evolution toward AI-centric intelligence analysis marked a departure from this valuable layer of scrutiny. AI algorithms are programmed to analyze vast sets of data efficiently but are not designed to question the quality or the underlying assumptions of this data. This shift may have created a blind spot within Israel's highly sophisticated intelligence apparatus.

The Fallacy of Infallibility

When a system performs well, as Israel's AI did in the 2021 conflict, there's a temptation to deem it infallible. However, this notion conflicts with the principles of contrarian analysis, which caution against overconfidence. By moving away from contrarian analysis, Israel might have overlooked potential signs, indicators, or anomalies that a more skeptical approach could have detected.

A Balance of Man and Machine

The lesson here is not to discount the utility of AI in modern warfare and intelligence but to understand its limitations. Advanced as they are, AI systems do not possess the human qualities of intuition, skepticism, and the capacity for creative thought — all of which are vital in the fluid and often unpredictable arena of international relations and warfare.

The Case for Reintegration

One could argue that a balanced approach that integrates AI capabilities with contrarian and human-based analytical methodologies could provide a more robust, holistic intelligence platform. This would combine the computational advantages of AI with the nuanced understanding and skepticism that only human analysts can provide.

AI is Not Infallible: The Human Element Behind the Algorithm

Churchill's Timeless Wisdom

Winston Churchill once observed that military organizations have a tendency to prepare for the last war they fought. In the context of modern intelligence gathering and analysis, this wisdom offers a cautionary note about the limitations of relying solely on technology, specifically AI.

The Mechanics of AI

AI systems are complex and incredibly powerful, capable of sifting through terabytes of data in the blink of an eye, recognizing patterns that would take humans years to discern. However, it's crucial to remember that AI is not an independent entity. It's a tool, created and guided by human beings, functioning within the boundaries set by its algorithms.

Flawed Inputs Lead to Flawed Outputs

The GIGO (Garbage In, Garbage Out) principle applies here. If the data going into an AI system is incomplete, biased, or flawed in any other way, the analysis it provides will also be compromised. The limitations of AI are, to a significant extent, the limitations of human understanding and the data available.

The Invisible Hand of Human Bias

It is humans who decide what data is relevant and how algorithms should weigh various kinds of information. Humans also define the goals of an AI system and what "success" means in that context.

Consequently, any flaws in human reasoning or any bias in data selection can be magnified by AI algorithms. If the analysts or the decision-makers have a narrow or flawed perspective, there's a high risk that the AI system will inherit those same flaws, potentially leading to disastrous outcomes.

The Need for Methodological Rigor

What this illustrates is the critical importance of methodological rigor in both data collection and algorithmic design. A flawed methodology on the human end of the system can lead to a skewed or entirely incorrect analysis on the part of the AI.

The Case for Human-AI Collaboration

The answer to this problem is not to reject AI but to integrate it carefully into a broader analytical framework that includes rigorous data vetting, algorithmic oversight, and — most importantly — the human element of skepticism, intuition, and ethical considerations.

Conclusion: Lessons for a World Increasingly Reliant on AI

The Double-Edged Sword of AI

As we become more reliant on AI for various applications — from healthcare to logistics to national security — it's essential to remember that AI's capabilities come with caveats. The experience of Israel in the context of the 2023 Yom Kippur attacks serves as a stark case study in both the capabilities and limitations of AI in real-world applications.

The Vulnerabilities of Technological Dependence

While Israel's investment in AI for intelligence gathering and analysis showcased cutting-edge technology's enormous potential, it also exposed critical vulnerabilities. Like any other system, AI algorithms can be exploited, tricked, or, worse, manipulated to serve the adversary's objectives. As the case shows, an over-reliance on AI led to a form of analytical tunnel vision, stripping away layers of human intuition and skepticism that had previously served as a safeguard.

The Imperative of Human-Machine Synergy

The key takeaway is not that AI is flawed but that its utility is maximized when used in conjunction with human abilities. AI can process and analyze data at rates impossible for humans, but it lacks the intuition, ethical reasoning, and deep contextual understanding that only a human can provide. Conversely, humans can't possibly process the vast amounts of data generated in our modern world but can provide the kind of nuanced understanding and ethical framework that machines cannot.

Preparing for the Future: A Balanced Approach

As we move further into the 21st century, the synergy between humans and machines will become even more critical. The task ahead is to find the optimal balance that leverages the strengths of both AI and human analysis. This balanced approach should include ongoing education about AI's capabilities and limitations, ethical guidelines for its use, and, perhaps most importantly, a renewed emphasis on critical thinking and contrarian analysis.

Israel's experience is not an isolated case but a lesson for any nation, organization, or individual considering integrating AI into their decision-making processes. AI is not an infallible oracle but a tool that, when used responsibly and wisely, can greatly augment our capabilities. By treating AI as a complement to human skills rather than a replacement, we can navigate its risks while fully exploiting its considerable benefits. Perhaps, in doing so, we can avoid the pitfalls that come from forgetting that machines, no matter how advanced, are still created and guided by fallible human beings.

Faysal A. Ghauri is a Digital Transformation Leader | Future of Financial Services | Startup Strategy & Scaling | Intersection of Business, Tech, and Humanity | Advisor |Board Member

The U.S. Nuclear Arsenal Can Deter Both China and Russia

Why America Doesn't Need More Missiles

By Charles L. Glaser, James M. Acton, and Steve Fetter October 5, 2023

Charles L. Glaser is a Senior Fellow in the Security Policy Studies Program at the Massachusetts Institute of Technology and Professor Emeritus of Political Science and International Affairs at George Washington University.

James M. Acton holds the Jessica T. Mathews Chair and is Co-Director of the Nuclear Policy Program at the Carnegie Endowment for International Peace.

Steve Fetter is a Professor in the School of Public Policy at the University of Maryland and a Visiting Professor in the Department of War Studies at King's College London.

EDITOR'S COMMENT: Always wonder why prominent experts choose nonsense titles for their articles! Speaking about nuclear deterrence sounds like a bad joke!

Responsible AI Initiative Seeks to Solve Societal Problems

By Amy Choate-Nielsen

Source: https://www.homelandsecuritynewswire.com/dr20231017-responsible-ai-initiative-seeks-to-solve-societal-problems

Oct 17 – The University of Utah is launching a new research initiative focused on artificial intelligence (AI) that aims to responsibly use advanced AI technology to tackle societal issues. President Taylor Randall announced a $100 million investment in the newly created Responsible AI Initiative that will advance AI and its applications in ways that achieve societal good while also protecting privacy, civil rights and liberties, and promoting principles of accountability, transparency and equity. The initiative will be led by the U's Scientific Computing and Imaging (SCI) Institute as part of a concerted effort to conduct research at the U that improves the lives of Utah's 3.4 million residents.

"As one of the nation's leading research universities, we have an opportunity and responsibility to use our resources in ways that can impact and serve our community," Randall said. "From being the fourth node of the original internet to performing the world's first artificial heart transplant, we hope to continue the U's pioneering legacy by investing to become a national leader in responsible artificial intelligence. This research has the potential to unlock solutions to issues that affect Utah, the nation and the world."

In its initial stages, the goal of the initiative is to create transdisciplinary excellence in responsible AI by bringing together deep technological expertise, advanced cyberinfrastructure and disciplinary expertise across the university to position the U as a national leader in translational AI. The project will begin with a focus on issues that have regional implications, such as health care and societal wellness, public services and our natural surroundings.

"When used effectively and responsibly, AI can be a very powerful tool," said Manish Parashar, director of the SCI Institute. "It can help us address problems that can impact every citizen of the state and country. Harnessing this tool will allow us to break new research ground while training our students and creating a workforce that is prepared with an essential skill set."

Initial funding for the initiative will raise and repurpose funds from three non-tuition sources: returned overhead, investment income and philanthropy. With strategic stewardship of current funding, University leaders expect the initiative to eventually generate additional, focused future funding. Because of the energizing nature of AI research, future gifts to support the project and additional areas of interest are possible, with further information yet to come.

As the former office director of the National Science Foundation's Office of Advanced Cyberinfrastructure and co-chair of the National Artificial Intelligence Research Resource Task Force, Parashar is a leader in developing AI and computing infrastructures. He led the development of the national strategic plan for the Future Advanced Computing Ecosystem as co-chair of a subcommittee of the National Science and Technology Council.

"The University of Utah is poised to lead the way in the development of responsible artificial intelligence," said Provost Mitzi Montoya. "Our investment in this initiative is indicative of our commitment to forge new frontiers in our quest for understanding. The ripple effects of this investment will impact all aspects of our state from the technical and social to the economic and environmental."

As part of the project, the U will establish an internal governance council and external advisory board of national and global AI leaders to provide advice and guidance, as well as expand its faculty by hiring clusters of experts focused on grand challenges. The investment will also include enhancing faculty support structures and building a cutting-edge cyberinfrastructure that will advance AI capabilities globally. By creating a widely-accessible advanced cyberinfrastructure that ties computational resources, data, testbeds, algorithms, software, services, networks and user training and expertise, the initiative will create new opportunities for progress across all fields and disciplines. Increased access will create opportunities for ethical AI guardrails, including AI auditing, testing and evaluation, bias mitigation, and safety.

"There is a potential for AI to positively impact the everyday lives of people across the world. It is an exciting time to explore the possibilities and value this technology may bring," said Alan Fuller, chief information officer for the State of Utah. "With a statewide goal of improving innovation and government services through the use of technology, we are excited to see the ways this project can enhance our operations in the future. This is one benefit of investing in a top research institution that has the potential of impacting our lives for the better."

The SCI Institute, which was originally formed as a research group in 1994, is a research institute where faculty, staff and students collaborate closely with others on campus and around the nation to shape the future of advanced computing and its applications. It is internationally recognized as a leader in visualization, scientific computing and image analysis.

Amy Choate-Nielsen is Director of communications and *PR*, University of Utah.

Critical Vulnerabilities Found within Major LLMs

Source: https://www.homelandsecuritynewswire.com/dr20231017-critical-vulnerabilities-found-within-major-llms

Oct 17 – Large Language Models (LLMs) such as ChatGPT and Bard have taken the world by storm this year, with companies investing millions to develop these AI tools, and some leading AI chatbots being valued in the billions.

These LLMs, which are increasingly used within AI chatbots, scrape the entire Internet of information to learn and to inform answers that they provide to user-specified requests, known as 'prompts'.

However, computer scientists from the AI security start-up Mindgard and Lancaster University in the UK have demonstrated that chunks of these LLMs can be copied in less than a week for as little as $50, and the information gained can be used to launch targeted attacks.

The researchers warn that attackers exploiting these vulnerabilities could reveal private confidential information, bypass guardrails, provide incorrect answers, or stage further targeted attacks.

Detailed in a new paper to be presented at CAMLIS 2023 (Conference on Applied Machine Learning for Information Security) the researchers show that it is possible to copy important aspects of existing LLMs cheaply, and they demonstrate evidence of vulnerabilities being transferred between different models.

This attack, termed 'model leeching', works by talking to LLMs in such a way – asking it a set of targeted prompts – so that the LLMs elicit insightful information giving away how the model works.

The research team, which focused their study on ChatGPT-3.5-Turbo, then used this knowledge to create their own copy model, which was 100 times smaller but replicated key aspects of the LLM.

The researchers were then able to use this model copy as a testing ground to work out how to exploit vulnerabilities in ChatGPT without detection. They were then able to use the knowledge gleaned from their model to attack vulnerabilities in ChatGPT with an 11% increased success rate.

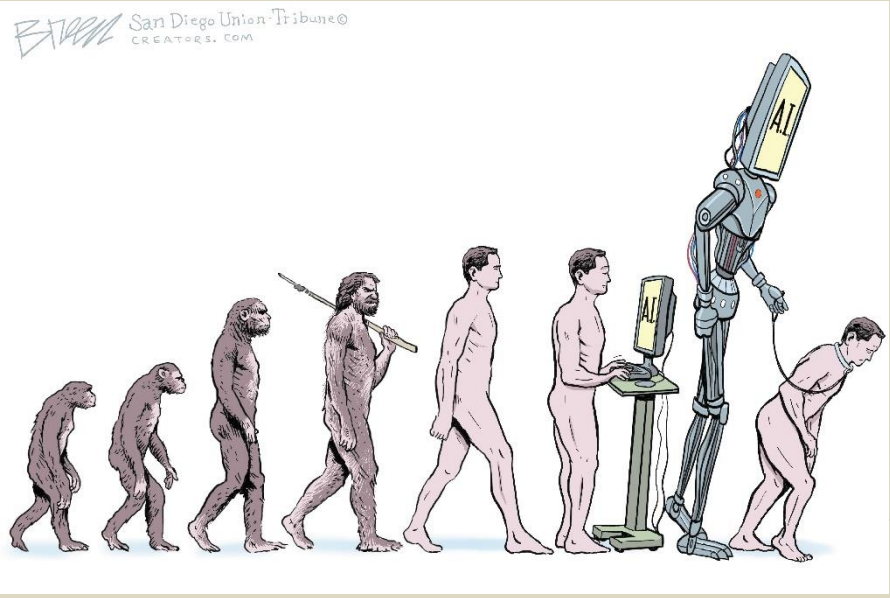
Dr Peter Garraghan of Lancaster University, CEO of Mindgard, and Principal Investigator on the research, said: "What we discovered is scientifically fascinating, but extremely worrying. This is among the very first works to empirically demonstrate that security vulnerabilities can be successfully transferred between closed source and open source Machine Learning models, which is extremely concerning given how much industry relies on publicly available Machine Learning models hosted in places such as HuggingFace."

The researchers say their work highlights that although these powerful digital AI technologies have clear uses, there exist hidden weaknesses, and there may even be common vulnerabilities across models.

Businesses across industry are currently or preparing to invest billions in creating their own LLMs to undertake a wide range of tasks such as smart assistants. Financial services and large enterprises are adopting these technologies but researchers say that these vulnerabilities should be a major concern for all businesses that are planning to build or use third party LLMs.

Dr Garraghan said: "While LLM technology is potentially transformative, businesses and scientists alike will have to think very carefully on understanding and measuring the cyber risks associated with adopting and deploying LLMs."

The paper, 'Model Leeching: An Extraction Attack Targeting LLMs', will be presented at CAMLIS 2023 in Arlington, Virginia USA which is held on October 19 and 20.




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

Disaster Management Insights: Lessons from the Field

By Luiz Henrique Hargreaves

Disaster and Emergency Preparedness, Homeland and Corporate Security, Crisis Management

Source

Sep 11 – In my years of studying and engaging with various disasters and incidents involving multiple casualties, I've gained valuable insights and reflections that I believe are essential for anyone interested in disaster medicine, emergency preparedness, and response. I'd like to share some of these crucial points and reflections in this article.

1. Disasters Begin and End Locally: All disasters have a local origin. They emerge within specific communities, impacting lives at the local level. Consequently, the primary responsibility for prevention and preparedness lies with local governments, working in collaboration with communities, private enterprises, and other stakeholders.

2. Priorities: The priority is always to save lives, and ensuring a safe scene before initiating any care is fundamental. In disaster preparedness, acknowledging and addressing the unique needs of vulnerable populations is a matter of life and death. It ensures that our plans and responses are inclusive and effective, leaving no one behind during times of crisis.

2. Vulnerability and Threats: Every disaster is secondary to a threat that explores a vulnerable community incapable of addressing the crisis with its own resources. Recognizing and addressing vulnerability is paramount, especially in the context of natural disasters, where threats are driven by natural phenomena. Always be alert to signs of potential chemical, biological, radiological, nuclear, and explosive emergencies. All efforts should be made to train the population to have an emergency plan, and a survival kit, obtain information from reliable sources, and know how to recognize alerts and alarms and what to do if they are activated. The population should be aware of local risks and ways they can be involved in mitigation efforts

3. Socioeconomic Vulnerability: Socioeconomically disadvantaged communities are disproportionately affected by disasters. Even before the disaster strikes, these communities often struggle with limited access to basic healthcare resources and inadequate sanitation facilities.

4. Integrated and Coordinated Management: Effective disaster management requires an integrated and coordinated approach. The Incident Command System serves as an excellent methodology for this purpose. It's important to note that disaster management is not the sole responsibility of a single institution; all organizations involved should be part of the solution, and be integrated and engaged.

5. Core Elements of Response: The core components of a disaster response are command, control, communications, and resources. These elements must work seamlessly together to provide an effective response.

6. Training and Exercises: Exercises and training are fundamental to emergency preparedness. They must be based on realistic scenarios designed to test response plans. If there is no plan to test and if the exercises are not subsequently evaluated, they lose their meaning.

7. Purposeful Simulations: Large-scale exercises should only be conducted after strategic and tactical levels have thoroughly tested response plans. These simulations encompass all levels, including the operational level, involve multiple agencies, and have well-defined objectives. They must be evaluated and should not be seen as theatrical presentations; they must serve a clear purpose.

8. Effective Communication: Effective communication is crucial during disasters. It informs the population and stakeholders about the ongoing situation and planned measures and prevents rumors and misinformation from exacerbating the crisis. Coordination in communication is key, and it must follow a plan.

9. Mitigation during Reconstruction: One of the most effective phases for mitigation is during the reconstruction process. Investing in resilience during this phase can significantly reduce the impact of future disasters.

10. Continuous Preparedness: The disaster cycle includes preparation/mitigation, preparedness, response, and recovery/reconstruction. It's important to remember that even while responding to a disaster, communities should not stop preparing for future events. A disaster can happen anytime and anywhere.

11. Informed Alerts and Alarms: Alerts and alarms are only effective if they provide clear information to the population about what is happening and what actions they should take.

12. Trained Assistance: Individuals should not rush to disaster sites without proper training and authorization to provide assistance. Self-dispatching can lead to further tragedy.

13. Learning from Past Disasters: Learning from past disaster experiences is essential. However, just because something hasn't happened before doesn't mean it won't happen in the future.

14. The Role of Volunteers: Volunteers are indispensable in all phases of the disaster cycle. Affiliated volunteers should follow organizational guidelines, and planning should exist to coordinate and guide non-affiliated volunteers.

15. Transparent Donation Campaigns: Donations should only be solicited after the affected community is informed about their specific needs, required quantities, distribution plans, and storage methods. Providing cash through a reliable and accountable channel is often the most effective way to assist an affected community. However, the risk of scams, corruption, and cyberattacks increases significantly during disasters. Therefore, stringent measures must be implemented to prevent any form of criminal misuse of donated funds.
16. Hospital Considerations: When disaster strikes, do not assume that the most severely injured victims will be the first to reach hospitals. Hospitals may be damaged or inaccessible. Hospitals need to be prepared to conduct decontamination at the entrance. In incidents with multiple casualties, many victims may go directly to the nearest hospital without undergoing any form of triage and may be contaminated. Hospital staff should always be involved in emergency response training, and it is highly recommended that they use the Hospital Incident Command System for incident management. Eventually, hospitals can be the point of origin for an incident with multiple casualties.
17. The Importance of Planning: The absence of planning often results in chaos during disaster responses.
18. Universal Vulnerability: Disaster does not discriminate; everyone is vulnerable to its effects.
19. Risk and Safety Realities: Finally, it's crucial to understand that there is no such thing as zero risk or 100% safety in any aspect of life.
In conclusion, disaster management is a complex endeavor involving many factors. By recognizing these principles and reflections, we can better prepare for, respond to, and recover from disasters. It's a shared responsibility that requires collaboration, planning, and continuous learning. Let's work together to build more resilient communities and minimize the impact of disasters on vulnerable populations.

Mortuary Logistic Challenges of Mass Fatality Incidents

By O. Shawn Cupp
Source: https://www.domesticpreparedness.com/articles/mortuary-logistic-challenges-of-mass-fatality-incidents

Today in the United States, some in society are hesitant to acknowledge or plan for "failure options" – in other words, admit that the worst of the worst can happen. The military requires planning for just about every situation including when operations do not go as planned. However, those in emergency management and domestic preparedness operations need to consider tragedy and events unimaginable to most people.

One "unimaginable" event that preparedness professionals must anticipate is a mass fatality incident on a regional or national level. Preparing for this type of event requires understanding the complex problem, ensuring adequate logistic resources, and detailed planning for this kind of incident. All three of these areas require careful and well thought out consideration.

The Complex Problem

The United States continues to improve preparedness efforts for a number of possible manmade and natural disasters. These improvements have occurred most notably since the 9/11 terrorist attacks in 2001 and Hurricane Katrina in 2005. Planners at the local, state, tribal, and federal levels continue to improve their plans and details of their responses to a number of likely events.

Nevertheless, the United States has little experience with a mass fatality incident on a national scale. The attacks of 9/11 and Hurricane Katrina were tragic but were not on the scale or scope of the 1918-1919 Spanish Flu pandemic, when a quarter of the U.S. population fell ill and more than 675,000 Americans died. Outside the United States, the 2004 Tsunami in South-East Asia and the 2011 earthquake, tsunami, and subsequent Fukushima Daiichi nuclear reactor failure are in the large-scale mass fatality incidents category, with numbers of deaths estimated close to 300,000 and 20,000, respectively. The need to recognize and strengthen fatality management, planning, and response are critical to recovery efforts during a mass fatality incident.

Regardless of the size of the mass fatality incident, the medical examiner/ coroner (ME/C) is the legal authority to conduct victim identification (or augment the lead investigative agencies to complete victim identification). The ME/C determines the cause and manner of death and manages death certification. The ME/C is also responsible for other medico-legal activities such as notification of next of kin. The number of deceased is a significant driver in the amount and type of resources needed to search, recover, and identify decedents. In general, the higher the number of fatalities, the more resources required for managing and processing the remains. Understanding this requirement involves planners recognizing the need for greater numbers of adequately trained people to effectively manage a mass fatality incident.

Culturally, death in the United States is often considered a taboo topic. However, in 2014, the Centers for Disease Control and Prevention (CDC) estimated 2.6 million deaths in the United States. Most of these deaths are anticipated and processed through normal funeral home channels. However, of these 2.6 million reported deaths, there were 135,928 accidental and 42,826 suicide deaths. The total number of U.S. deaths recorded each year by the CDC ranged from 2,148,463 in 1990 to 2,626,418 in 2014. Therefore, this information provides a predictable number for funeral homes and services to process and plan for on an annual basis. In addition, the number of caskets and cremations required each year are highly dependent on just-in-time logistics. Caskets and coffins are not stockpiled in large warehouses. Using "lean Six Sigma" business practices, materials to produce caskets are ordered, built, and delivered for just-in-time requirements. Based on material requirements that have been steady for almost 25 years, the U.S. funeral industry provides goods and services to citizens established on historical demands. This keeps costs down and provides a multitude of options for consumers. However, these options are costly, whereas throughput is the primary consideration during a mass fatality incident.

Decedent Remains Planning & Educational Resources

In response to a mass fatality/incident, planning for decedent management – which includes resources and mortuary options – is required. Options available for human remains in a mass fatality incident require prior planning (see Table 1). Ranging from caskets and cremation to more innovative approaches like

biodegradable alternatives, each option should be considered for use in a mass fatality incident. The following recommendations would help mitigate the logistical impact of mortuary disaster operations:

- Integrate planning for mass fatality incidents into planning exercise considerations and execute mortuary operations during exercises.
- Participate in national mass casualty exercises like the U.S. Northern Command (NORTHCOM) Chemical, Biological, Radiological, and Nuclear (CBRN) Response Command Post Exercise, "Vibrant Response."
- Explore plans that various hospitals, states, and regions have developed in response to mass fatality incidents. Each local, state, and tribal area is different, but planning for mass fatality incidents requires significant time and details to meet the demands of such an event.
- Vet options beyond caskets to mitigate the psychological impacts of a mass fatality incident.

TABLE 1. POSSIBLE OPTIONS FOR MORTUARY OPERATIONS

Options	Logistics considerations	Cost	Ease of use in domestic preparations
Casket	Materials, order times, number available	Relatively high	Acceptable means
Cremation	Crematorium facilities	Relatively high	Acceptable means
Remains Pouches	Requires prior planning	Relatively inexpensive	Less than acceptable except in emergencies
Freeze Dried	Still new option with limited facilities	Relatively high	Probably not a feasible option
Biodegradable	Newer option with limited facilities	Relatively high	Not standard practice or accepted across population

Further Recommendations

A mass fatality incident is a crisis that no emergency planner would want to endure, but the likelihood of such an event does exist. The complexity and related logistical concerns require more consideration as highlighted by incidents that have occurred in various parts of the world. Planning at the regional and national levels, during exercises, would provide leaders with a better understanding of this multifaceted problem.

In addition to the hyperlinked websites throughout this article, additional educational resources on the topic of mass fatality incidents include:

- *"Mass Fatality and Casualty Incidents: A Field Guide," by Robert A. Jensen (1999)*
- *"Mass Casualty and High Impact Incidents: An Operations Guide," by Henry T. Christen (2002)*
- *"Mass Fatalities: Managing the Community Response," by Peter R. Teahen (2011)*
- *"Mass Fatality Management Concise Field Guide," by Mary H. Dudley (2013)*
- *"Army Techniques Publication (ATP) 4-46, Contingency Fatality Operations" (2014)*

O. Shawn Cupp, Ph.D., is a professor of Force Sustainment and Management at the Department of Logistics and Resource Operations, U.S. Army Command and General Staff College (CGSC), Fort Leavenworth, Kansas. He is a retired Lieutenant Colonel who served over 20 years on active duty in the U.S. Army. Currently, he is entering his 17th year instructing at the Command and General Staff Officer Course in either a military or civilian capacity. He manages the Homeland Security Studies track of the Master of Military Art and Science (MMAS) of the CGSC thesis program. He also led collaborative efforts to develop, implement, and assess a college-level homeland security studies program with over 1,900 graduates during the past decade. During his tenure, he researched, taught, published, and presented on a variety of homeland security and agricultural security related issues to a wide range of audiences including graduate level instruction, university and civic organizations, and national level conferences. Presently, he is also an adjunct faculty member at the Department of Diagnostic Medicine/Pathobiology, College of Veterinary Medicine, Kansas State University, Manhattan, Kansas.


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