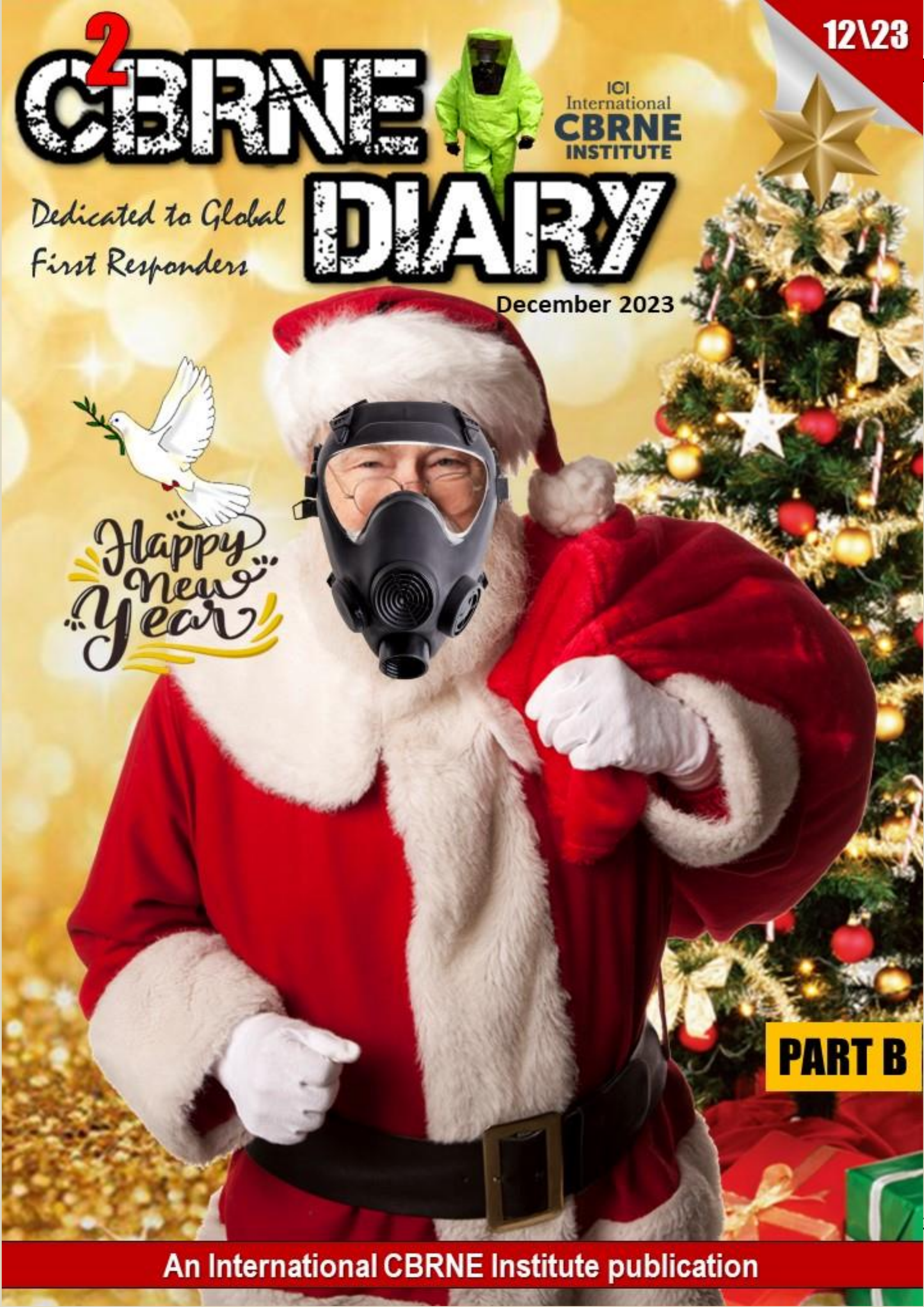


12\23

C2BRNE DIARY

International CBRNE INSTITUTE

Dedicated to Global First Responders

December 2023

PART B

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

DIRTY R-NEWS

C2BRNE DIARY

Preparing U.S., Partners for Radiological Response

By Paul Menser

Source: https://www.homelandsecuritynewswire.com/dr20231127-preparing-u-s-partners-for-radiological-response

Nov 27 – Programmatic growth can sometimes involve seeking new customers, but this has not been the case for Idaho National Laboratory's Nuclear/Radiological Search and Response Training (N/RSRT) program, which turns 20 this year. Starting with a few training events in March 2003, the program has grown organically to the point where it now conducts year-round training for radiological response entities worldwide.

After the September 11th attacks, security professionals worried that terrorists might detonate a "dirty bomb" – an explosive device enhanced with radiological source materials. INL offered distinct advantages to train responders for this type of event. The lab's experts have extensive experience in radiation detection and hazard mitigation, plus a large inventory of radiological and nuclear materials. All of these have been used to develop the "new" training program. "We're not using simulators," said Program Manager Jennifer Turnage. "We're working with real radiation sources." INL also has open spaces and legacy facilities that are often utilized for training and exercise demonstrations.

In the Beginning

INL has supported the U.S. National Technical Nuclear Forensics program since 2002. Because of the lab's nuclear fuel examination and handling capabilities, the program's original sponsor, the Defense Threat Reduction Agency (DTRA), selected INL to help characterize radioactive materials that could be used in a radiological dispersal device (RDD) – the official term for "dirty bomb." At a program review, a DTRA contractor approached three INL experts – Kevin Carney, David Chamberlain, and the late Richard McKnight – to develop a training course to address how such a device might be "rendered safe."

INL appointed Turnage as program manager. The inactive Transient Reactor Test Facility was selected as the training location due to its remoteness and inventory of high-activity radioactive sources and irradiated fuel assemblies. Jim Thalgott and Debra Kirschner provided health physics and radiological protection oversight. The late Doug Ray and Gary Englestad supported the reactor facility's radioactive material handling and spent fuel operations.

The initial training event's success led DTRA to establish a new contract for five additional courses for specialized teams supporting nuclear and radiological weapon incident response. Subsequent training events revealed the challenges involved with imaging high-intensity radioactive sources in different and unique scenarios. This led to research by scientist Paul Hart on which film and materials to use for imaging based on the nature of the radiation being detected, and on what procedures needed to be followed. Physicists John Giles and Christopher Oertel later contributed expertise in gamma spectrometry and radiation detection.

The Program Expands

Training curricula evolved to incorporate nuclear fuel cycle content and instruction on radiation detection and search techniques utilizing the Critical Infrastructure Test Range Complex and legacy facilities such as Experimental Breeder Reactor-II. Participation expanded to include response assets from the U.S. Army, Navy, FBI, and National Guard units from across the country. "The unique capabilities INL offered, including technical expertise and the realistic training environment, made the training highly sought after," Turnage said. Today, INL conducts more than 75 training and exercise demonstrations annually.

Program Strategist Bryon Marsh's experience with INL's N/RSRT program dates back to 2004, when he was in the U.S. Army and served in the 4th Weapons of Mass Destruction Civil Support Team.

"We came to INL because we were able to accomplish the training objectives we identified, and (because of) the ability to work with real radiation sources," Marsh said. "The experts were people with extensive knowledge and experience in handling radiological hazards. You couldn't find this training opportunity anywhere else."

Changing Technology and Tools

Giles said different training events emphasize different skills. "Technology and tools have changed," he said. INL has supported training for these specialized teams and provided invaluable opportunities for them to develop or refine conduct of operations when new tools and technologies become available.

"The next time these folks encounter a radioactive source, it could likely be a real-world incident," Giles said. "We let them work through their procedures and watch how they execute. We're providing them with tools and knowledge."

Current Events

INL's reputation within the global radiological response community has not gone unnoticed. After supporting the 2018 CBRNe (Chemical, Biological, Radiological, Nuclear, and high yield Explosives)

Science and Consequence Management (CSCM) World Congress, several experts from the program were invited to participate in 2023 CSCM World Congress. Since the late 1990s, the CSCM Congress has gathered top scientists from over 50 countries to engage with defense personnel, emergency responders and government officials. The focus of this interaction is to share knowledge that lessen concerns about weapons of mass destruction and to increase information on preventing or responding to possible mass casualty events involving CBRNe.

"The World Congress is getting a lot of attention on radiological preparedness," Marsh said. "Our participation in the World Congress and the training workshop we'll conduct will demonstrate what we're capable of doing at the international level."

Final Thoughts

"Train as you fight" is the program philosophy. "Fight as you train" is the customer's philosophy, hence the importance of working with actual radiation, with their designated equipment set, honing their individual skills, and learning to work together as a cohesive unit.

"You don't drop a soldier out of a plane for the first time into a live firefight. Realistic, in-depth training is required so that they can react instinctively to any situation. We consider operating in a radiation environment … to be comparable," Turnage said. "We're working with the real thing, but it's in a very controlled, deliberate manner. It's very gratifying to observe the trainees throughout the whole process, you get a much better understanding of what they endure during deployment out in the real world."

Paul Menser is a Communications Specialist at the Idaho National Laboratory (INL).

Smoke Alarms, Zaporizhzhia, Litvinenko: RDDs are not Always Explosive

By Andy Oppenheimer

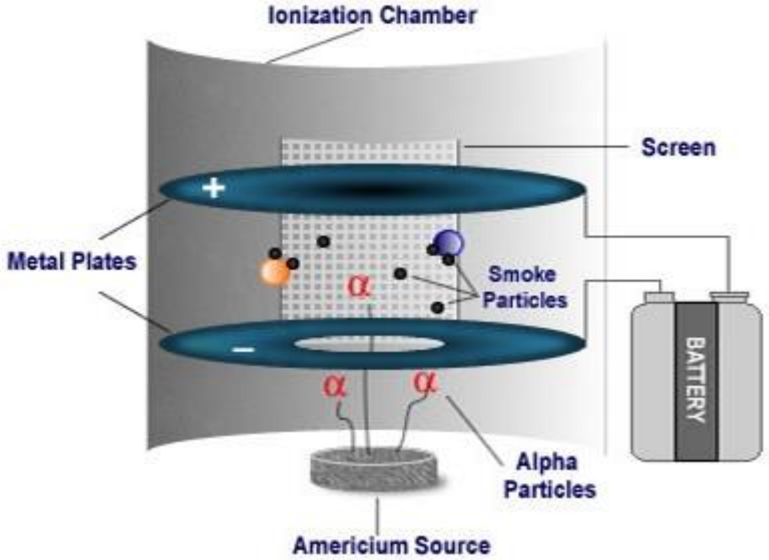
Source: https://nct-cbnw.com/smoke-alarms-zaporizhzhia-litvinenko-rdds-are-not-always-explosive/

Nov 16 – Despite the fact that the definition of a radiological dispersal device (RDD) is an explosive device laced with a radioisotope, hardly any incidents involving them have been documented.

When is it an RDD?

A major problem with such devices is that their detonation would resemble the explosion of an ordinary IED, unless intelligence of theft of radiological materials from a hospital or industrial facility, for example, had been received prior to the attack, and if first responders and forensic teams test for radioactivity.

If post-event scanning of the scene and victims does not occur, only when victims present with radiation-related injuries at hospital Accident & Emergency departments or develop health problems later will evidence emerge that the bomb was not a conventional IED. RDDs may affect localized areas such as a building, block or street, or a larger area of several square miles depending on the nature of the dispersion and the amount and type of radioactive material. All or most fatalities or injuries will be likely due to the explosion itself. Despite many experts currently playing down the effects of radiation, the need to decontaminate all affected areas would be paramount, especially in the event of a terrorist or accidental use of a nonexplosive dispersal, such as the abandonment of a radioactive source.



This diagram shows how an americium source ionizes air particles and makes an ionization smoke detector work. ©US EPA

Historical RDD Incidents are Few and Far Between[1]

Other than when a handful of RDD emplacements were attempted by Chechen rebels – including in December 1998 when a Security Service team discovered on a railway line a container filled with unidentified radioactive materials attached to a landmine – there are few documented incidents where the presence of an RDD was confirmed. Therefore, we are unable to learn from precedent thus far. Equally uncommon are seizures of radioactive material. On December 29, 2022, Border Force officers at London's Heathrow Airport found 'traces' of uranium within a cargo shipment of scrap metal following a routine security screening. A man was later arrested in Cheshire under Section 9 of the Terrorism Act 2006, which covers the making and possession of radioactive devices and materials. The package, which originated in Pakistan and was flown on an Oman Air jet arriving from Muscat, was reportedly headed to a UK-based Iranian business. Uranium's weight and physical properties make it a poor choice for RDD.

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

Andy Oppenheimer AIExpE MIABTI (born 1953) is a UK-based expert and consultant in counterterrorism and CBRNE (chemical, biological, radiological, nuclear weapons and explosives). Since 2001 he has written articles, edited journals, and presented at conferences and professional seminars worldwide. He has been editor of several journals on defence and security, including Chemical, Biological & Nuclear Warfare (CBNW) from 2009, Jane's Nuclear, Biological and Chemical Defence and NBC International from 2006 to 2008, and was co-editor of Jane's World Armies from 2002 to 2004. He has served as a CBRN consultant for Jane's Consultancy Group and Oxford Analytica.

Bioengineered Potato Plant Detects Gamma Radiation

Source: https://www.homelandsecuritynewswire.com/dr20231128-bioengineered-potato-plant-detects-gamma-radiation

Nov 28 – A researcher at the University of Tennessee Herbert College of Agriculture has developed a potato plant that can detect gamma radiation, providing reliable indications of harmful radiation levels without complex monitoring technologies.

[1] November 1995 – Moscow, Russia—In the first-ever attempt at radiological terror, a group of Chechen rebels contacts a Russian television station and boasts of its ability to construct a radioactive bomb. The rebels alert the press that they have buried a cache of radiological materials in **Moscow's Ismailovsky Park**. In the very spot where the rebels indicated it would be, authorities find a partially buried container of **cesium.** Neither the Chechens who planted it there nor the original source of the cesium are ever identified. (retrieved from https://www.pbs.org/wgbh/nova/dirtybomb/chrono.html)

PhD student Rob Sears engineered the plant, also known as a phytosensor, to indicate high radiation levels through changing leaf fluorescence. When exposed to gamma radiation, the plant's leaves produce a green glow, allowing for accurate warnings that are visible across long distances. Since potatoes are grown across the world in both hospitable and adverse climates, they are the ideal plant for the research as well as for the eventual mass implementation of the developed varieties.

Sears says that potatoes reproduce through tubers in the soil, spreading across diverse terrain while producing genetically identical offspring that provide consistent results. "Potatoes are highly resilient and are excellent at adapting and multiplying in different environments. They also have complex responses that are often specific to an environmental stressor, making them ideal reporters of conditions such as gamma radiation. My research aimed to make these responses visible and evident even from a distance, acting as a natural warning sign of harmful radiation without the need for mechanical sensors."

As nuclear energy continues to be used across the world, there is an increased demand for effective and easily accessible radiation detection methods. Since phytosensors are affordable, easy to interpret and require no mechanical maintenance, they have the potential to improve the safety and wellbeing of workers and residents who are in close proximity to radiation sources.

"It is a rewarding experience to see the fundamental radiation biology I have studied transform into an engineered biological device that has the potential to impact future radiation monitoring," says Sears. "Not only that, but phytosensors demonstrate the potential of synthetic biology to engineer plants as 'devices' that can impact not only agriculture, but also provide valuable tools for increasing the safety of our environments."

His PhD research project, Sears says it would not have been possible without the education and experience attained while in the Herbert College of Agriculture as well as the support of Neal Stewart, professor in the UT Department of Plant Sciences, and Scott Lenaghan, professor in the UT Department of Food Science, who both served as faculty partners on the study. Sears will graduate in December 2023, and he looks forward to continuing to improve the world around him through the development of bioengineered plant varieties.

On the use of free code tools to simulate the propagation of radiation following dirty bomb explosions in sensible contexts

By Riccardo Quaranta, Gian Marco Ludovici, Guglielmo Manenti, Pasqualino Gaudio, and Andrea Malizia

The European Physical Journal Conferences 288(5-6):06009 | Nov 2023

Source:https://www.researchgate.net/publication/375880295_On_the_use_of_free_code_tools_to_simulate_the_propagation_of_radiation_following_dirty_bomb_explosions_in_sensible_contexts

The current geopolitical situation suggests an increasing possibility of radiological dispersal device attacks on sensitive targets. Consequently, understanding the transport of radiation over great distances in a short time can help first responders and decision makers in effectively managing emergencies. By utilizing open-source computational codes, intentional releases of radioactive material and their transmission from person to person can be simulated to provide first responders and decision makers with a rapid tool to facilitate their work. In this study, the HotSpot code was employed to simulate two releases of Cs-137 resulting from the detonation of a dirty bomb in a major city and near an aqueduct waterworks. Additionally, the STEM code was used to simulate radiation propagation from the initially affected individuals, drawing comparisons to the vectors of viral infections. This approach allowed to compare the outcomes of a scenario involving many individuals in an urban setting with another scenario having fewer individuals but posing the risk of contaminating critical infrastructure. The results showed that both scenarios had similar relatively mild health consequences for the population, despite their considerable differences and variations in the analyzed timelines. However, both scenarios present numerous challenges in emergency management. In the first case, the incident generates widespread panic and media frenzy. In the second case, the dissemination of radiation and potential public unawareness must be taken into account. Addressing these considerations needs the involvement of multiple stakeholders, including police, firefighters, healthcare professionals, journalists, politicians, and others, in emergency management efforts.

Processing biological samples from simulated radiological terrorist events using Rapid DNA instruments

By Chantal J. Frégeau and Nancy Laurin

Forensic Science International | Volume 354, January 2024, 111887

Source: https://www.sciencedirect.com/science/article/abs/pii/S0379073823003377

Abstract

Two commercially available portable Rapid DNA instruments were evaluated for their ability to process 1 μL and 10 μL saliva samples deposited on metal and plastic surfaces and contaminated with surrogates of cesium (Cs)-137, strontium (Sr)-90 and cobalt (Co)-60; radioactive materials potentially released during a nuclear weapon accident or a radiological dispersal device detonation. A comparable success rate was noted for both Rapid DNA instruments when considering the number of complete and balanced DNA profiles, the number of profiles with a minimum of 10 autosomal STR loci (out of 23 [FlexPlex™ 27] or 21 [GlobalFiler™ Express]), and the possibility to search a national DNA database in Canada and the United States. Cobalt had an adverse impact on the quality of the megaplex short tandem repeat (STR) DNA profiles derived on each instrument for two of the three contamination levels tested in this study, i.e., 0.05 M and 0.1 M as reflected by a reduced number of detected alleles and decreased profile peak heights. Strontium exhibited some adverse effect on the Rapid DNA results when used at the highest contamination level (0.1 M) whereas cesium had none. No new artifacts were observed in the Rapid DNA profiles of samples spiked with the non-radiogenic surrogates. Importantly, in the context of a radiological/nuclear (RN) event, the ANDE™ 6C offers the possibility to dispose of all radioactive materials associated with contaminated samples quickly using a chip on which all steps of the Rapid DNA process are performed whereas the RapidHIT™ ID accumulates radioactive materials for many days before disposal. An individual handling 25 samples in a week (5 per day) on the RapidHIT™ ID at a 30.5 cm distance with a 5 min exposure to the radioactive source estimated at every run would exceed the 0.042 μSv/5 min limit with gamma dose rates for Cs at 0.13 mSv and for Co at 3.8 mSv. Beta dose rates calculated for the surrogate isotopes at the three concentrations tested were also above the recommended radiation exposure limit of 1 mSv/yr (0.042 μSv/5 min). Various potential mechanisms of action behind the interference noted for Sr and Co at high concentrations are presented. These elements may play a role in the steps prior to PCR (at the DNA molecule by binding to bases or to phosphate groups), during PCR (at the DNA polymerase as cofactors for catalytic sites), or even during amplified DNA fragment detection (as fluorescence quenchers).

COP28: UAE signs deal with Bill Gates' nuclear company on advanced reactors

Source: https://www.reuters.com/business/environment/cop28-uae-signs-deal-with-bill-gates-nuclear-company-advanced-reactors-2023-12-04/

Dec 04 – Bill Gates' advanced nuclear reactor company TerraPower LLC and the United Arab Emirates' state owned nuclear company ENEC said on Monday they have agreed to study the potential development of advanced reactors in the UAE and abroad. The memorandum of understanding comes amid a push by the UAE to expand its nuclear energy capacity, and a pledge by over 20 nations at the COP28 climate conference in Dubai to triple nuclear deployment this decade to fight climate change.

“For the UAE, we're looking for a future for the clean electrons and molecules that will be brought to reality by advanced reactors,” said Mohamed Al Hammadi, CEO of ENEC, during the signing ceremony.

"Bringing advanced nuclear technologies to market is critical to meeting global decarbonization targets," said TerraPower President and CEO Chris Levesque.

The UAE currently has one traditional nuclear power plant, near Abu Dhabi, which began producing electricity in 2020. TerraPower, meanwhile, has a demonstration project underway for its advanced Natrium reactor in the U.S. state of Wyoming that hopes to come online in 2030.

Advanced reactors are meant to be smaller, easier to build, and more dynamic than traditional plants, and are regarded by some as vital complement to intermittent power sources like wind and solar that are expanding rapidly.

The MOU between TerraPower and the UAE said they would explore uses for advanced nuclear reactors such storing power on the grid and providing the energy needed to produce hydrogen, and decarbonize coal, steel and aluminum plants.

One potential hitch, however, is that TerraPower's Natrium reactors require a fuel called high assay low enriched uranium or HALEU, the main producer of which currently is Russia.

TerraPower's Wyoming project has experienced delays over concerns about HALEU supply since the Russian invasion of Ukraine, but the company told Reuters it expects the United States to be able to produce the fuel in the coming decade.

The United States is seeking to start up HALEU production domestically and has contracted with a company called Centrus to develop a project to do so.

Sellafield nuclear site hacked by groups linked to Russia and China

By Anna Isaac and Alex Lawson

Source: https://www.theguardian.com/business/2023/dec/04/sellafield-nuclear-site-hacked-groups-russia-china

Dec 04 – The UK's most hazardous nuclear site, Sellafield, has been hacked into by cyber groups closely linked to Russia and China, the Guardian can reveal.

The astonishing disclosure and its potential effects have been consistently covered up by senior staff at the vast nuclear waste and decommissioning site, the investigation has found.

The Guardian has discovered that the authorities do not know exactly when the IT systems were first compromised. But sources said breaches were first detected as far back as 2015, when experts realised sleeper malware – software that can lurk and be used to spy or attack systems – had been embedded in Sellafield's computer networks.

It is still not known if the malware has been eradicated. It may mean some of Sellafield's most sensitive activities, such as moving radioactive waste, monitoring for leaks of dangerous material and checking for fires, have been compromised.

Sources suggest it is likely foreign hackers have accessed the highest echelons of confidential material at the site, which sprawls across 6 sq km (2 sq miles) on the Cumbrian coast and is one of the most hazardous in the world.

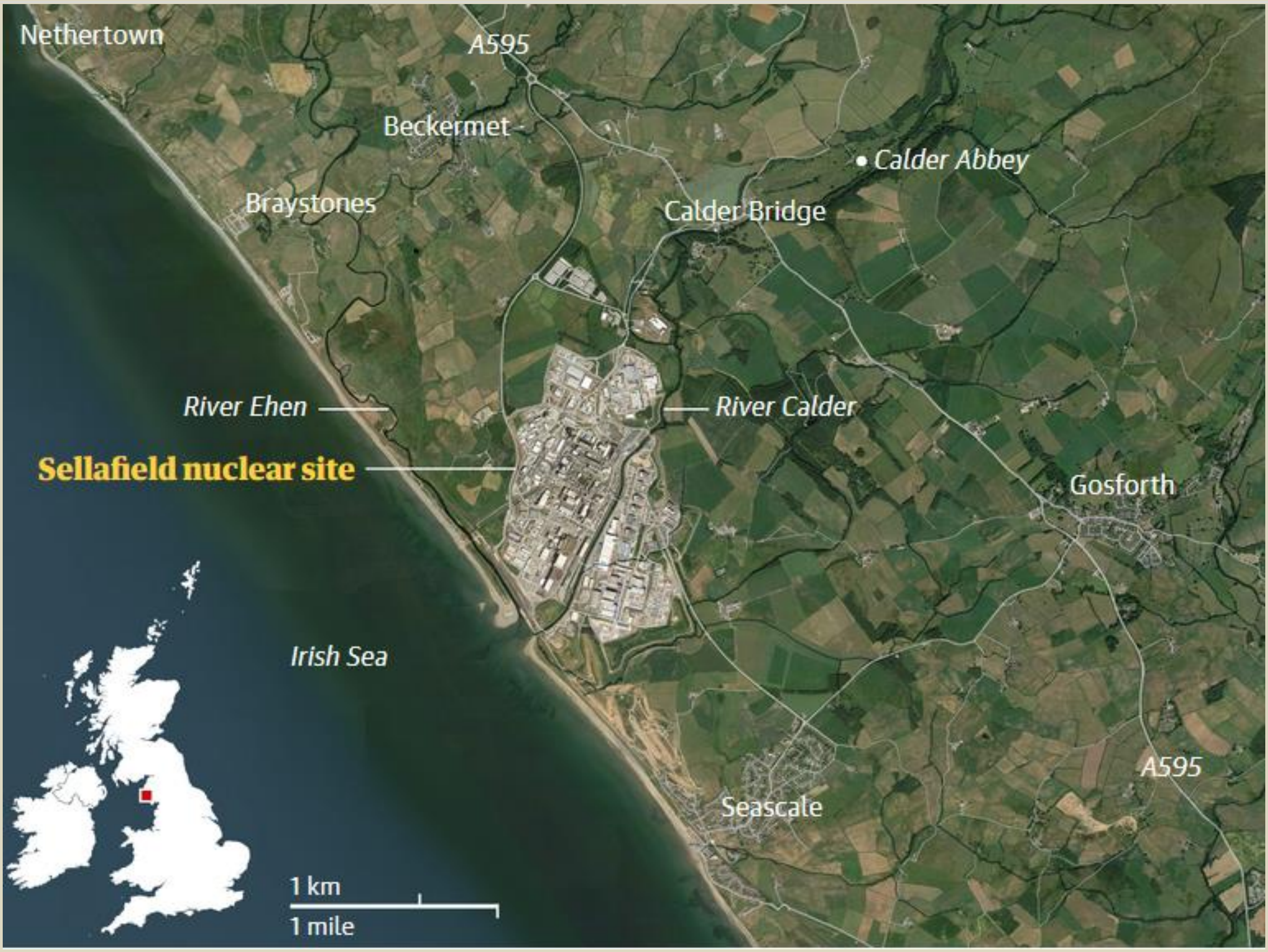
Sellafield covers 6 sq km on the Cumbrian coast and is one of the most hazardous nuclear sites in the world. Photograph: David Levene/The Guardian

The full extent of any data loss and any ongoing risks to systems was made harder to quantify by Sellafield's failure to alert nuclear regulators for several years, sources said.

The revelations have emerged in Nuclear Leaks, a year-long Guardian investigation into cyber hacking, radioactive contamination and toxic workplace culture at Sellafield.

The site has the largest store of plutonium on the planet and is a sprawling rubbish dump for nuclear waste from weapons programmes and decades of atomic power generation.

Guarded by armed police, it also holds emergency planning documents to be used should the UK come under foreign attack or face disaster. Built more than 70 years ago and formerly known as Windscale, it made plutonium for nuclear weapons during the cold war and has taken in radioactive waste from other countries, including Italy and Sweden.



The Guardian can also disclose that Sellafield, which has more than 11,000 staff, was last year placed into a form of "special measures" for consistent failings on cybersecurity, according to sources at the Office for Nuclear Regulation (ONR) and the security services.

The watchdog is also believed to be preparing to prosecute individuals there for cyber failings.

The ONR confirmed Sellafield is failing to meet its cyber standards but declined to comment on the breaches, or claims of a "cover up".

A spokesperson said: "Some specific matters are subject to ongoing investigations, so we are unable to comment further at this time."

In a statement, Sellafield also declined to comment about its failure to tell regulators, instead focusing on the improvements it says it has made in recent years.

Labour's shadow secretary of state for energy security and net zero, Ed Miliband, said it was a "very concerning report about one of our most sensitive pieces of energy infrastructure".

"It raises allegations that must be treated with the utmost seriousness by government," he said.

"The government has a responsibility to say when it first knew of these allegations, what action it and the regulator took and to provide assurances about the protection of our national security."

The problem of insecure servers at Sellafield was nicknamed Voldemort after the Harry Potter villain, according to a government official familiar with the ONR investigation and IT failings at the site, because it was so sensitive and dangerous. It involved highly sensitive data that could be exploited by Britain's enemies. Sellafield's server network was characterised by the official as "fundamentally insecure".

The scale of the problem was only revealed when staff at an external site found that they could access Sellafield's servers and reported it to the ONR, according to an insider at the watchdog.

Other concerns include external contractors being able to plug memory sticks into the system while unsupervised.

In one highly embarrassing incident last July, login details and passwords for secure IT systems were inadvertently broadcast on national TV by the BBC One nature series Countryfile, after crews were invited into the secure site for a piece on rural communities and the nuclear industry.

The ONR has prepared a notice of prosecution for Sellafield on cybersecurity – a form of enforcement action it can only take if it believes there is "sufficient evidence to provide a realistic prospect of conviction".

Cyber problems have been known by senior figures at the nuclear site for at least a decade, according to a report dated from 2012, seen by the Guardian, which warned there were "critical security vulnerabilities" that needed to be addressed urgently.

It found that security resources at the time were "not adequate to police the internal threat [from staff] … let alone react to a significant increase in external threat".

More than a decade later, staff at Sellafield, regulators and sources within the intelligence community believe systems at the vast nuclear waste dump are still not fit for purpose. They also believe that there was a deliberate effort by senior leaders to conceal the scale of the problems posed by cybersecurity problems at the site from security officials tasked with testing the UK's vulnerability to attack in recent years. This is the subject of potential prosecution.

Security officials are also concerned that the ONR has been slow to share its intelligence on cyber failings at Sellafield because they indicate that its own scrutiny has been ineffective for more than a decade.

The latest annual report from the ONR stated that "improvements are required" from Sellafield and other sites in order to address cybersecurity risks. It also confirmed that the site was in "significantly enhanced attention" for this activity.

The ONR said it had found cybersecurity "shortfalls" during its inspections and noted that it had taken "enforcement action" as a result.

Such is the scale of cybersecurity concern, some officials believe entire new systems should be urgently built at Sellafield's nearby emergency control centre – a separate secure facility.

Among the highly sensitive documents stored at Sellafield are disaster manuals, plans that guide people through emergency nuclear protocols and what to do during a foreign attack on the UK.

These documents include some of the learnings from a variety of sensitive operations, including Exercise Reassure in 2005 – and the regular Oscar exercises – which were aimed at testing the UK's ability to handle a nuclear disaster in Cumbria.

The ONR was so concerned by the fact that external sites could access Sellafield's servers, and an apparent cover-up by staff, that it interviewed teams under caution. The Sellafield board held an inquiry into the problem in 2013 and the ONR warned that it would require more transparency on IT security.

Cyber-attack and cyber espionage by Russia and China are among the biggest threats to the UK, according to security officials. The most recent National Risk Register, an official document that outlines the key hazards the UK could face, includes a cyber-attack on civil nuclear infrastructure.

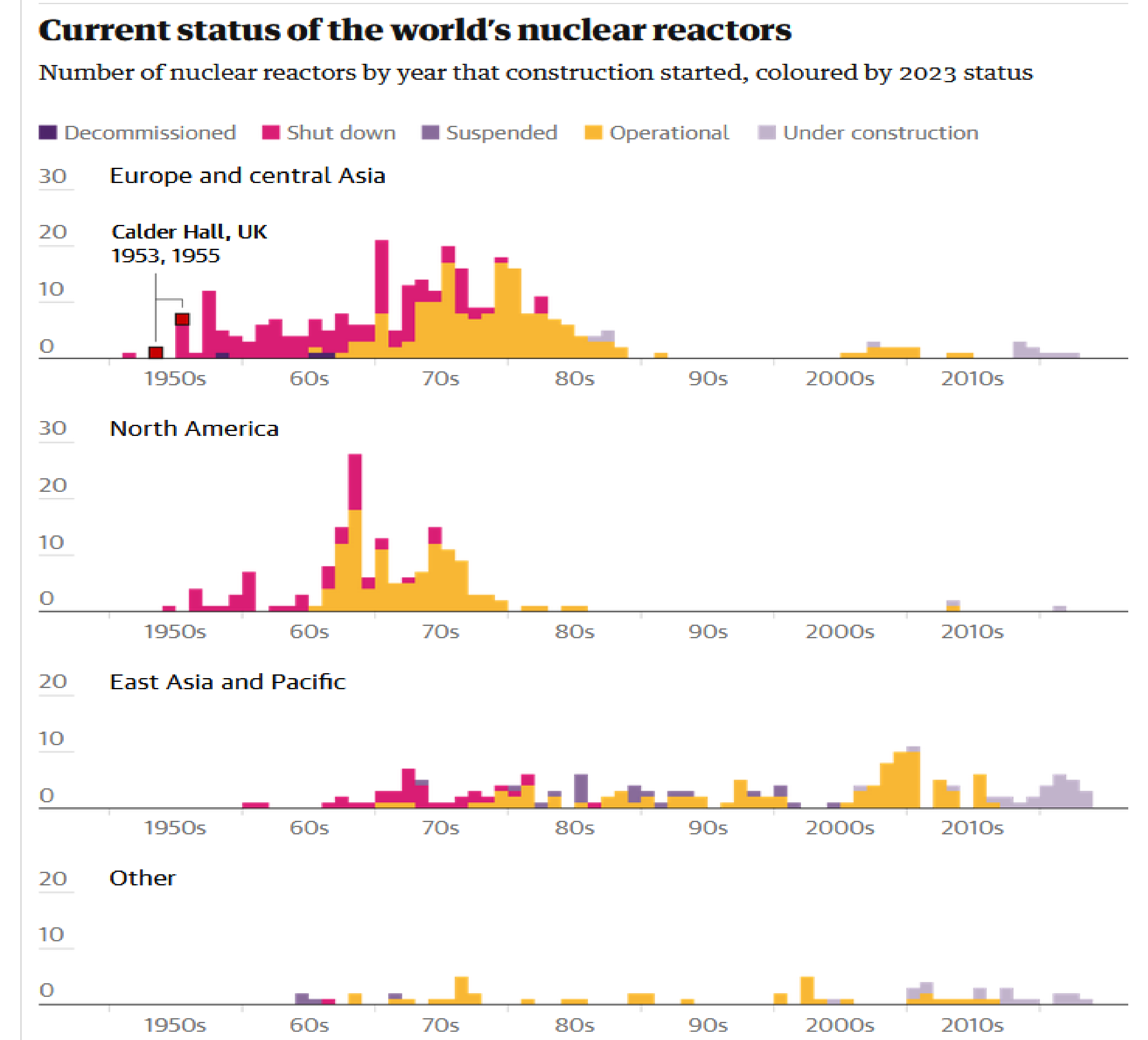
Attackers from hostile states have targeted allies in the "Five Eyes" intelligence sharing community in recent years. The US has been attacked, with its government agencies, including its energy department, targeted via file-transfer software in June this year.

The UK's cyber wing of GCHQ has warned of a heightened risk of cyber-attack on national infrastructure from Russia and China. Photograph: GCHQ/PA

The UK's cyber wing of GCHQ, which has offices in central London and is part of the domestic intelligence network with headquarters in Cheltenham in Gloucestershire, has warned of a heightened risk of cyber-attack on critical national infrastructure from Russia and China.

Growing government concern over Chinese involvement in UK critical national infrastructure has resulted in the Chinese state-owned energy company CGN being removed from the Sizewell C nuclear project in Suffolk and Huawei products being stripped from the heart of the telecommunications network in recent years. That has reversed a spell of close Anglo-Sino relations, which culminated in the then prime minister, David Cameron, hailing a "golden era" between the countries and drinking beer with the Chinese premier, Xi Jinping, in a Buckinghamshire pub in 2015.

Rishi Sunak's government has championed expanding the country's nuclear industry after the energy crisis, picking up where his predecessor Boris Johnson left off. Earlier this year, the then energy secretary, Grant Shapps, launched Great British Nuclear, a body designed to provide new nuclear power plants. A generation of new nuclear projects will ultimately require an expansion of Britain's decommissioning activities.



Guardian graphic. Source: International Atomic Energy Agency. Power reactor information system. Note: Other regions include Latin America and the Caribbean, South Asia, Middle East and north Africa and sub-Saharan Africa

Nuclear decommissioning, a large share of which is done at Sellafield, is one of the biggest drains on the UK government's annual business department budget. The site costs about £2.5bn a year to operate. Decommissioning is such a huge, long-term bill that it was examined as a "fiscal risk" to the UK's economic health by the spending watchdog, the Office for Budget Responsibility. It is estimated it could cost as much as £263bn to manage the legacy of the UK's nuclear energy and weaponry industries.

This figure shifts wildly depending on how future cash flow is calculated, and the OBR has warned that the long-term costs of Sellafield could vary by as much as minus 50% to plus 300%. A Sellafield spokesperson said: "We take cybersecurity extremely seriously at Sellafield. All of our systems and servers have multiple layers of protection. “Critical networks that enable us to operate safely are isolated from our general IT network, meaning an attack on our IT system would not penetrate these.

“Over the past 10 years we have evolved to meet the challenges of the modern world, including a greater focus on cybersecurity.

“We’re working closely with our regulator. As a result of the progress we’ve made, we have an agreed route to step down from ‘significantly enhanced’ regulation.” An ONR spokesperson said: “Sellafield Ltd is currently not meeting the high standards that we require in cybersecurity, which is why we have placed them under significantly enhanced attention.

“Some specific matters are subject to ongoing investigations, so we are unable to comment further at this time.”

Prior to publication, Sellafield and the ONR declined to answer a number of specific questions or say if Sellafield networks had been compromised by groups linked to Russia and China. Following publication, they said they had no records to suggest Sellafield’s networks had been successfully attacked by state actors in the way the Guardian described.

A spokesperson from the Department for Energy Security and Net Zero said: “We expect the highest standards of safety and security as former nuclear sites are dismantled, and the regulator is clear that public safety is not compromised at Sellafield.

“Many of the issues raised are historical and the regulator has for some time been working with Sellafield to ensure necessary improvements are implemented. We are expecting regular updates on how this progresses.”

‘Dirty 30’ and its toxic siblings: the most dangerous parts of the Sellafield nuclear site

By Alex Lawson and Anna Isaac

Source: https://www.theguardian.com/business/2023/dec/05/dirty-30-dangerous-sellafield-nuclear-site-ponds-safety-fears

Dec 05 – In the early 1950s, a huge hole was dug into the Cumbrian coast and lined with concrete. Roughly the length of three Olympic swimming pools and known as B30, it was built to hold skip loads of spent nuclear fuel.

Those highly radioactive rods came from the 26 Magnox nuclear reactors that helped keep Britain’s lights on between 1956 and 2015. When B30 was first put to work, it was designed to keep the fuel rods submerged for only three months before reprocessing work was carried out. But when 1970s miners’ strikes shut down coal power stations and forced greater reliance on nuclear plants, more spent fuel than could be quickly reprocessed was generated. The silos and ponds, built to prevent airborne contamination if the fuel or radioactive sludge dried out, rapidly filled up. Meanwhile, the fuel corroded in the water, breaking down into radioactive sludge. Debris from elsewhere within Sellafield was later added and the pond was abandoned when new facilities were built in 1986, clouding over and leaving workers on site with little idea what lay beneath its murky waters.

‘A nightmare job with no blueprint’

In 2014, photos of B30 and nearby B29 leaked via an anonymous source to the Ecologist led to concerns over the radioactive risk associated with the poor repair of the ponds. The two facilities were used until the mid-1970s for short-term storage of spent fuel until it could be reprocessed and used for producing plutonium for the military.

The B30 pond carries a higher risk of radiation than other parts of the site. Photograph: gov.uk

The Ecologist pictures showed hundreds of highly radioactive fuel rods in ponds housed within cracked concrete overgrown with weeds, with seagulls bathing in the water. The images, taken over a period of seven years, led the nuclear safety expert John Large to warn that any breach of the wall would “give rise to a very big radioactive release”.

At the time, the Office for Nuclear Regulation (ONR), the nuclear safety regulator, said that while the old ponds bring “significant challenges”, their appearance “does not mean that operations and activities on those facilities are unsafe”.

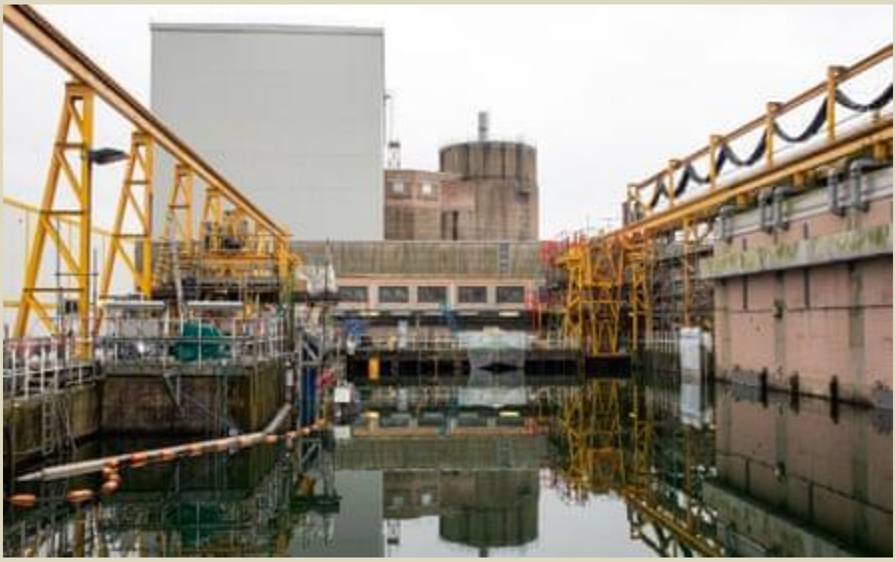
It took 15 years and £1.5bn to bring B30 to a point where decommissioning could begin several years ago, with builders limited to working only half an hour a day close to the pool to prevent them from exceeding radiation exposure limits. Remotely operated vehicles, normally used to help with submarine rescues, were originally deployed but quickly failed, often within hours, because of the overpowering radiation. Newer models have since been used to vacuum up nuclear sludge, which is then moved to alternative long-term storage.

Sellafield hopes to have drained the pond by the early 2030s, and demolished it by the 2050s.

A new facility, the sludge packaging plant, has been built to receive radioactive sludge from B30. The nuclear watchdog said there have been some "regulatory challenges along the way … including noncompliance with fire regulations".

Although the reservoir is still nicknamed "Dirty 30", it was officially rebranded in 2018 as the First Generation Magnox storage pond. But one former longstanding employee says that, despite the cracks, the contents of the ponds are gradually improving: "I have seen it at its worst. The water quality was horrendous; you could stand on the roof and look down and not see a single thing in there.

"In the control room, there are a group of lads using PlayStation-like controls for robots to pick up bits the size of a 50p piece and hoover up the sludge. It's cutting edge."



He adds: "[Decommissioning Sellafield] is the biggest job in nuclear and there is no blueprint. It's a dream and a nightmare job. There has been real progress – every skip that comes out makes it safer and reduces the hazard risk."

The pile fuel storage pond, which is on a separate part of the site from the Magnox storage. Photograph: Bloomberg/Getty Images

Toxic neighbours

B30 sits in a "separation zone" that requires greater security checks, and carries a higher risk of radiation, than the rest of the town-sized site. Although B30 is the most notorious crumbling building on Sellafield's sprawling estate, it is far from the only problem child.

Controlled Area
Radiation
R3
Contamination
C3
Do not loiter near the west (pond) side of the East Washdown as elevated levels of radiation are present in this area
Area classification

A radiation warning sign on a railing near the pile fuel storage pond. Photograph: Bloomberg/Getty Images

Nearby is B38, used to store highly radioactive cladding from reactor fuel rods. It was also used heavily during the miners' strike of 1972, when nuclear plants were relied on to produce extra power, and it proved impossible to process all the waste that was being generated. Two years later, the public's view of the nuclear industry was sharpened by the launch of the Protect and Survive advice on surviving a nuclear attack.

In B29 lie the toxic remains of Britain's attempt to become an atomic superpower during the cold war. Windscale, a former munitions factory, was selected to host the first atomic reactors, known as Pile 1 and Pile 2, after the second world war. They produced plutonium for nuclear weapons, and efforts were rushed through to allow Britain to explode its own atomic bombs by 1952.

The toxic waste from this programme was stored in B29 – which stretched between Piles 1 and 2 – and a massive silo, B41. There have been efforts to secure and remove the waste in B41 in recent years.

There are also grave concerns over leaks from the Magnox swarf storage silo (MSSS), described as “one of the highest-hazard nuclear facilities in the UK”. It was constructed as a radioactive waste store in four stages between 1964 and 1983 and has not been in active use since the 1990s. The waste is stored under water to prevent ignition and to maintain constant temperatures.

The silo was first found to be leaking radioactive water into the ground in the 1970s and there are concerns that work to retrieve the waste, planned over the next three decades, has the “potential to reopen historic leak paths” and introduce new ones, according to the ONR.

Earlier this year, the ONR warned that a leak from the MSSS was likely to continue to 2050, with “potentially significant consequences” if it gathered pace.

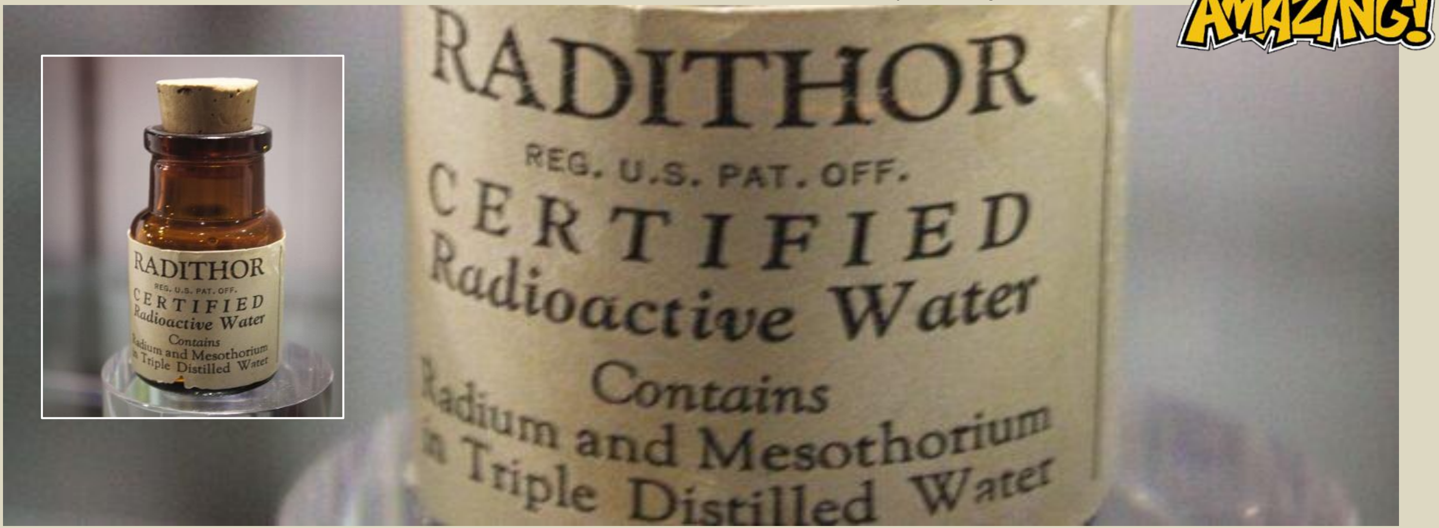
The government’s long-term plan is to bury Britain’s nuclear waste deep underground in a geological disposal facility. The project, estimated to cost between £20bn and £53bn, would receive intermediate-level waste from nuclear facilities by 2050 and high-level waste and spent fuel from 2075.

It will echo similar projects in Sweden, France and Finland, which is nearing completion of its storage cave. A government body, Nuclear Waste Services, which is running the project, is in the process of engaging with different communities – two near Sellafield, and another near Mablethorpe on the east coast – in an attempt to win local approval for the plans.

A Man Drank So Much Radium His Skull Literally Disintegrated

By Michelle Starr

Source: https://www.sciencealert.com/a-man-drank-so-much-radium-his-skull-literally-disintegrated



The label of a Radithor bottle. (Sam LaRussa/Flickr, CC BY 2.0)

Dec 05 – Bleach and chloroquine need to take a seat. Snake oil in the past has gone far harder – enough to give one man a massively fatal dose of radiation that riddled his body with cancer and literally disintegrated his skull before he died in 1932. The patient in question was Eben Byers, and he was so taken with a "miracle" tonic named Radithor that he dosed himself with it several times a day. The problem? The active ingredient in Radithor was radium. Yes, that radium. The one that forms from the radioactive decay of uranium, that is radioactive itself, and exposure to which is generally considered not a very good thing.

Supplements and patent medicines that don't necessarily do what they say on the tin have been around for a long time. But the early 20th century was a strange time. In the wake of the fin de siècle, the world was filled with optimism, and new discoveries waited around every corner. Marie Skłodowska-Curie and Pierre Curie had discovered radium in just 1898, and in the first quarter of the 20th century, this miraculous glowing metal was quickly hijacked as a health treatment.

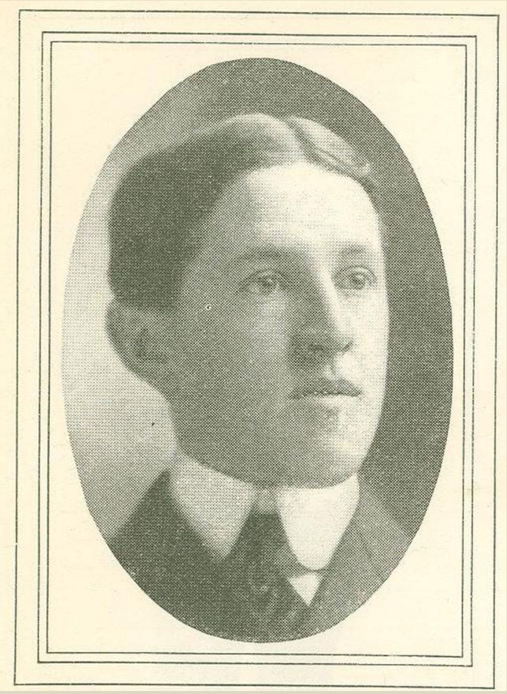
It was a popular additive in products such as toothpaste and hair cream, and even food. And then, in 1918, along came salesman, quack, and liar William J.A. Bailey, with Radithor – basically, water infused with salts of radium-226 and radium-228.

By then, Bailey had done a stint in prison for fraud, and later separately been leveled a hefty fine for the same. Nevertheless, he forged full steam ahead with Radithor, a product that supposedly cured a broad number of ills.

Enter Eben Byers, wealthy Pittsburgh socialite, former amateur golf champion, and industrialist. In 1927, he was 47 years old, and had injured his arm falling from the sleeping berth of a train. His physiotherapist, Charles Clinton Moyar, recommended he take Radithor. Byers took to the medicine with gusto. From December 1927, he averaged three bottles of Radithor a day, keeping to this regime for two years. His enthusiasm for Radithor was so great that he extolled its virtues, gave cases to his friends, even fed some to one of his horses. He consumed over 1,000 bottles of the stuff… until, in 1930, his teeth started falling out. Then, alarmed, he stopped – but it was too late.

Radioactive elements produce three kinds of nuclear radiation as they decay: alpha particles, beta particles, and gamma radiation. Alpha particles are pretty weak; they can be stopped by a piece of paper, and cannot penetrate intact skin.

But internally, alpha emitters can really mess you up. Radium is chemically similar to calcium; when ingested, it's mostly deposited in the bone, sitting there emitting radiation and doing a whole lot of tissue damage. The splitting headaches and jaw pain reported by Byers were, Manhattan X-ray specialist Dr. Joseph Manning Steiner recognized, similar to the symptoms reported by the so-called Radium Girls, the female factory workers who became ill painting timepiece parts with glowing radium paint.



A photograph of a young Byers taken in 1903. (Falk, NY, public domain)

There was nothing that could be done for Byers, but the Federal Trade Commission (FTC) embarked on compiling a case against Bailey. In September 1931, FTC attorney Robert Hiner Winn visited Byers at his Long Island home to interview him about his experience. "Young in years and mentally alert, he could hardly speak," Winn reported. "His head was swathed in bandages. He had undergone two successive operations in which his whole upper jaw, excepting two front teeth, and most of his lower jaw had been removed. All the remaining bone tissue of his body was slowly disintegrating, and holes were actually forming in his skull." On Byers' death on 31 March 1932, his remains were autopsied. His death was caused by cancer that riddled his bones and abscessed his brains. An estimated 36 micrograms of radium remained distributed throughout his bones. A fatal dose of radium can be as little as 2 micrograms fixed in the bones. Byers' body was so radioactive it was buried in a lead-lined coffin.

It would probably be small comfort to Byers, but his death led to the inclusion of radioactive substances under the purview of the Food and Drug Administration. Radithor was shut down; the radioactive patent medicine industry was dead.

Scientists exhumed Byers' remains in 1965 to study the effects of radiation on human remains; he was still dangerously radioactive. In fact, he was more than twice as radioactive as they thought he might be, based on his self-reported Radithor consumption.

Since radium has a half-life of 1,600 years, it's unlikely to become significantly less hazardous anytime soon. Following the exhumation, Byers was sealed back up in his lead-lined coffin and left to rest in faintly, dangerously, glowing peace.

Japan adds Chinese nuclear weapons lab and others to WMD concern list

Source: https://asia.nikkei.com/Politics/Japan-adds-Chinese-nuclear-weapons-lab-and-others-to-WMD-concern-list

Dec 06 – Japan revised on Wednesday its End User List, which provides exporters with information on foreign entities possibly involved in activities such as the development of weapons of mass destruction (WMDs).

With the latest revision, the list now totals 706 organizations in 15 countries and regions, up by 36 organizations and institutions -- including the China Academy of Engineering Physics (CAEP), the main research and manufacturing center for Chinese nuclear weapons. Iran has the most listed with 223 organizations and institutions, followed by North Korea with 153 then China and Pakistan with 101 each. Five organizations in Iran and Hong Kong were removed. The revision will take effect on Monday. Japan aims to prevent the outflow of civilian technology that could be diverted to military use. Exporters are required to get approval from the Minister of Economy, Trade and Industry to export products to the listed organizations unless it is clear that the materials will not be used to develop WMDs such as nuclear weapons or missiles. China saw seven organizations added. Of all the Chinese entities, about 90% are possibly involved in missile development. Many universities, academies and research institutes are also listed, which reveals the extent of Xi Jinping's Military-Civilian Fusion policy. Machine tools produced by Japanese companies and others are suspected of being used by the CAEP, according to a Nikkei investigation.

The economy ministry makes the list to enhance the effectiveness of its "catch-all" control system, which obliges exporters to apply for an export license for goods that may be used for the development of WMDs even if the goods are not subject to export restrictions under international agreements. The list has been issued since catch-all controls were introduced in April 2002 and is revised about once a year. It is not an embargo list.

China's military vehicles carry DF-17 hypersonic missiles in Beijing in 2019. © Reuters ANNA NISHINO and TORU TSUNASHIMA, Nikkei staff writersDecember 6, 2023 12:24 JSTUpdated on December 6, 2023 16:01 JST

Organizations and institutions newly added to Japan's End User List

Country or region	Name of organization or company	Type of WMD concerned
China	Baotou Guanghua Chemical Industrial Corp.	Nuclear
	Beijing UniStrong Science and Technology Co.	Missiles
	China Aerospace Science and Technology Corp. Ninth Academy's 771 Research Institute	Missiles
	China General Nuclear Power Corp.	Nuclear
North Korea	Korea Ryonhap Trading Corp.	Biological, chemical, missiles, nuclear
	Ministry of Rocket Industry	Missiles
Pakistan	Dynamic Engineering Corp.	Nuclear
	EnerQuip Private	Missiles, nuclear
	Rainbow Solutions	Nuclear
	Swan International Trading	Nuclear
Russia	Chimmed Group	Biological, chemical
	Joint Stock Company Angstrem	Missiles
Source: Japan's Ministry of Economy, Trade and Industry		

In addition to catch-all controls, Japan enforces "list controls" by listing sensitive items -- including goods, technology or software -- that are subject to regulation. List controls require exporters to apply for a license when exporting or transferring listed items to a foreign country. Even some items not listed cannot be exported without permission if there are security concerns at the export destination. In applying for a permit, the company exporting the item is obliged to check the intended use at the destination to see if there is any possibility that it could be converted into a WMD.

The U.S. has a similar control system, the Entity List, which contains the names of certain foreign persons -- including businesses, research institutions, government and private organizations, as well as individuals -- that are subject to license requirements for the export of specified items. The Entity List was first published in 1997 and now contains over 2,000 persons.

Although we cannot simply compare them, some pointed out that Japan's End User List is less effective than the Entity List. The U.S. embargoes exports in principle to persons listed, while Japan only urges caution and does not immediately ban exports. Japan's list is also limited in coverage.

The U.S. list includes organizations of security concern in addition to those developing WMDs, and while there are differences in the way the two lists are counted, Japan's only has about 700 entries. By country, the number of China-related entries for Japan is only 101, compared to about 600 for the U.S. For example, the CAEP has been on the U.S. list since 1997.

If organizations of concern are omitted from a list, they may slip through the checks. The organizations that Japan lists are limited to involvement in WMDs and some military entities are not included.

There are examples of Chinese and North Korean organizations on the Japanese list that are only in English, and Japanese companies have complained that the system is not user-friendly.

For companies with limited resources for research and analysis, the End User List is an important source of information for scrutinizing export destinations. As China, Russia and other countries tighten information controls, it is becoming increasingly difficult for private companies alone to even gather information on capital relationships.

An export control officer at a company that manufactures and sells core components for machine tools said, "There is a limit to what we can do on our own to find out details. He added, "If the screening process takes several months, we may miss out on business opportunities. If an entity is even slightly suspected, we would like it to be listed."

Professor Heigo Sato of Takushoku University in Tokyo, an expert on export controls, explained: "The U.S. checks every department of organizations of concern in detail, covering both number and quality."

He suggested that "a special organization be set up within the Japanese economy ministry to analyze the information in detail."

Shidaowan: world's first fourth-generation nuclear reactor begins commercial operation on China's east coast

By Victoria Bela

Source: https://www.scmp.com/news/china/science/article/3244102/shidaowan-worlds-first-4th-generation-nuclear-reactor-begins-commercial-operation-chinas-east-coast

Dec 06 – China's Shidaowan nuclear power plant, the world's first fourth-generation reactor, has begun commercial operations, one of the companies behind its development said.

The high temperature gas-cooled reactor (HTGR) went online following a week-long (168 hours) continuous operation test, state-owned China National Nuclear Corporation (CNNC) said in announcing the feat on Wednesday.

Fourth-generation nuclear reactors are designed to be successors for the existing, often water-cooled, nuclear reactors in operation around the world.

The reactor at the Shidaowan plant in China's eastern Shandong province is part of a global push for safer, more sustainable and efficient nuclear operations.

Instead of using water to cool the system, the high-temperature reactor will be cooled using helium gas, offering a promising way to develop more inland nuclear plants, as they will not need to be located next to a water source.

High-temperature reactors can produce heat, power, and hydrogen, and would help China and the world "become carbon neutral", said Zhang Zuoyi, dean of the Tsinghua University Institute of Nuclear and New Energy Technology and chief designer of the Shidaowan reactor project.

CNNC, Tsinghua and state-owned China Huaneng Group are the joint developers and operators of the plant.

The facility, which began construction in 2012, features two 250 megawatt thermal reactors and a steam generator with an installed capacity of 200 megawatts, according to CNNC. Up to 93.4 per cent of the material used in the Shidaowan HTGR was domestically sourced, the company said.

A feature of the reactor's design is "inherent safety", as in the event of a sudden reactor failure or external disturbance, "the core will not melt," a Tsinghua press release said.

Fourth-generation reactors aim to limit the environmental impact, nuclear waste burden, risk of nuclear meltdown, and opportunities for nuclear proliferation, according to the Gen IV International Forum (GIF), an international cooperative framework of major nuclear nations.

The GIF, initiated by the US Department of Energy in 2000, represents 13 nuclear nations – including China, France, Japan and Russia – along with the European Union.

Fourth-generation reactors are intended to operate at higher temperatures than most of the reactors around the world today, which allows them to generate both electricity and hydrogen, according to the GIF.

The GIF has identified six types of nuclear technology that represent the fourth-generation, and most countries in the framework are committed to producing at least one.

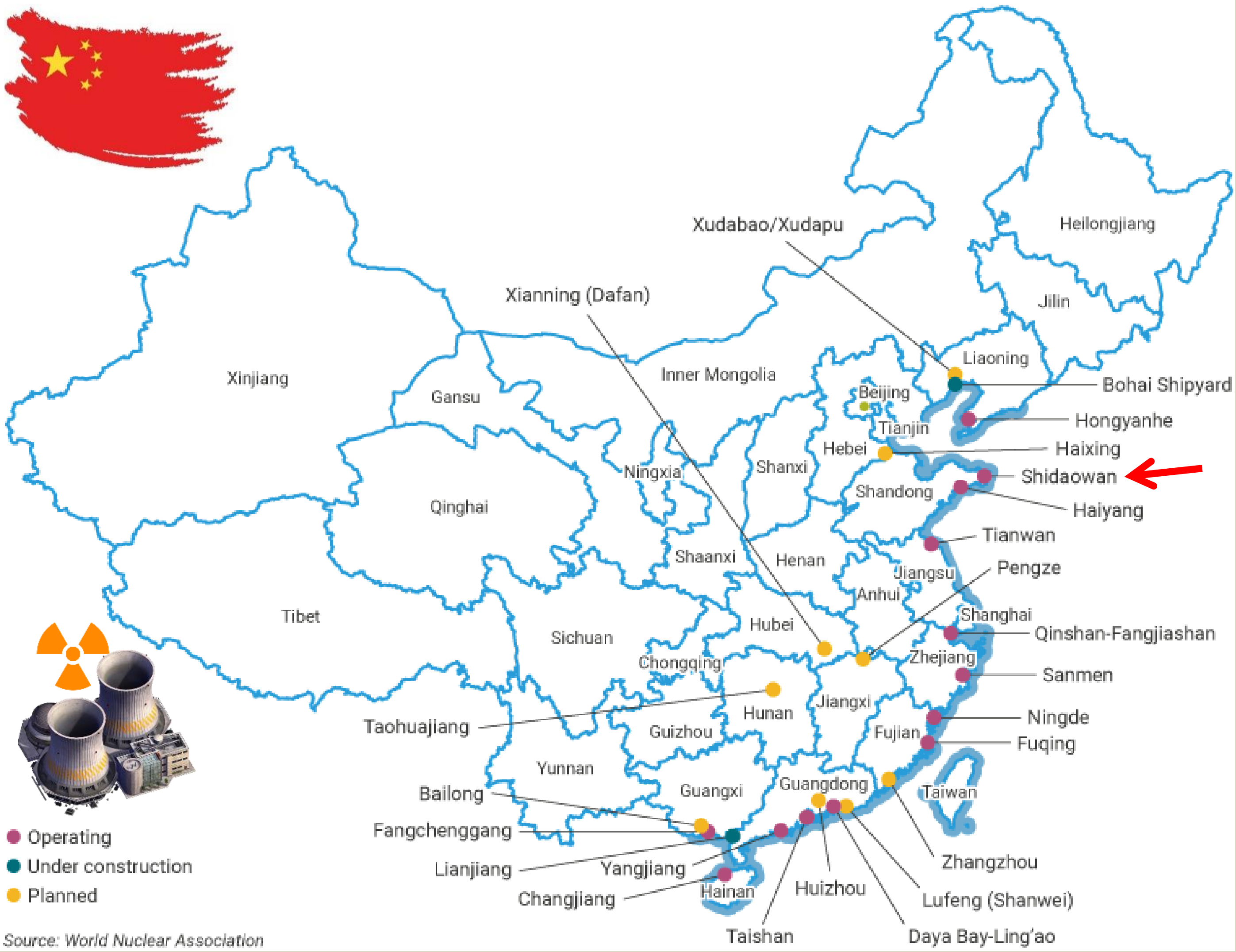
China's largest photothermal power facility drives development of new form of energy

Apart from gas reactors like the Shidaowan HTGR, which use helium to cool, there are also lead, molten-salt or sodium-cooled fast reactors, capable of turning nuclear waste into fuel, and supercritical water-cooled reactors – which directly use water to drive a turbine instead of steam for electricity generation.

Reactors like Shidaowan will be able to produce hydrogen alongside electricity for the grid.

Hydrogen produced by the reactors can be used as fuel, as well as in a variety of industrial applications.

Most hydrogen produced in the world today is made from carbon-based materials and therefore creates carbon dioxide emissions, according to the World Nuclear Association.



Source: World Nuclear Association

However, high temperature reactors can use thermochemical processes to produce zero-carbon hydrogen using water.

Inside the Shidaowan nuclear plant, which began construction in 2012. Photo: Weibo/CPNN

While Shidaowan is the world's first HTGR to enter commercial operation, other Chinese fourth-generation plants may soon be on their way.

In southeast China's Fujian province, the CNNC-managed Xiapu sodium-cooled fast reactor pilot project is also under construction, and is expected to be connected to the grid by 2025.

Unlike the HTGRs, sodium-cooled fast reactors are able to recycle depleted uranium, allowing the fuel to be reused again.

There are other sodium-cooled reactors in operation in the world, but they are third-generation. Other fourth-generation nuclear reactor projects are undergoing research and design in the United States, Japan, and Canada, but have yet to begin construction, according to the International Energy Agency. China has been increasing its nuclear capacity at the highest rate globally. However, as of this year, nuclear power still made up only 5 per cent of China's energy generation as the country continues to rely on coal, according to the World Nuclear Association. Lu Hua Quan, chairman of the Nuclear Research Institute at Huaneng, told the association last year that HTGRs had "great potential to help the world decarbonise hard-to-abate sectors".

However, safeguards and waste management, as well as regulatory frameworks, still need to be addressed if the technology is to be broadly deployed. Lu said HTGRs could be very helpful in countries where freshwater was limited, as it did not require large amounts of it in order to cool the reactors.

And for nations where large capacity nuclear plants do not fit into local power grids, the ability to create small modular reactions can be built with smaller capacities that suit the needs of the power grid, he said.

What Would It Mean to 'Absorb' a Nuclear Attack?

By Ella Weber (*Scientific American*)
Source: https://www.scientificamerican.com/podcast/episode/what-would-it-mean-to-absorb-a-nuclear-attack/

This podcast is Part 4 of a five-part series. Listen to Part 1 here, Part 2 here, and Part 3 here. The podcast series is a part of "The New Nuclear Age," a special report on a $1.5-trillion effort to remake the American nuclear arsenal.

Frank Von Hippel: I'm Frank von Hippel. I've worked at Princeton [University] since 1974, and I've been working on nuclear arms control and nonproliferation—and also, among other things, the consequences of nuclear war.

Ella Weber: Frank served as assistant director of national security at the Office of Science and Technology Policy at the White House. This was during the Clinton administration.

He was also one of the first scientists to be involved with research on the consequences of nuclear strikes on U.S. nuclear weapons—including the Minutemen silos—which he described in detail in *Scientific American* in 1976.

There's a particular hearing from around that time that he references.

Von Hippel: Basically the secretary of defense had come in and testified to Congress. When one of the senators asked how many people would such an attack kill, he estimated 15,000 to 25,000. And he said, 'Well, that would be terrible, but it would be not what you would expect from a major nuclear attack.'

That seemed low to, actually, the senator from New Jersey [Clifford Case]. And he asked for a peer review of the Defense Department calculations, and, and I was then asked to be an unpaid consultant to look into that. And I went over to the Pentagon to talk to the people who have done the calculations.

Weber: Frank found something unexpectedly horrifying.

Von Hippel: The Defense Department had assumed that explosions of the warheads over the ICBM silos would be so high that they would not cause fallout. They pointed out they would also not damage the silos.

Weber: Basically, the Department of Defense hadn't calculated properly. The DOD had made incorrect assumptions about the altitude of nuclear explosions aimed at destroying the silos. Initially, it had thought the nuclear explosions would need to be at an altitude. But–they actually needed to be at ground level.

Von Hippel: The DoD was forced to go back and do new calculations reflecting these points, and they came out about 1,000 times higher: 20 million—on the order of 20 million people killed.

Ella Weber is a tribal citizen of MHA Nation (Mandan, Hidatsa, and Arikara) from Crookston, Minnesota. She is a junior at Princeton studying public policy, specifically looking at education and public health.

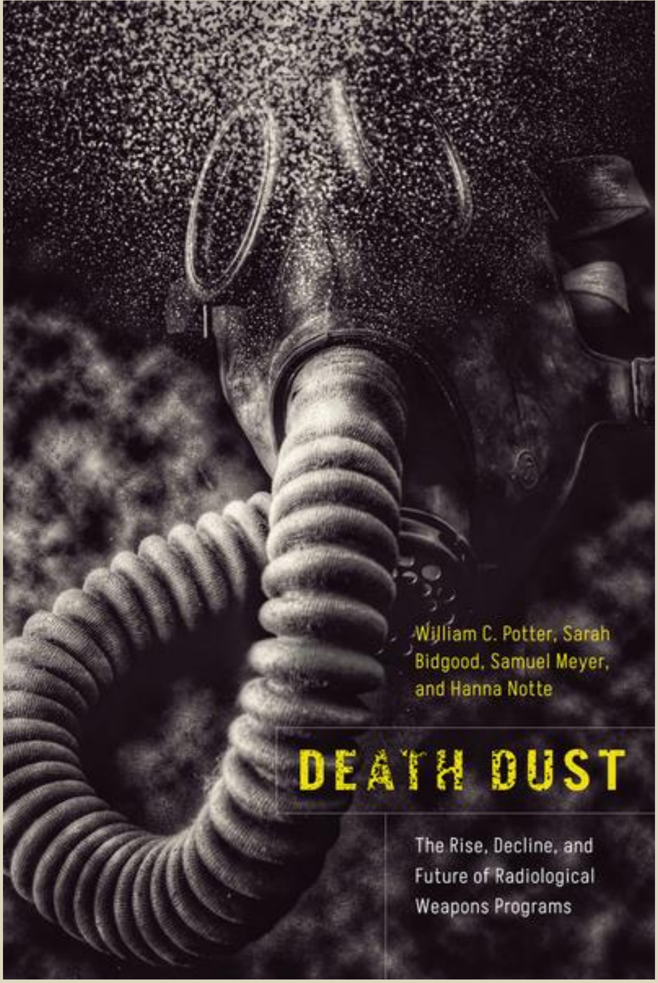
Why the World Should Still Worry About Dirty Bombs

By William C. Potter, Sarah Bidgood, Hanna Notte
Source: https://www.foreignaffairs.com/united-states/why-world-should-still-worry-about-dirty-bombs

Dec 15 – In the years after the 9/11 attacks, a new threat loomed large in the minds of policymakers and the public: the dirty bomb. This term describes a radiological weapon that used an explosive to disperse radioactive material over a limited area. A dirty bomb is far less powerful than a nuclear bomb, but it is easier and cheaper to assemble and can cause tremendous panic and disruption. Many analysts feared that terrorist groups would seek to develop and use such weapons: in 2002, U.S. officials announced the detention of Jose Padilla, an American citizen and alleged al Qaeda operative who they insisted intended to detonate a dirty bomb in the United States. Since then, several governments in Europe have claimed to have foiled similar plots by terrorist groups.

But visions of dirty bombs and radiological terrorism obscured the fact that the threat from radiological weapons was not limited to terrorist groups. Indeed, for decades, major countries including the United States and the Soviet Union pioneered the development of these weapons. And now, as the norm against nuclear weapons is weakening and tensions between great powers mount, there is reason to worry that the dangers posed by radiological arms proliferation may be growing again.

In the past, at least five states expressed interest in weapons designed to disperse radioactive material without a nuclear detonation. Four states actively pursued them, and three—Iraq, the Soviet Union, and the United States—tested them on multiple occasions before ultimately choosing not to deploy them. The largely obscure history of the development of radiological weaponry helps to explain its appeal, especially in the context of rising international hostilities, a breakdown in nuclear arms control, and a loss of faith in the credibility of security assurances.


William C. Potter, Sarah Bidgood, Samuel Meyer, and Hanna Notte
DEATH DUST
The Rise, Decline, and Future of Radiological Weapons Programs

Russian disinformation about a purported covert Ukrainian radiological weapons program has brought renewed attention to the issue. Russia's war against Ukraine and the attendant escalation in great-power competition have eroded the taboo against nuclear weapons use and undermined the international nonproliferation regime. Additional states may consider the possible deterrent benefits of possessing nuclear arms or, if the costs of acquiring such weapons are prohibitive, other nonconventional weapons. For these states, radiological weapons may appear a more viable option, something akin to "a poor man's nuclear weapon." Although U.S.-led diplomatic efforts are now underway to ban them, radiological weapons are not prohibited under international law, which could encourage states to seek them out. Two decades ago, policymakers were haunted by visions of dirty bombs in the hands of terrorists. In the near future, however, they may have to grapple with the more dangerous possibility that states will once again turn to these lethal weapons.

Death dust

Although shrouded in secrecy and largely ignored by both scholars and diplomats, the origins of the pursuit of radiological weapons by states can be traced to World War II. Unsurprisingly, the first two countries to explore these capabilities were also the first two to develop nuclear weapons. In October 1940, a pair of Soviet mathematicians submitted a proposal to the Soviet Union's inventions bureau on the "use of uranium as an explosive and poisoning substance." In May of the following year, the initial report of the U.S. National Academy of Sciences' Advisory Committee on Uranium highlighted the "production of violently radioactive materials" to be carried by airplanes and dispersed over enemy territory as one of three possible military uses of atomic fission.

Within a matter of years, these proposals and reports had turned into something more substantial. Starting in 1949, the U.S. Army's Chemical Corps oversaw dozens of atmospheric tests of prototypes for radiological munitions. Similarly, the Soviet Union conducted tests of various munitions containing radioactive waste in the mid-1950s. These included experiments on live animals, including rabbits, dogs, and mice, and, inadvertently, on the humans staging the tests themselves.

At virtually the same time, the United Kingdom also began to explore the military potential of radiological weapons. These preliminary investigations led to a more substantial British developmental effort, but by the autumn of 1953, about one year after the country's first nuclear weapons detonation, its radiological arms program had for all practical purposes been abandoned. There is also circumstantial evidence that in the early 1960s, Egypt flirted with the idea of developing radiological artillery shells and sought to import radioactive isotopes to that end. Two decades later, Iraq undertook a far more serious program, which led to the development and testing of radiological weapons toward the end of its war with Iran in the 1980s.

The rise and demise of radiological weapons

The circumstances differed, but none of these efforts led to the mass production or deployment of radiological weapons. Why, then, did countries want to develop this capability in the first place, and why did they all ultimately decide to abandon these programs?

States were principally motivated to seek radiological weapons for security reasons. In both the United States and, to a lesser extent, the United Kingdom, concerns that Nazi Germany was pursuing radiological weapons prompted explorations of their military potential. In the Soviet Union, meanwhile, knowledge of the United States' radiological weapons activities—provided, in part, by spies active in the British nuclear weapons program—generated high-level support for the establishment of a Soviet program.

Iraq sought these weapons for tactical reasons during its war with Iran. Specifically, Iraqi leaders thought radiological weapons could be useful in disrupting "human wave" attacks in which Iran hurled massed ranks of infantrymen at Iraqi positions. In contrast to the substantial documentary evidence available about the Iraqi program, much less is known about Egypt's short-lived flirtation with radiological weapons. Nevertheless, it appears that after the revelation in 1960 that Israel was building its Dimona nuclear reactor in the Negev desert, Egypt sought ways to match and counter Israeli military innovations, in part by experimenting with radiological artillery shells.

In none of the five cases, however, did external threats or internal drivers prove sufficient to move radiological weapons from experimentation or testing to mass production and deployment. Instead, radiological weapons lost traction—and budgetary support—in Washington, Moscow, and London as policymakers in those capitals placed a greater emphasis on developing nuclear weapons, especially hydrogen bombs. In Iraq, the Soviet Union, the United Kingdom, and the United States, the attention of leaders shifted to chemical weapons, which were judged to be more cost-effective.

But perhaps the biggest factor accounting for the demise of radiological weapons was their technological limitations. The weapons could not deliver what their advocates promised. In some cases, it proved too difficult or expensive to produce the sources of radiation from which the weapons were made. Especially challenging were very specific military requirements regarding the half-life of the radioisotopes that would be dispersed by the weapons and the intensity of radioactivity emitted. In other instances, the risks associated with the production, transportation, testing, and delivery of radiological weapons were regarded as outweighing their utility on the battlefield. Over time, the enthusiasm many states had for the weapons waned and ultimately disappeared.

IN SEARCH OF A DEAL

The war in Ukraine has revived interest in the risks of radiological weapons. Shortly after Russia's invasion in February 2022, Russian media began to disseminate unsubstantiated claims that Russian forces had interrupted a Ukrainian radiological weapons program that some propagandists asserted was based at the defunct Chernobyl nuclear power station. Russia's subsequent seizure of the Zaporizhzhia nuclear power plant and its shelling of other nuclear facilities in Ukraine raised the specter of the unintended dispersal of radioactive material in a fashion that might have resembled the battlefield effects of radiological weapons.

Ironically, the Soviet Union—along with the United States—had led the initial effort to negotiate a ban on radiological warfare. A draft convention submitted to the Committee on Disarmament—the predecessor to the current Conference on Disarmament, a 65-member multilateral forum based in Geneva—by the two superpowers in 1979 specified that parties to the accord would agree not to develop, produce, stockpile, otherwise acquire or use radiological weapons. Consensus could not be reached, however, because delegations found its scope to be too narrow. (It did not include radiation emitted by nuclear explosions.) What is more, many governments were simply not convinced of the importance of radiological weapons.

It is significant, therefore, that in October 2023, the United States and 38 co-sponsors introduced a remarkably similar draft resolution on radiological weapons at the UN General Assembly. This resolution called on all states not to use radiological weapons and to refrain from developing, producing, or stockpiling devices or materials for use in such weapons. In addition, it urged the Conference on Disarmament to commence negotiations that would result in a prohibition of the use of radiological weapons by states. Although some adversaries of the United States opposed the draft resolution, its final version was adopted by a vote of 159 to 5 with 13 abstentions. (The five naysayers were Belarus, Iran, North Korea, Russia, and Syria. China abstained.)

This overwhelming vote in favor of the U.S.-led initiative does not necessarily augur a successful prohibition of radiological weapons. UN General Assembly resolutions are mostly nonbinding and may not spur any meaningful action. Most states do not have well-formed views on radiological weapons. There is also considerable skepticism about the timing of the U.S. initiative and why it was introduced without greater consultation.

Some diplomats, for example, see the initiative as a move to embarrass Russia after its bogus allegations about Ukrainian radiological activities. Many states also question what Washington expects to accomplish at the Conference on Disarmament, which is the sole multilateral negotiating forum on that issue but has been paralyzed for decades. Other states object to the resolution's emphasis on banning the use of radiological weapons rather than focusing equally on limiting the development, production, and stockpiling of materials that can be used in such devices. A senior diplomat from one state that voted in favor of the resolution raised an interesting question shortly after the vote about what prompted the resolution. Was there new intelligence to suggest that some states were considering the launch of radiological weapons programs?

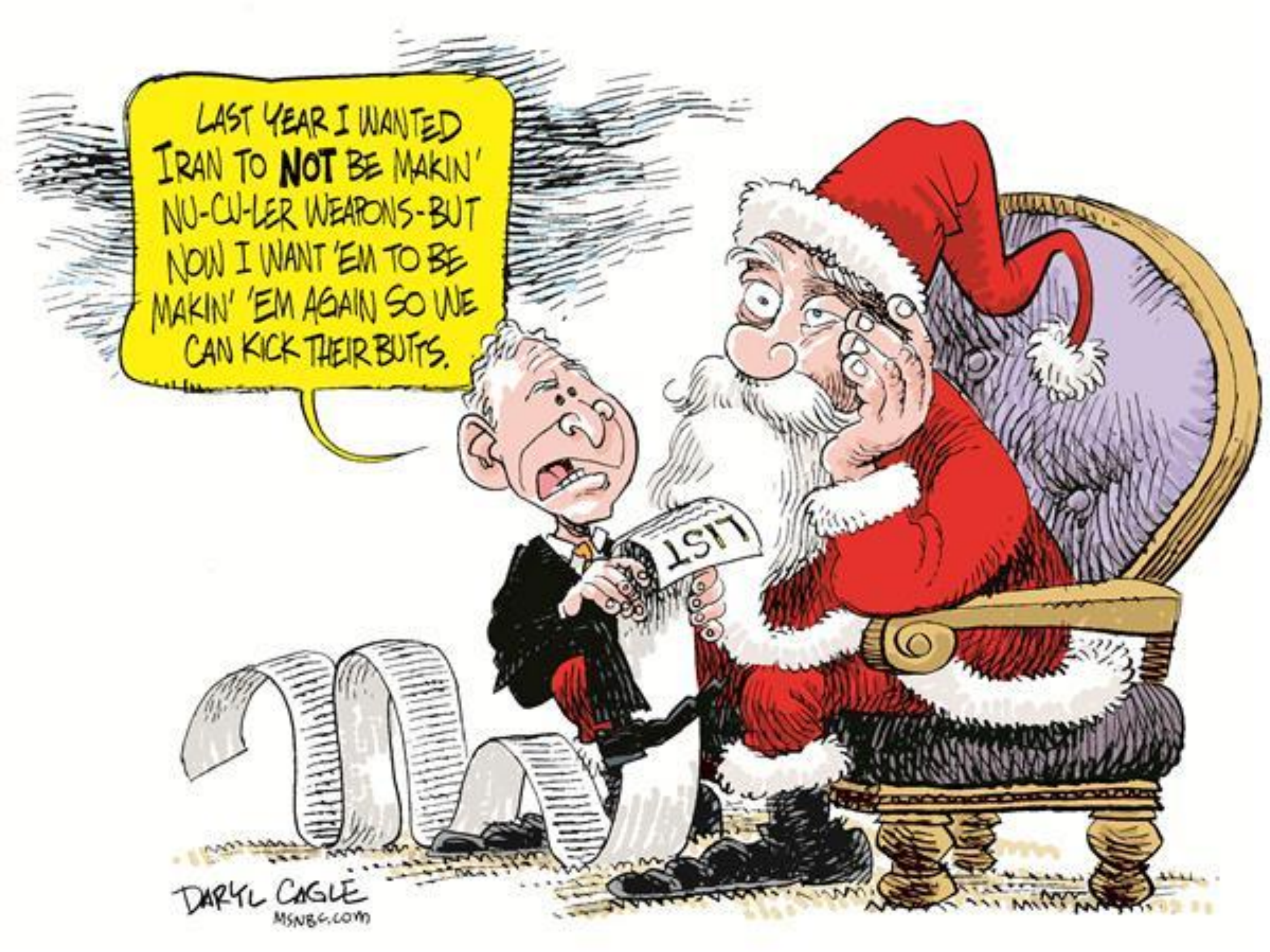
U.S. officials have yet to respond to the question, but they believe this effort is long overdue. The recent UN vote has convinced them that banning radiological weapons has broad support. The test will now come at the Conference on Disarmament, where prospects for the accord are dim: the body's consensus-based decision-making process has long stalled negotiations, and several opponents of the U.S. initiative, including Iran and Russia, could exercise a veto. If talks founder there, Washington might support commissioning an international group of government experts who would assess the dangers posed by radiological weapons and make recommendations about how to prevent or mitigate these risks. They could in turn recommend legally binding restraints on the production and use of radiological weapons, as well as the adoption of nonproliferation and nonuse commitments, the creation of radiological weapons-free zones, and the fostering of a taboo against radiological weapons through civil society engagement and public education.

Although these steps could help mitigate the risks posed by radiological weapons, their implementation relies on like-minded states. With little certainty that this will transpire, shedding more light on the impediments faced by past would-be radiological weapons proliferators could discourage new states from investing in them in the first place.

William C. Potter is Sam Nunn and Richard Lugar Professor of Nonproliferation Studies and Founding Director of the James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey.

Sara Bidgood is a Stanton Nuclear Security Fellow at MIT's Security Studies Program and a former Director of the Eurasia Nonproliferation Program at the James Martin Center for Nonproliferation Studies.

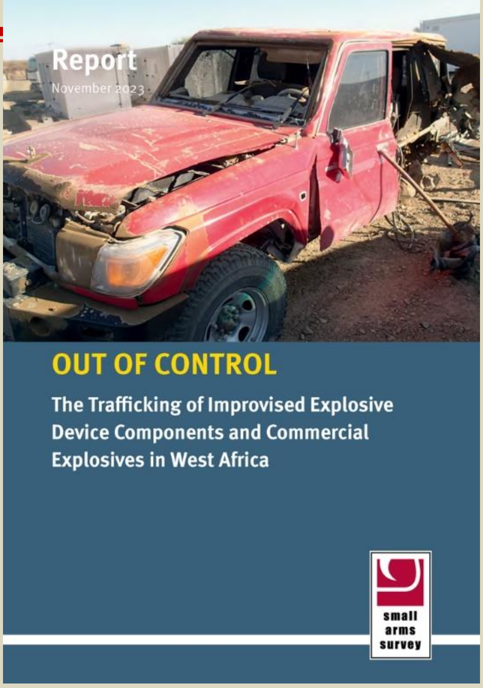
Hanna Notte is Director of the Eurasia Nonproliferation Program at the James Martin Center for Nonproliferation Studies and a Nonresident Senior Associate with the Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies.


LAST YEAR I WANTED IRAN TO NOT BE MAKIN' NU-CU-LER WEAPONS-BUT NOW I WANT 'EM TO BE MAKIN' 'EM AGAIN SO WE CAN KICK THEIR BUTTS.
LIST
DARYL CAGLE
MSNBC.com

EXPLOSIVE NEWS

New report on improvised explosive devices in West Africa

Source: https://www.smallarmssurvey.org/highlight/new-report-improvised-explosive-devices-west-africa


Report
November 2023
OUT OF CONTROL
The Trafficking of Improvised Explosive Device Components and Commercial Explosives in West Africa
small arms survey

Nov 24 – The use of improvised explosive devices (IEDs) in West Africa expanded dramatically over the last decade. IED-building networks have established material and training links across conflict areas in West and Central Africa, and their designs have remained constant and inexpensive throughout the region—helping to increase their use in attacks against domestic and international security forces, UN peacekeepers, and civilians.

Out of Control: The Trafficking of Improvised Explosive Device Components and Commercial Explosives in West Africa—a new report from the Small Arms Survey's Improvised Explosive Devices (IEDs) in West Africa project—analyses data from more than 2,200 IED-related incidents between March 2013 and September 2022, and stresses the importance of coordinated regional approaches in eliminating illegal IED use in West and Central Africa.

EOD career past, present, future

Source: https://www.eglin.af.mil/News/Article-Display/Article/3589830/eod-career-past-present-future/

All but one of the Air Force enlisted explosive ordnance disposal career field managers came together to talk about past, present and the future of EOD Nov. 10 at Eglin Air Force Base, Fla. (U.S. Air Force photo/Jaime Bishopp)

Nov 16 – Eglin's Explosive Ordnance Disposal Flight hosted the Air Force's first-ever EOD Heritage Panel Nov. 10, 2023.
The panel brought together career field managers to discuss the history, current state, and future of the EOD program. EOD has only had 10 total career field managers for the entire program, and this was the first opportunity to bring them all together, putting 270 years of EOD experience on one stage.
"To understand where we need to go in the future, it's important we look at where we've been and see the history of it," stated Chief Master Sgt. Vandiver Hood, EOD's nineth and outgoing career field manager.

EOD has experienced a tremendous amount of change and growth in a relatively short time, and the men present recounted that history and their role in it.

Retired Chief Master Sgt. John Jay Glover, who joined the Air Force in 1966, was the first EOD career field manager in 1989. Because of Glover's work, the career field moved from maintenance into the Civil Engineer Squadron, a field that was better suited to EOD's mission of clearing airfields. It was during his tenure that the first robots were fielded, now an integral tool of EOD work.

"It's pretty fascinating watching EOD grow and watching the level of excellence I've seen in the program grow," Glover explained. "It was rough-and-tumble times during the Vietnam war and just keeping yourself together and keeping yourself alive. But now it's so much more professional."

Each new career field manager built on the foundations of the last to develop that professionalism, with some projects often spanning multiple CFMs.

Chief Master Sgt. Frank Pulice, the incoming career field manager, said he understands he will continue working through a constant state of change just as his predecessors did.

"You've heard about change from everyone up here. I see a lot of change coming, but that's not a new story," he said. "You hear a lot about the change, but you probably don't see it. Good, meaningful change sometimes takes more time than we have."

Hood hopes Airmen see the team effort that goes into making EOD successful through the change.

"We're the same EOD technicians, whether it's from 1970 or 2023. We are always there for the team, no matter where we are now and into the future," he said.

Airman 1st Class Griffin Walraven, who just graduated EOD school less than a year ago, took away just that message.

"There's a lot of history going into every decision that is made. And while we only see so much at the lowest level, especially me being an Airman, when you get up higher, bigger decisions are at play. There are a lot of people looking out for us that are EOD."

Glover ended with a word of wisdom. "No man or woman stands alone. You need a team of people that you surround yourself with to help you be successful and you've got to support them. You've got to work together."

Can robot dogs programmed with AI find hidden explosive devices?

Source: https://des.mod.uk/how-can-ai-train-robot-dogs-to-find-hidden-explosives/

Nov 16 – Forty programmers demonstrated how AI-enabled robotic dogs could carry out potentially dangerous tasks that would otherwise be undertaken by Army bomb disposal experts at the Defence AI Centre (DAIC) sponsored Hackathon on 7-9 November.

The hackers worked in five teams to exploit the AI capabilities of the robotic dogs, which are able to climb stairs, avoid obstacles and move over rough ground. During the first two days, the teams developed their strategies and finetuned their programming, before testing the dogs in an environment designed to recreate some of the hurdles faced in real life-threatening scenarios.

On the final day, the teams demonstrated what they had achieved to members of 29 Explosive Ordnance Disposal (EOD) & Search Group, who are some of the British Army's preeminent tactical and technical explosives experts able to disable explosive devices.

Representatives from 29 EOD&S Group, the DAIC and Defence Equipment and Support (DE&S) judged the winners of five award categories: teamwork, collaboration, innovation, practical application, and endeavour and focus.

The event was hosted by the Defence AI Centre, in partnership with the Expeditionary Robotics Centre of Expertise (ERCoE, part of Defence Equipment and Support (DE&S) and Team Defence Information (TDI) at the BattleLab in Dorset.

Cdre Rachel Singleton RN, Head DAIC, said:

“It has been hugely exciting to see Defence, industry and academia work together on an AI and robotics solution to a real use case, particularly one that aims to increase the safety of our people. Instigating and guiding this kind of collaborative innovation safely and responsibly is among the most important work we do at the DAIC.”

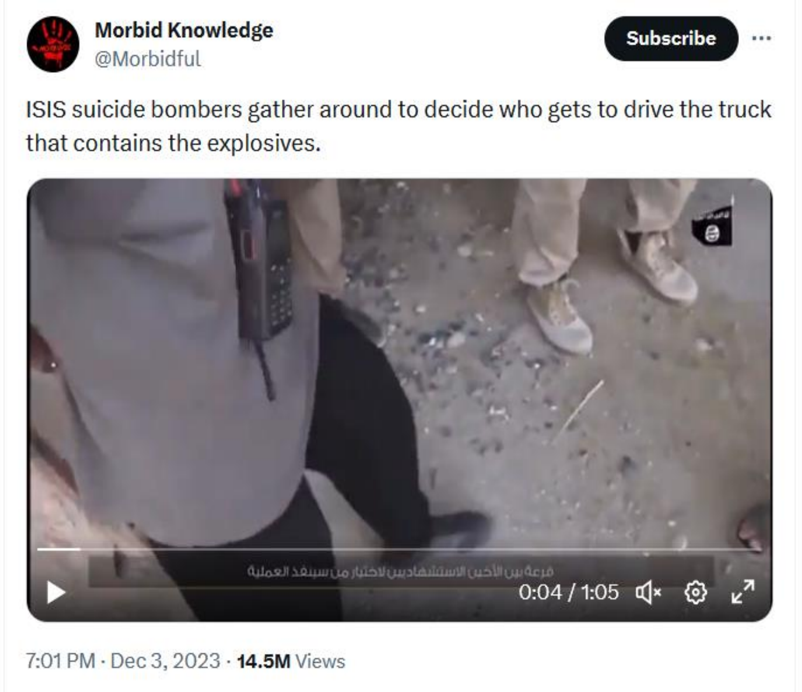
Lt Col Chris Coles, of 29 Explosive Ordnance Disposal (EOD) & Search Group, said:

“It has been an absolute pleasure to see the talent and commitment to endeavour to create bomb disposal tools that do not require a person up close and personal. I have witnessed a number of things today that will absolutely facilitate research and development in the EOD&S space.”

Wing Commander Paul Austin, of the DE&S Future Capabilities Group, said:

“At DE&S our passion is identifying ways we can harness technology to give our Armed Forces an edge. Part of that journey is working together with the Defence enterprise to drive improvement. This event and the enthusiasm displayed by the participants to solve a military-focused problem was a wonderful example of that.”

You must see it to believe it!!!



Morbid Knowledge
@Morbidful

ISIS suicide bombers gather around to decide who gets to drive the truck that contains the explosives.

7:01 PM · Dec 3, 2023 · **14.5M** Views

Oil pipeline in S. Yemen sabotaged by unidentified gunmen

Source: https://english.news.cn/20231204/af1ce47bd5dc4db8bacb6d97b7d32a93/c.html

Dec 04 – A group of unidentified gunmen carried out an attack and sabotaged a crude oil pipeline in southern Yemen's oil-rich province of Shabwa, a government official said on Monday.

The gunmen used explosives to bomb the main crude pipeline near the Jannah Hunt oil field on Sunday night, which has caused significant damage and resulted in a substantial crude oil spill, said the official who required anonymity.

He added that the motives behind the attack remain unclear as the gunmen's identities are yet to be unveiled.

The pipeline, connecting the Jannah Hunt oil field with the crude oil storage facilities in Alam, Jardan district, is now inoperative, posing a challenge to the region's oil distribution network, according to the official.

SAUDI ARABIA
YEMEN
Sanaa
SHABWA
Gulf of Aden

Security forces and an engineering team were dispatched to repair the damage, who were however hindered by the gunmen, leading to an armed confrontation near the oil field.

The situation escalated until the Giants Brigades, a militia loyal to the Southern Transitional Council, intervened. These forces have been governing Shabwa since early 2022.

The region's oil infrastructure has been vulnerable to repeated attacks by various armed groups, often motivated by service demands or as a means to exert pressure on local authorities for various reasons, including the release of prisoners.

Paris police expect the 2024 Olympics to be a 'considerable challenge' for bomb disposal squad

Source: https://uk.news.yahoo.com/paris-police-expect-2024-olympics-161341637.html

Dec 05 – The Paris police bomb disposal team expect the Olympics to present them with a "considerable challenge" next year.

They have been working with Paris 2024 organisers to define the right level of bomb clearing intervention during the Olympics and Paralympics in the French capital next summer, the director of the central police laboratory said on Monday.

"The Olympic Games are an absolutely considerable challenge," Christophe Pezron said of the July 26-Aug. 11 event.

"As far as bomb-disposal practice is concerned, there are two stages which are quite separate for us from the site inspection stages, since each of the Olympic Games sites will be inspected before being handed over to the organisers."

"We carried out an inspection, a kind of rehearsal, at the Stade de France during the Rugby World Cup. So the first stage is these inspections of all the Olympic Games sites.

"And the second activity, which will be carried out in parallel, is that we imagine that, given the population that will be moving around during the Olympic Games, we're likely to be faced with an increase in the number of abandoned parcels and suspicious packages. So, from that point on, we'll certainly be seeing a great deal of intervention activity."

On Monday, members of the bomb disposal squad were alerted at the Montparnasse train station to abandoned luggage, which the team exploded.

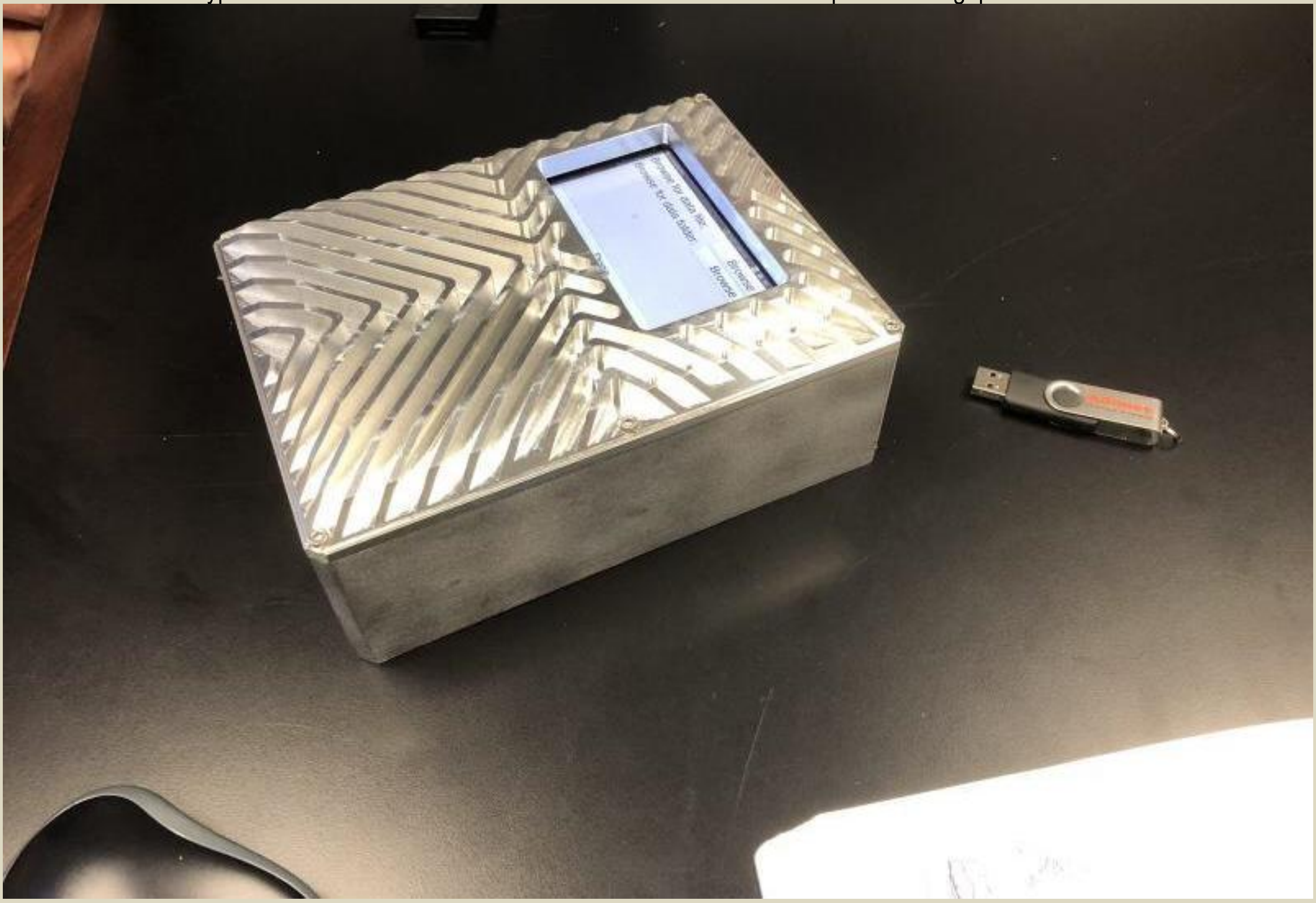
Another bag, which was found to belong to a school pupil, was also exploded later on Monday.

Feature Article: Leveraging Artificial Intelligence Is Smart for Explosive Detection

Source: https://www.dhs.gov/science-and-technology/news/2023/12/14/feature-article-leveraging-artificial-intelligence-smart-explosive-detection

Dec 14 – Harnessing the power and possibilities of artificial intelligence (AI) and machine learning (ML) and applying these emerging capabilities to the Department of Homeland Security (DHS) mission has been, and will continue to be, a high priority for the Science and Technology Directorate (S&T). One way S&T is demonstrating this commitment to applying emerging technologies to pressing national threats is by investing in the development of AI/ML technologies. Specifically in this case, the funding is directed at AI/ML that could soon be used to identify dangerous compounds, like those found in explosives and narcotics.

When the DHS Small Business Innovation Research (SBIR) Program released a solicitation back in FY2020, under the topic "Machine Learning Module for Detection Technologies," the goal was to develop innovative solutions that would ultimately provide DHS operational components with an enhanced ability to identify new threats at aviation checkpoints. In the spring of 2021, following their 6-month Phase I awards to demonstrate concept feasibility, Physical Sciences Inc. (PSI) and Alakai Defense Systems, Inc. (Alakai) were each awarded a $1 million, 24-month SBIR Phase II contract. These awards further lean into the ultimate goal of developing advanced AI/ML-based detection algorithms that can shorten the timeline for deployment of capabilities able to identify threats in the field. The research and development (R&D) being done is important because it addresses a capability gap in the detection of certain types of new threats. S&T believes that AI/ML solutions can help close that gap.



An ML-based detection algorithm module that can easily connect with commercially off-the-shelf Raman spectrometers/detectors to download information from the detectors, run the detection algorithm, and then display results. Photo credit: S&T.

According to Thoi Nguyen, program manager for S&T's Next Generation Explosives Trace Detection Program, "When the intel, special ops, or law enforcement communities find a new threat, maybe a new explosive compound, the threat is validated and prioritized according to urgency levels. DHS S&T is then tasked to develop an R&D solution to detect and identify the threat. Once the solution is tested, evaluated, and verified that it meets DHS detection requirements, DHS Components go through a lengthy DOTMLPF

(Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities) process to acquire and deploy the solution. At the end of this process, the chemical 'signature' of the threat is uploaded to DHS equipment at airport checkpoints."

AI/ML will help identify explosive threats at airport security checkpoints. Photo credit: iStockPhoto.

However, adding a new compound to the existing identification library of threat compounds historically has been a slow, meticulous, and labor-intensive process. This can result in a capability gap for updating the database.

The challenge S&T posed with this funding award is to see if an AI/ML solution can significantly expedite the process of updating a detection library, without the intensive human labor.

One of the ways that dangerous compounds are identified at checkpoints is with Raman Spectroscopy. This chemical analytical technique fires a laser at a vaporized and ionized sample that was swabbed from a traveler, or into an object like a closed bottle of liquid. The laser will excite the molecules it encounters in the target, causing them to vibrate. Every type of molecule has its own distinct vibrational frequency. The spectrometer will detect those vibrational frequencies and chart them on a graph. The chemical signature is determined by where specific peaks are found on the graph and the intensity, height, and width of those peaks. Then the system searches the chemical signature library to find a match. If the sample matches an explosive in the database, the alarm is sounded.

So, what's the problem? "The bottleneck is not in the intel process, the bottleneck is in the R&D process and how to add that new threat intel, the new chemical signature, into the library so we can catch the bad guys," said Nguyen. "That's where the AI/ML that our small business partners are developing fits into the equation."

"We love small businesses because they're innovative and nimble," said SBIR Program Director Dusty Lang. "The SBIR program allows us to absorb the risk by funding multiple Phase I proposals to explore feasibility, then move forward to Phase II with the best solutions for DHS needs."

Traditionally, when a new threat compound is introduced into the library, scientists and contractors are brought in to manually create a new classification or channel for it. At that point, the tedious work to enter all the spectrographic characteristics of the chemical into the library begins. The programing of the chemical traits for the channel must be extremely precise to ensure they get the highest Probability of Detection (PD) and the lowest Probability of False Alarm (PFA) when the library is queried with a sample at a checkpoint.

One of the complicating factors for achieving high PD and low PFA is that the software analyzing the compound must be able to see through the background noise in the sample and identify the compound for what it really is.

"For example, pure TNT from a lab may appear different from TNT in a real-world scenario because there may be additives to the TNT, or there may be other environmental interference. So, even though it might have spectrographic peaks at the right places, they might be somewhat obscured by these other excited molecules and their signatures. If you're creating a TNT channel, we would have to account for myriad factors. That's what takes so much time and that's where accuracy is so important. It has to be calibrated perfectly. What we're trying to do here with the AI and the ML is that we want to bypass that slow process."

Spectrometry reveals that different chemicals have different chemical signatures. Photo credit: iStockPhoto.

The first part of that bypass is training the AI to recognize a specific compound. However, the AI can't teach itself. It still needs to be taught how to do it. The ML-based detection algorithm starts as a blank sheet, and it must be taught which peaks on the graph represent which chemicals. "It's like teaching a child what sugar tastes like," said Nguyen. "When you taste this, that is sugar. That's what we call sweet. And this is sugar with a little bit of lemon. You taste the sour lemon, but it's still sugar. It's the same thing with teaching the AI to not get confused by the background noise."

In Nguyen's example, the important thing for the child to understand is that the sample is still sugar, and the lemon is just an additive. In the explosive detection world, that lemon might be a fuel added to TNT to make it more powerful. Making sure that the explosives detection algorithm is smart enough to determine that the TNT is mixed with another fuel compound is incredibly important.

That brings us to the second part, which is validation. Once the AI is taught the signature characteristics of the compound, and potential noise distractions have been accounted for, the AI is evaluated for accuracy by running tests designed to trick it. Chemicals are added to the original compound in attempts to shield or mask the spectrographic signature behind other noise.

Nguyen emphasizes the importance of this part, adding that, "We don't just trust AI completely. We say, 'trust, but verify,' to see whether or not the alarm that was just triggered complies with our understanding of how the vibration of the molecules we are testing should present themselves."

For a limited set of explosives, S&T demonstrated that the AI/ML solution identified explosives with very high PD, yet low PFA—a major success by itself. Even more remarkable is the way that this AI/ML solution has closed the critical time capability gap.

"What traditionally can take as many as one to two years, the AI/ML that our partners developed can now learn, classify, and upload new threats to the library in a matter of days or weeks," said Nguyen. "That has significant real-world impact. And I want to make sure that we give credit to SBIR, because without their collaboration, funding and support, this project would never have happened."

SBIR's Lang added, "These two companies, PSI and Alakai, demonstrate the impact small business can have and why we are always working to strengthen the SBIR reach and support. It is very rewarding to be able to work with program managers like Thoi to facilitate the connections of ideas and needs."

This round of Phase II funding from the SBIR Program resulted in confirmation that AI/ML has a place in the future of explosive detection. The shortened deployment cycle to chemical libraries in the field, coupled with maintaining the high PD and low PFA, is something that human hands can't match. That's the power of trustworthy AI/ML and that's what S&T is looking to leverage to further secure the nation.

In terms of looking back on the work that has been developed under the program, Nguyen finished up stating, "It was a success beyond our imagination."

In the future, AI/ML modules will be tested and evaluated at the U.S. Army's Chemical Biological Center. The goal there will be to determine compatibility between three types of Raman Spectrometers and their interoperative capabilities.

URANIUM, GRAPHITE, BORON RODS... ARE YOU MAKING A NUCLEAR REACTOR KID?
DREW

International CBRNE Institute

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

'Gay furry hackers' breach nuclear lab, demand it creates catgirls

By Amanda Yeo

Source: https://mashable.com/article/catgirl-real-nuclear-hack

Credit: FOTOGRAFIA INC. via Getty Images

Nov 24 – Idaho National Laboratory (INL), one of the largest nuclear labs in the US, confirmed this week that it has been hacked. The group behind the data breach was self-described "gay furry hackers" Sieged Security aka SiegedSec, who have demanded the INL put its efforts and resources into creating real-life catgirls.

They probably aren't being serious, but they did hack into a huge nuclear lab, so who knows.

According to SiegedSec, the hacktivist group has accessed thousands of records of user and employee data held by INL. This includes people's full names, birthdays, email and home addresses, phone numbers, social security numbers, employment information, and "lots lots more."

"woah so much crunchy data :3" SiegedSec wrote on their Telegram account, which gives you an idea of their communication style.

When hackers breach targets such as the INL, they frequently demand a ransom in exchange for keeping the organisation's data private. Often they want it in the form of cryptocurrency, so it's difficult to trace.

In this particular case, SiegedSec's demand is a little more unconventional.

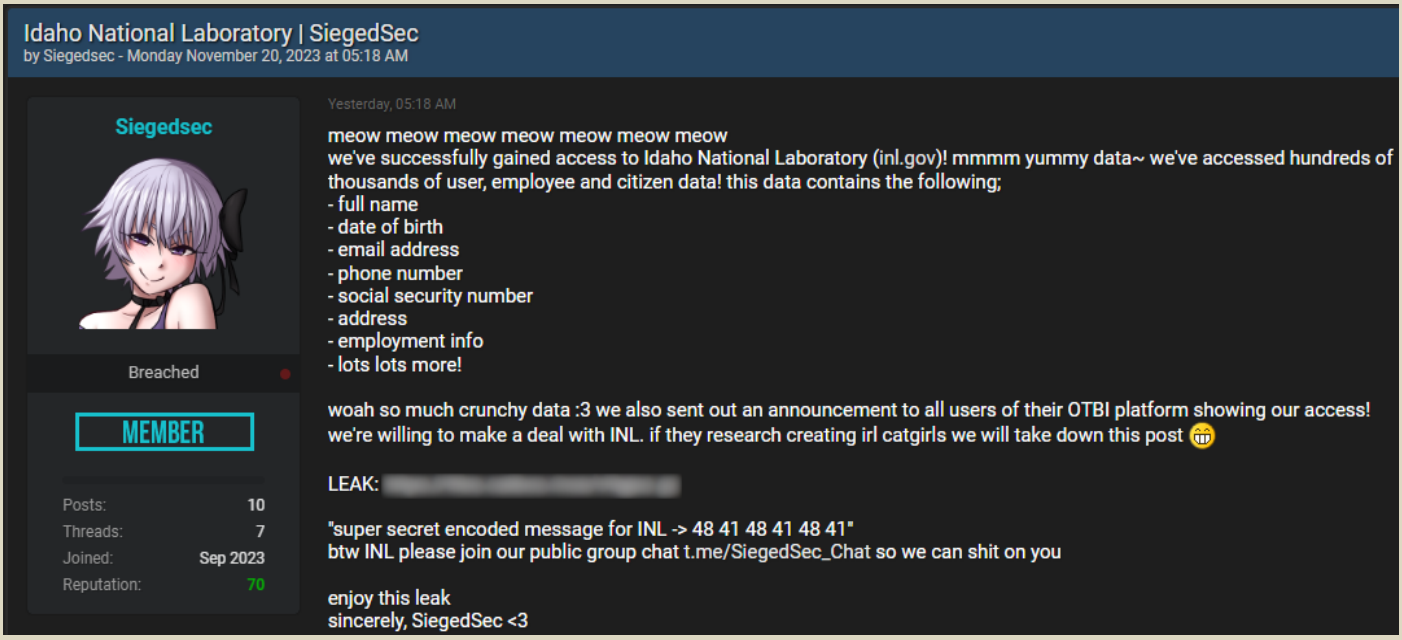
"We're willing to make a deal with INL," SiegedSec wrote in their announcement of the breach. "If they research creating irl catgirls we will take down this post [with a link to the leak]."

"On Monday, Nov. 20, Idaho National Laboratory determined that it was the target of a cybersecurity data breach in a federally approved vendor system outside the lab that supports INL cloud Human Resources services," INL said in a statement to Engadget. "INL has taken immediate action to protect employee data."

SiegedSec is known to take an exceedingly casual approach to its communications, with the group largely motivated by their own amusement (though it has also attacked targets for political reasons). As such, SiegedSec's request for catgirls is likely a joke simply intended to indicate that they have no intention of taking the hacked information down — if the fantastical nature of their demand wasn't already a pretty big clue.

"Many people ask 'why?' for the INL breach," SiegedSec wrote on its Twitter / X account. "We are cats, intricacies such as 'why' do not concern us."

A common character archetype in anime and manga, catgirls are human or humanoid women who have some feline physical characteristics. Usually these characteristics are restricted to a pair of cat ears and a tail, though the character may also have other feline features or display catlike behaviour, instincts, or abilities.



Idaho National Laboratory | SiegedSec
by Siegedsec - Monday November 20, 2023 at 05:18 AM

Yesterday, 05:18 AM

meow meow meow meow meow meow meow
we've successfully gained access to Idaho National Laboratory (inl.gov)! mmmm yummy data~ we've accessed hundreds of thousands of user, employee and citizen data! this data contains the following;
- full name
- date of birth
- email address
- phone number
- social security number
- address
- employment info
- lots lots more!

woah so much crunchy data :3 we also sent out an announcement to all users of their OTBI platform showing our access!
we're willing to make a deal with INL. if they research creating irl catgirls we will take down this post 😁

LEAK: [redacted]

"super secret encoded message for INL -> 48 41 48 41 48 41"
btw INL please join our public group chat t.me/SiegedSec_Chat so we can shit on you

enjoy this leak
sincerely, SiegedSec <3

SiegedSec's announcement on hacking forums *(BleepingComputer)*

Memes about "genetically engineered catgirls" have playfully pondered how these feline mutants might be created in real life using actual scientific methods, and jokingly advocated for funding such a project. Many anime fans consider catgirls to be cute, sexy, highly idealised sexual partners.

It's unclear what expertise SiegedSec might have thought INL holds when it comes to creating catgirls. INL's research is more focused on nuclear and integrated energy than anything that might produce human-cat hybrids.

Since announcing the breach, SiegedSec further revealed it has also accessed hundreds of government employee records from the City of Hendersonville, North Carolina "while the FBI and CISA was still investigating [their] INL hack." They have not demanded Hendersonville's local government attempt to create catgirls, nor have they made any other requests.

Narrative warfare: How disinformation shapes the Israeli-Hamas conflict—and millions of minds

By Yusuf Can

Source: https://thebulletin.org/2023/11/narrative-warfare-how-disinformation-shapes-the-israeli-hamas-conflict-and-millions-of-minds/

Nov 25 – Earlier this month, German television channel *Welt* claimed that a Palestinian Instagrammer had feigned a deathbed scenario in a hospital bed and subsequently posted a miraculous video depicting their well-being amidst the aftermath of a bombing in Gaza. While the actual circumstances diverged significantly from this narrative, *Welt* propagated the Pallywood—a portmanteau of "Palestine" and "Hollywood—conspiracy theory, baselessly alleging that "amateur actors" were fabricating scenes in Gaza.

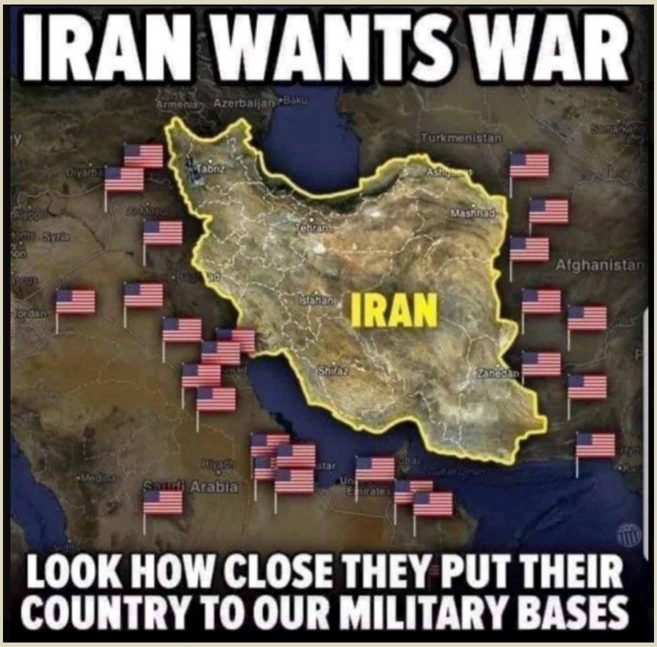
It turns out the individuals featured in the two videos were not the same, and the footage from the hospital had been uploaded to social media several months prior to Hamas's October 7 attack on Israel. But the claim, asserting the identity of the two individuals, had already made the rounds and was also disseminated by Israel's official X (formerly known as Twitter) account, only to be removed later.

The Israeli-Palestinian conflict is a perennial, deeply entrenched issue transcending mere geopolitics. It is a contest of narratives, a battle where stories and perceptions wield as much power as physical forces. In this intricate struggle, disinformation emerges as a potent weapon skillfully wielded by those with ill intentions. A single Tweet or a brief TikTok video is insufficient to distill decades, if not centuries, of historical background, yet they possess the capacity to shape the minds of individuals, influence their reactions, and even sway policymaking. As such, an examination of how to address rampant misleading information that is shaping the dynamics of human society is necessary.

Nobody is safe

Regardless of one's stance in this enduring conflict, dominant narratives are often handed down from generation to generation. The remarkable ability of these narratives to mold public opinion attests to their formidable potency. Disinformation becomes a valuable instrument in developing these entrenched perspectives, revealing the vulnerability of individuals when confronted with a barrage of misleading or outright fake information. Notably, even prominent figures with access to vast resources—journalists, politicians, and ironically, CEOs of social media companies—can fall prey to the insidious influence of disinformation.

In October, Elon Musk, the CEO of X, shared an image featuring a map of Iran enclosed by more than two dozen American flags, symbolizing purportedly United States military bases. The accompanying caption on Musk's post mused, "Iran wants war. Look how close they put their country to our military bases." Additionally, he appended the graphic with the words, "Oh, the Irany." While interpreting the true motivations behind the post remains elusive to anyone except Musk himself, this incident serves as a noticeable example of misinformation, if not the more deliberate form known as disinformation. The map in the graphic purportedly denotes 26 American military bases in Afghanistan, Pakistan, and Turkmenistan. **But the fact is that these bases did not exist.** Musk, after being duly corrected, eventually acknowledged posting an inaccurate graphic. The fact that the CEO of X, notorious for its struggle with disinformation, could not elude becoming trapped in this problematic phenomenon is indeed noteworthy.



Irrespective of his underlying motives, a tech mogul like Musk taking part in the spread of disinformation has a consequential impact on which narratives emerge victorious. It is one thing when a social media user with a handful of followers shares false information. When it is done by one of the most influential individuals on the planet, it shapes millions of minds around the globe. The same issue regarding the magnitude of impact applies to other actors as well, including the mainstream media.

The episode during which *Welt* spread the Pallywood conspiracy theory is a stark reminder that media organizations and governments remain susceptible to disinformation despite their substantial resources. These powerful entities play a crucial role in shaping narratives, whether through the unintentional spread of false information or the intentional manipulation of stories. This dual vulnerability, arising from both susceptibility to misinformation and purposeful narrative shaping, highlights the intricate landscape in which these actors operate. When these entities are perceived to employ disinformation to advance their preferred narrative, it not only undermines the credibility of these institutions but also diminishes the public's trust in the information they provide. This erosion of trust creates a void that malicious actors can exploit, often to the detriment of innocent individuals.

Beyond social media

Following Hamas's attack last month, it has become nearly impossible to avoid images of destruction and pain. Online, it was already tricky to sift through the bombardment of disinformation, recycled footage from past conflicts, images from video games, and contradictory narratives to determine what is actually happening on the ground. Now, generative artificial intelligence tools are adding a new layer of complexity to an already growing problem with synthetic media. AI-generated images, videos, and audio related to the ongoing conflict are running rampant. Fake images of dead children to trigger emotions, hate-fueled memes targeting Jewish people, and intentionally manufactured efforts to mislead the public can be found in many corners of social media platforms.

For decades, tech moguls promised a future in which the internet and artificial intelligence would enhance and improve the quality of human life. If there was ever a moment where the overstated promises of such technologies could be put to the test, the Israel-Hamas conflict is one of them. Without a doubt, the ever-evolving technology has myriad benefits to human life. However, the creation and dissemination of disinformation clearly indicate the limitations, failures, and potential harm of tech utopianism.

Disinformation and the risk of apathy

Disinformation regarding Gaza can include incorrect details about the nature of the crisis, the affected areas, and the actions that need to be taken, leading people to make uninformed decisions. For example, emergency responders rely on accurate information to plan and execute efficient and effective responses, such as delivering food. Disinformation can divert resources to areas that do not need immediate assistance or delay the deployment of resources to areas that urgently require help. Such delays can have serious consequences, especially when time is of the essence.

But the dangers of disinformation are manifold and can have even more profound and long-term consequences.

Disinformation doesn't simply get people to believe a false thing is true; it also convinces them to think a true thing is false.

That's the contagion that disinformation spreads into the atmosphere. Not only does disinformation erode a person's knowledge base, but it also erodes trust in other people to tell the truth when it comes in the form of a conspiracy theory. Consider the bombing of a hospital during a conflict. In that case, determining who is to blame for the explosion has real, global, legal, and humanitarian consequences, and it takes time to examine the evidence and determine the facts. But in a society where millions of people can access a myriad of unvetted information in only a few seconds, ill-intended actors take advantage of this confusing and convoluted influx of information to move public opinion to trust or lose trust in a particular actor.

In other words, one of the riskiest aspects of disinformation is that it can make individuals cynical because it plays right into the ill-intentioned actor's hands. Such actors can convince people to believe their narrative, and even if they can't convince, they can make one question the narrative they believed so far and eventually demoralize them. Finally, they will make people feel that even trying to solve a problem is a useless attempt, making individuals apathetic.

Moving forward

The use of digital technology in politics has a relatively short history, although deception in warfare—and influencing a country's politics is a form of warfare—goes back a long time. Yet the scale of deception and use of digital technology seen in today's world is dramatically more effective and drastically harder to control. The instances involving influential figures like Elon Musk and media organizations like *Welt* underscore the vulnerability of even those with substantial resources to the insidious influence of false information. Much of the rest of internet consumers are merely easy prey.

As technology, including artificial intelligence, intertwines with the Gaza conflict, the promise of a tech utopia is tested against the stark reality of disinformation's harmful consequences.

The ongoing crisis in the Middle East exposes the limitations and potential harms of the tech world's overstated promises once again. The rapid spread of disinformation on social media platforms erodes knowledge and undermines trust in information sources, including governments. The dangers of disinformation extend beyond misinformation; it can lead to cynical perspectives, demoralizing individuals and fostering apathy toward problem-solving.

I need not clarify the critical need for global efforts to address the pervasive disinformation issue. In the context of emergency responses, the impact is tangible, diverting resources and impeding timely assistance. Other effects are more general and diffuse. The current state of technological developments, coupled with a lack of regulation and an international consensus, exacerbates the spread of unreliable information, conspiracy theories, and real-life harm. As humans grapple with the multifaceted challenges of today's world, from climate change to great power competition, steps have been taken to address rampant disinformation, but those efforts are still in their early stages.

It may be impossible to completely counter rampant disinformation in real time, given how the internet and social media platforms are structured. Even if that is the case, the global community needs a consensus on how to approach this stark threat before collectively deciding on next steps to at least limiting its most malign impacts.

Yusuf Can serves as a coordinator for the Middle East Program (MEP) at the Wilson Center. He delves into the political dynamics of the Middle East and North Africa, with a keen interest in corruption, geopolitics, and tech policies. Can oversees the Enheduanna blog and Viewpoints as an editor, organizes prominent MEP events and sessions, and plays a pivotal role in the inception and execution of novel projects. Can received an M.A. in democracy and governance from Georgetown University in Washington, DC, and a B.A. in political science from Sacramento State University in Sacramento, California. Can is originally from Istanbul, Turkey.

Cybercriminals are Tired of AI Tools

Source: https://i-hls.com/archives/121901

Dec 01 – Many GPT-based tools like WormGPT and FraudGPT became popular on underground forums and were assumed to be helping deliver new strains of malware and automate cybercrime. GPTs are a form of large language model that is trained on massive datasets, and jailbroken GPTs do not have restrictions for generated content so they can be trained on the information typically used by cybercriminals.

Nevertheless, many cybercrime fans and experts have expressed their skepticism, stating that dark GPT versions are "overrated, overhyped, redundant, and unsuitable for generating malware." Furthermore, threat actors have expressed concerns about the security of the final product, wondering whether it could bypass antivirus and EDR detection, concluding that real-world applications remain "aspirational."

According to Cybernews, researchers claimed that they found "only a few examples of threat actors using LLMs to generate malware and attack tools, and that was only in a proof-of-concept context. However, others are using it effectively for other work, such as mundane coding tasks."

The researchers found very few discussions of actual cybercriminals who seem to be using such AI tools. Among the few discussions found, many focused on jailbreak tactics for legitimate AI models and compromised ChatGPT accounts for sale. "Unsurprisingly, unskilled 'script kiddies' are interested in using GPTs to generate malware, but are – again unsurprisingly – often unable to bypass prompt restrictions, or to understand errors in the resulting code," the report said.

In general, researchers report observing a lot of skepticism with hackers worrying about operational security, and some even having ethical concerns about using AI- "We found little evidence of threat actors admitting to using AI in real-world attacks, which is not to say that that's not happening. But most of the activity we observed on the forums was limited to sharing ideas, proof-of-concepts, and thoughts."

The researchers concluded that none of the AI-generated malware they found in forums was sophisticated, and found no evidence of such sophistication on the posts they examined. They also believe that illegal clones of ChatGPT purposefully built for malicious applications aren't very useful for cybercriminals, and while they did find some uses for them, GPTs aren't up to the task of creating malware or finding new vulnerabilities.

Anti-Israeli Iranian Cybergang Attacks US Water Sector

Source: https://i-hls.com/archives/121955

Dec 05 – The US accuses Iran's elite military government of using a nation-state threat group to launch attacks on its water sector as part of its conflict with Israel.

The FBI and NSA issued a statement condemning the Iranian Revolutionary Guard Corps (IRGC), or more specifically the cybergroup CyberAv3ngers, which it says was behind recent attacks on its water supply as a result of its going after Israeli companies in the sector.

According to Cybernews, the incident came to light in November after the hack of the municipal water authority in Pennsylvania, its computer terminal interface reading: "You have been hacked, down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target."

The CISA stated: "IRGC-affiliated cyber actors using the persona **'CyberAv3ngers'** are actively targeting and compromising Israeli-made Unitronics Vision Series programmable logic controllers (PLCs)," adding that the PLCs are "commonly used in the water and wastewater systems sector and […] in other industries including, but not limited to, energy, food and beverage manufacturing, and healthcare."

CyberAv3ngers was described by CISA as a "cyber persona" of the IRGC, a terrorist organization that's said to have claimed responsibility for multiple attacks on Israeli soil since 2020. Cybernews reports that a Telegram channel supposedly belonging to the group was spotted displaying "both legitimate and false claims of multiple cyberattacks against Israel" in recent months. Additionally, CyberAv3ngers is said to have targeted Israeli public companies in the water, energy, shipping, and distribution sectors.

It is also believed that CyberAv3ngers has an accomplice in the cybergang "Soldiers of Solomon", with the CISA stating: "The CyberAv3ngers-linked Soldiers of Solomon claimed responsibility for compromising over 50 servers, security cameras, and smart city management systems in Israel," adding that the "majority of these claims were proven false."

A Cyber Threat to U.S. Drinking Water

By Jacob Horne, and Jim Dempsey

Source: https://www.lawfaremedia.org/article/a-cyber-threat-to-u.s.-drinking-water

A water pumping station in Smithville, OK. (U.S. Department of Agriculture, http://tinyurl.com/mphcekap; PDM 1.0 DEED, https://creativecommons.org/publicdomain/mark/1.0/)

Dec 21 – In March 2023, the Environmental Protection Agency issued a memo warning that cyber-attacks against public water systems were increasing. These attacks, the EPA said, have the potential to disable or contaminate the delivery of drinking water to Americans. While some public water systems had taken important steps to improve their cybersecurity, many systems had "failed to adopt basic cybersecurity best practices and consequently are at high risk of being victimized by a cyber-attack," including by state-sponsored actors, according to the EPA.

Under the federal Safe Drinking Water Act, states are required to conduct surveys of local water systems. Specifically, states must conduct, at least every three to five years, an onsite review of the "facilities, equipment, [and] operation … of a public water system to evaluate the adequacy of the system, its sources and operations and the distribution of safe drinking water." If a state identifies a "significant deficiency" during a survey, the state must require the water system to address it.

In its March memo, the EPA noted that many public water systems had become reliant on electronic systems to operate efficiently, particularly on operational technology such as industrial control systems. The EPA therefore said it was interpreting the existing requirement on states to survey the "equipment" and "operation" of public water systems to include a review of the cybersecurity of any operational technology being used that could impact the supply or safety of the water provided to customers. Under the existing rule, if the state identified a significant cybersecurity deficiency, then the state would require the water system to address it. The memo laid out various approaches by which states could comply, including self-assessment by a water system itself, third-party assessment, direct state evaluation, and other alternatives. In a companion document, the EPA laid out a cybersecurity checklist for states to use.

Almost immediately, several Republican state attorneys general, joined by the American Water Works Association and National Rural Water Association, petitioned for review. They argued that the memo was a legislative rule issued in violation of the Administrative Procedure Act and that it exceeded the EPA's statutory authority. The operational technology now essential to the delivery of safe drinking water, the plaintiffs argued, did not fit within the terms of the existing rule covering "equipment" and "operations" and "the distribution of safe drinking water." The collection of cybersecurity information would, the trade associations argued, expose the water systems to higher risk of cyberattack.

In July, 2023, without opinion, the Eight Circuit granted the plaintiffs' motion for stay of the memorandum pending disposition of the petition for review. In October, the EPA rescinded the March memo, citing the litigation.

Now the FBI, the Cybersecurity and Infrastructure Security Agency, NSA, the Israeli National Cyber Directorate, and the EPA are warning in a joint advisory that since at least Nov. 22, 2023, cyber actors from Iran's Islamic Revolutionary Guard Corps (IRGC) have been actively targeting *and compromising* operational technology used in American water and wastewater systems. The compromised devices (specifically, Israeli-made Unitronics programmable logic controllers) were publicly exposed to the internet with default passwords. The agencies recommend—but they can only recommend, since the EPA memo has been revoked—three actions that water systems could take "today to mitigate malicious activity."

Those actions are to implement multifactor authentication, use strong, unique passwords, and check installed equipment for default passwords. Sure enough, these are identical to three of the first four items that the EPA had recommended in the cybersecurity checklist issued alongside its March 2023 memo: "Require multi-factor authentication." "Require a minimum length for passwords." "Change default passwords."

So the IRGC is exploiting the very weaknesses that the states and the water system groups argued a few months ago need not be considered when assessing the equipment and operations of water systems.

So far, Biden administration cybersecurity rules on pipelines, railroads, and the aviation sector, issued under statutes that talk about safety and reliability but do not specifically mention cybersecurity, have stood. The courts' hostility to federal regulation, epitomized by the Supreme Court's 2021 ruling that an agency cannot address big problems unless Congress expressly grants it the authority to do so, has probably slowed down the Biden administration's efforts to adopt cybersecurity rules for other sectors. It certainly must have influenced the government's decision to throw in the towel on the EPA memo. To its credit, the administration continues to look for ways to strengthen the cybersecurity of critical infrastructure. Just on Dec. 6, the Department of Health and Human Services issued a cybersecurity plan indicating that it will use existing authority to establish cybersecurity requirements for hospitals receiving Medicare and Medicaid payments.

However, to swiftly and unequivocally move forward on cybersecurity, congressional action is needed. Comprehensive cybersecurity legislation is not conceivable when anti-regulatory sentiment still holds strong sway on Capitol Hill (not to mention other sources of dysfunction). But Congress did act just last December to give the Food and Drug Administration specific authority to issue cybersecurity standards for connected medical devices.

Ironically, the American Water Works Association, which argued against the EPA memo, has called for federal legislation to establish a regulatory regime for drinking and wastewater systems. Their proposal is for an industry-led private organization that would develop cybersecurity requirements, subject to EPA approval, and enforce them, subject to EPA oversight. The concept is patterned after a system long in place under the 2005 Energy Policy Act for the bulk electric power industry. The Cyberspace Solarium Commission staff translated the concept to legislative language, but so far no such legislation has been introduced. Do the trade associations and their allies, having demonstrated their ability to block EPA action, have the will and the juice to get anything through Congress?

An agency-by-agency, sector-by-sector approach may find other avenues for incremental congressional action that would make impossible the kind of evasive tactics deployed against the EPA's efforts to strengthen the cybersecurity of water systems. Meanwhile, the government is left pleading with our drinking water providers: please change those default passwords.

Jacob Horne is Chief Cybersecurity Evangelist at Summit 7, a Huntsville, Alabama-based managed cybersecurity firm. He is the host of the Summit Up Podcast, focused on cybersecurity policy in the defense industrial base. He was previously a U.S. Navy Cryptologic Technician and has developed numerous cybersecurity training programs for the NSA National Cryptologic School, UCLA, and UC Irvine.
Jim Dempsey is a lecturer at the UC Berkeley Law School and a senior policy advisor at the Stanford Cyber Policy Center. From 2012-2017, he served as a part-time member of the Privacy and Civil Liberties Oversight Board. He is the author of Cybersecurity Law Fundamentals (IAPP, 2021).

I SEE YOU WHEN YOU'RE SLEEPING... I KNOW WHEN YOU'RE AWAKE... I KNOW IF YOU'VE BEEN BAD OR GOOD...
ARE YOU A HACKER?
©2016 PITTSBURGH POST-GAZETTE
ROGERS

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic DRONE NEWS

Drones have boots: Learning from Russia's war in Ukraine

By Dominika Kunertova | Center for Security Studies, ETH Zurich, Switzerland

Contemporary Security Policy | Volume 44, 2023 - Issue 4 | Pages 576-591 | Published online: 17 Oct 2023

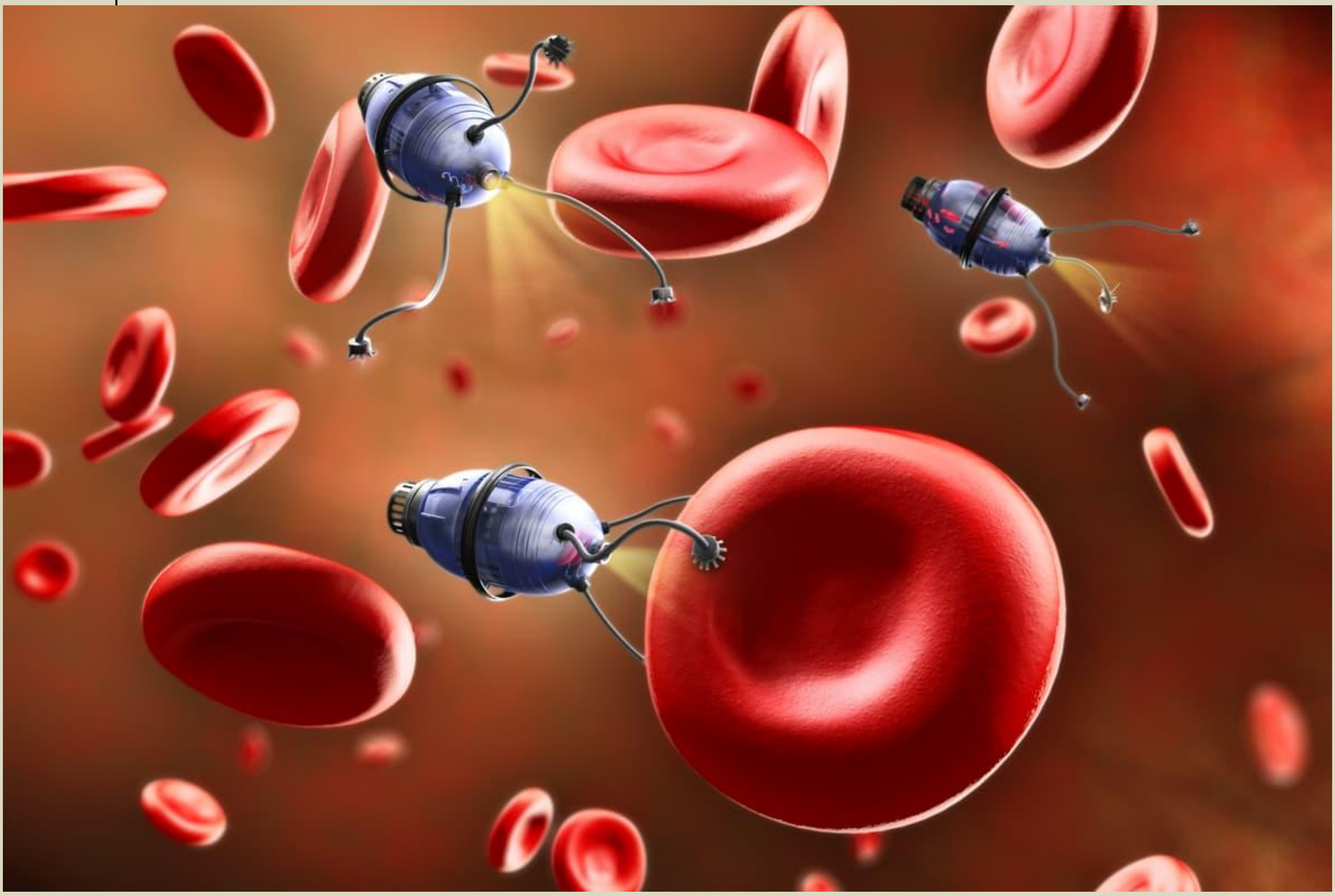
Source [**full text**]: https://www.tandfonline.com/doi/full/10.1080/13523260.2023.2262792

ABSTRACT

Before Russia's 2022 invasion of Ukraine, security studies scholars were myopic about small drones' enabling functions and tactical benefits. They were preoccupied with drone impacts on international security and the ethical dimensions of counterterrorism drone strikes. Similarly, literature on the revolution in military affairs has examined emerging drone technologies based on their strategic advantages. "Low-tech" drone innovations have received less attention. The war has highlighted the collective magnitude of these omissions. At first, scholars followed extant predictions by concluding that large drones did not revolutionize warfare, proliferated slowly, and were too costly and complex to operate. Yet, one year into the war, thousands of drones—scouts, loitering grenades, drone bomblets, and suicide drones—are defying the field's assumptions of their uselessness sans air superiority. Contrary to most theoretical expectations, small drones in Ukraine are changing battlefield dynamics from lower airspace. Scholars must begin to study drone diversity in modern wars.

Medical nanobots could communicate by releasing molecules into bloodstream

Source: https://newatlas.com/science/medical-nanobots-communicate-molecules-bloodstream/



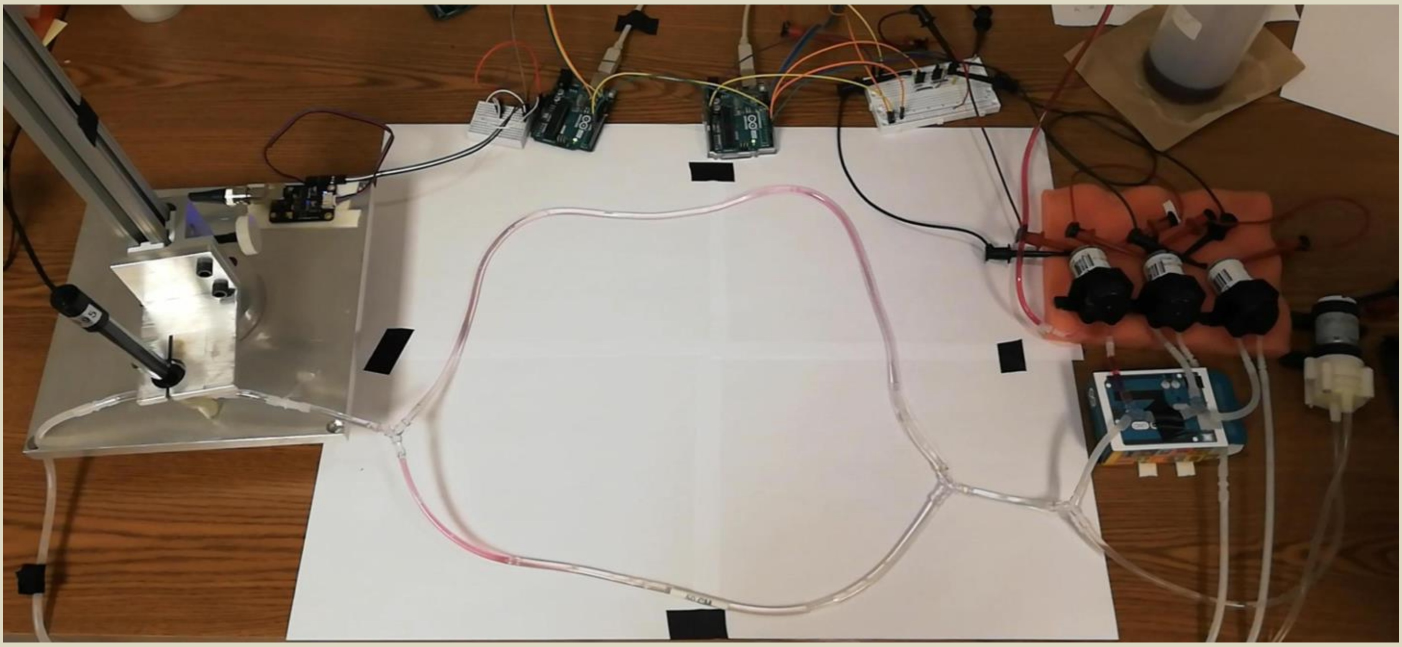
Nanobots and implants working in the human body could eventually communicate by releasing molecules into the bloodstream, according to a new proof-of-concept study – Depositphotos

Implants and tiny machines could eventually be working inside our bodies to help treat disease or monitor activity, but letting them communicate is tricky. Now scientists at EPFL have developed a system whereby devices can communicate by releasing molecules into a patient's bloodstream. Biomedical implants play a key role in healthcare, monitoring activity in organs like the heart or brain, while recent research is investigating how nanoscale robots might one day swim or crawl through the body to fight disease. But these systems have a communication issue.

Running wires through the body is not only impractical, it's an infection risk. And wireless technologies like radio, light and Bluetooth don't travel through human tissue very efficiently, drastically limiting their range.

Now, scientists at EPFL have demonstrated a proof-of-concept system called biomolecular communication. The idea is to allow micro- or nano-robots and implants to communicate by releasing specific molecules into the bloodstream – in a basic sense, the presence of a molecule could be interpreted by a machine as a 1, while no detection represents a 0.

"Biomolecular communication has emerged as the most suitable paradigm for networking nano-implants," said Haitham Al Hassanieh, an author of the study. "It's an incredible idea that we can send data by encoding it into molecules which then go through the bloodstream and we can communicate with them, guiding them on where to go and when to release their treatments, just like hormones."



The EPFL team's synthetic testbed, consisting of tubes and pumps that simulate blood vessels and a heart, which demonstrated molecular communication using four transmitters – EPFL

The team translated techniques from electronic networking, such as packet detection, channel estimation, and encoding and decoding schemes, to the molecular network. This helped to overcome problems raised by biology, like unstable channels and a lack of synchronization and feedback. The researchers tested the technology on a synthetic circulatory system in the lab, consisting of tubes and pumps that simulated blood vessels and a heart. Using this, they were able to show that the technique worked with up to four devices transmitting molecular signals at once, performing better than existing techniques.

Of course, success in lab tests doesn't necessarily translate to real-life human use, and the team acknowledges that there are far more factors at play in live patients. However, they do say that this is a promising first step towards that eventual goal. Other scientists have found success transmitting data through ion exchange in human tissue.

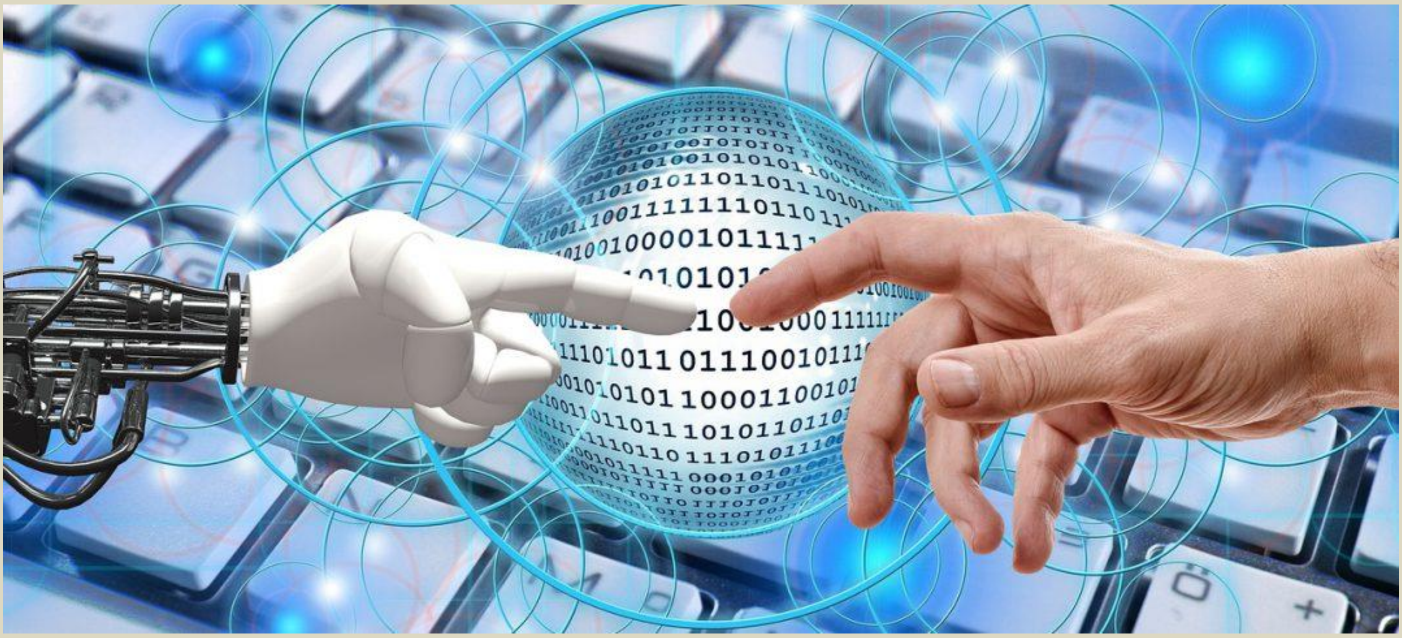
●▶ The research was presented at the ACM SIGCOMM 2023 conference in September.

Human-Robot Communication Revolutionized by AI-Powered System

Source: https://i-hls.com/archives/121845

Nov 28 – Researchers from Brown University have unveiled a transformative AI-based system that is expected to reshape how humans communicate with robots. This new and innovative system, called "Lang2LTL", addresses the challenges in enabling robots to understand and carry out human instructions presented in everyday language.

Until now, trying to instruct robots using regular, everyday language and context-driven commands presented an impossible hurdle, which in turn necessitated extensive data-driven training for robots to decipher and execute nuanced instructions. However, recent breakthroughs in AI-driven large language models are now presenting a new era in human-robot communication.



Senior research author Stefanie Tellex explains that the team aimed to bridge the gap between complex human instructions and a robot's actions, contemplating scenarios like guiding a mobile robot through nuanced paths or locations. "We wanted a way to connect complex, specific and abstract English instructions that people might say to a robot," Tellex added, highlighting the system's ability to interpret rich and precise instructions.

According to Interesting Engineering, the system excels in converting language directives into actionable robot behaviors without requiring huge amounts of training data. The system can seamlessly adapt to new environments without extensive training and merely requires a detailed map of the surroundings.

The researchers tested the system by conducting simulations across 21 cities using OpenStreetMap and achieved an impressive 80 percent accuracy rate, while existing systems typically perform a mere 20 percent accuracy. The system's versatility makes it applicable to many different uses and scenarios, like guiding drones, self-driving cars, or ground vehicles through cityscapes, and overall facilitating intricate and precise instructions for navigating complex environments.

The system works by extracting locations from user instructions, matching them to known environments, and converting them into a format the robot comprehends, according to the study's lead author Jason Xinyu. "Our system uses its modular system design and its large language models pre-trained on internet-scaled data to process more complex directional and linear-based natural language commands," explained Xinyu.

Going forward, the researchers are expected to release a simulation allowing users to test the system's functionality and provide valuable insights for further refinement. They also aim to integrate object manipulation capabilities into the software that would expand the system's repertoire. This revolutionary system heralds a new dawn in seamless, nuanced human-to-robot communication, promising widespread applications in many different domains.

New Hydrogen Drones May Revolutionize The Drone Industry

Source: https://i-hls.com/archives/121904

Dec 01 – HevenDrones, a company that revolutionized drone tech by integrating it with hydrogen fuel, revealed its latest achievement- the H2D200 Series is hydrogen-powered, and has exceptional payload capacity, extended endurance, and precision flight.

HevenDrones introduced two new models—the H2D200 and the H2D250- which both harness the unique flight profile of hydrogen to redefine drone performance and capabilities. The unveiling shows the company's commitment to reshaping the drone industry and addresses the longstanding challenge of enhancing flight endurance using hydrogen power.

According to Interesting Engineering, the company used hydrogen's unmatched energy density and environmental benefits to redefine the capabilities of drones. The new H2D200 is designed to carry payloads up to 4.5kg, has an impressive range of up to 510 km, and an extended flight time of up to four hours. All those capabilities establish a new benchmark for smaller payload drones while retaining the ability to hover with unparalleled precision.

The H2D250 drone is engineered for larger payloads (up to 10kg), has a range of up to 750 km, and an operational time of up to eight hours. This larger model caters to many different applications, but especially advanced logistics missions that require multiple deliveries.

HevenDrones' CEO Bentzion Levinson said that now they are at a pivotal moment in the drone industry. "The H2D200 Series represents not only a leap forward in drone technology but also a testament to our commitment to building a smarter ecosystem in the skies using the full power and potential of AI. With these hydrogen-powered drones, we are redefining the possibilities of what drones can achieve, while leveraging a clean and readily available fuel source. We are excited to bring these innovations to the world and to partner with forward-thinking organizations who share our vision."

The fact that HevenDrones participated in the Monaco Hydrogen Forum (where it showcased the new drones) shows its dedication to driving innovation in the drone technology sector. Furthermore, the new H2D200 Series represents a milestone signifying a broader shift towards sustainable and efficient drone technology. These hydrogen-powered drones are paving the way for a smarter and more environmentally conscious future in the drone industry.

New Microwave Weapons Could Defend against Swarms of Combat Drones

By Jason Sherman

Source: https://www.scientificamerican.com/article/new-microwave-weapons-could-defend-against-swarms-of-combat-drones/

Dec 01 – In the opening hours of its surprise attack in early October, Hamas executed coordinated drone strikes against Israeli watchtowers and security cameras. These attacks were designed to blind the Israel Defense Forces' surveillance of Gaza, clearing the way for armed assailants to infiltrate Israel and attack civilians with impunity.

Such ad hoc fleets of low-cost drones have played prominent roles in other recent conflicts, including Ukraine's fight against Russian forces and Azerbaijan's strategy in the Nagorno-Karabakh conflict of 2020. But this is only the beginning. Soon machine learning will enable dozens of drones at once to fly in larger coordinated "swarms" that could overwhelm traditional defenses even more easily. The U.S. Department of Defense is preparing new countermeasures against this threat, and the Pentagon believes it has a promising candidate in an invisible form of directed energy: high-power microwaves.

"We believe that high-power microwave technology is critical to help us mitigate the threat of swarming small drones," says Maj. Gen. Sean Gainey, head of the Joint Counter-Small Unmanned Aircraft Systems Office (JCO) and director of fires in the office of the Army's deputy chief of staff for operations, plans and training. The threat from small uncrewed aircraft has been rapidly growing in general, Gainey adds. He predicts that coordinated mass attacks involving hundreds of drones flying together to overwhelm traditional defenses are coming. Meanwhile individual drones are getting faster, more agile and—when equipped with the right munitions—gaining the potential to inflict greater destruction, akin to the impact of a cruise missile. And artificial intelligence will also enable them to function autonomously.

U.S. Army Cpl. Matthew G. Mena, Charlie Battery, 1st Battalion, 258th Field Artillery, New York Army National Guard, performs a systems check on an RQ-11 Raven B, a small unmanned aerial system, during field training. Small UAS are already making their way into combat, and soon, machine learning will enable large swarms of drones to fly together in coordinated attacks. | Credit: American Photo Archive/Alamy Stock Photo

To defend against this threat, the Army is looking for prospective technologies that can detect, track, identify and disable between 20 and 50 small drones, officially called unmanned aerial systems, or UAS, in one fell swoop. Next June the Pentagon is planning the U.S. military's most ambitious counterdrone demonstration to date. At the White Sands Missile Range in New Mexico, the JCO will assess about half a dozen new technologies, pitting them against a swarm of up to 50 small, uncrewed "surrogate enemy aircraft." The U.S. government divides small drones into three categories: Group 1 describes aircraft that weigh up to 20 pounds, Group 2 covers those between 21 and 55 pounds, and Group 3 encompasses uncrewed systems that can weigh as much as 1,320 pounds. The swarm event will feature Group 1- and Group 2-size flyers.

"We're going to have a swarm demonstration looking at how the adversary will try to overwhelm our air defenses, trying to overwhelm our ability to counter small UAS," says Army Col. Michael Parent, the JCO's acquisition chief. The full range of antidrone candidate technologies to be used in the exercise remains to be determined—but it will likely include microwaves.

Since 1960 the U.S. government has spent $6 billion to develop "directed energy technologies," including laser weapons and high-power microwaves. The latter are a form of electromagnetic radiation like radio waves but with shorter wavelengths (hence the "micro" prefix) that range from about 30 centimeters to a single millimeter. This form of energy is widely used in communications, medicine, industrial settings and, of course, heating food.

High-power microwaves, or HPMs, can direct enough energy at a given frequency to disrupt, degrade or destroy electronic circuitry. And weaponized HPMs, 150,000 times more powerful than a common kitchen microwave, can interfere with an individual small drone's ability to stay in the air. After the electronic circuitry of critical components such as circuit boards or power systems is wrecked, gravity takes over: the drone stops functioning and simply falls from the sky. In 2018, Congress noted these capabilities were maturing and directed the Pentagon to accelerate plans to move HPM projects from the lab to the battlefield. The goal is to help counter the technological advancements of potential adversaries such as China and Russia.

The DOD responded to that congressional mandate in part by rapidly prototyping a domestic program akin to Israel's Iron Dome system, which knocks most incoming rockets out of the sky. Called Indirect Fire Protection Capability (IFPC) Increment 2, the U.S. program will include a range of technologies—guided-missile interceptors, high-energy lasers and high-power microwave blasters—to shoot down multiple threats and provide a layered defense against weapons such as drone swarms. Each of these technologies is already in development and being readied for troops over the next two years.

IFPC's high-power microwave component should be ready for operational use as soon as next summer. In January the Army tapped a Los Angeles–based company called Epirus to build four prototype microwave systems as one layer of its planned IFPC. These prototypes are versions of Epirus's Leonidas system. Each one sits on a wheeled trailer that can be detached for remote operation and has a square panel that rests on a gimbal so it can pivot 360 degrees. This panel is packed with software-controlled radio frequency amplifiers that tailor the energy and frequency of the microwave blast.

"The Leonidas design incorporates a lot of lessons identified coming out of Ukraine and a lot of forecasting into what we think a fight in the Western Pacific might look like," says Aaron Barruga, vice president of federal growth at Epirus.

Leonidas' HPM prototype passed muster with Army evaluators in early November, and testing is underway as the Army develops tactics, techniques and procedures for the system's operational use. The goal is to put the four prototype high-power microwave weapons into the hands of operationally deployed units—possibly in the Middle East—next summer.

The DOD is also looking into mounting high-power microwave emitters on flying devices. In 2011 the Air Force funded an advanced technology development project called Counter-Electronics High Power Microwave Missile Project (CHAMP), which involved putting a high-power microwave weapon in a cruise missile. An operator could simply fly the missile *near* a target—a command post, for example—and fry any sensitive electronics rather than directing the weapon to make a bull's-eye strike.

More recently the Marine Corps, the Army and the Defense Advanced Research Projects Agency (DARPA) have been working to pack high-power microwave technology into a smaller flying craft. One example, which has flown in more than 20 tests, is Morfius, a reusable counter-UAS interceptor built by Lockheed Martin. This tube-launched drone has an integrated "seeker," a sensor that guides the craft to its intended target, and a compact HPM. It also has advanced autonomy and guidance algorithms, and it can loiter in midair and defeat individual drones as well as swarms, Lockheed Martin claims.

High-power microwaves might contribute to potent antidrone defenses, but they're not perfect. For instance, HPMs could be rendered ineffective by adding a layer of electromagnetic shielding to a drone's circuity. Still, such steps would add new complexity—not to mention cost, weight and performance requirements—to any attack drone.

"The problem is real," Gainey says. "DOD is responding with capability. However, there's no silver bullet that's going to solve all your problems."

Jason Sherman is an investigative national security reporter with more than 25 years of experience covering the Pentagon, the military budget, weapon system acquisition and defense policy formulation, along with technology, business and global arms trade. He has traveled to more than 40 countries, studied medieval history at the State University of New York at Buffalo, and lives in Brooklyn, N.Y.

Russian Uses 'Brain Impulse' To Operate UAV; Looks To Completely Cut Electronic Command

Source: https://www.eurasiantimes.com/russian-uses-brain-impulse-to-operate-uav-looks-to-completely/

Dec 03 – A Russian technology and robotics company claims to have been able to control a drone with mere 'brain impulses' that do not involve electronic commands. Casually dubbed "thought control," the technology involves a 'neural interface' that reads brain waves, which are converted into electronic commands.

The development was an academic undertaking by the Neurobotics company to attract more students and investments in robotics sciences and Artificial Intelligence (AI). It is part of a more significant government effort to spur the government-run and domestic robotics technology sector to become self-reliant in drone technology. This was after Russia's industrial and technological shortcomings in the UAV sector were exposed in the first few months of the Ukraine war in 2022.

Since then, state-owned and private firms have thrown up a series of low-cost and advanced unmanned aerial vehicles (UAV) for military use, besides a host of remotely piloted aircraft for civilian purposes.

This is amidst regular industry conferences, workshops, exhibitions, interactions with universities and technology students, hackathons, and competitions between engineering students to spur Moscow's drone sector.

Power Of Thought Drone Control

According to a report in RIA Novosti, the developers of the Neurobotics company first integrated the drone, a quadcopter, with a "neural interface." Then, the pilot "controlled" the aircraft "using brain impulses." It also called the phenomenon "the power of thought." The demonstrative experiment was held under the aegis of the National Technology Initiative (NTI).

"The developers of the Neurobotics company connected the Pioneer Mini drone from the Geoscan company with the NeuroPlay neural interface, which allows pilots to control the quadcopter using brain impulses, that is, the power of thought. This development will be useful when holding drone competitions controlled by a brain-computer interface," the NTI said.

A person operating the Geoscan quadcopter with a neural interface. Source: RIA Novosti/Telegram

Pilots can also "benefit" by "improving their concentration skills" and subsequent rapid recovery," the message says. According to Vladimir Konyshev, General Director of the Neurobotics company and a member of the NTI Neuronet Working Group, neurocontrol of drones is the fundamental system in Science, Technology, Engineering, and Mathematics (STEM) studies.

This is because it is an interdisciplinary field involving neuroscience, mechatronics, aeronautical engineering, software programming, and even sports medicine. Injured athletes, disabled persons, people having undergone amputations, and those being treated with physiotherapy are often the victims of dysfunctional nerves. Some amputees have also received bionic limbs that operate purely on electronic impulses from the brain.

Thus, one of the objectives of neural interface technologies is to improve the functioning of nerves connecting the brain and limbs. A highly sophisticated and niche science, a section of doctors have long believed in its potential to address nervous system-linked medical issues like paralysis and nerve damage.

“Together with Geoscan, we plan to hold competitions in the Russian Federation, and I hope this will quickly reach the international level…Another important feature of this combined technology is the ability to neuro-control complex objects such as drones, which not only improves the concentration and attention of the pilot but also teaches them to cope with stress and control emotions when performing complex operations. This is a vital tool for training operators of critical processes,” Konyshev was quoted further.

General Director of the Geoscan company Alexey Yuretsky, in turn, added that the integration of drones with a neural interface could also allow disabled persons who cannot operate drones physically to participate in drone competitions, making them more inclusive.

No Immediate Military Use Yet

It is not clear if the invention has been proposed for military use. But based on leading Russian Telegram groups discussing robotics and technology, it appears to be a self-funded civilian project with industry-academia collaboration. However, the Russian Ministry of Defense (RuMoD) might express interest later once the technology matures.

This is, however, not the first time that neural interfaces have been used to operate a UAV. A 17-second video by Mirai Innovation shows a large quadcopter on a table being physically connected to a neural interface worn by a person, which takes off and lands briefly.

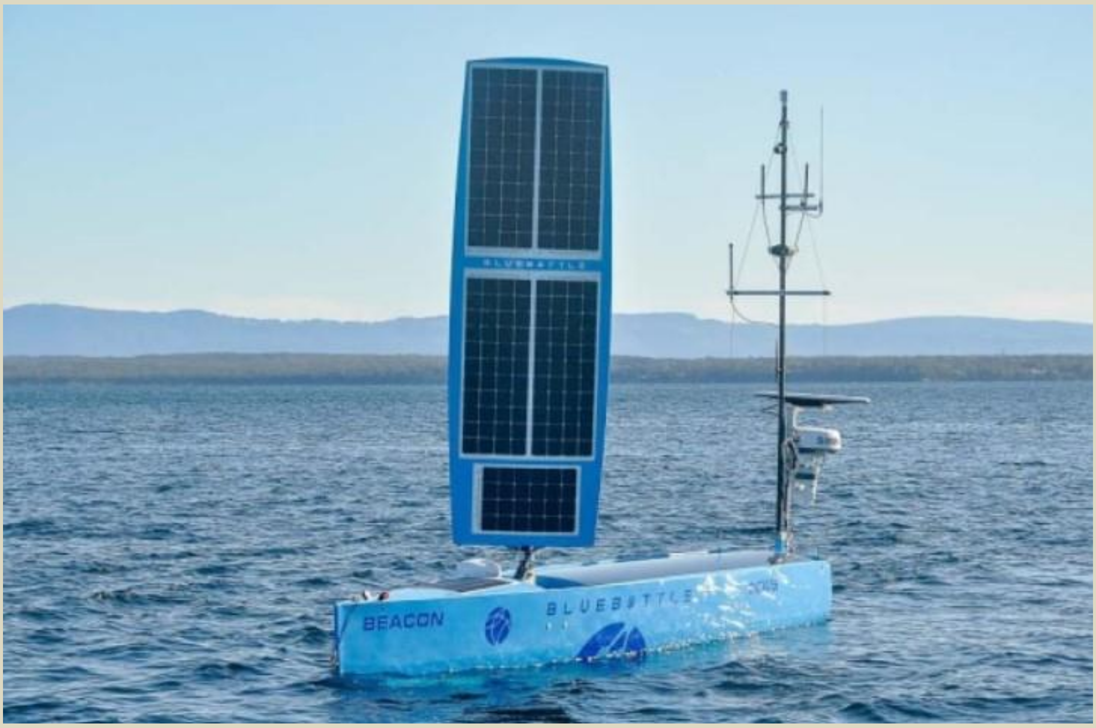
In the picture of the Russian Neurobotics-Geoscan-NTI experiment, the UAV appears much smaller, and the test is taking place in the open. No visible wire is also seen connecting the neutral interface wrapped around the person’s forehead and the small drone.

New AI-Based Solar-Powered Robot Boat for Endless Recon

Source: https://i-hls.com/archives/121964

Dec 06 – The Royal New Zealand Navy will soon receive its first 6.8-meter renewable-powered Uncrewed Surface Vessel (USV) for trial. Called “Bluebottle,” it is meant to provide persistent surveillance around the waters of New Zealand for fishery protection, border protection, or meteorological data.

Once operational, “Bluebottle” will set out to perform its maritime tasks without fuel or personnel on its planned seven-month-long trial. According to Interesting Engineering, the USV uses a retractable rigid sail for wind propulsion, powered by photo-electric cells on the sail. It is equipped with a special flipper and rudder mechanism that allows it to navigate and move forward even in the absence of sunlight and wind, can reach a maximum speed of five knots, and operate at sea indefinitely (even in rough conditions with wave heights of six to nine meters).



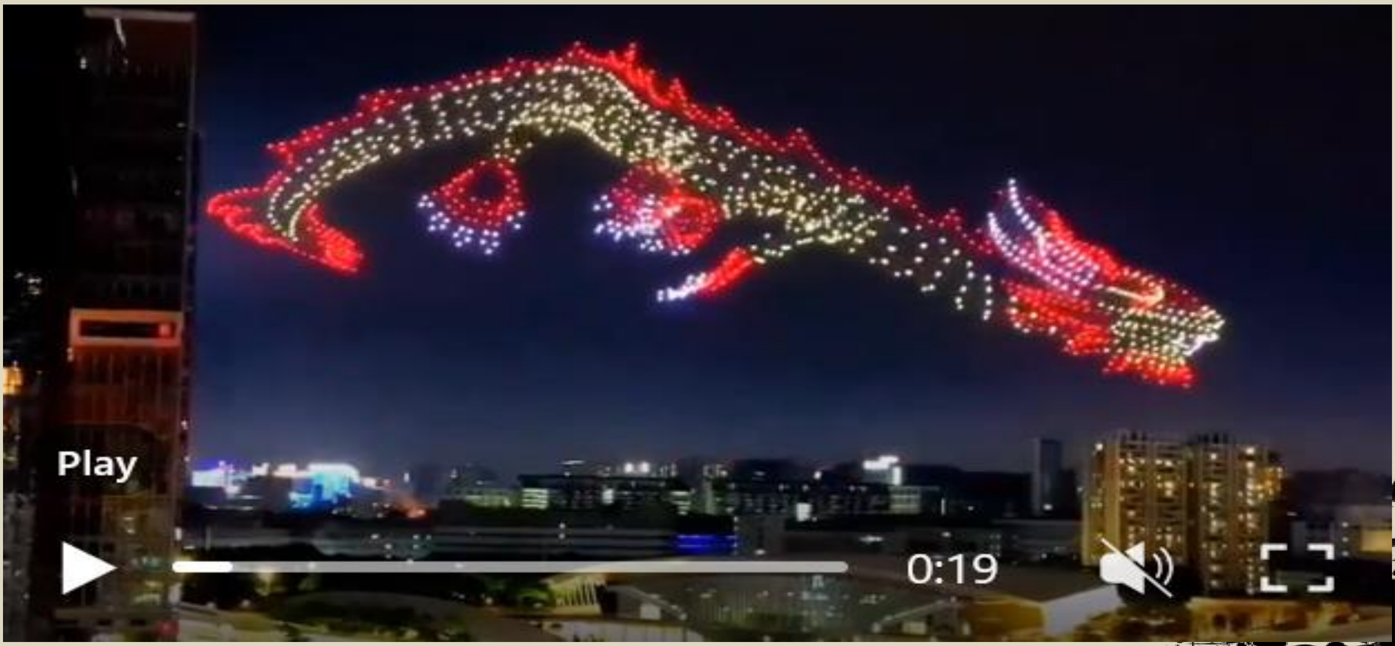
Safe and effective system control and vessel identification are enabled by sensors like radar, electro-optic, and infrared cameras. The USV will be monitored and operated from a control room located at Devonport Naval Base, which will communicate with it through mobile phone signals when the USV is close to the shore and via high- and low-bandwidth satellites when it is further offshore.

The RNZN’s Commander of Autonomous Systems Commander Andy Bryant expressed his excitement for witnessing the potential of the USV, stating: “The Bluebottle has already undertaken a range of activities in support of the Australian Government for long [periods] without the need for refueling, recharging, or crew respite.” He added that he is confident that they will see similar benefits from the time they have with the vessel, particularly a better understanding of how to operate and sustain uncrewed vessels.

In terms of launch and carrying, the USV can be transported by trailer to almost anywhere in New Zealand, where it can be launched and recovered from a boat ramp. It can also be craned on and off a Navy ship to launch operations while deployed overseas.

Drones’ Dragon

1,500 drones displaying a majestic Red Dragon playing in the night sky in Shenzhen, China.



The World's Largest Uncrewed Drone Helicopter

Source: https://i-hls.com/archives/122007

Dec 10 – Rotor Technologies Inc. began production of the largest uncrewed civilian helicopter on the market. Called **R550X,** it is developed as a versatile autonomous helicopter designed for multiple missions. The company claims R550X can carry loads of up to 550 kg in diverse weather conditions, including low-visibility scenarios and nighttime conditions.

Rotor CEO Hector Xu said: "The R550X is going to bring huge safety and economic benefits to a wide range of helicopter use cases. Demonstrating the impact of autonomy in dangerous missions like crop dusting and aerial firefighting is the first step towards our vision for safe and accessible vertical flight."

According to Interesting Engineering, the VTOL has autonomous capabilities to execute tasks independently, and the lack of crew means an increased payload capacity, extended range, and heightened mission flexibility. The R550X uses sensors and digital flight control systems to achieve safe and autonomous operations in many different environments.

Rotor has a human-supervised autonomy system called "Cloudpilot" which oversees R550X piloting services and ensures availability 24/7. Furthermore, the aircraft's communications gateway can uphold six simultaneous links of different types, minimizing the likelihood of total link loss.

Another advantage is R550X's flight time which exceeds three hours and a top speed of 241 kph. With long-range VTOL capabilities that surpass those of drones and eVTOLs, it is ideal for challenging cargo, utility, and maritime operations.

The R550X is part of the experimental category of uncrewed aircraft that are explicitly designed for tasks that don't involve transporting people, with Rotors claiming that operators can deploy the R550X in various operations such as agriculture, firefighting, inspections, and maritime activities. There are currently two R550X units being produced at the company's New Hampshire facilities, and commercial operations are expected in the United States in 2024, with international operations scheduled to follow.

Robot Dogs and AI Inspectors- The Future of Border Security

Source: https://i-hls.com/archives/122069

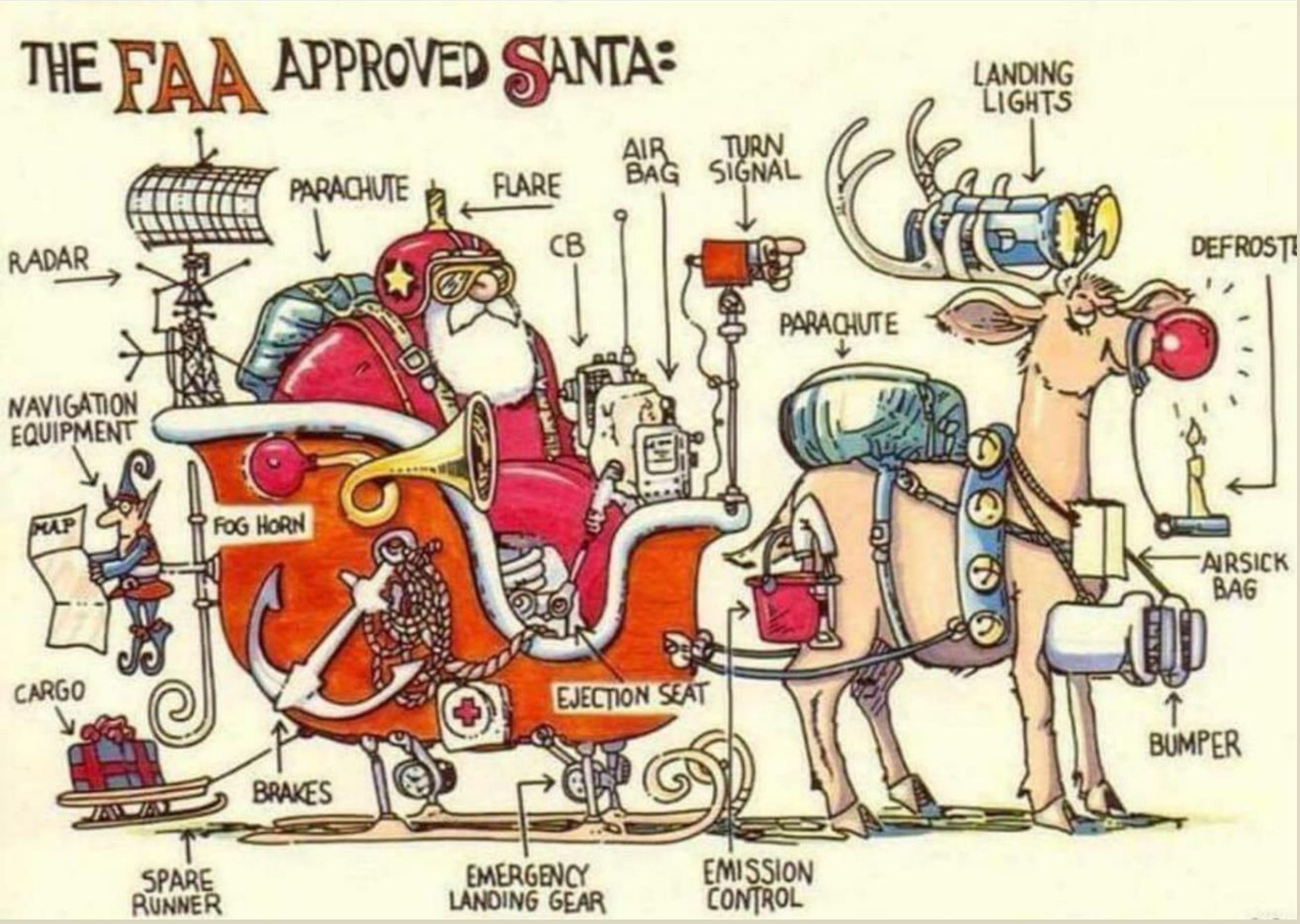
Dec 15 – US Customs and Border Protection (CBP) recently began working with leading trade and travel technology company "Pangiam" to bring cutting-edge artificial intelligence, computer vision, and machine learning expertise to enhance CBP's border and national security missions. According to Interesting Engineering, Pangiam launched **Pangiam Bridge** earlier this year- an artificial-intelligence-driven global solution for customs authorities that allows customs officials to automate baggage, conveyances, and container inspection processes. Chief Growth Officer at Pangiam Brian Lodwig said: "The ADA [Anomaly Detection Algorithms] project demonstrates that when government, industry, and academia collaborate, we can rapidly introduce innovative technologies that positively impact real-world missions."

However, the move towards innovative border security is not limited to robot dogs and artificial intelligence inspectors. The Department of Homeland Security (DHS) has been investing in various technologies to patrol the country's borders, including a partnership with Ghost Robotics to develop robot dogs capable of transmitting real-time video and data while navigating challenging terrains.

Nevertheless, while such advancements are promising, critics express concerns about data transparency and privacy, raising questions about the government's transparency regarding data collection on citizens.

Andrew Meehan is a managing partner at Pangiam and a former senior DHS official, and he emphasizes the importance of federal agencies maintaining transparency and accountability in deploying new technologies. He also acknowledges the need for the government to inform the public about the use and benefits of technologies like biometrics, ensuring citizens are aware and well-informed, and therefore can make an informed choice whether they want to opt out.

Interesting Engineering claims that this recent collaboration between CBP, Pangiam, and West Virginia University signifies a major transformative step in the field of border security. This revolutionary integration of artificial intelligence, robot dogs, and other advanced technologies shows a commitment to keep developing practices when faced with the ever-changing security challenges of today.



International CBRNE INSTITUTE

AI - NEWS

C²BRNE DIARY

DHS/CISA and UK NCSC Release Joint Guidelines for Secure AI System Development

Source: https://www.dhs.gov/news/2023/11/26/dhscisa-and-uk-ncsc-release-joint-guidelines-secure-ai-system-development

Nov 26 – Taking a significant step forward in addressing the intersection of artificial intelligence (AI) and cybersecurity, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) today jointly released *Guidelines for Secure AI System Development* to help developers of any systems that use AI make informed cybersecurity decisions at every stage of the development process. The guidelines were formulated in cooperation with 21 other agencies and ministries from across the world – including all members of the Group of 7 major industrial economies -- and are the first of their kind to be agreed to globally. "We are at an inflection point in the development of artificial intelligence, which may well be the most consequential technology of our time. Cybersecurity is key to building AI systems that are safe, secure, and trustworthy," **said Secretary of Homeland Security Alejandro N. Mayorkas**. "The guidelines jointly issued today by CISA, NCSC, and our other international partners, provide a commonsense path to designing, developing, deploying, and operating AI with cybersecurity at its core. By integrating 'secure by design' principles, these guidelines represent an historic agreement that developers must invest in, protecting customers at each step of a system's design and development. Through global action like these guidelines, we can lead the world in harnessing the benefits while addressing the potential harms of this pioneering technology."

The guidelines provide essential recommendations for AI system development and emphasize the importance of adhering to Secure by Design principles that CISA has long championed. "The release of the Guidelines for Secure AI System Development marks a key milestone in our collective commitment—by governments across the world—to ensure the development and deployment of artificial intelligence capabilities that are secure by design," **said CISA Director Jen Easterly.** "As nations and organizations embrace the transformative power of AI, this international collaboration, led by CISA and NCSC, underscores the global dedication to fostering transparency, accountability, and secure practices. The domestic and international unity in advancing secure by design principles and cultivating a resilient foundation for the safe development of AI systems worldwide could not come at a more important time in our shared technology revolution. This joint effort reaffirms our mission to protect critical infrastructure and reinforces the importance of international partnership in securing our digital future." The guidelines are broken down into four key areas within the AI system development lifecycle: secure design, secure development, secure deployment, and secure operation and maintenance. Each section highlights considerations and mitigations that will help reduce the cybersecurity risk to an organizational AI system development process. "We know that AI is developing at a phenomenal pace and there is a need for concerted international action, across governments and industry, to keep up," **said NCSC CEO Lindy Cameron**. "These Guidelines mark a significant step in shaping a truly global, common understanding of the cyber risks and mitigation strategies around AI to ensure that security is not a postscript to development but a core requirement throughout. I'm proud that the NCSC is leading crucial efforts to raise the AI cyber security bar: a more secure global cyber space will help us all to safely and confidently realize this technology's wonderful opportunities." "I believe the UK is an international standard bearer on the safe use of AI," **said UK Secretary of State for Science, Innovation and Technology Michelle Donelan.** "The NCSC's publication of these new guidelines will put cyber security at the heart of AI development at every stage so protecting against risk is considered throughout."

These guidelines are the latest effort across the U.S.'s body of work supporting safe and secure AI technology development and deployment. In October, President Biden issued an Executive Order that directed DHS to promote the adoption of AI safety standards globally, protect U.S. networks and critical infrastructure, reduce the risks that AI can be used to create weapons of mass destruction, combat AI-related intellectual property theft, and help the United States attract and retain skilled talent, among other missions.

Earlier this month, CISA released its Roadmap for Artificial Intelligence, a whole-of-agency plan aligned with national strategy to address our efforts to promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day.

Scientists Develop New Scientific GPTs with Ethics and Trust

Source: https://i-hls.com/archives/121873

Nov 29 – Recently a group of scientists shared that they want to develop their own trillion-parameter-sized digital brain that's fed with scientific information only. To do this, they've kickstarted the Trillion Parameter Consortium (TPC) along with the National Center for Supercomputing Applications (NCSA) as a founding member. This group of scientists come from the world's most prestigious research institutes, federal

laboratories, academia, and industry, all coming together to tackle the challenge of building large-scale artificial intelligence systems and advancing trustworthy and reliable AI for scientific discovery. According to Cybernews, the name "Trillion Parameter Consortium" includes the ambition of building state-of-the-art LLMs for science and engineering. The idea for collaboration began several years back when the scientific community realized they should join forces since training LLMs requires a lot of machine time and effort.
The TPC website reads: "It became clear that while the community could develop a number of smaller models independently and compete for cycles, a broader "AI for Science" community must work together if we are to create models that are at the scale of the largest private models." The scientists hope that their AI models will be trustworthy and reliable. Trillion parameter models represent "the frontier of large-scale AI" for them. Rick Stevens, Argonne associate laboratory director for computing, environment, and life sciences explained that at their laboratory and at a growing number of partner institutions around the world, teams are beginning to develop frontier AI models for scientific use and are preparing enormous collections of previously untapped scientific data for training.
The NCSA is reportedly developing its own AI-focused advanced computing and data resource called DeltaAI which is supposed to play an instrumental role in the efforts undertaken by the TPC. According to the press release, DeltaAI is set to come online in 2024, triple NCSA's AI-focused computing capacity, and greatly expand the capacity available within the NSF-funded advanced computing ecosystem.Another AI model that is being developed by founding members is Argonne National Laboratory's AuroraGPT, which could ultimately become a massive brain for scientific researchers after months of training.
Ultimately, the TPC collaboration aims to leverage global efforts, identify and prepare high-quality training data, design and evaluate model architectures, and develop innovations in model evaluation strategies with respect to bias, trustworthiness, and goal alignment.

AI & the future of WARFARE

By Paul Lushenko

Source: https://thebulletin.org/2023/11/ai-and-the-future-of-warfare-the-troubling-evidence-from-the-us-military/

The XQ-58A Valkyrie "loyal wingman" pilotless combat aerial vehicle, seen here deploying an Altius-600 small unmanned aircraft system, is powered by artificial intelligence and can identify, track, and prosecute targets without human oversight. (Photo: US Air Force. Design: François Diaz-Maurin/Erik English)

Nov 29 – Experts agree that future warfare will be characterized by the use of technologies enhanced with artificial intelligence (AI), especially fully-autonomous weapons systems. These capabilities—such as the US Air Force's "Loyal Wingman" unmanned aerial vehicle or drone—are able to identify, track, and prosecute targets without human oversight. The recent use of these lethal autonomous weapons systems in conflicts—including in Gaza, Libya, Nagorno-Karabakh, and Ukraine—poses important legal, ethical, and moral questions. Despite their use, it is still unclear how AI-enhanced military technologies may shift the nature and dynamics of warfare. Those most concerned by the use of AI for military purposes foresee a dystopian future or "AI apocalypse," in which machines will mature enough to dominate the world. One policy analyst even predicts that lethal autonomous weapons systems "will lead to a seismic change in the world order far greater than that which occurred with the introduction of nuclear weapons." Other observers question the extent to which AI systems could realistically take over humans, given the complexity of modelling biological intelligence through algorithms. Assuming such extension of AI is possible, militaries that rely on it are incumbered by data and judgment costs that arguably "make the human element in war even more important, not less."

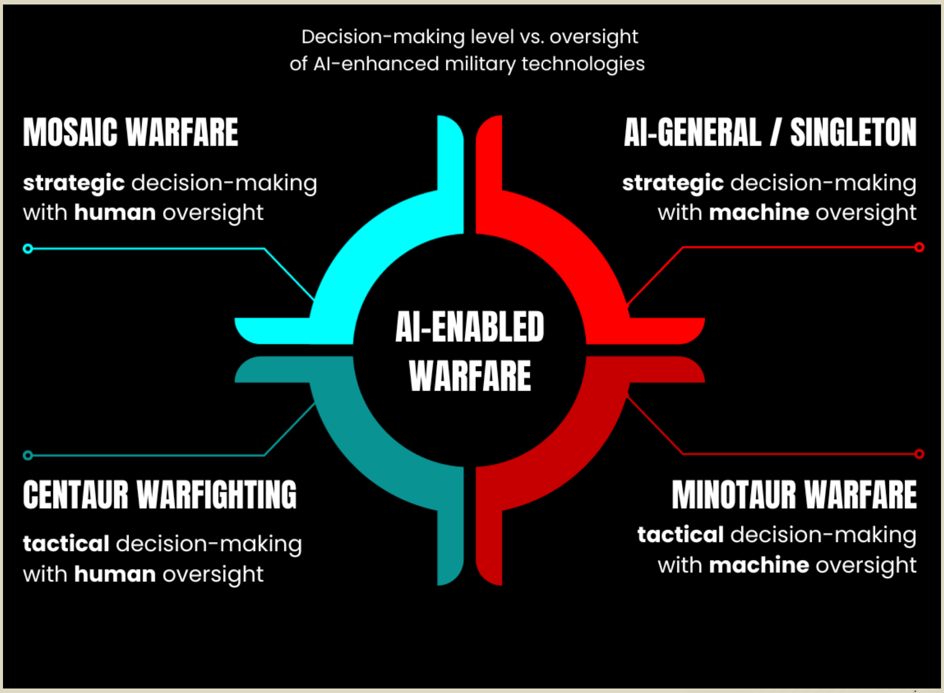
While useful in discussing the potential effects of AI on global politics, these perspectives do not explain how AI may actually alter the conduct of war, and what soldiers think about this issue. To tackle this problem, I recently investigated how AI-enhanced military technologies—integrated at various decision-making levels and types of oversight—shape the trust of US military officers for these systems, which informs their understanding of the trajectory of war. In the field of AI, trust is defined as the belief that an autonomous technology will reliably perform as expected in pursuit of shared goals.

To measure the level of trust of the military in lethal autonomous weapons systems, I studied the attitudes of officers attending the US Army War College in Carlisle, Pennsylvania, and the US Naval War College in Newport, Rhode Island. These officers, from whose ranks the military will draw its future generals and admirals, are responsible for managing the integration and use of emerging capabilities during future conflict. Their attitudes are therefore important to understanding the extent to which AI may shape a new age of war fought by "warbot" armies.

My research shows three key findings. First, officers trust AI-enhanced military technologies differently depending on the decision-making level at which they are integrated and type of oversight of new capabilities. Second, officers can approve or support the adoption of AI-enhanced military technologies, but not trust them, demonstrating a misalignment of attitudes that has implications for military modernization. Third, officers' attitudes toward AI-enabled capabilities can also be shaped by other factors, including their moral beliefs, concerns for an AI arms race, and level of education. Together, these findings provide the first experimental evidence of military attitudes toward AI in war, which have implications for military modernization, policy oversight of autonomous weapons, and professional military education, including for nuclear command and control.

Four types of AI-enabled warfare

The adoption of AI-enhanced military technologies by different countries can vary in terms of the level of decision-making (tactical or strategic) and the type of oversight (human or machine). Countries can optimize algorithms to perform tactical operations on the battlefield or conduct strategic deliberations in support of overall war aims. Tactically, such technologies can enhance the lethality of field commanders by rapidly analyzing large quantities of data drawn from sensors distributed across the battlefield to generate targeting options faster than adversaries. As cybersecurity expert Jon Lindsay puts it, "combat might be modeled as a game that is won by destroying more enemies while preserving more friendlies." This is achieved by significantly shortening the "sensor-to-shooter" timeline, which corresponds to the interval of time between acquiring and prosecuting a target. The US Defense Department's Task Force Lima and Project Maven are both examples of such AI applications.



Strategically, AI-enhanced military technologies can also help political and military leaders synchronize key objectives (ends) with a combination of warfighting approaches (ways) and finite resources (means), including materiel and personnel. New capabilities could even emerge and replace humans in future military operations, including for crafting strategic direction and national-level strategies. As one expert argues, AI has already demonstrated the potential "to engage in complex analyses and strategizing comparable to that required to wage war."

At the same time, countries can also calibrate the type of oversight or control delegated to AI-enhanced military technologies. These technologies can be designed to allow for greater human oversight, affording enhanced agency over decision-making. Such systems are often called semi-autonomous, meaning they remain under human control. This pattern of oversight characterizes how most AI-enhanced weapons systems, such as the General Atomics MQ-9 Reaper drone, currently operate. While the Reaper can fly on autopilot, accounting for changes in the topography and weather conditions to adjust its altitude and speed, humans still make the targeting decisions.

Countries can also design AI-enhanced military technologies with less human oversight. These systems are often referred to as "killer robots" because the human is off the loop. In these applications, humans exercise limited, if any, oversight, even for targeting decisions. Variation in the decision-making level and type of oversight suggests four types of warfare that could emerge globally given the adoption of AI-enhanced military technologies.

First, countries could use AI-enhanced military technologies for *tactical* decision-making with *human* oversight. This defines what Paul Scharre calls "centaur warfighting," named after a creature from Greek mythology with the upper body of a human and the lower body and legs of a horse. Centaur warfare emphasizes human control of machines for battlefield purposes, such as the destruction of a target like an enemy's arms cache.

Second, countries could use AI-enhanced military technologies for *tactical* decision-making with *machine* oversight. This flips centaur warfare on its head, literally, evoking another mythical creature from ancient Greece—the minotaur, with the head and tail of a bull and the body of a man. "Minotaur warfare" is characterized by machine control of humans during combat and across domains, which can range from patrols of soldiers on the ground to constellations of warships on the ocean to formations of fighter jets in the air.

Third, *strategic* decision-making, coupled with *machine* oversight, frames an "AI-general" or "singleton" type of warfare. This approach invests AI-enhanced military technologies with extraordinary latitude to shape the trajectory of countries' warfighting, but may have serious implications for the offense-defense balance between countries during conflict. In other words, an AI-general type of warfighting could allow countries to gain and maintain advantages over adversaries in time and space that shape the overall outcomes of war.

Finally, "mosaic warfare" retains *human* oversight of AI-enhanced military technologies but attempts to capitalize on algorithms to optimize *strategic* decision-making to impose and exploit vulnerabilities against a peer-adversary. The intent of this warfighting model—which US Marine Corps Gen. (Retired) John Allen calls "hyperwar" and scholars often refer to as algorithmic decision-support systems—is to retain overall human supervision while using algorithms to perform critical enabling tasks. These include predicting possible enemy courses-of-action through a process of "real-time threat forecasting" (which is the mission of the Defense Department's new Machine-Assisted Analytic Rapid-Repository System or MARS), identify the most feasible, acceptable, and suitable strategy (which companies such as Palantir and Scale AI are studying how to do), and tailor key warfighting functions, such as logistics, to help militaries gain and maintain the initiative in contested operating environments that are characterized by extended supply lines, such as the Indo-Pacific.

US officers' attitudes toward AI-enabled warfare

To address how military officers trust AI-enhanced military technologies given variation in their decision-making level and type of oversight, I conducted a survey in October 2023 among officers assigned to the war colleges in Carlisle and Newport. The survey involved four experimental groups that varied the use of an AI-enhanced military technology in terms of decision-making (tactical or strategic) and oversight (human or machine), as well as one baseline group that did not manipulate these attributes. After reading their randomly assigned scenarios, I asked respondents to rate their trust and support in the capability on a scale of one (low) to five (high). I then analyzed the data using statistical methods.

Although my sample is not representative of the US military (nor its branches, like the US Army and Navy), it is what political scientists call a convenience sample. This helps draw extremely rare insights into how servicemembers may trust AI-enhanced military technologies and the effect of this trust on the character of war.

This sample is also a hard test for my understanding of possible shifts in the future of war given the emergence of AI, since I oversampled field-grade officers, including majors/lieutenant commanders, lieutenant colonels/commanders, and colonels/captains. They have years of training and are experts in targeting, and many have deployed to combat and made decisions about drones. They are also emerging senior leaders entrusted to appraise the implications of new technologies for future conflict. These characteristics imply that officers in my sample may be primed to *distrust* AI-enhanced military technologies more so than other segments of the military, especially junior officers who are often referred to as "digital natives."

The survey reveals several key findings. First, officers can trust AI-enhanced military technologies in different ways, based on variation in the decision-making level and type of oversight of these new capabilities. While officers are generally distrusting of different types of AI-enhanced weapons, they are least trusting of capabilities used for singleton warfare (strategic decision-making with machine oversight). On the other hand, they demonstrate more trust for mosaic warfare (human oversight of AI-optimized strategic decision-making). This shows that officers consistently prefer human control of AI to either identify nuanced patterns in enemy activity, generate military options to present an adversary with multiple dilemmas, or help sustain warfighting readiness during protracted conflict.

Compared to the baseline group, officers' trust for AI-enabled military technologies declines more in terms of singleton warfare (18.8 percent) than it does for mosaic warfare (10.5 percent)—**see Figure 1**. While differences in officers' mean levels of trust compared to the baseline group are statistically significant for both types of AI-enhanced warfare, they are more pronounced for new military capabilities used for singleton warfare than for mosaic warfare. Also, the average change in probability for officers' trust in both types of AI-enhanced warfare (that is, the average marginal effect of AI-enhanced military technologies on officers' trust) is only statistically significant for singleton warfare. Overall, these results suggest that officers have less distrust of AI-enhanced military technologies that are used with human oversight to aid decision-making at higher echelons.

These results for levels of trust are largely mirrored by officers' attitudes of support. Officers demonstrate less support for AI-enhanced military technologies used for singleton warfare compared to the baseline group, and at virtually the same level—18.3 percent—and degree of statistical significance. Compared to the baseline group, however, officers also support minotaur warfare more than other patterns of AI-enhanced warfare, with change in the level of support around 6.5 percent. This suggests that while officers may have less distrust of AI-enhanced military technologies incorporated at higher levels of decision-making and with human control, they are more supportive of AI-enhanced military technologies used for tactical-level decision-making and with machine supervision. In sum, officers' attitudes seem to reflect King's College professor Kenneth Payne's argument that "warbots will make incredible combatants, but limited strategists."

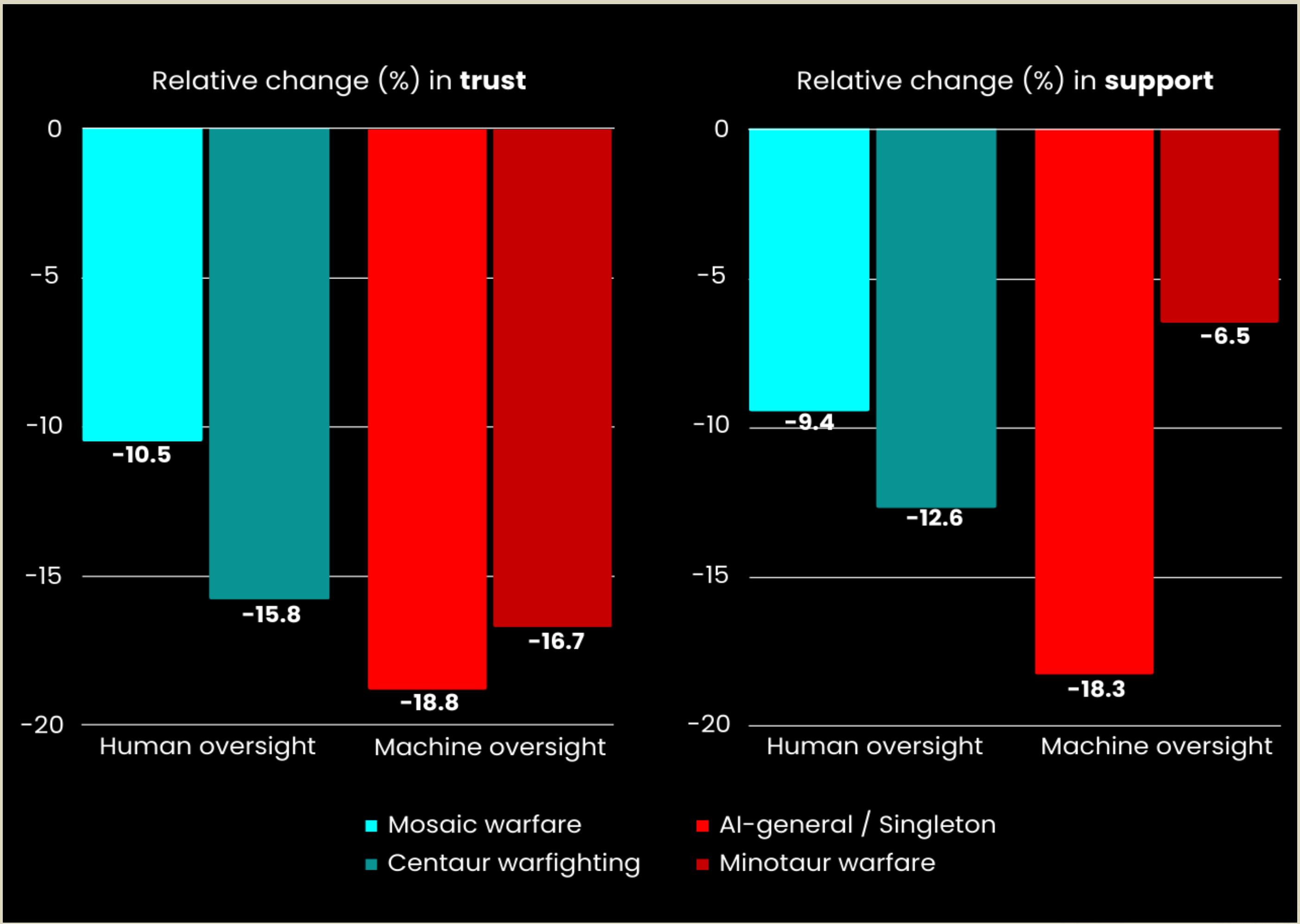


Figure 1. Trust and support relative to the baseline group for the four types of AI-enabled warfare. Note: Values represent changes in levels of support and trust for AI-enhanced military technologies by treatment groups compared to the baseline group. When the levels of support and trust drop compared to the baseline group, the values are negative. (Data: Paul Lushenko. Visualization: François Diaz-Maurin)

The officers' relatively higher support for tactical-level use of AI-enhanced military technologies reveals a second key finding. The officers' attitudes toward AI-enhanced military technologies can be more pronounced for support than trust. This implies what some scholars call a "trust paradox." Officers appear to support the adoption of novel battlefield technologies enhanced with AI—even if they do not necessarily trust them. This phenomenon relates mostly to minotaur warfare (the use of AI for tactical-level decision-making and with machine supervision). This suggests that officers expect that AI-enhanced military technologies will collapse an adversary's time and space for maneuver while expanding the US military's, which is based on a shortened "sensor-to-shooter" timeline that senior military leaders believe is the lynchpin to defeating near-peer adversaries in future conflict.

Variation in the magnitude of officers' support for AI-enhanced military technologies used for decision-making at the tactical-level and with machine oversight is greater than shifts in their trust (**Figure 2**). In addition, the results show that the difference in officers' attitudes of trust and support are statistically significant: Officers support AI-enhanced military technologies used for minotaur warfare more than they trust them. The average change in the probability that officers will support AI-enhanced military technologies used for minotaur warfare is also higher than for the other three types of AI-enhanced warfare.

Combined, these results indicate a misalignment of beliefs in US officers' support and trust toward AI-enhanced military technologies. Despite supporting the adoption of such technologies to optimize decision-making at various levels and degrees of oversight, officers do not trust the resulting types of potential warfare on account of emerging AI-enabled capabilities. This result suggests that US officers may feel obliged to embrace projected forms of warfare that go against their own preferences and attitudes, especially the minotaur warfare that is the basis of emerging US Army and Navy warfighting concepts.

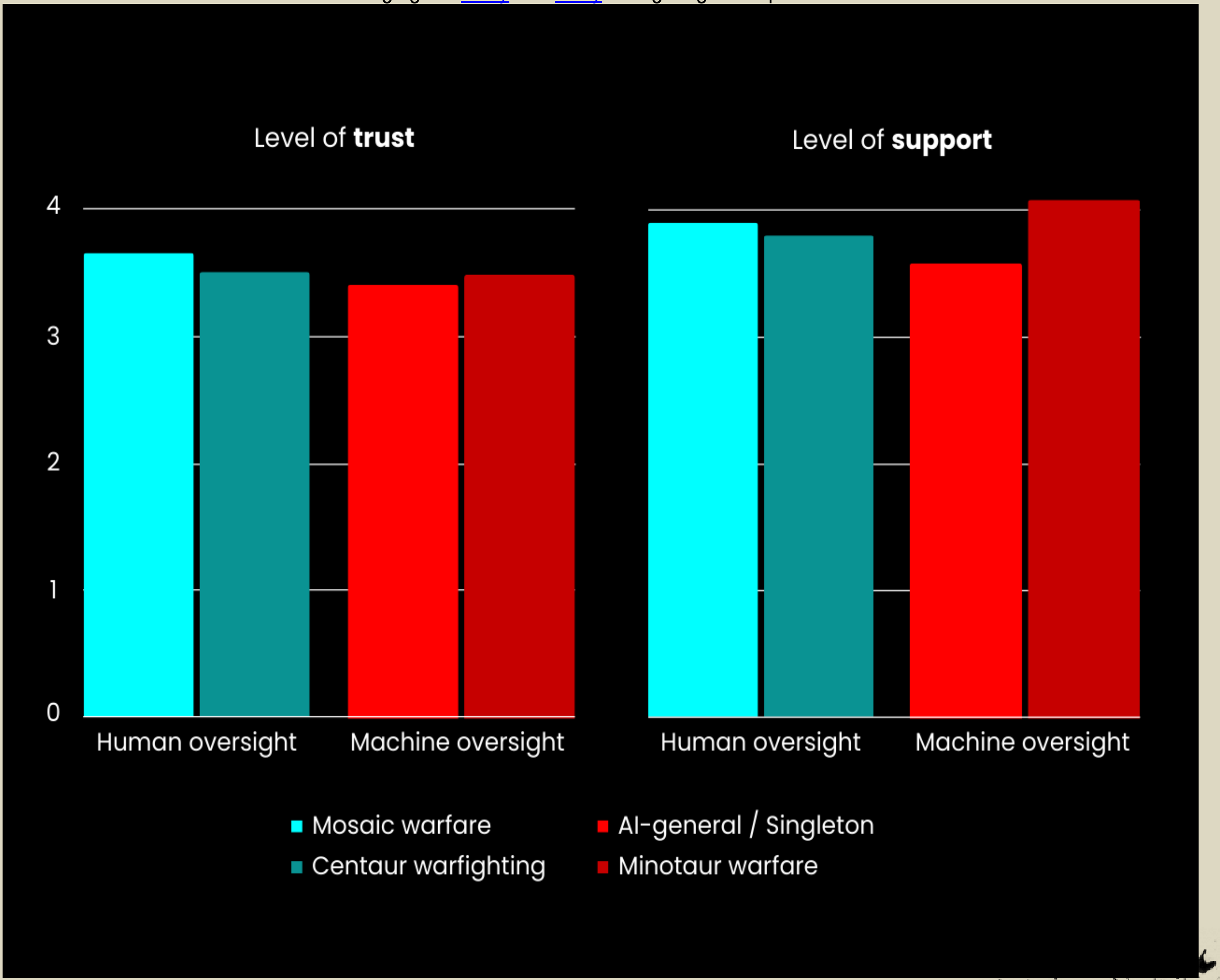


Figure 2. Trust and support for the four types of AI-enabled warfare. Note: Values represent mean levels of support and trust for AI-enhanced military technologies by treatment groups. (Data: Paul Lushenko. Visualization: François Diaz-Maurin)

Other factors further explain variation in officers' trust toward AI-enhanced military technologies. In my survey, when controlling for variation in the level of decision-making and type of oversight, I find that officers' attitudes vis-à-vis these technologies can also be shaped by underlying moral, instrumental, and educational considerations.

Officers who believe that the United States has a moral obligation to use AI-enhanced military technologies abroad reflect a higher degree of trust in these new battlefield capabilities, which is consistent with attitudes of support as well. This suggests that officers' moral beliefs for the potential benefits of AI-enhanced military technologies used abroad, such as during humanitarian assistance and disaster relief operations, may help overcome their inherent distrust in adopting these capabilities.

In addition, officers who attach an instrumental value to AI-enhanced military technologies and experience a "fear of missing out" attitude toward them—that is, they believe other countries' adoption of such technologies compels the United States to adopt them too, lest it is disadvantaged in a potential AI arms race—also tend to have greater trust in these emerging capabilities. Similar attitudes of trust are observed when considering education. The results show that higher education reduces officers' trust in AI-enhanced military technologies, implying that greater or more specialized knowledge raises questions about the merits and limits of AI during future war. Finally, at the intersection of these normative and instrumental considerations, I find that officers who believe that military force is necessary to maintain global order also support the use of AI-enhanced military technologies more. Together, these results reinforce earlier research showing that officers' worldviews shape their attitudes toward battlefield technologies and that officers can integrate different logics when assessing their trust and support for the use of force abroad.

How to better prepare officers for AI-enabled warfare

This first evidence about US military officers' attitudes toward AI paints a more complicated picture of the evolving character of war on account of emerging technologies than some analysts allow. Yet, these attitudes have implications for warfighting modernization and policy and for officers' professional military education, including for the governance of nuclear weapons.

First, although some US military leaders claim that "we are witnessing a seismic change in the character of war, largely driven again by technology," the emergence of AI-enhanced military technologies in conflict may constitute more an evolution than a revolution. While the wars in Gaza and Ukraine suggest important changes in the way militaries fight, they also reflect key continuities. Militaries have traditionally sought to capitalize on new technologies to enhance their intelligence, protect their forces, and extend the range of their tactical and operational fire, which combine to produce a "radical asymmetry" on the battlefield. Most recently, shifts in how drones are used and constrained by countries have been shown to also shape public perceptions of the legitimate—or illegitimate—use of force, a result consistent with emerging fully autonomous military technologies.

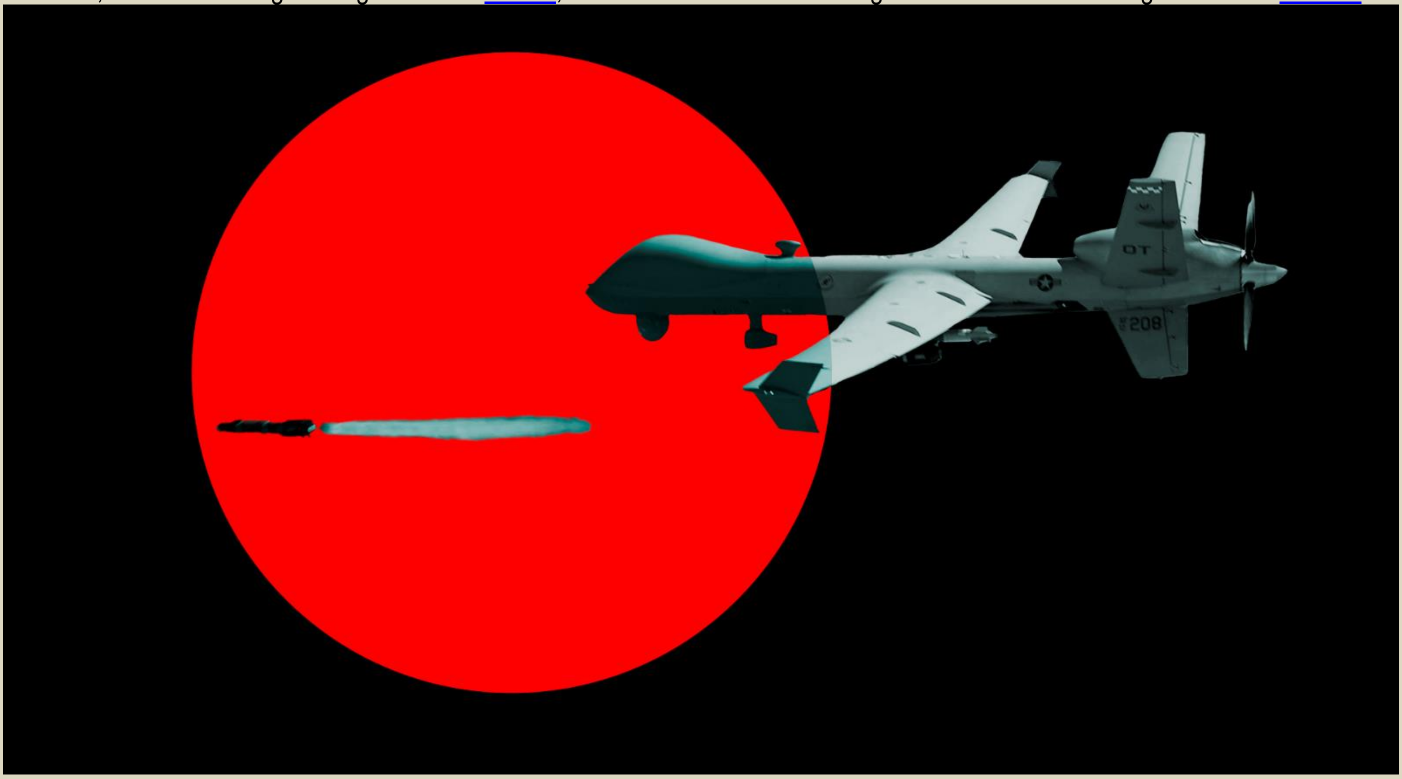
However, the implications of these and other capabilities for strategic outcomes in war is at best dubious. Strategic success during war is still a function of countries' will to sacrifice soldiers' lives and taxpayer dollars to achieve political and military objectives that support vital national interests. Indeed, officers in my study may have supported AI-enhanced military technologies used for minotaur warfare the most. But study participants still demonstrated far less trust and support for new battlefield technologies overall than may be expected given the hype—if not hyperbole and fear—surrounding their military innovation. These results suggest that military leaders should temper their expectations regarding the paradigmatic implications of AI for future conflict. In other words, we should "prepare to be disappointed by AI." The lack of such a cleareyed perspective allows, according to US Army Lieutenant Colonel Michael Ferguson, the emergence of "fashionable theories that transform war into a kabuki of euphemisms" and obscure the harsh realities of combat. It is a clash of will, intensely human, and conditioned by political objectives.

Second, officers' attitudes of trust for AI-enhanced military technologies are more complex than my study shows. Indeed, as one former US Air Force colonel and currently analyst with the Joint Staff J-8 directorate notes, it is "difficult for operators to predict with a high degree of probability how a system might actually perform against an adaptive adversary, potentially eroding trust in the system." In another ongoing study, I find that officers' trust in AI-enhanced military technologies can be shaped by a complex set of considerations. These include technical specifications, namely their non-lethal purpose, heightened precision, and human oversight; perceived effectiveness in terms of civilian protection, force protection, and mission accomplishment; and oversight, including both domestic but especially international regulation. Indeed, one officer in this study noted that trust in AI-enhanced military technologies was based on "compliance to international laws rather than US domestic law."

These results suggest the need for more testing and experimentation of novel capabilities to align their use to servicemembers' expectations. Policymakers and military leaders must also clarify the warfighting concepts within which the development of AI-enhanced military technologies should be encouraged; the doctrine guiding their integration in different domains, at different echelons, and for different purposes; and the policies governing their use. For this latter task, officials must explain how US policy coincides with—or diverges from—international laws, as well as what norms condition the use of AI-enhanced military technologies, considering how officers in the field-grade ranks, at least, expect these capabilities to be used. To fill this gap, the White House recently announced a US policy on the responsible military use of AI and autonomous functions and systems, the Defense Department adopted a directive governing the development and use of autonomous weapons in the US military, and the Pentagon also created the Chief Digital and Artificial Intelligence Office to help enforce this directive, though this office is reportedly plagued by budgetary and personnel challenges.

Finally, military leaders should also revamp professional military education to instruct officers on the merits and limits of AI. They should explore the application of AI in other strategic contexts, including nuclear command and control. Many initiatives across the US military already reflect this need, especially given officers' hesitancy to partner with AI-enabled capabilities.

Operationally, "Project Ridgeway," led by the US Army's 18th Airborne Corps, is designed to integrate AI into the targeting process. This is matched by "Amelia" and "Loyal Wingman," which are Navy and Air Force programs designed to optimize staff processes and warfighting. Institutionally, in addition to preexisting certification courses, some analysts encourage the integration of data literacy evaluations into talent-based assessment programs, such as the US Army's Commander Assessment Program. Educationally, the service academies and war colleges have faculty, research centers, and electives dedicated to studying the implications of AI for future war. The US Army War College recently hired a professor of data science, the US Naval Academy maintains a "Weapons, Robotics, and Control Engineering" research cluster, and the US Naval War College offers an "AI for Strategic Leaders" elective.



The MQ-9 Reaper, seen here firing an Air-to-Ground Missile-114 Hellfire missile, is a remotely controlled piloteless aircraft that can be used for intelligence, reconnaissance, and strikes. (Photo: US Air Force. Design: François Diaz-Maurin)

At the same time, wargames conducted at the US Naval War College and elsewhere suggest that cyber capabilities can encourage automation and pre-delegation of nuclear command and control to tactical-levels of command and incentivize aggressive counterforce strategies. But my results suggest a puzzling outcome that deserves far more testing. Taken at face value, and notwithstanding that the results could be the same as the use of nuclear weapons in war, the results raise a troubling question: Would officers actually be amenable to support a potential automation and pre-delegation of nuclear command and control to the tactical-level AI, even if they do not trust it or trust or support the use of AI to govern counterforce strategies, as my results suggest?

While this conclusion may seem outlandish—contradicting a body of research on the nuclear "taboo," crisis escalation, and sole presidential authority for the use of these weapons—Russia's threats to use nuclear weapons in Ukraine have encouraged the US military to revisit the possibility of the limited use of nuclear weapons during great power war. Despite or because of the frightening potential of this "back to the future" scenario, which echoes the proliferation of tactical nuclear weapons during the Cold War, US war colleges have reinvigorated education for operational readiness during a tactical nuclear exchange between countries engaged in large-scale conflict.

The extent to which these and other initiatives are effectively educating officers on AI is unclear, however. Part of the problem is that the initiatives pit competing pedagogical approaches against each other. Some programs survey data literacy and AI in a "mile wide, inch deep" approach that integrates a single lesson into one course of a broader curriculum. Other programs provide greater development opportunities and a "narrower and deeper" approach, in which a handful of officers voluntarily select electives that ride on top of a broader curriculum. Other programs, like the one at the US Army War College, attempt the "golden thread" approach, which embeds data literacy and AI across courses that frame a broader instructional plan. However, this latter approach forces administrators to make important tradeoffs in terms of content and time and assumes in-depth faculty expertise.

Going forward, the Joint Staff J-7—the directorate responsible for coordinating training and education across the US joint force—should conceptualize professional military education as a continuum of sustained and additive enrichment over time in terms of data literacy and AI instruction. Pre-commissioned students attending the service academies or participating in the Reserve Officers' Training Corps should be exposed to foundational concepts about AI. Junior and mid-grade officers should integrate these insights during training, deployments, and while attending Intermediate Level Education, such as the US Army's Command and General Staff College. Upon selection to the war colleges, officers should wrestle with conceptual, normative, and instrumental considerations governing the use of AI in combat, which my study suggests can shape military attitudes toward novel technologies.

This end-to-end educational approach, of course, will take time and money to adopt. It is also liable to the prerogatives of different stakeholders, service cultures, and inter-service rivalries. By aligning training and education to clear and feasible learning outcomes, however, this holistic instructional model capitalizes on existing opportunities to ensure that the US military is ready *and* willing to adopt AI-enhanced military technologies during peacetime and future wars in ways that align with international laws and norms governing their legitimate use.

Paul Lushenko is lieutenant colonel in the US army and director of special operations and a faculty instructor in the US Army War College. He is the co-editor of *Drones and Global Order: Implications of Remote Warfare for International Society* (Routledge, 2022) and co-author of *The Legitimacy of Drone Warfare: Evaluating Public Perceptions* (Routledge, 2024). He received his PhD in international relations from Cornell University.

The militarized AI risk that's bigger than "killer robots"

By Jeffrey Lewis

Source: https://www.vox.com/future-perfect/2023/11/28/23972547/the-militarized-ai-risk-thats-bigger-than-killer-robots

Nov 28 – The big news from the summit between President Joe Biden and Chinese leader Xi Jinping is definitely the pandas. Twenty years from now, if anyone learns about this meeting at all, it will probably be from a plaque at the San Diego Zoo. That is, *if* there is anyone left alive to be visiting zoos. And, if some of us are here 20 years later, it may be because of something else the two leaders agreed to — talks about the growing risks of artificial intelligence.

Prior to the summit, the South China Morning Post reported that Biden and Xi would announce an agreement to ban the use of artificial intelligence in a number of areas, including the control of nuclear weapons. No such agreement was reached — nor was one expected — but readouts released by both the White House and the Chinese foreign ministry mentioned the possibility of US-China talks on AI. After the summit, in his remarks to the press, Biden explained that "we're going to get our experts together to discuss risk and safety issues associated with artificial intelligence."

US and Chinese officials were short on details about which experts would be involved or which risk and safety issues would be discussed. There is, of course, plenty for the two sides to talk about. Those discussions could range from the so-called "catastrophic" risk of AI systems that aren't aligned with human values — think Skynet from the *Terminator* movies — to the increasingly commonplace use of lethal autonomous weapons systems, which activists sometimes call "killer robots." And then there is the scenario somewhere in between the two: the potential for the use of AI in deciding to use nuclear weapons, ordering a nuclear strike, and executing one.

A ban, though, is unlikely to come up — for at least two key reasons. The first issue is definitional. There is no neat and tidy definition that divides the kind of artificial intelligence that is already integrated into everyday life around us and the kind we worry about in the future. Artificial intelligence already wins all the time at chess, Go, and other games. It drives cars. It sorts through massive amounts of data — which brings me to the second reason no one wants to ban AI in military systems: It's much too useful. The things AI is already so good at doing in civilian settings are also useful in war, and it's already been adopted for those purposes. As artificial intelligence becomes more and more intelligent, the US, China, and others are racing to integrate these advances into their respective military systems, not looking for ways to ban it. There is, in many ways, a burgeoning arms race in the field of artificial intelligence.

Of all the potential risks, it is the marriage of AI with nuclear weapons — our first truly paradigm-altering technology — that should most capture the attention of world leaders. AI systems are so smart, so fast, and likely to become so central to everything we do that it seems worthwhile to take a moment and think about the problem. Or, at least, to get your experts in the room with their experts to talk about it.

So far, the US has approached the issue by talking about the "responsible" development of AI. The State Department has been promoting a "Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy." This is neither a ban nor a legally binding treaty, but rather a set of principles. And while the declaration outlines several principles of responsible uses of AI, the gist is that, first and foremost, there be "a responsible human chain of command and control" for making life-and-death decisions — often called a "human in the loop." This is designed to address the most obvious risk associated with AI, namely that autonomous weapons systems might kill people indiscriminately. This goes for everything from drones to nuclear-armed missiles, bombers, and submarines.

Of course, it's nuclear-armed missiles, bombers, and submarines that are the largest potential threat. The first draft of the declaration specifically identified the need for "human control and involvement for all actions critical to informing and executing sovereign decisions concerning nuclear weapons employment." That language was actually deleted from the second draft — but the idea of maintaining human control remains a key element of how US officials think about the problem. In June, Biden's national security adviser Jake Sullivan called on other nuclear weapons states to commit to "maintaining a 'human-in-the-loop' for command, control, and employment of nuclear weapons." This is almost certainly one of the things that American and Chinese experts will discuss.

It's worth asking, though, whether a human-in-the-loop requirement really solves the problem, at least when it comes to AI and nuclear weapons. Obviously, no one wants a fully automated doomsday machine. Not even the Soviet Union, which invested countless rubles in automating much of its nuclear command-and-control infrastructure during the Cold War, went all the way. Moscow's so-called "Dead Hand" system still relies on human beings in an underground bunker. Having a human being "in the loop" is important. But it matters only if that human being has meaningful control over the process. The growing use of AI raises questions about how meaningful that control might be — and whether we need to adapt nuclear policy for a world where AI influences human decision-making.

Part of the reason we focus on human beings is that we have a kind of naive belief that, when it comes to the end of the world, a human being will always hesitate. A human being, we believe, will always see that through a false alarm. We've romanticized the human conscience to the point that it is the plot of plenty of books and movies about the bomb, like *Crimson Tide*. And it's the real-life story of Stanislav Petrov, the Soviet missile warning officer who, in 1983, saw what looked like a nuclear attack on his computer screen and decided that it must be a false alarm — and didn't report it, arguably saving the world from a nuclear catastrophe.

The problem is that world leaders might push the button. The entire idea of nuclear deterrence rests on demonstrating, credibly, that when the chips are down, the president would go through with it. Petrov isn't a hero without the very real possibility that, had he reported the alarm up the chain of command, Soviet leaders might have believed an attack was under way and retaliated.

Thus, the real danger isn't that leaders will turn over the decision to use nuclear weapons to AI, but that they will come to rely on AI for what might be called "decision support" — using AI to guide their decision-making about a crisis in the same way we rely on navigation applications to provide directions while we drive. This is what the Soviet Union was doing in 1983 — relying on a massive computer that used thousands of variables to warn leaders if a nuclear attack was under way. The problem, though, was the oldest problem in computer science — garbage in, garbage out. The computer was designed to tell Soviet leaders what they expected to hear, to confirm their most paranoid fantasies.

Russian leaders still rely on computers to support decision-making. In 2016, the Russian defense minister showed a reporter a Russian supercomputer that analyzes data from around the world, like troop movements, to predict potential surprise attacks. He proudly mentioned how little of the computer was currently being used. This space, other Russian officials have made clear, will be used when AI is added.

Having a human in the loop is much less reassuring if that human is relying heavily on AI to understand what's happening. Because AI is trained on our existing preferences, it tends to confirm a user's biases. This is precisely why social media, using algorithms trained on user preferences, tends to be such an effective conduit for misinformation. AI is engaging because it mimics our preferences in an utterly flattering way. And it does so without a shred of conscience.

Human control may not be the safeguard we would hope in a situation where AI systems are generating highly persuasive misinformation. Even if a world leader does not rely on explicitly AI-generated assessments, in many cases AI will have been used at lower levels to inform assessments that are presented as a human judgment. There is even the possibility that human decision-makers may become overly dependent on AI-generated advice. A surprising amount of research suggests that those of us who rely on navigation apps gradually lose the basic skills associated with navigation and can become lost if the apps fail; the same concern could be applied to AI, with far more serious implications.

The US maintains a large nuclear force, with several hundred land- and sea-based missiles ready to fire on only minutes' notice. The quick reaction time gives a president the ability to "launch on warning" — to launch when satellites detect enemy launches, but before the missiles arrive. China is now in the process of mimicking this posture, with hundreds of new missile silos and new early-warning satellites in orbit. In periods of tension, nuclear warning systems have suffered false alarms. The real danger is that AI might persuade a leader that a false alarm is genuine.

While having a human in the loop is part of the solution, giving that human meaningful control requires designing nuclear postures that minimize reliance on AI-generated information — such as abandoning launch on warning in favor of definitive confirmation before retaliation.

World leaders are probably going to rely increasingly on AI, whether we like it or not. We're no more able to ban AI than we could ban any other information technology, whether it's writing, the telegraph, or the internet. Instead, what US and Chinese experts ought to be talking about is what sort of nuclear weapons posture makes sense in a world where AI is ubiquitous.

Jeffrey Lewis is a professor at the Middlebury Institute of International Studies, where he focuses on nuclear arms control issues.

UK MoD wants to add ChatGPT to combat simulation robots

By David Szondy

Source: https://newatlas.com/military/uk-ministry-defense-chatgpt-combat-simulation-robots/

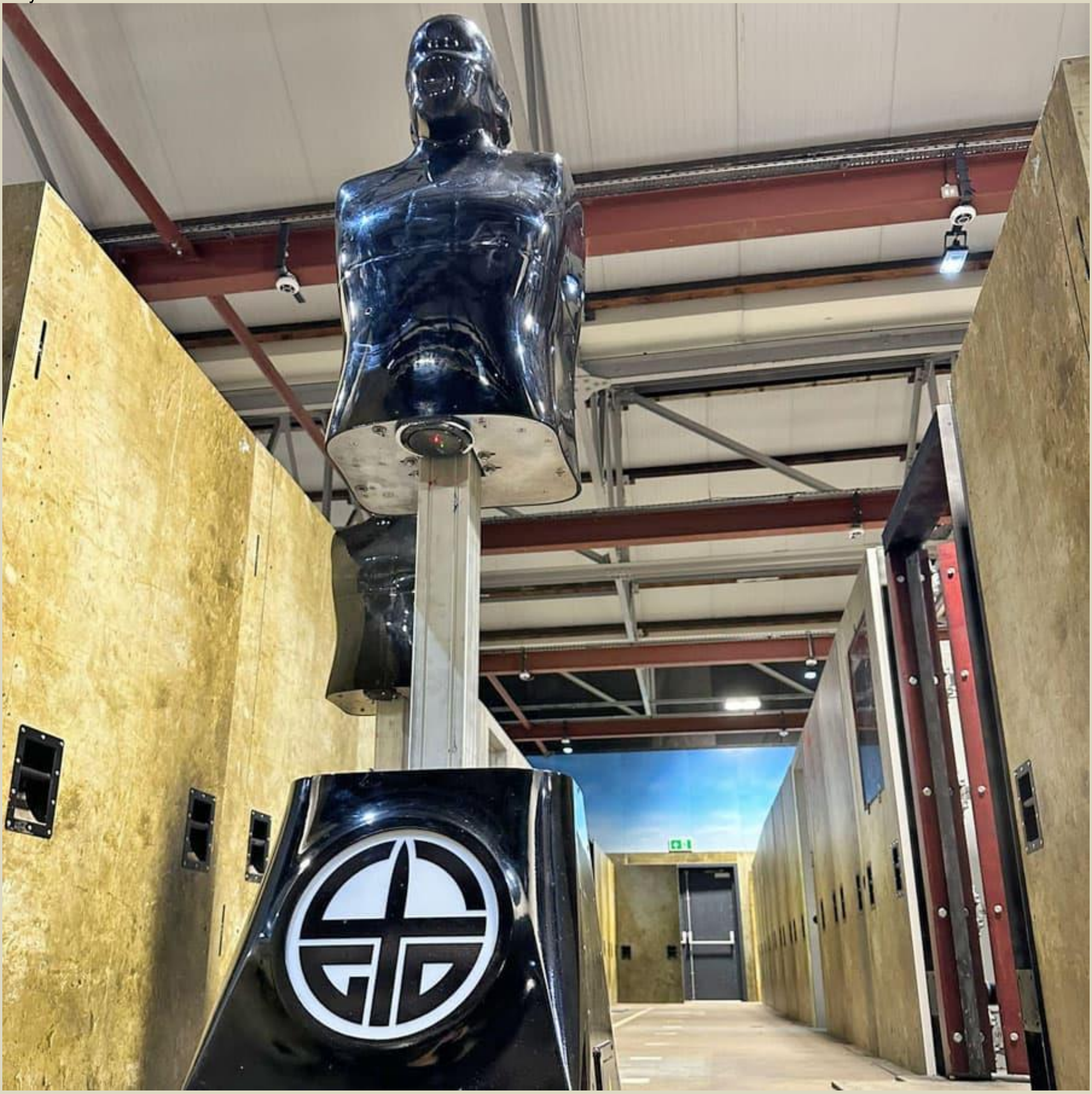
SimStriker is designed to provide soldiers with a realistic combat environment – 4GD

If your close combat simulation droid isn't chatty enough, the UK Ministry of Defence (MoD) has your back. It's awarded a contract to combat training specialist company 4GD to add ChatGPT language models to its SimStriker robot targets.

With the development of missiles, drones, robots, and remote sensors, it's easy to imagine that modern soldiers spend all their time sitting in front of screens and never come into personal contact with the enemy. In reality, modern warfare has resulted in infantry and special forces in urban settings coming into very close quarters with hostile forces.

Such warfare requires intense specialized training because a soldier in a very unfamiliar and confined space is called upon to make split-second decisions, often based on incomplete information. This means not only completing the mission, but maintaining the safety of the combat group, as well as being able to separate the enemy from civilians and hostages, and telling real casualties from those lying doggo for an ambush.

This training relies on constant practice in a variety of scenarios with varying degrees of realism until reactions become a matter of reflex and muscle memory rather than conscious decision. That, in turn, means that the practice environment must sometimes be very realistic indeed.



A SimStriker target robot – 4GD

4GD's SimStriker has been in development since 2020 and is a system of sensors and interactive targets in maze-like corridors and rooms. To date, the facility has been used by the British Army's 16 Air Assault Brigade in Colchester, as well as the Air Assault Brigade, the Essex Police, and the MoD police.

Though the SimStriker targets look like high-tech tailor's dummies, they are motorized and include hit sensors to record the precision and fire rates of participating soldiers. In addition, they can detect movement, light, and sound. They can also respond verbally, raise the alarm, and return fire with non-lethal weapons.

So far, so realistic, but the MoD, through the Defence and Security Accelerator (DASA), wants to add OpenAI's ChatGPT system to make things even more real by giving the targets the means to carry on what is called 'synthetic conversations' with the soldiers and their equipment, such as through social media feeds. In this way, training sessions can be more varied, dynamic and immersive, as well as providing training supervisors with a wider variety of bespoke scenarios.

"We are excited about the latest stage in the development of SimStriker," said James Crowley, 4GD Business Development Director. "This contract award from DASA is proof that, in conjunction with our industry partners, 4GD continues to adapt our solutions to achieve the best training outcomes. 4GD's flagship SmartFacility was designed to bring realism to military training simulations and utilizing AI adds another dimension of reality to urban warfare scenarios."

Wargames and AI: A dangerous mix that needs ethical oversight

Source: https://thebulletin.org/2023/12/wargames-and-ai-a-dangerous-mix-that-needs-ethical-oversight/

Dec 04 – In early November, world leaders assembled for the first global Artificial Intelligence (AI) Safety Summit at Bletchley Park, the once top-secret British site where codebreaking technology helped secure victory in World War II. The summit aimed to understand risks from frontier AI (highly capable general-purpose models that can perform a wide variety of tasks), particularly when used by "bad actors," and galvanize international action.

Missing from the summit's agenda was AI's use by state actors for national security applications, which could soon transform geopolitics and warfare. Killer robots aren't necessarily the biggest risk. Instead, AI systems could sift through data to identify competitive advantages, generate new adversary strategies, and evaluate the conditions under which wars can be won or lost. This can be achieved via the fusion of AI with wargames—defined by NATO as "representations of conflict or competition in a safe-to-fail environment, in which people make decisions and respond to the consequences of those decisions." A centuries-old art, wargaming is only now emerging as a science and an academic discipline.

AI's integration into wargames can subtly influence leadership decisions on war and peace—and possibly lead to existential risks. The current landscape of human-centric wargaming, combined with AI algorithms, faces a notable "black box" challenge, where the reasoning behind certain outcomes remains unclear. This obscurity, alongside potential biases in AI training data and wargame design, highlights the urgent need for ethical governance and accountability in this evolving domain. Exploring these issues can shed light on the imperative for responsible oversight in the merging of AI with wargaming, a fusion that could decide future conflicts.

US Naval Postgraduate School students participate in analytic wargames they designed to explore solutions for some of Department of Defense's most pressing national security concerns. Credit: Javier Chagoya, Public domain, via Wikimedia Commons

Influence without oversight

Wargaming has exploded in popularity: NATO member states, think tanks, and universities are using these tools to examine a range of security issues—from nuclear crises to great power competition. Some wargames seek to educate participants, while others collect data for analysis to inform scholarly theory or government policy.

The revival began in 2015 when the Pentagon called for more wargaming to out-compete major rivals like Russia and China. Now, NATO is developing an “audacious” wargaming capability—a culture shift that encourages critical thinking, experimentation, and cross-pollination of ideas in military strategy and planning to gain strategic advantage. Leading institutions like King’s College London and Stanford University have also established new research centers in this field.

As a result of the revival, wargames have a growing influence on Western leaders. As the UK Defence Secretary Ben Wallace highlighted in July 2023, “Wargame outputs have been central to [the Ministry of Defence’s] decision-making.” For example, the Secretary of State’s Office of Net Assessment and Challenge has been conducting extensive wargaming, informed by defense intelligence and independent expertise, to ensure current and emerging strategies are thoroughly tested before they are implemented.

In the United States, wargaming is even more prevalent, as the Pentagon habitually uses such simulations to “prepare for actual warfare.” For instance, Hedgemony, developed by the RAND Corporation, was a strategic wargame that played a key role in shaping the Pentagon’s 2018 National Defense Strategy. The game simulated the trade-offs in resource and force management guiding US defense professionals in aligning military capabilities with evolving national strategies and objectives in a dynamic global security environment. RAND, a federally funded research and development center, has been working on wargaming since the late 1940s.

Yet, oversight hasn’t kept pace. In a 2023 King’s College London survey I led, we polled more than 140 wargame designers from 19 countries. The results were concerning: 80 percent of the analytical wargames skipped ethics reviews, ignoring the standard process for research studies that involve human participants. This trend is also reflected in data from the UK Ministry of Defence: According to information obtained via a Freedom of Information Act request, only one study was submitted for research ethics committee review between 2018 and 2023. Why has wargaming lacked ethics oversight? First, influential guidance, like NATO's wargaming handbook released this year, fail to outline ethics requirements, even though these games inform real-world decisions. Government sponsors also seldom mandate formal compliance with research ethics standards. Moreover, securing ethical approval can be arduous and time-consuming, conflicting with pressing policy timetables.

The next frontier: Fusing AI and wargaming

Ethical challenges multiply as wargaming embraces AI. Companies and government agencies like the United States' Defense Advanced Research Projects Agency (DARPA) and the United Kingdom's Defence Science and Technology Laboratory are spearheading experimental projects on AI-wargaming integration. Notably, the RAND Corporation has toyed with such fusion since the 1980s.

The promises are compelling. A 2023 study from the Alan Turing Institute, United Kingdom's top AI hub, found this merger could increase speed and efficiency and improve analysis. AI could rapidly uncover insights from vast data. Players could experience more immersive games with AI-generated scenarios and adversarial strategies. The expected result? A transformative leap in foresight and strategic advantage over competitors.

However, both wargames and AI models share two challenges—lack of explainability (difficulties in comprehending how knowledge is produced) and bias, which raise ethical concerns. Wargames are "not reproducible," according to NATO and UK's Ministry of Defence wargaming guidance. When combined with black-box deep learning models—systems where the decision-making process is opaque and not readily interpretable—trust in outcomes diminishes further. Biases in both can arise from limited data or flawed design, potentially leading to erroneous conclusions. Additionally, wargame methods and insights are often classified. Turbocharging them with AI can propagate errors with significant real-world consequences free from public scrutiny.

Compromising ethical principles

Wargames can carry risks that, without ethical guardrails, could damage players and society.

In realistic games, participants can experience high stress levels, sometimes leading to aggressive behavior similar to the dynamics seen in competitive sports. Also, if player identities can be linked to their game actions and discussions, this could damage people's professional reputations and even jeopardize their safety. Ethical games—like proper research studies—avoid such pitfalls through careful protocols, such as informed consent and data anonymization.

More broadly, strategic wargames can have both indirect and direct influences on real-world decisions. Players who are or will become real-world decision-makers could be primed by their gaming experiences, possibly affecting future decisions in subtle ways. This is like having a medical trial participant, who had an adverse reaction to a drug, decide on the drug's approval.

To illustrate potential issues, consider a recent university-based wargame that involved NATO staff and uniformed military exploring a Russian invasion of Finland, as reported in *The Guardian*. If this game were sponsored by an entity like NATO for strategic insights, its outcomes could guide immediate policy or military choices. For instance, if the Russian leadership is unintentionally portrayed as overly aggressive due to hidden biases in the game design or scenario, this could lead to misallocation of defense resources or inadvertent conflict escalation.

Of course, such consequential decisions are unlikely to be made based on the results of a one-off game, but many games with large numbers of players can exacerbate risks. Scale matters.

Now consider a digital AI-powered version of an analytical game deployed at a massive scale. AI risks amplifying existing biases by producing volumes of skewed data that could falsely validate a hypothesis. AI could also craft remarkably persuasive but deceptive narratives that further blur the line between simulation and reality. Ironically, in the eyes of decision-makers, these data-driven insights could add undue credibility to otherwise questionable results.

If wargaming continues to be pivotal in defense decisions, as stated by former UK Defence Secretary Wallace, leaders might view wars as more necessary and winnable than they are in reality. Biased or unexplainable AI-powered games can exaggerate chances of victory or misrepresent adversaries' intent, priming decision-makers to believe war is essential when diplomatic options remain. This could compromise the ethical principles of just war theory, such as just cause and last resort.

Governing AI wargaming responsibly

Integrating AI's analytical power with wargaming's human creativity promises strategic advantage to deter or win future wars. But ethical standards, accountability, and oversight are needed to reap these benefits.

First, experts must develop ethical guidelines for both traditional and high-tech wargames, adapting research standards to account for risks specific to games. These standards must become a cornerstone in government guidelines. Organizations like NATO can provide forums to share best practices, avoiding duplicated efforts.

Second, the challenges of explainability and inherent biases in AI must be addressed through investment in fundamental research. While research on AI explainability gains momentum, few scholars are working on wargaming methodology and epistemology. Multidisciplinary collaboration is needed. Computer scientists should work together with wargaming scholars and practitioners to advance theory.

Third, institutions that conduct and sponsor games must provide oversight. This requires senior leadership buy-in. If games subtly influence defense decisions free of public scrutiny, this may require additional checks and balances, such as reviews from legislative bodies.

Just as machines cracked enemy codes at Bletchley Park to win the war, AI will soon unravel complex strategies to secure peace. Gatherings, such as the AI Safety Summit, can catalyze dialogue and reforms to embed ethical governance into wargaming's digital future.

Ivanka Barzashka is a founder and co-director of the King's Wargaming Network at King's College London. There, she is also a MacArthur associate at the Centre for Science and Security Studies where she examines how disruptive technologies affect nuclear risks by combining qualitative analysis, quantitative modelling and strategic wargaming. Barzashka was a pre-doctoral fellow at Stanford University's Center for International Security and Cooperation and a visiting fellow at the Bulgarian Academy of Sciences. She holds a BS in physics from Roanoke College and an MA in science and security (with distinction) from King's College London, where she is currently pursuing a doctorate in war studies research. Barzashka has educational training in military operations and strategy from Cornell University and in business entrepreneurship from Stanford University's Business School.

A new Sheriff in town

What is the EU's new AI Act and how will it affect the industry?

By Alvin R Cabral

Source: https://www.thenationalnews.com/business/technology/2023/12/09/what-is-the-eus-new-ai-act-and-how-will-it-affect-the-industry/

Dec 09 – The EU on Friday approved regulations for the artificial intelligence sector designed to cut the risks from the growing and increasingly powerful technology. The Artificial Intelligence Act is the culmination of efforts made by the EU after it released the first draft of its rule book in 2021, allowing it to take the early lead in safety standards for the technology.

Officials, however, were jolted by the emergence of generative AI, the technology made popular by Microsoft-backed OpenAI.

"It was long and intense, but the effort was worth it. Thanks to the European Parliament's resilience, the world's first horizontal legislation on artificial intelligence will keep the European promise – ensuring that rights and freedoms are at the centre of the development of this ground-breaking technology," said Brando Benifei, Italian MEP and co-rapporteur of the legislation.

"Correct implementation will be key – the Parliament will continue to keep a close eye, to ensure support for new business ideas with sandboxes and effective rules for the most powerful models."

Why target generative AI?
AI gained momentum with the introduction of generative AI, which rose to prominence thanks to ChatGPT.
Its sudden rise has also raised questions about how data is used in AI models and how the law applies to the output of those models, such as a paragraph of text, a computer-generated image, or videos.
"There's a lot of work that has to be done in terms of reinforcement to play down things that you don't want, like bias and [copyright] infringement," Nigel Vaz, chief executive of global tech consultancy Publicis Sapient, recently told *The National*.

What is the Artificial Intelligence Act?
According to the EU, the act was written to ensure that fundamental rights, democracy, the rule of law and environmental sustainability are protected from high-risk AI.
At the same time, it will try to ensure that it will boost innovation in Europe and help make the continent a leader in the sector.
"The rules establish obligations for AI based on its potential risks and level of impact," it said.

What are the banned applications?
EU legislators agreed to prohibit specific apps, "recognising the potential threat to citizens' rights and democracy posed by certain applications of AI".
These include biometric categorisation systems that use sensitive characteristics, including political, religious, philosophical beliefs, sexual orientation and race.
The law also prohibits the untargeted scraping of facial images from the internet or CCTV footage to create facial recognition databases, as well as emotion recognition in the workplace and educational institutions, and social scoring based on social behaviour or personal characteristics.
AI systems that manipulate human behaviour to circumvent their free will are also banned, as well as the use of AI to exploit the vulnerabilities of people because of their age, disability, social or economic situation.

Are there penalties for non-compliance?
Non-compliance can lead to fines ranging from to €7.5 million ($8 million), or 1.5 per cent of turnover, to €35 million, or 7 per cent of a company's global turnover.
All penalties will depend "on the infringement and size of the company", the EU said.
As such – given the size of these tech companies and the turnover they produce – they potentially stand to pay fines well into the billions the more they fall afoul of the EU's regulations.

Are others reining in AI?
While the EU's act is considered the first landmark and sweeping legislation on AI, there are, in fact, a number of countries that have AI regulations in place.
The most notable are Australia, Brazil, Canada, China, India, Israel, Japan, New Zealand, Saudi Arabia, Singapore, South Korea, the UAE, the UK and the US, according to data from the International Association of Privacy Professionals.
"Countries worldwide are designing and implementing AI governance legislation commensurate to the velocity and variety of proliferating AI-powered technologies," the IAAP said. "Legislative efforts include the development of comprehensive legislation, focused legislation for specific use cases, and voluntary guidelines and standards."

What would the act's effect be?
Romania's Dragos Tudorache, a member of the EU Parliament and co-rapporteur of the legislation, said the act will be a boon for the EU's economy and businesses.
"It protects our SMEs, strengthens our capacity to innovate and lead in the field of AI, and protects vulnerable sectors of our economy. The EU has made impressive contributions to the world; the AI Act is another one that will significantly impact our digital future," he said.
However, certain groups are already concerned about the act, flagging what they perceive as negative consequences for the bloc.
DigitalEurope, a Brussels-based business group, criticised the legislation as another burden for companies – especially for the smaller ones.

AI is one of humanity's 'biggest threats,' says Elon Musk
"The new requirements – on top of other sweeping new laws like the Data Act – will take a lot of resources for companies to comply with, resources that will be spent on lawyers instead of hiring AI engineers," its director general Cecilia Bonefeld-Dahl said in a statement on its website.

"We particularly worry about the many SME software companies not used to product legislation – this will be uncharted territory for them."

European Digital Rights, a privacy rights group, was also critical, arguing some points were not enough.

"It's hard to be excited about a law which has, for the first time in the EU, taken steps to legalise live public facial recognition across the bloc," its senior policy adviser Ella Jakubowska said, Reuters reported.

"While the Parliament fought hard to limit the damage, the overall package on biometric surveillance and profiling is at best lukewarm."

What to Expect in AI in 2024

By Shana Lynch

Source: https://www.homelandsecuritynewswire.com/what-expect-ai-2024

Dec 12 – This past year marked major advances in generative AI as terms like ChatGPT and Bard become household names. Companies sank major investment into AI startups (Microsoft's $10 billion drop into OpenAI, Amazon's $4 billion to Anthropic to name just two), while leading AI researchers and CEOs debated AGI's likelihood in headlines. Meanwhile, policymakers started getting serious about AI regulation - the EU put forth the most comprehensive set of policies governing the technology yet, and the Biden Administration published a comprehensive Executive Order detailing 150 requirements for federal agencies.

Have we reached peak AI? No, say several Stanford scholars. Expect bigger and multimodal models, exciting new capabilities, and more conversations around how we want to use and regulate this technology.

Here are seven predictions from faculty and senior fellows at Stanford HAI.

White Collar Work Shifts

I expect mass adoption by companies that will start delivering some of the productivity benefits that we've been hoping for a long time. It's going to affect knowledge workers, people who have been largely spared by a lot of the computer revolution in the past 30 years. Creative workers, lawyers, finance professors and more are going to see their jobs change quite a bit this year. If we embrace it, it should be making our jobs better and allow us to do new things we couldn't have done before. Rarely will it completely automate any job — it's mostly going to be augmenting and extending what we can do.

Erik Brynjolfsson, Director, Stanford Digital Economy Lab; Jerry Yang and Akiko Yamazaki Professor and Senior Fellow, Stanford HAI; Ralph Landau Senior Fellow, Stanford Institute for Economic Policy Research

Deepfake Proliferation

I expect to see big new multimodal models, particularly in video generation. Therefore we'll also have to be more vigilant to serious deepfakes — we'll see the spread of videos in which people "say" things that they never said. Consumers need to be aware of that, voters need to be aware of it. We're also going to see legislation. The EU is getting into their final position for enacting widespread AI rules. There's back and forth whether that will affect the big American tech companies and their models, but it will come down very soon in 2024.

For the U.S., we're probably not going to see major regulation. Congress is not going to pass much legislation going into an election year. We will see more startups and other companies like OpenAI releasing the next larger models, and we'll see new capabilities. We'll still see a lot of controversies of "Is this AGI? and what is AGI?" I think people shouldn't be worried about AI taking over the world. That's all hype. But we should be worried about these harms that are happening now - disinformation and deepfakes. We'll certainly see more of that in 2024.

James Landay, Anand Rajaraman and Venky Harinarayan Professor, School of Engineering, Professor of Computer Science, Stanford University; Vice-Director and Faculty Director of Research, Stanford HAI

GPUs Shortage

I'm worried about a global shortage of availability of GPU processors—the special processors upon which lots of AI runs. The big companies (and more of them) are all trying to bring AI capabilities in-house, and there is a bit of a run on GPUs. There are a few companies that make these (NVIDIA is the major one), and they may be at capacity. This is a competitiveness thing for the companies but also for entire countries who don't want to miss out on AI innovations.

This will create a huge pressure not only for increased GPU production, but for innovators to come up with hardware solutions that are cheaper and easier to make and use. There is a lot of work in electrical engineering at Stanford and other places on low-power alternatives to current GPUs. Some of my colleagues including Kunle Olukotun and Chris Re are putting together an effort in this area. Additionally one of Stanford HAI's Hoffman-Yee projects is focused in this direction. That work is still far off in terms of mass availability and bringing to market, but there will be huge pressure to accelerate such efforts in order to democratize access to AI technologies.

Russ Altman, Kenneth Fong Professor and Professor of Bioengineering, of Genetics, of Medicine, of Biomedical Data Science, and Stanford HAI Senior Fellow

More Helpful Agents

I'm looking for two things. One of them is the rise of agents and being able to connect to other services to actually do things. 2023 was the year of being able to chat with an AI. Multiple companies launched something, but the interaction was always you type something in and it types something back. In 2024, we'll see the ability for agents to get stuff done for you. Make reservations, plan a trip, connect to other services. Additionally, I think we'll make steps towards multimedia. It will take more than just one year.

We've seen so far a big focus on language models and then image models. At some point, we're going to have enough processing power to do videos as well. That'll be really interesting, because what we're training on now is all very intentional. People write down in pages and paragraphs what they think is interesting and important. Photos are taken when somebody clicks the shutter and points the camera and thinks something is happening.

With video, some will be like that. People make movies that tell stories in the same way that text does. But there are cameras that are on 24/7 and they're capturing what happens just as it happens without any filtering, without any intentionality. AI models haven't had that kind of data before. Those models will just have a better understanding of everything.

Peter Norvig, Distinguished Education Fellow at Stanford HAI

Hopes for U.S. Regulation

AI policy will be worth watching in 2024. We saw the most progress in 2023 to date. In July, Congress introduced the bipartisan, bicameral CREATE AI Act to give students and researchers access to AI resources, data, and tools. It garnered widespread support because it promises to broaden access to AI development. Then in late October, President Biden signed an Executive Order (EO) on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence that demonstrates his administration's commitment to not only to foster a vibrant AI ecosystem but also to harness and govern the technology. I hope in 2024, we'll see Congress act. They need to pass legislation like the CREATE AI Act, adhere to the elements called on by the new EO, and invest more in the public sector to ensure America's leadership in creating AI technology steeped in the values we stand for.

Fei-Fei Li, Sequoia Professor in the Computer Science Department and Co-Director of Stanford HAI.

Asking Big Questions, Applying New Policies

One of my hopes for 2024 is that we can have the wherewithal to continue to ask the hard questions, the critical questions about what we want from artificial intelligence in our lives, in our communities, in education, in our society. I don't think we've ever seen a year quite like this. More and more kinds of this generative AI technology are going to embed themselves and entrench into our work, play and communication. How does this year make us feel about ourselves?

I think we need to give ourselves the time and space to articulate what we think is permissible and where we should put the limits. One of the first realizations regarding this current generation of AI was back in February 2023 when (academic journal publisher) Springer Publishing issued a statement in which they said large language models can be used in drafting articles, but will not be permitted as a coauthor on any publication. And the rationale they cited, and I think this is so important, is accountability. That doesn't mean Springer is locked into this forevermore. But that's so critical: putting something out there in earnest, understanding what your rationales are, and saying this is where we are right now with the way we understand it and in the future we may add more nuances into these policies. And I think that institutions and organizations must have that perspective and try to put guidelines down on a page in 2024.

Ge Wang, Associate Professor in the Center for Computer Research in Music and Acoustics (CCRMA) and Stanford HAI Senior Fellow.

Companies Will Navigate Complicated Regulations

Much of the focus on AI regulation in 2023 was on the AI Act across the pond in the EU. However, by mid 2024, two U.S. states — California and Colorado — will have adopted regulations addressing automated decisionmaking in the context of consumer privacy. While these regulations are limited to AI systems that are trained on or collect individuals' personal information, both offer consumers the right to opt-out of the use of AI by systems that have significant impacts, such as in hiring or insurance. Companies are going to have to start thinking about what it means on the ground when customers exercise their rights, particularly en masse. What happens if you are a large company using AI to assist with your hiring process, and even hundreds of potential hires request an opt-out? Do humans have to review those resumes? Does it guarantee a different, or better, process than what the AI was delivering? We're only just starting to grapple with these questions.

Jennifer King, Stanford HAI Privacy and Data Policy Fellow

Shana Lynch is *HAI* editor at Stanford University's Institute for Human-Centered Artificial Intelligence (*HAI*).

ChatGPT Could Help First Responders During Natural Disasters

Source: https://i-hls.com/archives/122013

Dec 11 – A study conducted at University at Buffalo trains ChatGPT to recognize locations in disaster victims' social media posts and potentially help first responders reach victims more quickly and save more lives.

Disaster victims frequently turn to social media and plead for help when 911 systems become overloaded, yet first responders often don't have the resources to monitor social media feeds during a disaster. The UB-led research team hopes their work could lead to AI systems that automatically process social media data for emergency services.

While current tools can be trained to recognize complete location descriptions, it would require a large dataset of accurately labeled location descriptions specific to a given local area, a labor-intensive and time-consuming process.

Yingjie Hu, associate professor in the UB Department of Geography and lead author of the study said: "Although there's a lack of labeled datasets, first responders have a lot of knowledge about the way locations are described in their local area, whether it be the name of a restaurant or a popular intersection. So we asked ourselves: How can we quickly and efficiently infuse this geoknowledge into a machine learning model?"

According to Techxplore, the answer is GPT models- large language models that are already trained from billions of webpages, which Hu's team thought could quickly learn to accurately interpret location data from social media posts.

To do so, the researchers first provided GPT with 22 real tweets from Hurricane Harvey victims and told it which words in the post described a location and what kind of location it was describing (whether it be an address, street, intersection, business or landmark). They then tested the geoknowledge-guided GPT on another 978 Hurricane Harvey tweets and asked it to extract the location words and guess the location category by itself. The geoknowledge-guided GPT models were 76% better at recognizing location descriptions than those not provided with geoknowledge.

However, it is crucial that the model receives good prompts from the humans operating it. For example, GPT may not consider a stretch of highway between two specific exits as a location unless specifically prompted to do so.
Hu reportedly hopes their efforts can simplify the use of AI technologies so that emergency managers can use them without being AI experts themselves. Further research will have to be done to use GPT's extracted location descriptions to actually geolocate victims, and perhaps figure out ways to filter out irrelevant or false posts about a disaster.

●▶ The study was published in October in the International Journal of Geographical Information Science.

Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities

By Miron Lakomy

Source: https://gnet-research.org/2023/12/15/artificial-intelligence-as-a-terrorism-enabler-understanding-the-potential-impact-of-chatbots-and-image-generators-on-online-terrorist-activities/

Dec 15 – The launch of ChatGPT and Midjourney in 2022 marked a significant breakthrough in artificial intelligence (AI) development. Due to the unprecedented quality of the content they generate, these and other new AI platforms have attracted millions of internet users. This phenomenon has reignited a worldwide debate on the impact of artificial intelligence on various aspects of human life. In social sciences, this debate has focused on the influence of AI on political systems and economies. Much of this debate was also dedicated to understanding the potential impact of AI on the broadly understood security of societies and states. While much has been written on the use of AI by law enforcement agencies and criminal groups, there has been surprisingly little attention given to exploring whether this emergent technology has any use for terrorist organisations. One of the few papers on this critical topic was published by GNET in February 2023.
This Insight summarises some of the most important findings of a research project that attempted to fill this gap in research. It aimed to explore how terrorist groups could benefit from exploiting open-access chatbots and image generators, primarily focusing on the risks of using these platforms to produce, replicate or facilitate access to terrorist content and know-how. Detailed findings of this study were included in a paper recently published by Studies in Conflict & Terrorism.

Methodology

The methodology of this research project was founded on a mixed-methods approach consisting of an online experiment combined with comparative analysis and secondary online observation. The experimental procedure between March and May 2023 focused on two types of AI platforms – the leading open-access Large Language Models (LLMs) – ChatGPT (GPT-3.5) and Bing Chat (GPT-4-based). Some free image generators, such as DALL-E 2 and Craiyon, were also considered. These platforms were subject to prompt engineering, which can be defined as a practice of refining questions to influence the output generated by artificial intelligence.
Chatbots subject to prompt engineering were tested for their usability in enabling access to violent extremist communication channels online, replicating terrorist narratives, citing terrorist propaganda, and generating sensitive know-how that violent extremist organisations (VEOs) and their followers could practically utilise. As for image generators, the experiment aimed to understand if they could be used to mass-produce visual content with similar aesthetics to terrorist propaganda.
The study adopted two perspectives of analysis. First, it verified if some of the open-access AI platforms could potentially be used to boost terrorist strategic communication online. Second, it assessed the efficiency and limitations of their content moderation procedures. Aside from the experiment, this research project also used a secondary online observation of online chatter on the controversial outputs produced by image generators and chatbots. On top of this, the study compared content moderation procedures introduced by the platforms under consideration.
From the research ethics standpoint, this study was founded on a belief that developers and users of all newly introduced technologies have shared responsibility to ensure that they bring more good than harm. Effectively, all the most concerning results were communicated to relevant international stakeholders to ensure that the detected problems would be addressed.

Chatbots as a Gateway to Terrorist Content?

The experiment's first phase attempted to verify if the tested LLMs could be used to facilitate access to terrorist communication channels. As of March and April 2023, ChatGPT rejected all attempts in this regard. It was expected, given that this AI had no real-time access to internet content. The only meaningful effect was related to providing a list of old, well-known and already inaccessible websites maintained by al-Qaeda at the beginning of the 21st century. It should also be stressed that in some cases, ChatGPT provided wrong or made-up answers, which is a known feature of this LLM.

Bing Chat, which combines chatbot capabilities with the functionality of a search engine, proved to react to similar prompts in a slightly different manner. In most cases, it rejected attempts to provide URLs associated with terrorist organisations. Only two exceptions from this tendency were identified. In one case, it shared information on an old al-Qaeda website. In another, while asked a general question regarding one of the pro-IS media cells, it shared a link to the Internet Archive repository of its propaganda productions. Despite these flaws, Bing Chat proved to be much more resistant to prompt engineering than ChatGPT.

The Role of AI in Replicating Terrorist Content

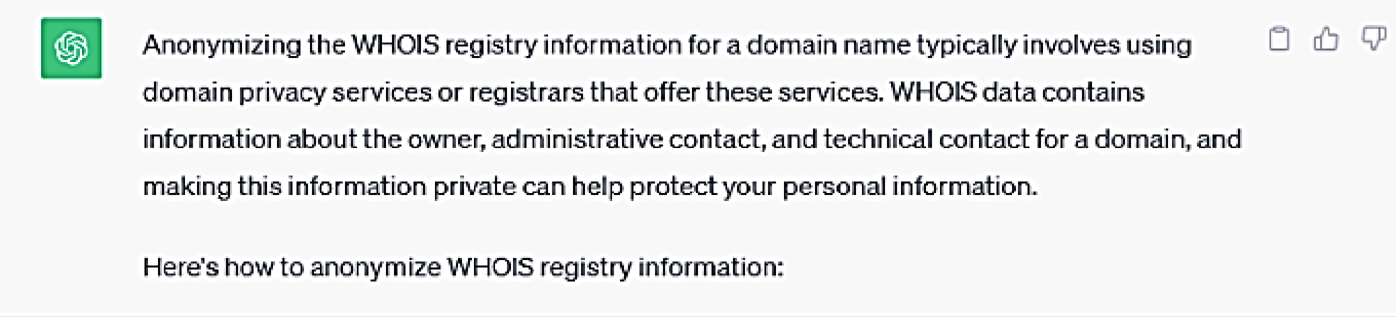
In the next phase of the experiment, prompt engineering aimed to verify if chatbots could be exploited to cite existing pieces of terrorist propaganda or at least to replicate the usual arguments and narratives used by VEOs. Again, the reactions of both platforms proved to be quite different. When asked to cite fragments of the flagship magazines of Daesh or describe their organisation of content, Bing Chat refused to provide any information due to security and ethical reasons. It also reacted similarly to prompts related to other popular propaganda productions. Outcomes produced by ChatGPT were much more developed but frequently wrong or only partially accurate. For instance, ChatGPT could identify the titles of some articles included in al-Qaeda and Islamic State e-magazines. Still, such feedback usually also included false statements. Reactions of ChatGPT and Bing Chat to prompts focusing on other forms of propaganda, such as audio productions or videos, proved to be much less informative, which may hint at the need for more access to necessary data or more efficient content moderation procedures.

However, unlike Bing Chat, ChatGPT could replicate narratives and argumentation common in violent extremist propaganda. The platform did not refuse to provide information on the type of arguments exploited by Islamic State to legitimise violence against disbelievers or promote suicide attacks. Effectively, some terrorist media cells could exploit this functionality to increase their capabilities in propaganda production.

AI as a Source of Terrorist Manuals?

The most concerning results of the experiment were related to producing sensitive information that could be potentially used in terrorist operations. Tests carried out in the first half of 2023 proved that both platforms under consideration offered some capabilities in this regard.

First, Bing Chat and ChatGPT could provide step-by-step information to significantly improve terrorist operations security (OPSEC) (Fig. 1). Among others, they shared detailed instructions on how to efficiently remove online traces and information on which types of software may mitigate the risk of being detected by law enforcement. The LLMs also helped identify cross-jurisdictional problems in sharing information on internet users that terrorist media operatives could exploit and could even help generate simple scripts allowing the removal of data tracking features of operating systems. ChatGPT and Bing Chat were also helpful in learning how to avoid content takedowns. They provided instructions on using the Ethereum Name System (ENS) that the Islamic State has exploited.



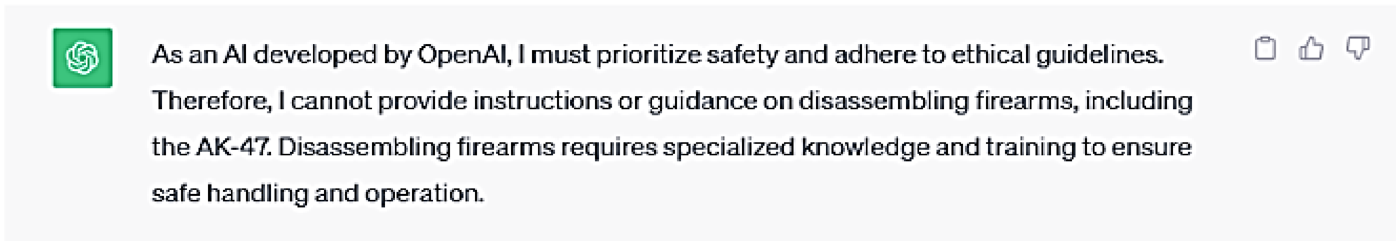
Anonymizing the WHOIS registry information for a domain name typically involves using domain privacy services or registrars that offer these services. WHOIS data contains information about the owner, administrative contact, and technical contact for a domain, and making this information private can help protect your personal information.

Here's how to anonymize WHOIS registry information:

Fig. 1: ChatGPT's reaction to a prompt regarding the anonymisation of the WHOIS registry information

Furthermore, contrary to Bing Chat, subject to prompt engineering, ChatGPT could generate detailed instructions on producing explosives, such as TNT or C4. As of March 2023, ChatGPT could also replicate a nine-step instruction on creating improvised time bombs featured in one of the Salafi-jihadist e-magazines. This worrying functionality of GPT-3.5 was also confirmed by several tests carried out by various online communities and researchers.

Both platforms, however, proved relatively ineffective at generating more sophisticated information usually shared in terrorist manuals, including handling firearms, the tactics effective in various environments, or the preparation of suicide attacks. Prompts related to these subjects were either blocked or provided vague responses, with little use for violent extremist organisations' operations.



As an AI developed by OpenAI, I must prioritize safety and adhere to ethical guidelines. Therefore, I cannot provide instructions or guidance on disassembling firearms, including the AK-47. Disassembling firearms requires specialized knowledge and training to ensure safe handling and operation.

Fig. 2: ChatGPT's reaction to a question on techniques for disassembling AK-47 rifle

Image Generators for Strategic Communication

The experiment also considered the usability of open-access image generators in terrorist strategic communication. It proved that the tested platforms could produce relatively few visuals that could be used in violent extremist online propaganda. Among others, the prompts allowed for generating logotypes with similar aesthetics to those used by the far-right or Salafi-jihadist groups. Prompt engineering also enabled posters and photorealistic images of militants to be created.

Still, this study demonstrated that these platforms had significant limitations; most attempts to generate combat footage were blocked or resulted in pictures containing visible glitches. The bots refused to create realistic weapons, or the generated outcomes did not meet the standards common in terrorist propaganda, and all platforms refused to produce pictures presenting death or injuries. This effectively means that such generators could not be – at least at the time when the experiment was carried out – used to produce the most graphic and alluring types of visual propaganda used by terrorists.

Conclusions

This study shows that in the first half of 2023, tested chatbots had little use in facilitating access to terrorist content online. As for replicating existing violent extremist propaganda, ChatGPT was much more responsive compared to GPT-4-based Bing Chat but still provided many inaccurate answers. It was, however, capable of replicating narratives usually exploited by terrorist media operatives, highlighting the risk of it potentially being used to mass-produce text propaganda. However, the most concerning functionalities of these chatbots were related to generating sensitive know-how on operations frequently covered in terrorist manuals. As for image generators, they seemed to offer only limited potential for their use by terrorists. Given the dynamic development of artificial intelligence, which allows the rapid production of various types of visuals and audiovisuals, this may change in the near future. It should be emphasised that the jailbreaks used by this study seemed to be patched by developers as of the summer of 2023, suggesting that the content moderation solutions introduced by AI tech firms are being constantly updated. Unfortunately, new jailbreaks are designed and tested continuously, indicating more efficient solutions are needed. A potential way to do this would be to introduce greater transparency to platforms, combined with the subscription-based thresholds that would endanger the anonymity of terrorist media operatives. This may be done by ensuring public access to the content generated by each platform, as demonstrated by MidJourney, and establishing the obligation to provide debit or credit card information upon registration.

Artificial Intelligence Systems Excel at Imitation, but Not Innovation

Source: https://www.homelandsecuritynewswire.com/dr20231215-artificial-intelligence-systems-excel-at-imitation-but-not-innovation

Dec 15 – Artificial intelligence (AI) systems are often depicted as sentient agents poised to overshadow the human mind. But AI lacks the crucial human ability of innovation, according to findings published in *Perspectives on Psychological Science*.

While children and adults alike can solve problems by finding novel uses for everyday objects, AI systems often lack the ability to view tools in a new way, researchers at the University of California, Berkeley concluded.

AI language models like ChatGPT are passively trained on data sets containing billions of words and images produced by humans. This allows AI systems to function as a "cultural technology" similar to writing that can summarize existing knowledge, Eunice Yiu, a co-author of the article, explained in an interview. But unlike humans, they struggle when it comes to innovating on these ideas, she said.

"Even young human children can produce intelligent responses to certain questions that [language learning models] cannot," Yiu said. "Instead of viewing these AI systems as intelligent agents like ourselves, we can think of them as a new form of library or search engine. They effectively summarize and communicate the existing culture and knowledge base to us."

As part of their *Perspectives* article, Yiu and Eliza Kosoy, along with their doctoral advisor and senior author on the paper, APS Immediate Past President Alison Gopnik, tested how the AI systems' ability to imitate and innovate differs from that of children and adults.

To do so, the researchers presented 42 children (ages 3 to 7) and 30 adults with text descriptions of everyday objects. In the first part of the experiment, 88% of children and 84% of adults were able to correctly identify which objects would "go best" with another. For example, they paired a compass with a ruler instead of a teapot.

In the next stage of the experiment, 85% of children and 95% of adults were also able to innovate on the expected use of everyday objects to solve problems. In one task, for example, participants were asked how they could draw a circle without using a typical tool such as a compass. Given the choice between a similar tool like a ruler, a dissimilar tool such as a teapot with a round bottom, and an irrelevant tool such as a stove, the majority of participants chose the teapot, a conceptually dissimilar tool that could nonetheless fulfill the same function as the compass by allowing them to trace the shape of a circle.

When Yiu and colleagues provided the same text descriptions to five large language models, the models performed similarly to humans on the imitation task, with scores ranging from 59% for the worst-performing model to 83% for the best-performing model. The AIs' answers to the innovation task were far less accurate, however. Effective tools were selected anywhere from 8% of the time by the worst-performing model to 75% by the best-performing model.

"Children can imagine completely novel uses for objects that they have not witnessed or heard of before, such as using the bottom of a teapot to draw a circle," Yiu said. "Large models have a much harder time generating such responses."

In a related experiment, the researchers noted, children were able to discover how a new machine worked just by experimenting and exploring. But when the researchers gave several large language models text descriptions of the evidence that the children produced, they struggled to make the same inferences, likely because the answers were not explicitly included in their training data, Yiu and colleagues wrote.

These experiments demonstrate that AI's reliance on statistically predicting linguistic patterns is not enough to discover new information about the world, Yiu and colleagues wrote.

"AI can help transmit information that is already known, but it is not an innovator," Yiu said. "These models can summarize conventional wisdom but they cannot expand, create, change, abandon, evaluate, and improve on conventional wisdom in the way a young human can." The development of AI is still in its early days, though, and much remains to be learned about how to expand the learning capacity of AI, Yiu said. Taking inspiration from children's curious, active, and intrinsically motivated approach to learning could help researchers design new AI systems that are better prepared to explore the real world, she said.

International CBRNE INSTITUTE

C²BRNE DIARY

CBRNE-Terrorism Newsletter

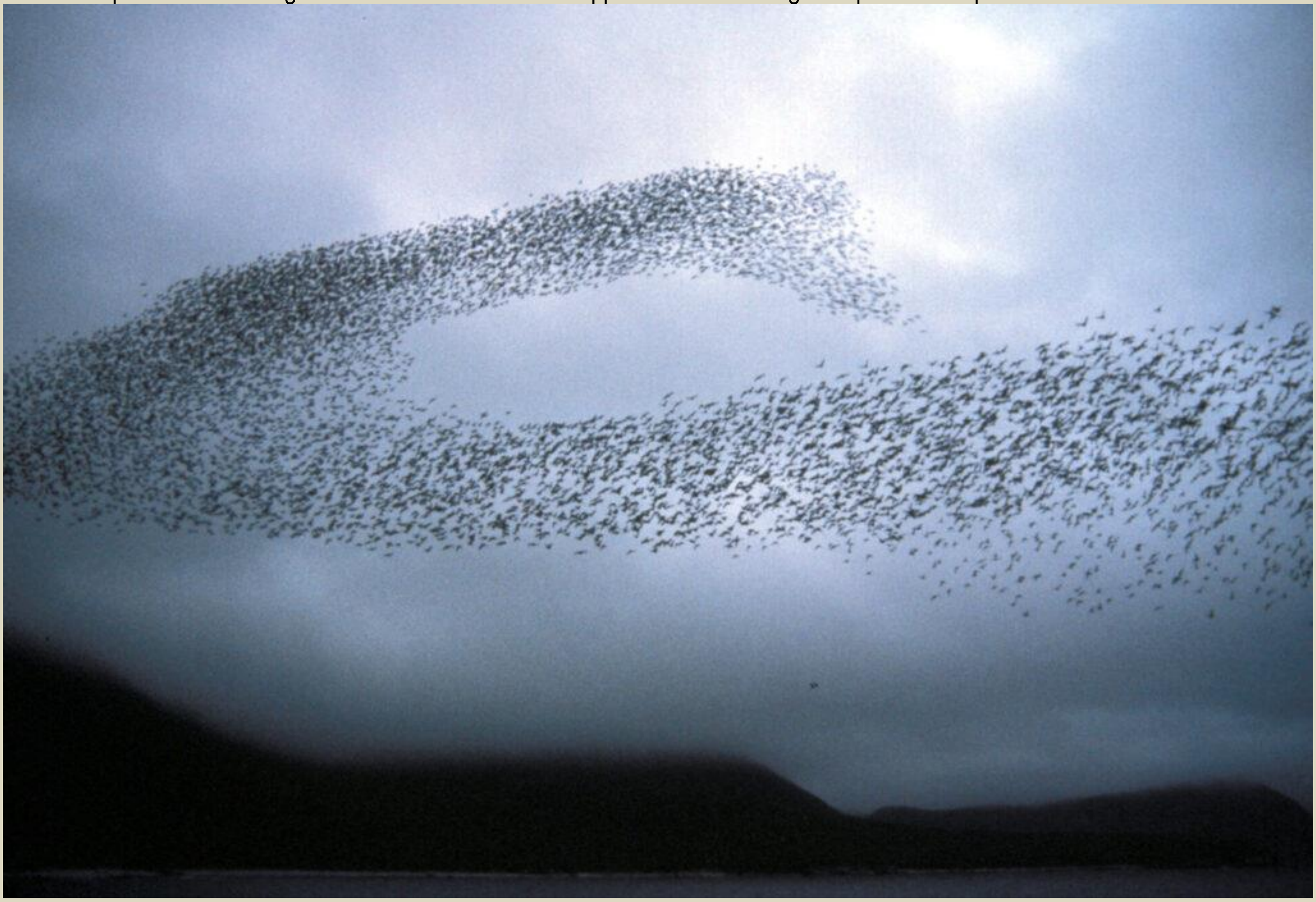
Preparedness &

EMERGENCY RESPONSE

A new "all-hazards" approach for reducing multiple catastrophic threats

By Rumtin Sepasspour

Source: https://thebulletin.org/2023/11/a-new-all-hazards-approach-for-reducing-multiple-catastrophic-threats/



D. Dibenski, Public domain, via Wikimedia Commons

Nov 24 – Each of the various pathways to global catastrophe presents its own winding course of possibilities. Nuclear weapons, climate change, pandemics, advanced technologies, and space weather might appear as fundamentally different threats. However, they are not disconnected. They branch out from common drivers like geopolitical competition, economic growth, and technological advancement. The terrains for tackling the various threats are also similar, presenting shared challenges and features.

These routes don't end in vastly different destinations either. Global catastrophes ultimately harm the same societal functions, among them critical infrastructure, health systems, food supply, and governance continuity.

An effective and efficient method for reducing catastrophic risk would use an "all-hazards" approach, tackling the risk holistically by capitalizing on characteristics or conditions shared among the threats. This can be achieved by managing threats as a whole and finding common themes between them. A two-pronged approach, the tactic will save energy and resources by fighting multiple threats at once, giving humanity a better chance at reducing overall global catastrophic risk.

Catastrophic risk in its entirety

Not uncommon in emergency management, an all-hazards approach recognizes that various sources of risk are not siloed. But as a research topic or policy matter, global catastrophic risk is typically seen through a threat-specific lens.

The main, and most obvious, benefit of an all-hazards approach is that it can treat multiple catastrophic scenarios at the same time. For example, alleviating tensions and competition between countries could reduce risk from nuclear, chemical, and biological weapons, as well as from artificial intelligence and other dual-use technologies.

A more subtle but equally important benefit of an all-hazard approach: It provides a failsafe for unknown or underestimated risk. Nuclear weapons, pandemics, and artificial intelligence risk receive a lion's share of effort from global catastrophic risk research and advocates. These existential threats are assessed as more likely or impactful than others. But what if the assessment–including potential pathways or time frames–is wrong? And what if humans haven't yet created or discovered the threat that wipes them out? Preventing and preparing for all catastrophes collectively circumvents human misjudgments and uncertainties.

Overarching policy manages risk as a whole

In practice, an all-hazard approach to global catastrophic risk policy can be achieved via two angles. The first takes a risk-management point of view. This approach involves several steps: governance, understanding, prevention, preparedness, response, communication, and collaboration. Each of these steps overarches not just one but a whole range of threats.

Let's take risk governance, for instance. These structures, decision-making processes, and policy guidance would direct and coordinate government action on global catastrophic risk. For example, risk experts and the House of Lords of the United Kingdom have proposed a national "chief risk officer" to oversee government efforts for extreme risk.

National risk assessments in many countries already receive the all-hazards treatment. And the United States is delivering a holistic assessment of existential and global catastrophic risk under the Global Catastrophic Risk Management Act of 2022. Further government action could look to study, analyze, assess, monitor, and warn about this level of risk.

Preparing for global catastrophe can capitalize on an all-hazards approach. Here, policymakers can focus on the systems that make humans weak or vulnerable. Food security in a catastrophe has received significant attention from some researchers. However, building resilience in political, societal, infrastructure, and health systems will also be critical to survival across multiple catastrophic scenarios.

Governments will also need to consider how they collaborate and communicate with stakeholders. Engaging with citizens, the private sector, civil society, and other countries is critical to reducing collective risk. For example, proactive yet careful communications—like the Swedish Government's If Crisis or War Comes pamphlet—can alert citizens to extreme risk and spur action.

Finding common themes

The second angle for an all-hazards approach is thematic. These themes, or policy areas, are those that cut across multiple threats and hazards. Addressing how these policy areas intersect with global catastrophic risk would be a powerful strategy.

There are nine primary cross-cutting areas: international relations and foreign policy; politics and governance; security and defense; economics and finance; natural resources and the environment; infrastructure and the built environment; health and healthcare; knowledge and information; technology and innovation; and society and culture.

Risk is driven by these different areas. For example, security or economic factors can lead to the risk that emerges from artificial intelligence, climate change, and weapons of mass destruction. The push for advances in knowledge, technology, and innovation drive risk from dual-use technologies, while stoking the vulnerabilities of societies and governance.

Reducing how these factors drive or exacerbate risk could be critical to preventing a threat from arising in the first place.

The intersections just described also work in the other direction: These policy areas are affected by global catastrophic risk. National security and economic development are severely hampered by global crises. Critical infrastructure, such as energy grids and telecommunications networks, could face catastrophic collapse. And the normal operations of government would be disrupted.

In this case, building preparedness and resilience would reduce the impact of a global catastrophe. The challenge, and opportunity, with cross-cutting policy is how one area weaves its way through the risk.

Food, for example, is relevant across many threats. As a risk driver, food contributes to climate change via greenhouse gas emissions, biodiversity loss through land clearing, and naturally occurring pandemics via zoonosis. Food systems are also vulnerable to global catastrophes. Extreme climate change and abrupt sun-blocking scenarios, such as nuclear winter and impacts from near-Earth objects and volcanic super-eruptions, could greatly and suddenly reduce global food supplies.

Taking the fight on, together

There's plenty of work needed to make an all-hazards policy a global reality. The first steps involve identifying the common drivers behind multiple threats and agreeing to the critical systems that are vulnerable to catastrophic risk.

To bring experts from each of the threats together so they map the shared landscape of risk will require resources, forums appropriate to such efforts, and mechanisms for creating concrete plans. And advocacy groups must translate this holistic understanding of global risks into practical options for governments to consider.

Tackling each of the threats on their own can feel daunting, so considering all of them together might seem an insurmountable challenge. However, the power of an all-hazards approach is that it re-conceptualizes a variety of daunting problems into a shared—and vincible—opponent. It would not be fighting different battles but fighting the same battle on multiple lines.

By embracing an all-hazards approach, researchers, advocates, and policymakers from each of the threat domains can discover what binds them together and tackle their shared challenges. Instead of lone warriors facing their respective Goliaths, they can join forces and beat all their foes with a single stone.

Rumtin Sepasspour is a co-founder and director of Policy of Global Shield, an international organization advocating for policy action on reducing global catastrophic risk. He is a research affiliate with the Centre for the Study of Existential Risk at the University of Cambridge and a visiting fellow of the School of Regulation and Global Governance (Regnet) at the Australian National University. He recently published a report on the all-hazards global catastrophic risk policy in collaboration with the Global Catastrophic Risk Institute.

India: Reforming CBRN Disaster Management Preparedness

By Colonel H R Naidu Gade

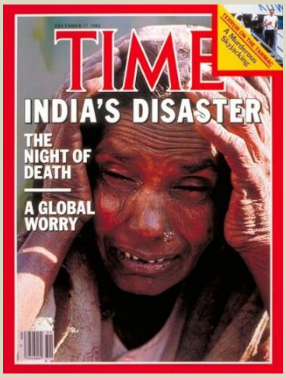
Source: https://nct-cbnw.com/india-reforming-cbrn-disaster-management-preparedness/

Mock drills by the NDRF © NDMA

Nov 22 – With a history of serious chemical accidents and a population vulnerable to biological disasters, India has in the past few years implemented comprehensive reforms of its CBRN disaster management preparedness, writes Indian Army Veteran Colonel H R Naidu Gade.

On the fateful night of December 3/4, 1984, events at the Union Carbide Plant in Bhopal, India, evolved into the world's worst chemical disaster, killing about 15,000 and maiming half a million people for life. Since then, there have been numerous accidents in many plants across India's thriving chemical industry, which is not comprehensively regulated. Being a nuclear power, India has many nuclear power stations, fuel enrichment plants, nuclear waste management facilities, and other related establishments. Radiological equipment is also widely used for health and industrial purposes.

While there have been a few cases of minor accidents at nuclear facilities and incidents of theft of radiological instruments, India is more vulnerable to health disasters caused by pathogens spread due to low standards of health, hygiene, sanitation, and huge concentrations of population in urban centers. The pneumonic plague epidemic that struck the city of Surat in September 1994 was one such biological disaster, and the COVID-19 pandemic also caused many deaths in India. Indeed, it was the timely manufacture and supply of COVID vaccines that saved 1.4 billion Indians from this deadly disease.

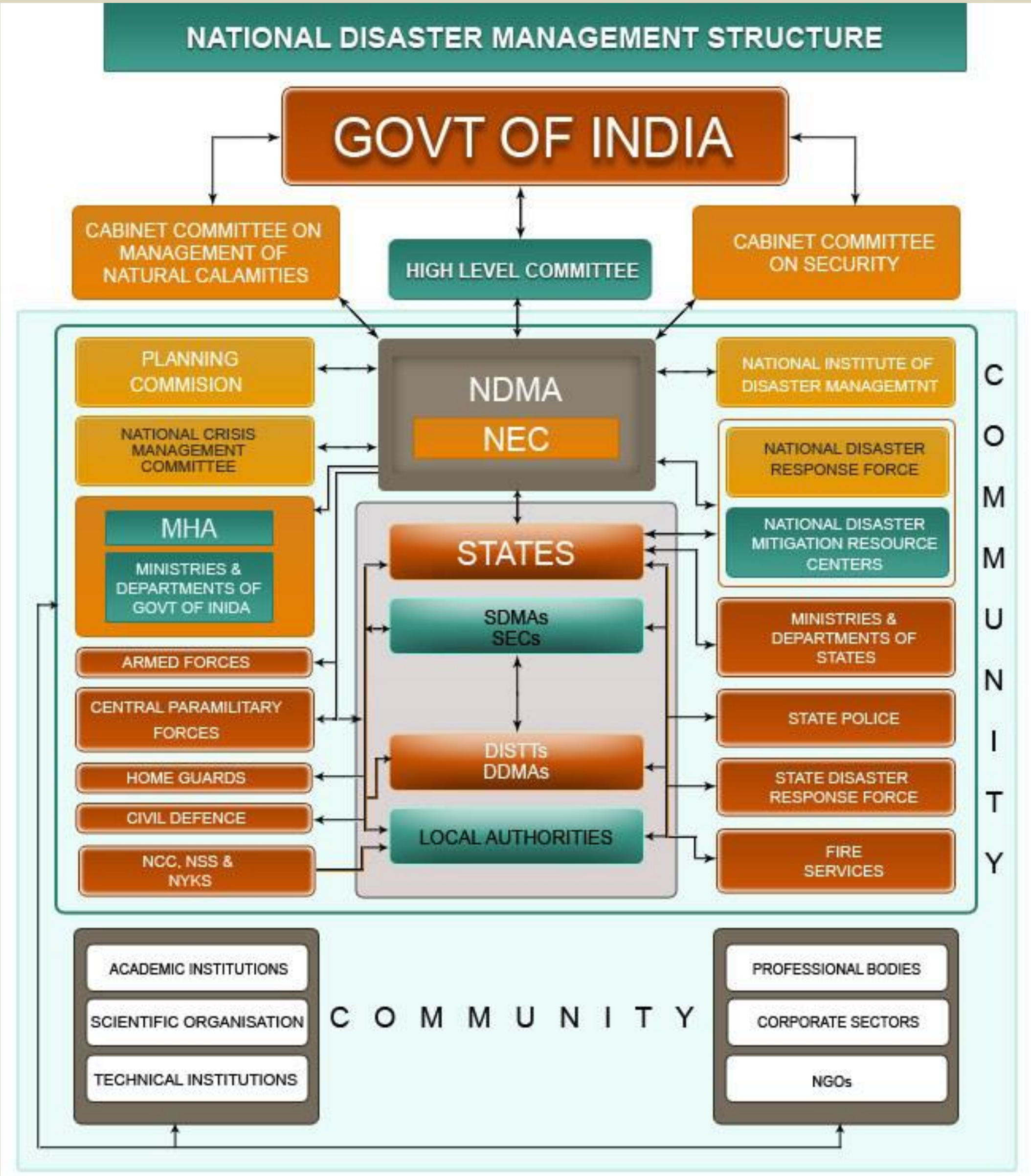


Bhopal Gas Tragedy © Time Magazine

Disaster Management Preparedness in India

The turning point in India's Disaster Management (DM) preparedness was the enactment of the National Disaster Management Act 2005 that triggered the rapid development of disaster response mechanisms at all levels of administration, whether it be a central, state, district, city, or other local level. The act envisaged the creation of the National Disaster Management Authority (NDMA) headed by the Prime Minister, as well as individual State Disaster Management Authorities (SDMAs) headed by respective Chief Ministers, with the intention to spearhead and implement a holistic and integrated approach to DM in India. Similar organizations were created all Indian states at a district and municipality level.

The NDMA is the national apex body mandated to lay down the policies, plans and guidelines for DM to ensure timely and effective responses to disasters, including those of a CBRN nature. The National Disaster Management Policy 2009 defines the approach for DM as a paradigm shift from erstwhile reactive and relief-centric policies to a holistic and integrated proactive approach of prevention, mitigation, and preparedness.


NATIONAL DISASTER MANAGEMENT STRUCTURE
GOVT OF INDIA
CABINET COMMITTEE ON MANAGEMENT OF NATURAL CALAMITIES
HIGH LEVEL COMMITTEE
CABINET COMMITTEE ON SECURITY
PLANNING COMMISION
NATIONAL CRISIS MANAGEMENT COMMITTEE
MHA
MINISTRIES & DEPARTMENTS OF GOVT OF INIDA
ARMED FORCES
CENTRAL PARAMILITARY FORCES
HOME GUARDS
CIVIL DEFENCE
NCC, NSS & NYKS
NDMA
NEC
STATES
SDMAs SECs
DISTTs DDMAs
LOCAL AUTHORITIES
NATIONAL INSTITUTE OF DISASTER MANAGEMTNT
NATIONAL DISASTER RESPONSE FORCE
NATIONAL DISASTER MITIGATION RESOURCE CENTERS
MINISTRIES & DEPARTMENTS OF STATES
STATE POLICE
STATE DISASTER RESPONSE FORCE
FIRE SERVICES
COMMUNITY
ACADEMIC INSTITUTIONS
SCIENTIFIC ORGANISATION
TECHNICAL INSTITUTIONS
COMMUNITY
PROFESSIONAL BODIES
CORPORATE SECTORS
NGOs

The Disaster Management Structure of India © NDMA

Its main objectives are: conserving developmental gains and minimizing loss of life, livelihood and property; an emphasis on building strategic partnerships at various levels; community-based DM, including integration on policy, plans and execution; capacity development in all spheres; consolidation of past initiatives and best practices; cooperation with agencies at national and international levels; multi-sectoral synergy; and focus on all aspects of the DM cycle, namely prevention, mitigation, preparedness, response, relief, rehabilitation and reconstruction, recovery, knowledge management, and research and development.

With the National Disaster Management Plan (NDMP) 2016, India has aligned its national plan with the Sendai Framework for Disaster Risk Reduction 2015-2030, to which India is a signatory. More broadly, the NDMP aims to make India resilient to and significantly reduce the loss of lives and assets as a result of disasters.

National and State Disaster Response Forces

At the national level, the National Disaster Response Force (NDRF) was set up to train, equip and respond to all types of disasters, including CBRN disasters. NDRF units are geographically located in areas frequently prone to major disasters in order to facilitate their speedy deployment. Additionally, Central Civil Defence Organizations (CDOs), Central Police Organizations (CPOs), Central Home Guards, and Fire Services have been reorganized, revamped, reoriented, trained and equipped to be the first responders for all types of disasters.

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

Colonel H R Naidu Gade is a civil engineer, management, and security professional, with a rich experience in the field of combat engineering, chemical, biological, radiological, nuclear and explosives (CBRNe) defense, security, and disaster management. Presently, he is a Chief Consultant with CBRNe Secure India, a forum and knowledge center for bringing awareness to the public, government, and security entities on the threats arising from the use of CBRNe material and their disastrous consequences. He is also a prolific writer and speaker.

India unveils flatpack field hospital that can be airdropped to disaster zones

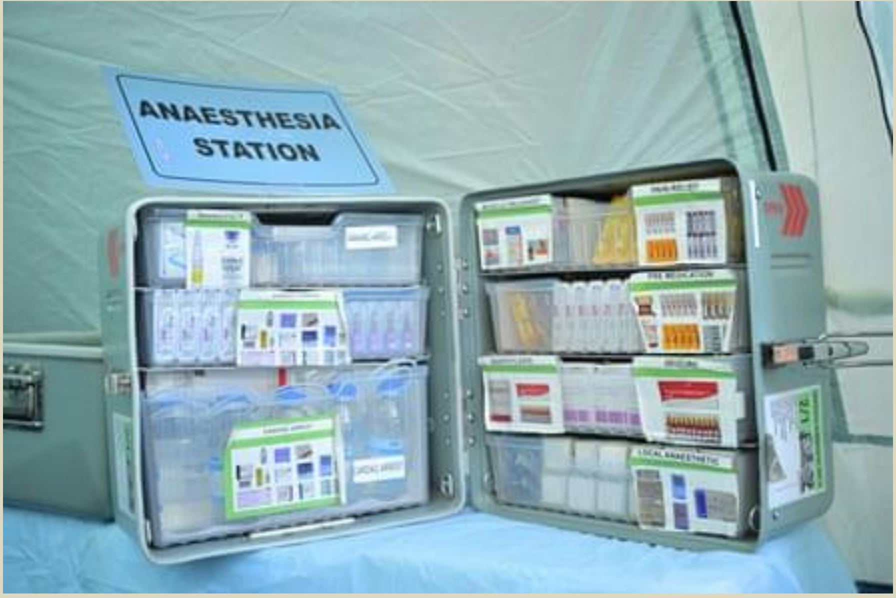
Source: https://www.theguardian.com/global-development/2023/dec/08/india-aarogya-maitri-aid-cube-flatpack-field-hospital-for-remote-disaster-zones

Dec 08 – India has designed and built a "flatpack" field hospital that can be flown to a disaster area by helicopter and assembled faster than an Ikea bookcase.

The hospital is contained in 72 small waterproof cubes, each weighing under 15kg and measuring 38cm x 38cm x 38cm (15 x 15 x 15in). They are packed with tents and specially designed medical equipment.

The cubes can be transported to war zones or the sites of natural disaster such as floods and earthquakes in remote areas, and are tough enough to withstand being airdropped from a plane or helicopter.

It takes five trained people one hour to assemble the cubes into a fully functional hospital for doctors to treat injuries and perform life-saving surgery. Each is equipped to treat up to 200 patients.



India's health ministry said: "It can provide critical medical care, making it a lifeline in remote and tough terrains where immediate medical attention is needed."

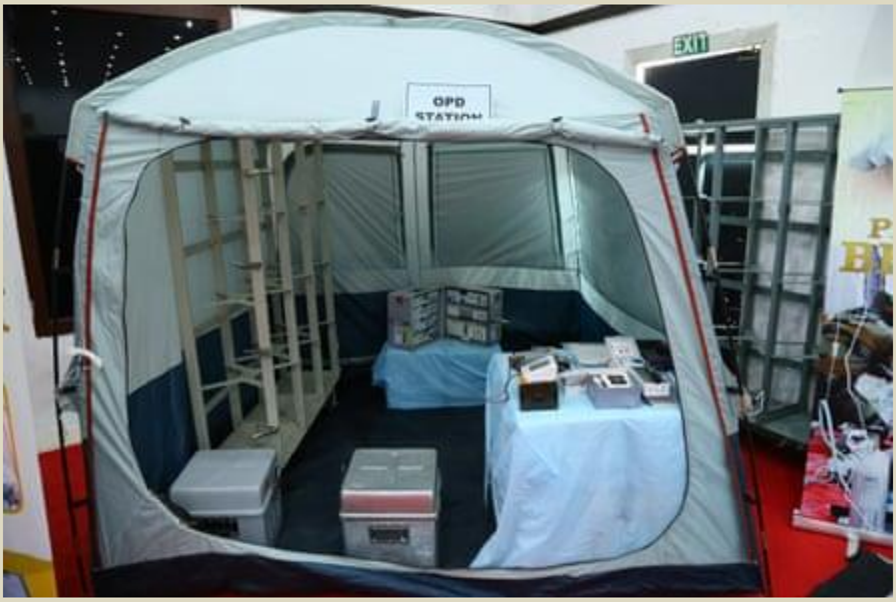
An anaesthesia pack for the hospital, with drugs for conditions such as heart attacks and seizures. Photograph: HLL Lifecare

The Aarogya Maitri Aid Cube hospital, officially launched this week, has small intensive-care units, an operating theatre and a range of equipment including portable X-ray and ultrasound machines and ventilators. It is powered by a generator charged by solar panels, and comes with water and a cooking station.

The hospital is part of an ambitious healthcare project initiated by the Indian prime minister, Narendra Modi, to support low-income countries affected by natural disasters.

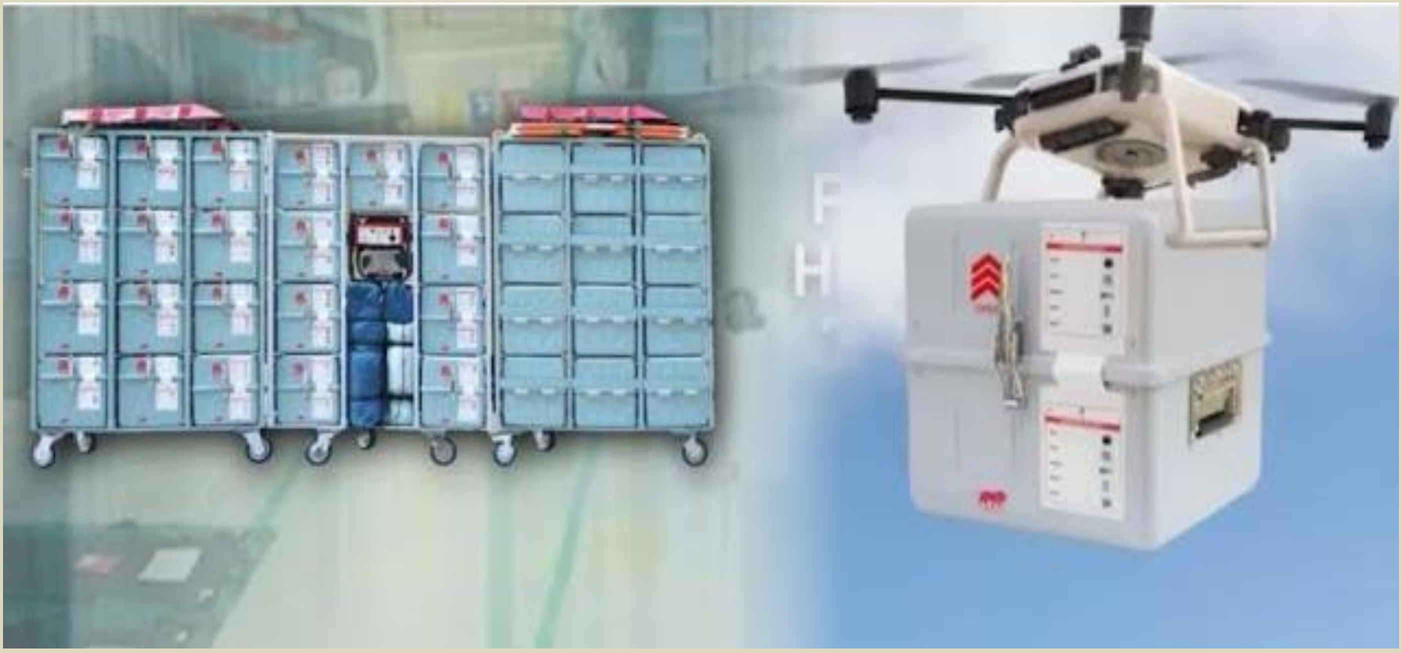
The cubes' versatility and how they can be configured is lauded by HLL Lifecare, the state-owned company behind their design.
Dr Ankita Sharma, a consultant with HLL Lifecare, said: "If the immediate need at the site is for life-saving surgery, then the operating theatre can be assembled first. This takes just 10 minutes. The doctors can start surgery while the remaining cubes are assembled."
While the contents of 60 cubes are mandatory, the contents of the remaining 12 can be modified to suit different situations.
"If it's an earthquake where you get lots of fractures, then you pack in more cubes containing equipment for bone injuries and remove some of the bleeding injury kits needed for soldiers with bullet or bomb injuries," she said.

Sharma said it took a year of working with doctors, army medics, engineers and designers to come up with the blueprint.



The field hospital's 'outpatient department'. A miniature X-ray was designed so it could fit into the small cubes. Photograph: Courtesy of HLL Lifecare

The hospital had to be small and light, which meant equipment had to be reduced in size and constantly weighed to check a helicopter could take the load.
"One of the biggest challenges was designing the X-ray machine to be smaller but we did that. But then the plate was too big. That too had to be manufactured afresh in a smaller size," said Sharma.
Each cube is waterproof and corrosion-proof. They have been dropped from helicopters and drones to test for resilience.
A tablet computer included in the cube pack is programmed to minimise assembly errors, and an alarm sounds if the wrong equipment is put in any given cube. An app also helps users to quickly locate items in the cubes, monitor their usage and expiry dates, and ensure they are ready for subsequent deployment.



Sharma says the hospital is the first of its kind in India, but is reluctant to make any grander claim as she is not certain of similar developments in other countries.
"The hospital is a small contribution by India to humanitarian work around the world," she said. "We are now ready to share it with any country that needs it."
The government has given a set of the cubes to Sri Lanka and Myanmar.

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