08\22

CBRNE DIARY

Dedicated to Global First Responders

August 2022

HELLO Summer

PART B

Needle Jihad?

Al Qaeda chief killed

Langya virus

AI: In 6 hours 1000 components more deadly than VX

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C2BRNE DIARY

DIRTY R-NEWS

Further Indications of Iran's Renewed Interest in Maraging Steel for its Nuclear Enrichment Program

By Sarah Burkhard and David Albright

Source: https://www.homelandsecuritynewswire.com/dr20220723-further-indications-of-iran-s-renewed-interest-in-maraging-steel-for-its-nuclear-enrichment-program

July 23 – A 2021 Atomic Energy Organization of Iran (AEOI) video and International Atomic Energy Agency (IAEA) reporting have revealed Iran's renewed interest in metal bellows in its advanced centrifuges. In the case of the IR-6 centrifuge, this interest may represent the development of a design change, since earlier Iran declared this centrifuge as having carbon fiber bellows. The most logical choice for the metal in these bellows, based on characteristics of gas centrifuges, is maraging steel.

Maraging steel bellows are well known to be used in the IR-2m centrifuge, but Iran has not made any of these centrifuges in years, leading to speculation that the bottleneck was the maraging steel.

Another indication that Iran is intensifying its interest in maraging steel in its centrifuge program is an early 2021 announcement of a translation of a Western textbook on maraging steel. Two researchers affiliated with Iran's Shahid Beheshti University translated a 2009 book about maraging steel, titled "Maraging Steels: Microstructure Modeling, Properties and Applications." The description of the book, part of the 2021 announcement on the website of Shahid Beheshti University, emphasizes properties that are examined, including "corrosion and mechanical properties," especially for use of maraging steel in the nuclear industry. It further highlights that the nuclear industry "requires more sensitivity and precision in the manufacture of parts used in this industry." Another part directly references the need to improve certain parts in the nuclear industry, possibly a direct reference to maraging steel centrifuge components: "The need to improve the quality of various parts in order to increase the efficiency of equipment, access to optimal production processes and reduce production costs, multiplies the importance of material design and its manufacturing process." [1]

The book, originally written by United Kingdom-based Dr. Wei Sha and Dr. Zhanli Guo, is available in English language and was translated to Farsi by Dr. Noushin Yesaul and Dr. Seydamir Hossein Faqhi. It was edited by Mehdi Abbasi. Yesaul and Faqhi have also translated "An introduction to nuclear materials: principles and applications" together. According to a Fars News report from late 2021, Faqhi was appointed by AEOI-head Mohammad Eslami to lead the AEOI's Institute of Nuclear Sciences and Technologies. [2] He has also written about radiation measurements. [3] Yesaul has separately also written about uranium hexafluoride corrosion, [4] vacuum technology, and explosive forming. [5] Of the original British authors, neither appears to have a background in nuclear technologies, and neither the original English description of the book nor the authors' preface cite nuclear as a main industry. [6]

This book may show an ongoing interest in maraging steel, as well as a recognition of problems confronting Iran's nuclear industry. Given that the main use of maraging steel in Iran's nuclear program is in centrifuges, this book may indicate a revived or intensified interest in using maraging steel in its advanced centrifuges.

The 2021 announcement and the English book, based on its table of contents, do not discuss the manufacturing of maraging steel, a difficult technical process that eludes many countries particularly with regard to the production of high quality, high grade maraging steel suitable for use in Iran's advanced centrifuges. It remains a public mystery if Iran can make high grade maraging steel or if it has found a new international supplier willing to defy sanctions and trade controls. However, recent indications suggest one or both of these possibilities are occurring or are planned.

1. "Maraging steels were published," Shahid Beheshti University, March 11, 2021, [Google translated], https://news.sbu.ac.ir/w/%D9%81%D9%88%D9%84%D8%A7%D8%AF%D9%87%D8%A7%DB%8… ?

2. "Seyed Amirhossein Faqhi became the head of the Research Institute of Nuclear Sciences and Technologies," Fars News, November 27, 2021, [Google translated] https://www.farsnews.ir/news/14000906000883/%D8%B3%DB%8C%D8%AF-%D8%A7%D9… ?

3. Author page for Seyed Amir Hossein Faqhi, Elmnet.ir, [Google translated] https://elmnet.ir/author/%D8%B3%DB%8C%D8%AF%D8%A7%D9%85%DB%8C%D8%B1%D8%A… ?

4. Book page for "Corrosion of materials under UF6 gas," Emalls.ir, [Google translated] https://emalls.ir/%D9%85%D8%B4%D8%AE%D8%B5%D8%A7%D8%AA_%DA%A9%D8%AA%D8%A7%D8%A8-%D8%AE%D9%88%D8%B1%D8%AF%DA%AF%DB%8C-%D9%85%D9%88%D8%A7%D8%AF-%D8%AA%D8%AD%D8%AA-%DA%AF%D8%A7%D8%B2-UF6–%D8%A7%D8%AB%D8%B1-%D9%86%D9%88%D8%B4%DB%8C%D9%86-%DB%8C%D8%B3%D8%A7%D9%88%D9%84–%D9%86%D8%B4%D8%B1-%D8%AF%D8%A7%D9%86%D8%B4%DA%AF%D8%A7%D9%87-%D8%B4%D9%87%DB%8C%D8%AF%D8%B1%D8%AC%D8%A7%DB%8C%DB%8C~id~8736636?

5. Author page for Naushin Yesaul, Elmnet.ir, [Google translated] https://elmnet.ir/author/%D9%86%D9%88%D8%B4%DB%8C%D9%86-%DB%8C%D8%B3%D8%… ?

6. The English version is available on Amazon at https://www.amazon.com/Maraging-Steels-Microstructure-Applications-Engineering/dp/1845696867.

David Albright is President and Founder of, and **Sarah Burkhard** is Research Associate at, the Institute for Science and International Security.

Preventing a Dirty Bomb: Vulnerabilities Persist in NRC's Controls for Purchases of High-Risk Radioactive Materials

GAO-22-103441 *Published: Jul 14, 2022. Publicly Released: Jul 21, 2022.*
Source: https://www.gao.gov/assets/gao-22-103441.pdf

Radioactive materials are commonly used for things like treating cancer and sterilizing medical instruments. But even a small amount could be used in a dirty bomb, which uses conventional explosives to spread radioactive material.
The Nuclear Regulatory Commission issues licenses to people and organizations that need to possess radioactive material. However, our investigators used shell companies and fraudulent licenses to purchase radioactive materials from 2 different vendors in the U.S.
We recommended that the NRC add security features to its licenses to make it harder for people to use a fraudulent license to purchase radioactive material.

What GAO found

The Nuclear Regulatory Commission's (NRC) current system for verifying licenses does not adequately protect against the purchase of high-risk radioactive materials using a fraudulent license. Licenses control the type and quantity of radioactive material allowed to be possessed. Quantities of radioactive materials are defined as category 1 through 5, with 1 being the most dangerous. Using shell companies with fraudulent licenses, GAO successfully purchased a category 3 quantity of radioactive material of concern from two different vendors in the U.S. Specifically, GAO provided a copy of a license that GAO forged to two vendors, subsequently obtained invoices, and paid the vendors. GAO refused to accept shipment at the point of delivery, ensuring that the material was safely and securely returned to the sender.
As GAO has previously reported, a category 3 quantity of radioactive material can, on its own, result in billions of dollars of socioeconomic costs if dispersed using a dirty bomb. By purchasing more than one shipment of a category 3 quantity of radioactive material, GAO also demonstrated that a bad actor might be able to obtain a category 2 quantity by purchasing and aggregating more than one category 3 quantity from multiple vendors. NRC officials told GAO that NRC plans to proceed with existing initiatives to implement new verification regulations by late 2023 but does not plan to take immediate corrective actions to address the issues that GAO found.

Radioactive Material Delivered to GAO's Shell Company (box on left)

NRC requires a valid license to possess category 3 quantities of radioactive material, but the paper licenses it issues can be altered and used to make illicit purchases of radioactive materials. During this investigation, GAO created forged licenses to facilitate purchases. GAO's shell companies were successful in acquiring the material because they are not subjected to more stringent controls required for purchases of larger quantities of material. GAO's investigation demonstrates that the integrity of NRC's current license verification processes can be compromised.

Why GAO Did This Study

Radioactive materials are commonly used throughout the U.S. in technological devices for medical, industrial, and research purposes. However, these materials, if used improperly, can be harmful and dangerous. For example, in the hands of terrorists, even a small amount could be used to construct a radiological dispersal device, also known as a dirty bomb. A dirty bomb uses conventional explosives to spread radioactive material.
GAO was asked to review NRC's license verification system for high-risk radioactive materials. This report examines (1) the effectiveness of NRC's license verification system for ensuring that high-risk radioactive materials are not purchased using a forged or altered license and (2) vulnerabilities that could affect NRC's ability to verify licenses for the

purchase of high-risk radioactive material. GAO conducted a covert investigation of controls on purchasing radioactive materials. Additional details on GAO's covert testing will be included in an Official Use Only version of this report that will be issued soon.

Recommendations
GAO recommends that NRC (1) immediately require vendors to verify category 3 licenses with the appropriate regulatory authority and (2) add security features to its licensing process that improve the integrity of the process and make it less vulnerable to altering or forging licenses. To address our recommendations, NRC proposed a rulemaking to strengthen licensing. However, vulnerabilities will remain until NRC implements the rule.

Analysis of a dirty bomb attack in a large metropolitan area: simulate the dispersion of radioactive materials

By S. Biancotto, A. Malizia, M. Pinto, G.M. Contessa, A. Coniglio and M. D'Arienzo
Journal of Instrumentation, Volume 15, February 2020
Source: https://iopscience.iop.org/article/10.1088/1748-0221/15/02/P02019/pdf

The potential for a radiological or nuclear attack has been widely acknowledged in the last two decades. The use of a dirty bomb by terrorist organizations is considered to be a credible threat for which policymakers and relevant security agencies must prepare. Radioactive materials are stored in thousands of facilities around the world and may not be adequately protected against theft. This article analyzes a hypothetical dirty bomb attack in a large metropolitan area, evaluating the radiation dose to the involved population. The dispersion of radioactive materials is simulated using HOTSPOT code, considering a number of possible radionuclides (alpha, beta and gamma emitters) and scenarios. The findings of the present study corroborate and extend previous research demonstrating that it is unlikely that the atmospheric dispersion of radioactive material contained in a dirty bomb would produce deterministic effects in the exposed population. The radioactive material would be dispersed into the air resulting in relatively low doses. However, depending on the situation, the explosion of a dirty bomb is likely to contaminate properties (rendering them temporarily uninhabitable), thereby requiring potentially costly cleanup. Furthermore, due to the general fear of radiation, pervasive psychological effects are expected.

A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach

By H. Rosoff and D. von Winterfeldt
Risk Analysis | June 2007; Volume 27, Issue 3: pp. 533-546
Source: https://onlinelibrary.wiley.com/doi/10.1111/j.1539-6924.2007.00908.x

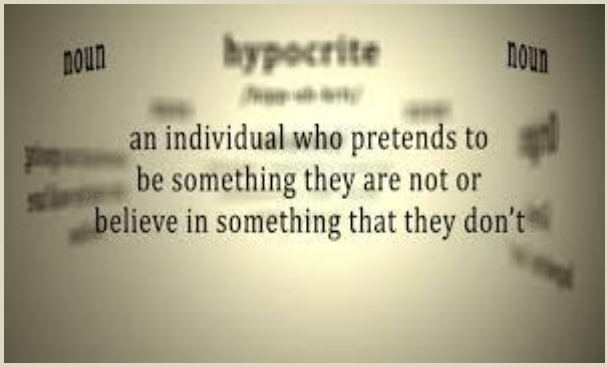
This article analyzes possible terrorist attacks on the **ports of Los Angeles and Long Beach** using a radiological dispersal device (RDD, also known as a "dirty bomb") to shut down port operations and cause substantial economic and psychological impacts. The analysis is an exploratory investigation of a combination of several risk analysis tools, including scenario generation and pruning, project risk analysis, direct consequence modeling, and indirect economic impact assessment. We examined 36 attack scenarios and reduced them to two plausible or likely scenarios using qualitative judgments. For these two scenarios, we conducted a project risk analysis to understand the tasks terrorists need to perform to carry out the attacks and to determine the likelihood of the project's success. The consequences of a successful attack are described in terms of a

radiological plume model and resulting human health and economic impacts. Initial findings suggest that the chances of a successful dirty bomb attack are about 10–40% and that high radiological doses are confined to a relatively small area, limiting health effects to tens or at most hundreds of latent cancers, even with a major release. However, the economic consequences from a shutdown of the harbors due to the contamination could result in significant losses in the tens of billions of dollars, including the decontamination costs and the indirect economic impacts due to the port shutdown. The implications for countering a dirty bomb attack, including the protection of the radiological sources and intercepting an ongoing dirty bomb attack are discussed.

World dangerously close to nuclear war, warns Britain's top security chief

Source: https://www.the-sun.com/news/5874797/world-close-nuclear-war/

July 27 – The world is dangerously close to nuclear war, Britain's top security chief warned yesterday.
National Security Adviser Sir Stephen Lovegrove sounded the alarm as China and Russia upgrade their weapons of mass destruction.
And he said the war in Ukraine, coupled with the secretive regimes in both Moscow and Beijing, means we are "more likely to see 'escalation wormholes' — sudden, unpredictable failures in the fabric of deterrence causing rapid escalation to strategic conflict".
Speaking in Washington DC at the Centre for Strategic and International Studies, he said nuclear war was averted during the Cold War only because the Soviet Union and Nato were able to speak to each other with a mutual understanding which he said does not exist today.
China and Russia have made "repeated violation" of international treaties on nukes, while North Korea and Iran also pose a nuclear risk.
He warned of "the pace and scale with which China is expanding its nuclear and conventional arsenals and the disdain it has shown for engaging with any arms control agreements".
Sir Stephen called on Nato to be "eternally vigilant" to the prospect of rogue states developing nukes.
He warned against regional arms races emerging as a result.
He added: "We have clear concerns about China's nuclear modernisation programme that will increase both the number and types of nuclear weapon systems in its arsenal."



EDITOR'S COMMENT: And what is Britain doing exactly to avoid the possibility of a nuclear war? Hypocrites!

Kim threatens to use nukes amid tensions with US, S. Korea

Source: https://news.yahoo.com/kim-threatens-nukes-amid-tensions-023528238.html

July 28 — North Korean leader Kim Jong Un warned he's ready to use his nuclear weapons in potential military conflicts with the United States and South Korea, state media said Thursday, as he unleashed fiery rhetoric against rivals he says are pushing the Korean Peninsula to the brink of war.
Kim's speech to war veterans on the 69th anniversary of the end of the 1950-53 Korean War was apparently meant to boost internal unity in the impoverished country amid pandemic-related economic difficulties. While Kim has increasingly threatened his rivals with nuclear weapons, it's unlikely that he would use them first against the superior militaries of the U.S. and its allies, observers say.
"Our armed forces are completely prepared to respond to any crisis, and our country's nuclear war deterrent is also ready to mobilize its absolute power dutifully, exactly and swiftly in accordance with its mission," Kim said in Wednesday's speech, according to the official Korean Central News Agency.

He accused the United States of "demonizing" North Korea to justify its hostile policies. Kim said regular U.S.-South Korea military drills that he claimed target the North highlight U.S. "double standards" and "gangster-like" aspects because it brands North Korea's routine military activities — an apparent reference to its missile tests — as provocations or threats.
Kim also alleged the new South Korean government of President Yoon Suk Yeol is led by "confrontation maniacs" and "gangsters" who have gone further than previous South Korean conservative governments. Since taking office in May, the Yoon government has moved to strengthen Seoul's military alliance with the United States and bolster its own capacity to neutralize North Korean nuclear threats including a preemptive strike capability.
"Talking about military action against our nation, which possesses absolute weapons that they fear the most, is preposterous and is very dangerous suicidal action," Kim said. "Such a dangerous attempt will be immediately punished by our powerful strength and the Yoon Suk Yeol government and his military will be annihilated."
South Korea expressed "deep regret" over Kim's threat and said it maintains a readiness to cope with any provocation by North Korea in "a powerful, effective manner." In a statement read by spokesperson Kang In-sun, Yoon's presidential national security office said South Korea will safeguard its national security and citizens' safety based on a solid alliance with the United States. It urged North Korea to return to talks to take steps toward denuclearization.
Earlier Thursday, South Korea's Defense Ministry repeated its earlier position that it's been boosting its military capacity and joint defense posture with the United States to cope with escalating North Korean nuclear threats.
In April, Kim said North Korea could preemptively use nuclear weapons if threatened, saying they would "never be confined to the single mission of war deterrent." Kim's military has also test-launched nuclear-capable missiles that place both the U.S. mainland and South Korea within striking distance. U.S. and South Korean officials have repeatedly said in the past few months that North Korea is ready to conduct its first nuclear test in five years. Kim is seeking greater public support as his country's economy has been battered by pandemic-related border shutdowns, U.S.-led sanctions and his own mismanagement. In May, North Korea also admitted to its first COVID-19 outbreak, though the scale of illness and death is widely disputed in a country that lacks the modern medical capacity to handle it. "Kim's rhetoric inflates external threats to justify his militarily focused and economically struggling regime," said Leif-Eric Easley, a professor at Ewha University in Seoul. "North Korea's nuclear and missile programs are in violation of international law, but Kim tries to depict his destabilizing arms buildup as a righteous effort at self-defense."
Experts say North Korea will likely intensify its threats against the U.S. and South Korea as the allies prepare to expand summertime exercises. In recent years, the South Korean and U.S. militaries have canceled or downsized some of their regular exercises due to concerns about COVID-19 and to support now-stalled U.S.-led diplomacy aimed at convincing North Korea to give up its nuclear program in return for economic and political benefits.
During Wednesday's speech, Kim said his government recently set tasks to improve its military capability more speedily to respond to military pressure campaigns by its enemies, suggesting that he intends to go ahead with an expected nuclear test.
But Cheong Seong-Chang at the private Sejong Institute in South Korea said North Korea won't likely conduct its nuclear test before China, its major ally and biggest aid benefactor, holds its Communist Party convention in the autumn. He said China worries that a North Korean nuclear test could give the United States a justification to boost its security partnerships with its allies that it could use to check Chinese influence in the region. North Korea recently said it is moving to overcome the COVID-19 outbreak amid plummeting fever cases, but experts say it's unclear if the country can lift its strict restrictions soon because it could face a viral resurgence later this year. During Wednesday's event, Kim, veterans and others didn't wear masks, state media photos showed. On Thursday, North Korea reported 11 fever cases, a huge drop from the peak of about 400,000 a day in May. North Korea has rejected U.S. and South Korean offers for medical relief items. It has also said it won't return to talks with the United States unless it first abandons its hostile polices on the North, in an apparent reference to U.S.-led sanctions and U.S.-South Korean military drills.

EDITOR'S COMMENT: Kim's behavior is totally different than that of Erdogan against the US (a nuclear power) or even Ukraine against Russia. The sociopath leader of South Korea will push the button himself without remorse believing that he protects his country despite the consequences. This is a real threat that should be taken seriously.

Will Seoul and Washington make Riyadh nuclear weapons ready?

By Henry Sokolski
Source: https://thebulletin.org/2022/07/will-seoul-and-washington-make-riyadh-nuclear-weapons-ready/

July 26 – Iran's nuclear program, oil, and human rights dominated Biden's much-anticipated first presidential trip to the Middle East earlier this month. But there is one topic President Biden chose not to showcase during his visit with Saudi Crown Prince Mohammed Bin

Salman Al Saud—the Kingdom's most recent interest in nuclear energy—and the nuclear weapons proliferation concerns that come with it.

Saudi Crown Prince Mohammed bin Salman in 2019. In a 2018 CBS News interview, the crown prince said that his country would obtain a nuclear weapon if Iran does

Only weeks before Biden's visit, Riyadh invited South Korea, Russia, and China to bid on the construction of two large power reactors. On that bid, Korea Electric Power Company (KEPCO) is the most likely winner. KEPCO has already built four reactors for Riyadh's neighbor, the United Arab Emirates, and is the only vendor to bring a power reactor of its own design online in the Middle East. South Korea also is the only government to provide reliable, generous financing, free of political strings—something neither Moscow nor Beijing can credibly claim.

And then, there's this: Any Korean sale would be covered by a generous 2011 South Korean nuclear cooperative agreement with Riyadh that explicitly authorizes the Saudis to enrich any uranium it might receive from Seoul. Under the agreement, Riyadh could enrich this material by up to 20 percent, without having to secure Seoul's prior consent.

That should set off alarm bells.

Do the Saudis want a bomb?

In 2018, Crown Prince Mohammed Bin Salman announced that "if Iran developed a nuclear bomb, we will follow suit as soon as possible." As if to prove the point, late in 2020, word leaked that the Saudis have been working secretly with the Chinese to mine and process Saudi uranium ore. These are steps toward enriching uranium—and a possible nuclear weapon program.

Unlike the Emirates, which legally renounced enriching uranium or reprocessing spent fuel to separate plutonium, the Kingdom insists on retaining its "right" to enrich. Also, unlike most members of the International Atomic Energy Agency (IAEA), Saudi Arabia refuses to allow intrusive inspections that might help the IAEA find covert nuclear weapons-related activities, if they exist, under a nuclear inspections addendum known as the Additional Protocol.

Saudi Arabia's enrichment program and refusal to adopt the Additional Protocol, doubled with a possible permissive South Korean reactor sale, could spell trouble. South Korea currently makes its nuclear fuel assemblies using imported uranium, which mainly comes from Australia. This ore is controlled by Australia's uranium export policy, which requires that the uranium be monitored by the IAEA and that materials derived from it not be retransferred

to a third country without first securing Australia's consent. Yet, if Seoul decides to pass Australian uranium on to Riyadh, the Saudis are free to enrich it up to 20 percent at any time without having to secure anyone's approval. In addition, Riyadh could proceed to enrich this material without having to agree to intrusive IAEA inspections under the Additional Protocol, making it easier for Riyadh to enrich beyond 20 percent uranium 235 without anyone knowing.

Can Washington block the reactor export?

In Washington, the US nuclear industry understandably is miffed that Riyadh excluded Westinghouse from bidding on the Saudi reactors. Meanwhile, State Department officials say that KEPCO can't sell Riyadh its APR-1400 reactor because it incorporates US nuclear technology that is property of Westinghouse. KEPCO, they insist, would first need to secure US Energy Department approval under US intangible technology transfer controls (known as Part 810 authorizations). This requirement, they argue, gives Washington the leverage it needs to impose nonproliferation conditions on South Korea's reactor export to Riyadh.

This sounds fine. But there's a catch. South Korean officials insist that its APR-1400 design, which uses a Combustion Engineering data package that Westinghouse now owns, is entirely indigenous. Focusing on the matter of technology transfer authority also begs a bigger question: Does the Republic of Korea need Washington's blessing to begin enriching uranium itself or to transfer enrichment technology to other countries, such as Saudi Arabia?

The short answer is no.

South Korea has always been free to enrich uranium and transfer uranium enrichment technology to other countries so long as the uranium it enriched or the enrichment technology it shipped wasn't of US origin. America's veto over South Korean enrichment only applies to uranium that comes from the United States. As I learned from a recent interview of the two top negotiators of the 2015 US-Republic of Korea civilian nuclear cooperation agreement, Seoul has always known this. Yet, South Korea asked that Washington explicitly grant it authority to enrich uranium in the 2015 agreement—something Washington has yet to grant. According to the negotiators, South Korean officials preferred to have political permission from Washington to do so, even though they did not legally need it.

South Korea and the United States have a choice

South Korea's previous administration under President Moon Jae-in announced in 2021 that South Korea would not export reactors to countries that had not yet agreed to adopt the IAEA's Additional Protocol. Is this pledge one that President Yoon Suk-yeol will uphold? Or will Yoon reverse this policy in his effort to go all out to secure the reactor sale to Riyadh?

Similarly, how committed is the Biden Administration to prevent Saudi Arabia from enriching uranium and reprocessing spent reactor fuel? Previous administrations have tried to keep Riyadh clear of such activities. Will Washington keep Seoul's and Saudi Arabia's feet to the fire on this or will the administration's desire to close ranks with South Korea and Saudi Arabia push these nonproliferation concerns to the sidelines? Anyone interested in preventing the further spread of nuclear weapons in the Middle East should want to know the answers.

Henry Sokolski is the executive director of the Nonproliferation Policy Education Center in Arlington, Virginia, and the author of *Underestimated: Our Not So Peaceful Nuclear Future* (2019). He served as deputy for nonproliferation policy in the office of the US secretary of defense during the George H.W. Bush administration.

Are Vladimir Putin's nuclear threats a bluff? In a word – probably

By Matthew Sussex

Source: https://au.news.yahoo.com/vladimir-putin-nuclear-threats-bluff-200533323.html

July 28 – Russian President Vladimir Putin habitually rattles his nuclear sabres when things start looking grim for Moscow, and has done so long before his ill-advised invasion of Ukraine.

In February 2008, he promised to target Ukraine with nuclear weapons if the United States stationed missile defences there. In August the same year, he threatened a nuclear war if Poland hosted the same system. In 2014, Foreign Minister Sergei Lavrov warned that Russia would consider nuclear strikes if Ukraine tried to retake Crimea.

A year later, the Kremlin said it would target Danish warships with nuclear missiles if they participated in NATO defence systems. And within the space of a few months – in December 2018 and February 2019 – Putin warned the US that nuclear war was possible, and then promised to target the American mainland if it deployed nuclear weapons in Europe.

Since the invasion of Ukraine, the Kremlin has waggled its nuclear arsenal so many times it's starting to become tedious. Even the most peripheral slight is apparently fair game, like

former President Dmitry Medvedev's invocation of nuclear retaliation if the International Criminal Court (ICC) pursued war crimes investigations against Russian soldiers.

Deterrence

One explanation for Russia's behaviour is that it's attempting to deter NATO from attacking it. For nuclear deterrence to be effective, states possessing such weapons require three things, commonly referred to as the "Three Cs": capability, communication and credibility. Russia certainly has the first of these. With nearly 6,000 nuclear warheads it's the world's most heavily armed nuclear state. It also communicates – loudly and with regularity – those capabilities.

But the question of credibility remains an open one, reliant on the perceptions of others. Put simply, the US and other nuclear states must believe Russia will use nuclear weapons under a certain set of conditions, usually in retaliation for a similar attack or when it faces a threat to its survival.

But will it really use them?

Russia's declared nuclear doctrine identifies the circumstances under which it would employ nuclear weapons in a fairly rational and sensible manner.

Its 2020 Basic Principles on Nuclear Deterrence stresses that Russia will reserve the right to use nuclear weapons "in response to the use of nuclear and other types of weapons of mass destruction against it and/or its allies". Or, if Russia comes under such severe conventional attack that "the very existence of the state is in jeopardy". Putin's spokesman Dmitry Peskov addressed this directly on March 28, stating "any outcome of the operation [in Ukraine] of course isn't a reason for usage of a nuclear weapon".

Yet this has not prevented widespread acceptance of the view that Russia would use nuclear weapons in order to seize the advantage in escalation control. This idea, commonly referred to as "escalate to de-escalate" is even embedded in the US 2018 Nuclear Posture Review's assessment of Russian intentions. But the Kremlin's perpetual nuclear signalling has much more to do with its attempts to intimidate and attain reflexive control over the West. In other words, it's seeking to get the US and other NATO members to so fear the prospect of nuclear war that they will accede to Russian demands. That makes it a coercive strategy, but crucially one that relies on never actually being tested. There are plenty of signs this is working. In April 2022, Germany's Chancellor Olaf Scholz based his decision not to supply heavy weapons to Ukraine with the justification that "there must not be a nuclear war".

A number of Western commentators have also begun reconsidering the "nuclear taboo", worrying Putin might resort to nuclear weapons in Ukraine if he feels backed into a corner, or to turn the tide of the war. One particularly agitated opinion piece in the New York Times called for immediate talks before major power war became inevitable.

It makes little sense for Russia to go nuclear in Ukraine

But what if the Kremlin's recent nuclear threats are aimed less at NATO and more at Kyiv? Under those conditions, the logic of nuclear deterrence (threatening a non-nuclear country) do not apply. There are several reasons Putin might seek to use nuclear weapons against Ukraine: a decapitating strike, to destroy a large portion of Ukraine's armed forces, to cripple Ukrainian infrastructure and communications, or as a warning. This also generally means using different types of nuclear weapons. Rather than large city-busting bombs, Russia would employ smaller non-strategic nuclear warheads. It certainly has plenty of them: about 2,000 warheads in Russia's stockpile are tactical nuclear weapons. But none of these scenarios make sense for Russia. While Moscow has returned to regime change in Ukraine as a war aim, using a nuclear weapon to take out Volodymyr Zelenskyy would be difficult and risky. It presupposes ironclad intelligence about his location, entails significant loss of civilian life, and requires Moscow to accept significant destruction wherever Zelenskyy might be. It would hardly look good for victorious Russian forces to be unable to enter an irradiated Kyiv, for instance. Punching nuclear holes in Ukrainian lines is equally risky. Ukraine's army has deliberately decentralised so it can operate with maximum mobility (often referred to as "shoot and scoot"). Putin would have to order numerous nuclear attacks for such a tactic to be effective. And he would be unable to prevent radioactive fallout from potentially blowing over "liberated" portions of Donbas under Russian control, not to mention Western Russia itself. Another possibility is a high-altitude detonation over a city, doing no damage but causing a massive electromagnetic pulse (EMP). An EMP attack would fry electrical systems and electronics, bringing critical infrastructure to a standstill. But again, it would be difficult to limit EMP burst effects to Ukraine alone, and it would leave Moscow with very little remaining usable industry.

Finally, the Kremlin might seek a demonstration effect by detonating a nuclear device away from populated areas, or even over the Black Sea. This would certainly attract attention, but would ultimately be of psychological value, without any practical battlefield utility. And Russia would join the US as the only countries to have used such weapons in anger.

Is Russia rational?

In all this, there's naturally a big caveat: the assumption Russia's regime is rational. Having accrued vast personal fortunes and a taste for luxury, Russia's rulers are likely in no hurry to commit suicide in a major nuclear cascade. However, since there's no way of being certain, the West must continue to take Russian nuclear posturing seriously – but also with healthy skepticism. Indeed, if the West capitulates to Russian demands due to fears of nuclear war, it will further embolden Putin and show other nations nuclear brinkmanship is appealing. But Russia arguably faces the bigger risk here. If Putin uses nuclear weapons against Ukraine or a NATO member it would also make it very difficult for states that have quietly supported it (such as China) or sought to benefit from its pariah status through trade (like India) to continue to do so. It would also likely engender a broader war that he has tried hard to avoid. Let's continue to hope Moscow, although often misguided, remains rational.

Matthew Sussex is a Fellow, Strategic and Defense Studies Centre, Australian National University.

EDITOR'S COMMENT: What a naïve, superficial, ignorant title revealing a sense of grief that we are not currently experiencing a nuclear holocaust! [The armchair expert definition was added by the Editor]

Iran's Missile Arsenal

Source: https://www.iranwatch.org/our-publications/weapon-program-background-report/table-irans-missile-arsenal

The IRGC Aerospace Museum in Tehran. Image credit: Fars News Agency.

July 27 – Iran's missile arsenal is the largest and most diverse in the Middle East. In 2022, U.S. Central Command's General Kenneth McKenzie stated that Iran possesses "over 3,000" ballistic missiles. This does not include the country's burgeoning land-attack cruise missile force.[1] Iran has made substantial improvements over the past decade in the precision and accuracy of its missiles, which make them an increasingly potent conventional

threat.[2] The focus on precision and accuracy has been accompanied by a self-imposed missile-range limit of 2,000 km, first publicly acknowledged in 2015. Iran could, however, abandon the limit at any time, and indeed is developing a system—the Khorramshahr—that, if deployed, would seemingly nullify it. Finally, despite an early reliance on liquid-fueled missiles, Iran has since placed a greater emphasis on developing solid-propellant missiles. This trend will likely continue.[3]

Many Iranian missiles are inherently capable of carrying nuclear payloads, which has long been an international concern: U.N. Security Council resolution 2231 "calls upon" Iran "not to undertake any activity related to ballistic missiles designed to be capable of delivering nuclear weapons." U.N. restrictions on Iranian procurement of missile technology, as well as targeted sanctions on entities involved in missile development, remain in place through 2023. Nonetheless, Iran has persisted in developing a wide array of ballistic and cruise missiles that are either inherently or potentially capable of carrying a nuclear warhead, as well as space launch vehicles (SLVs) that use many of the same technologies as longer-range ballistic missiles.

Iran has employed missiles in combat on multiple occasions since 2017, including a ballistic missile attack on Iraqi bases hosting U.S. forces in 2020. Iran has also transferred missiles to proxies such as Yemen's Houthi rebels, who have used them to strike civilian targets in Saudi Arabia and the United Arab Emirates.

The table below sets forth what is publicly known, claimed, or estimated about the capabilities of Iran's missiles that are most likely to be used either as nuclear-weapon delivery vehicles or for conventional strikes against high-payoff targets, such as bases or infrastructure.[4]

Name	Type[5]	Max Range	Payload	Propulsion	CEP[6]	Status
Shahab-1 (Scud B)	SRBM	up to 300 km	770-1,000 kg	liquid fuel, single stage	~500m	deployed
Shahab-2 (Scud C)	SRBM	~500 km	~700 kg	liquid fuel, single stage	700 m	deployed
Qiam-1	SRBM	700-800 km	650 kg	liquid fuel, single stage	<500 m[7]	deployed
Qiam-1 (mod.)[8]	SRBM	700-800 km	650 kg	liquid fuel, single stage	~100m	deployed
Fateh-110 (including Khalij Fars and Hormuz[9])	SRBM	300 km	500 kg	solid fuel, single stage	100 m[10]	deployed
Fateh-313	SRBM	500 km	<500 kg[11]	solid fuel, single stage	10-30 m[12]	deployed
Zolfaghar (including Zolfaghar Basir[13])	SRBM	700 km	450-600 kg	solid fuel, single stage	10-30 m[14]	deployed
Dezful	SRBM	1,000 km	450-600 kg	solid fuel, single stage	10-30m[15]	deployed
Shahab-3	MRBM	1,300 km	750-1,000 kg	liquid fuel, single stage	~3 km	deployed
Ghadr	MRBM	1,600 km	~750 kg	liquid fuel, single stage	300m	deployed
Emad	MRBM	1,800 km	~750 kg	liquid fuel, single stage	<500 m	deployed
Kheibar Shekan	MRBM	1,450 km	450-600 kg	solid fuel, single stage	unknown	tested
Sejjil	MRBM	2,000 km	~750 kg	solid fuel, two stage	unknown	deployed

Name	Type[5]	Max Range	Payload	Propulsion	CEP[6]	Status
Khorramshahr-1 and -2 (BM-25/Musudan)	MRBM[16]	2,000-4,000 km	500-1,800 kg	liquid fuel, single stage	~1.5 km	tested
Meshkat/Soumar (Kh-55)	LACM	unknown[17]	unknown	turbofan engine	N/A	possibly deployed
Hoveizeh	LACM	1,350 km	unknown	turbojet engine	N/A	possibly deployed
Ya Ali	LACM	700 km	unknown	turbojet engine	N/A	tested
Quds-1[18]	LACM	700-800 km	unknown	turbojet engine	N/A	deployed[19]
Safir	SLV	2,100 km[20]	500-750 kg[20]	liquid fuel, two stage	N/A	retired
Simorgh	SLV	4,000-6,000 km[20]	500-750 kg[20]	liquid fuel, two stage	N/A	no successful launches
Qased	SLV	2,200 km[20]	1,000 kg[20]	liquid 1st stage; solid 2nd and 3rd stages	N/A	operational
Zuljanah	SLV	4,000-5,000 km[20]	1,000 kg[20]	solid 1st and 2nd stages, liquid 3rd stage	N/A	tested

Footnotes:

[1] Independently estimating the size of Iran's missile arsenal is difficult, given the paucity of reliable information relating to its missile quantities. The U.S. Air Force and some non-governmental organizations have released estimates in the past, but these lack specificity and usually only estimate the number of launchers, not the missiles themselves, since launchers are, in principle, easier to track and count. For an example of a U.S. Air Force estimate, see "2020 Ballistic and Cruise Missile Threat," U.S. National Air and Space Intelligence Center, pp. 21, 25, January 2020, available at https://media.defense.gov/2021/Jan/11/2002563190/-1/-1/1/2020%20BALLISTIC%20AND%20CRUISE%20MISSILE%20THREAT_FINAL_2OCT_REDUCEDFILE.PDF. For an example of a non-governmental estimate, see "The Military Balance 2021," International Institute for Strategic Studies, January 2021, p. 339, available at https://hostnezt.com/cssfiles/currentaffairs/The%20Military%20Balance%202021.pdf.

[2] Precision is the ability of a weapon to impact where it is aimed; accuracy is the ability of the user to aim the weapon at the true location of the desired target and of the weapon to be precise enough to hit it. Accuracy thus takes into account target acquisition and tracking capabilities. For example, Iran's development of capable surveillance drones has served to improve the accuracy of its missile forces.

[3] Missiles can be classified according to whether they are liquid-fueled or solid-fueled. A liquid-fueled missile engine generally can produce more thrust per pound of fuel than a solid-rocket motor but is more complex and can require many precision-machined and moving parts. Some types of liquid-fueled missiles must also be fueled at their launch site, which makes them easier for an opponent to detect and destroy. Solid rocket motors are relatively economical and easier to maintain and store. Solid fuel also allows for a more rapid launch. Solid-fueled missiles are therefore generally less vulnerable in combat. Iranian engineers do not appear to have the wherewithal to design and build a liquid-fueled engine from scratch, but they do possess that ability for solid-fueled motors. The ability to build new systems tailored to Iran's military needs, in addition to the operational advantages, helps explain Iran's increasing preference for solid-fuel missiles.

[4] The table does not include missiles or artillery rockets with a maximum range below 300 km, missiles that have only been displayed as mock-ups, surface-to-air missiles, or anti-ship cruise missiles. Nor does it include derivatives, variants, or renamed copies of Iranian missiles that have been used by Iran's regional proxies, such as the Houthis. The capabilities of those missiles can be best assessed by referencing the Iranian missiles they are modeled after. For example, the Houthis' Burkan-2H ballistic missile closely resembles the Iranian Qiam-1.

[5] Ballistic missiles can be divided into five classes based on range: close-range (less than 300 km), short-range (300 to 1,000 km), medium-range (1,000 to 3,000 km), intermediate-range (3,000 to 5,500 km), and intercontinental (more than 5,500 km). Iran's ballistic missile

arsenal is composed mainly of short-range ballistic missiles (SRBMs) and medium-range ballistic missiles (MRBMs), although some work on longer-range missiles is suspected. Space launch vehicles (SLVs) are designed to launch satellites into orbit but could potentially be reconfigured as ballistic missiles due to their similar characteristics. Land-attack cruise missiles (LACMs) function essentially as pilotless aircraft and do not fly on a ballistic trajectory, thus posing a challenge to missile defense systems.
[6] Missile precision is commonly measured by circular error probable (CEP): the radius within which, on average, half of all missiles fired will land. For example, given a missile with a CEP of ten meters, if one hundred were launched at a target, on average fifty would land within ten meters of the target.
[7] As the Qiam-1 was one of the missiles used in the January 2020 strike on U.S. forces in Iraq, which was widely considered accurate, it is possible that the Qiam-1's CEP has improved.
[8] This has been called Qiam-2 by some independent analysts, but not by official Iranian sources.
[9] The Khalij Fars is the anti-ship variant of the Fateh-110, while the Hormuz is the anti-radar variant.
[10] Iran has reportedly developed a guidance kit for the Fateh-110 that, when attached, can reduce its CEP to 30 meters or less.
[11] Inferred from the fact that the Fateh-313 has a smaller nose cone than the Fateh-110, its base model.
[12] Based on its likely use in the January 2020 ballistic missile attack against U.S. forces and damage assessments of that attack.
[13] The Zolfaghar Basir is the anti-ship variant of the Zolfaghar.
[14] Based on its likely use in the January 2020 ballistic missile attack against U.S. forces and damage assessments of that attack. Also based on similar assessments following the Great Prophet 17 military exercise in December 2021.
[15] Based on its use in the Great Prophet 17 military exercise suggesting it has precision similar to that of the Zolfaghar.
[16] Iran claims that the Khorramshahr's maximum range is 2,000 km, thus complying with the reported self-imposed range limit of 2,000 km for all Iranian missiles. The greater range of the Soviet SS-N-6 and North Korean Musudan (BM-25) missiles, on which the Khorramshahr is based, suggests that the true maximum range of the Khorramshahr may be as high as 4,000 km. The differing range estimates may be partially explained by different assumptions about the warhead mass; the official Iranian claim was based on an 1,800 kg warhead. If the payload were reduced to 500 kg, the Khorramshahr may be capable of achieving a range of at least 3,000 km. If so, it would be classified as an intermediate-range ballistic missile (IRBM).
[17] In 2001, Iran illicitly acquired six Soviet-made Kh-55 air-launched cruise missiles, which have a range of up to 2,500 km. In 2012, an Iranian official claimed that Iran's forthcoming copy of the Kh-55, modified to have a solid-rocket booster for ground launch, would have a range exceeding 2,000 km. In 2019, however, an official claimed the missile's range was only 700 km. There is not sufficient open-source evidence to verify either of the claims, but it is unlikely that Iran has successfully reverse-engineered a turbofan engine with the capabilities to match those of the original Soviet type.
[18] The Quds-1 was first publicly displayed by the Houthis in Yemen, but it is also suspected to be in the Iranian arsenal. It was used in the September 2019 attack on Saudi Aramco facilities. Although the Houthis claimed responsibility for that attack, the UN Panel of Experts on Yemen presented evidence in its 2020 final report that the missile's components were made in Iran and that the attack could not have been launched from Houthi-controlled territory. The Houthis have also displayed a missile named Quds-2, which may be a longer-range variant.
[19] Based on the assumption that the 2019 attack on Saudi Aramco facilities was launched from Iran.
[20] Estimate if reconfigured as a ballistic missile.

Iran's Nuclear Timetable: The Weapon Potential

By Valerie Lincy and Gary Milhollin
Source: https://www.iranwatch.org/our-publications/articles-reports/irans-nuclear-timetable-weapon-potential

July 21 – This timetable estimates how soon Iran could enrich enough uranium to fuel a small nuclear arsenal. It assumes Iran would try to build an arsenal of five warheads of the implosion type – the goal Iran set for itself when it began to work on nuclear weapons decades ago. With its thousands of gas centrifuges, some operating and some in storage, Iran can enrich uranium to a grade suitable for nuclear reactor fuel or to a higher grade suitable for nuclear weapons. On January 5, 2020, Iran announced that it would no longer observe any limit (such as that set by the nuclear accord of 2015) on the use of its centrifuges, or on the possession of uranium they enrich. Since then, Iran has expanded its stockpile of enriched uranium, increased the enrichment level of that stockpile, and brought more advanced centrifuges into operation.
The potential is estimated as of mid-May 2022, the date of inspection contained in the latest public report by the International Atomic Energy Agency (IAEA). Because Iran has reduced

its cooperation with the Agency, it is no longer able to verify Iran's stockpile of enriched uranium. The Agency's reports are only able to estimate its contents. The analysis below is based on those estimates.

Summary

Iran's nuclear program has reached the point at which, within a few months, Iran could enrich enough uranium for five fission weapons. For that uranium to pose a nuclear weapon threat, however, it would have to be processed further, and the other components of a successful weapon would have to be ready to receive the processed uranium. These additional steps, together with the several months for enrichment, mean that Iran cannot yet make a dash to a small nuclear arsenal within a practical length of time. Such a dash would probably be detected before it could succeed, and would invite retaliation Iran could not deter. A dash to a single weapon would take less time but would not be practical. Such a weapon would have to be tested,[1] which would consume all the nuclear material the dash produced.

Iran's ability to enrich uranium quickly has improved with its recent progress in the testing and deployment of more powerful centrifuge models. Centrifuge performance is measured in separative work units (SWU), which indicates the work required to increase the concentration of the fissionable U-235 isotope. Iran has installed several cascades of these new models in production lines where they have steadily increased both the size and enrichment level of Iran's uranium stockpile. This progress increases the risk of secret sites – permitting them to be smaller and easier to hide. Iran has used such sites to carry out illicit activity in the past and they continue to pose the greatest nuclear weapon risk. That risk has increased further recently because of Iran's decision to limit inspections by the IAEA, block IAEA access to recorded data from centrifuge production plants, and refuse to cooperate with the Agency's investigation of three suspicious sites.

These steps by Iran are parts of the long nuclear game Iran has been playing for decades.

Nuclear Weapon Potential of Iran's Centrifuges and Enriched Uranium

As of May 2022, Iran was operating 32 cascades of IR-1 centrifuges as well as seven cascades of more powerful centrifuges (six IR-2m cascades and one IR-4 cascade) at the Natanz Fuel Enrichment Plant (FEP). In addition, Iran was operating up to 1,044 IR-1 centrifuges and had been operating 166 more powerful IR-6 centrifuges at the Fordow Fuel Enrichment Plant (FFEP) and several hundred more centrifuges at the Natanz pilot plant, notably the IR-4 and IR-6. Iran also had several thousand IR-1 centrifuges in storage at Natanz and continues to test other more powerful centrifuge models in smaller numbers at the Natanz pilot plant. Some of these models are adding to Iran's enriched uranium stockpile. By deploying them in larger numbers, Iran would be able to produce nuclear weapon fuel more quickly.

Iran's centrifuges have not produced uranium usually defined as weapon-grade, which is uranium enriched to 90% in the isotope U-235. All of Iran's production has been at lower grades. Thus, the lower-grade uranium would have to be enriched further to reach at least 90%. The estimates below assume that, in a dash to make weapons, Iran would rely on its IR-1 and IR-2m centrifuges now operating, and would use its accumulated stockpile of enriched uranium[2] to produce nuclear weapon fuel. Iran's enriched uranium stockpile already contains sufficient uranium to fuel five nuclear warheads with further enrichment.[3] The estimates also assume that the IR-1 centrifuges currently operating will perform at the same rate they have in the past and that the IR-2m centrifuges would perform at 80% of their estimated nominal output.[4]

Estimated minimum time it would take Iran's IR-1 and IR-2m centrifuges presently installed in production mode to enrich enough uranium for	
	As of May 15, 2022
One weapon	1.2 weeks[5]
Two weapons	2.1 weeks[6]
Three weapons	3.7 weeks[7]
Four weapons	6.7 weeks[8]
Five weapons	11.3 weeks[9]

These estimates are the minimum theoretical times it would take Iran's known installed centrifuges, operating continuously at their proved capacity, to accomplish the required amount of work. The time actually needed in practice would be greater. The estimates assume that only the IR-1 and IR-2m centrifuges, which have been successfully operating in production mode for some time, would be used. The time estimate for five bombs can be expected to continue to fall, as Iran brings more centrifuges into production mode and raises the enrichment level of its uranium stockpile.

It is important to consider that the enriched uranium produced would be in a gaseous compound, uranium hexafluoride (UF6). It would take additional time to convert the uranium in the gas to metallic form, and then to cast and machine the metal into weapon components. According to the IAEA, Iran began work on uranium metal production in early 2021. The uranium metal, however, would only be a threat if Iran had already perfected all the other parts needed for a working weapon, such as the high explosives and firing circuit, and had made sure the parts would work together to achieve a nuclear explosion. There is ample evidence in the public domain that Iran has tried to achieve that goal (see Weaponization below), but no conclusive evidence that it has succeeded.

The Risk of Secret Sites

Intelligence agencies have long been unanimous in one prediction: If Iran makes nuclear weapons, it would do so at secret sites. The reasons are clear. If, in a dash to make weapons, Iran were to divert known (and therefore inspected) sites, material, or equipment to weapon making, it would risk detection before success, would violate the Nuclear Nonproliferation Treaty (NPT) and would make itself an international pariah. It would also invite an attack on the very sites, material and equipment it diverted. No country has ever chosen to make an illicit diversion and dash to weapons, probably for the reasons just stated.

The data below reveal that as Iran develops more powerful centrifuges, it would need ever smaller sites to enrich weapon quantities of uranium. And the smaller the site, the more difficult it will be to detect. For example, operating at 80% of its nominal capacity, Iran's IR-2m centrifuge, of which Iran has at least 1,000, could enrich the same amount of uranium as the IR-1 centrifuge in approximately one-fifth the space. Iran's enrichment plant at Fordow, which was publicly exposed in 2009, was built clandestinely by Iran to house about 3,000 centrifuges. For this reason, the estimates below use 3,000 centrifuges as the possible size of a secret enrichment plant.

Estimated minimum time it would take 3,000 of Iran's IR-2m[10] centrifuges operating at an assumed 80% of nominal capacity and starting with natural uranium to enrich enough uranium for	
One weapon:	Four months[11]
Five weapons:	One year and eight months[12]

These centrifuges would require only about 32,000 square feet, equal to approximately twice the size of the ice surface of a professional hockey rink.[13] Alternatively, Iran could decide to split these 3,000 IR-2m centrifuges equally among three smaller sites of approximately 11,000 square feet each. That would decrease the size of each site and therefore the likelihood of detection. Each site would be about two-thirds the size of the ice surface of a professional hockey rink.[14] By May 2022, Iran was operating six cascades of IR-2m centrifuges (1,044 machines) in production mode at the Natanz Fuel Enrichment Plant, as well as one cascade of IR-4 centrifuges, which are estimated to have a capacity similar to the IR-2m.[15]

Also by May 2022, Iran was feeding a cascade of up to 164 IR-4 centrifuges and a cascade of up to 164 IR-6 centrifuges in production mode at the Pilot Fuel Enrichment Plant,[16] and had operated a cascade of 166 IR-6 centrifuges in production mode at the Fordow Fuel Enrichment plant.[17] According to Iran, the IR-6 produces about 10 SWU per year, ten times as much as the IR-1. If so, it could enrich the same amount of uranium in a fraction of the space. Iran's claim to a capacity of 10 SWU has been strengthened recently by Iran's plan for Fordow, where two cascades of IR-6 machines are intended to produce the feed for the IR-1 centrifuges enriching up to 20% U-235.[18] To produce enough feed for this configuration, each IR-6 machine would have to produce at least 6.6 SWU.[19]

Estimated minimum time it would take 3,000 of Iran's model IR-6[20] centrifuges operating at an assumed 80% of nominal capacity and starting with natural uranium to enrich enough uranium for	
One weapon:	Two months[21]
Five weapons:	Ten months[22]

These IR-6 centrifuges would require approximately the same space as the model IR-2m centrifuges above, or approximately twice the size of the ice surface of a professional hockey rink. The space requirements above reveal that as Iran develops more efficient centrifuges, it could rely on ever smaller sites to enrich weapon quantities of uranium.

The Status of Weaponization Efforts

The analysis above assumes that Iran would use 16 kg of highly enriched uranium metal (about 90% U-235) in the finished core of each nuclear weapon. Sixteen kilograms are assumed to be sufficient for an implosion weapon. This was the amount called for in a design

for such a device that has circulated on the nuclear black market, to which Iran has had access.
Some experts believe that Iran could use less material, assuming Iran would accept a lower yield for each weapon. According to these experts, Iran could use as few as seven kilograms of this material if Iran's weapon developers possessed a "medium" level of skill, and if Iran were satisfied with an explosive yield slightly less than that of the bomb dropped on Hiroshima, Japan.[23] If Iran chose to use an amount smaller than 16 kg, the time required to make the fuel for each weapon would be less than estimated here. Or, in the amount of time estimated here, Iran could make a greater number of weapons. Iran could decide not to use such a smaller amount of uranium if Iran wanted to have more confidence that its weapons would work, or if it wanted to reduce the size of its weapons by reducing the amount of high explosive.
According to an investigation by the IAEA into "possible military dimensions" of Iran's nuclear program, Iran had a coordinated nuclear weapon program between 1999 and 2003. Specifically, the IAEA found that Iran developed several components of a nuclear weapon and undertook related research and testing. The investigation revealed Iran's efforts in the following areas:

- computer modeling of implosion, compression, and nuclear yield;
- high explosive tests simulating a nuclear explosion using non-nuclear material in order to see whether an implosion device would work;
- the construction of at least one containment vessel at a military site, in which to conduct such high explosive tests;
- studies on detonation of high explosive charges, in order to ensure uniform compression in an implosion device, including at least one large scale experiment in 2003, and experimental research after 2003;
- support from a foreign expert in developing a detonation system suitable for nuclear weapons and a diagnostic system needed to monitor the detonation experiments;
- manufacture of a neutron initiator, which is placed in the core of an implosion device and, when compressed, generates neutrons to start a nuclear chain reaction, along with validation studies on the initiator design from 2006 onward;
- the development of exploding bridgewire detonators (EBWs) used in simultaneous detonation, which are needed to initiate an implosive shock wave in fission weapons;
- the development of high voltage firing equipment that would enable detonation in the air, above a target, in a fashion only making sense for a nuclear payload;
- testing of high voltage firing equipment to ensure that it could fire EBWs over the long distance needed for nuclear weapon testing, when a device might be located down a deep shaft; and
- a program to integrate a new spherical payload onto Iran's Shahab-3 missile, enabling the missile to accommodate the detonation package described above.

Information obtained by Israeli intelligence and revealed in April 2018 indicates that Iran sought to preserve this program after 2003 by dividing its nuclear program between covert and overt activities and retaining an expert team to continue work on weaponization. This "atomic archive" includes blueprints, spreadsheets, charts, photos, and videos – apparently official Iranian documents – that provide additional detail about Iran's efforts to develop a working nuclear weapon that could be delivered on a ballistic missile.

Need for Enriched Uranium?

Iran has no need to enrich large quantities of uranium for reactor fuel, which is the stated aim of its centrifuge enrichment program. Russia is fueling Iran's only power reactor (at Bushehr) and stands ready to do so indefinitely at a cost much lower than Iran would incur by enriching the uranium itself.[24]
If Iran did try to make the fuel itself, it is unlikely that Iran could field enough centrifuges to do so within the next ten years, or even longer. A standard sized power reactor (1,000 MWe) such as Iran's reactor at Bushehr requires about 21 metric tons of low-enriched uranium fuel per year, which would require generating nearly 100,000 SWU.[25] Iran's centrifuges now produce about 9,000 SWU. Thus, Iran would have to increase its capacity more than tenfold to have any plausibility as a civilian effort.
In an October 2015 letter to then-President Hassan Rouhani, Iran's Supreme Leader Ali Khamenei called upon the government to develop a plan for the country's nuclear industry to achieve an annual uranium enrichment capacity of 190,000 SWU within 15 years. In order to accomplish this, Iran would have to manufacture, install, and operate almost 240,000 additional IR-1 centrifuges, based on their historic output. Or, Iran would have to perfect, manufacture, and deploy in production mode a lesser number of more powerful centrifuges. It is uncertain how long it would take Iran to accomplish either of these steps, but either would take many years.

Iran's Violations of Nuclear Accord

Following the U.S. withdrawal from the 2015 nuclear accord in May 2018, Iranian leaders threatened to stop implementing some of Iran's commitments under the accord. Approximately one year later Iran began doing so. The table below summarizes the steps Iran has taken since July 2019.

Date	Iran's Violations of the 2015 Accord
July 2019	Begins enriching uranium above the 3.67% U-235 limit set by the accord, to a level of up to 4.5% U-235.
August 2019	Exceeds the cap of 300 kg of UF6 on its stockpile of low-enriched uranium set by the accord.
September 2019	Expands its centrifuge research and development beyond the limits set by the accord, both in the number and type of more powerful centrifuge it operates.
November 2019	Resumes uranium enrichment at locations beyond those mandated by the accord, including the Fordow plant and the Natanz pilot plant.
January 2020	States it will no longer limit the number of centrifuges in operation, which had been capped at 5,060 IR-1 centrifuges operating at the Natanz Fuel Enrichment Plant.
July 2020	Announces plans to transfer more powerful IR-2m, IR-4, and IR-6 centrifuges from the Natanz pilot plant to the Natanz Fuel Enrichment Plant. The accord limits Iran to the use of IR-1 centrifuges at the Fuel Enrichment Plant.
October 2020	Installs IR-2m centrifuges and begins installing IR-4 centrifuges at the Natanz Fuel Enrichment Plant.
November 2020	Begins uranium enrichment in a cascade of 174 IR-2m centrifuges at the Natanz Fuel Enrichment Plant.
January 2021	Begins enriching uranium to the level of 20% U-235 at the Fordow plant and begins uranium enrichment in a second cascade of 174 IR-2m centrifuges at the Natanz Fuel Enrichment Plant.
February 2021	Begins installing IR-6 centrifuges at the Fordow plant and uses a facility in Isfahan to produce uranium metal, which the accord prohibits for 15 years.
February 2021	Stops implementing transparency measures, including the Additional Protocol to Iran's Comprehensive Safeguards Agreement and additional transparency and access measures allowed under the accord. Withholds access to data recorded by IAEA monitoring devices.
April 2021	Begins enriching uranium up to 60% U-235.
May 2021	Installs equipment to produce uranium metal in quantity.
June 2022	Removes IAEA monitoring devices installed pursuant to the 2015 accord.

Footnotes:

[1] In a dash, Iran would be expected to use its uranium to fuel a weapon with an implosion design, such as the bomb dropped on Nagasaki, Japan; such a weapon would have to be tested to prove it worked, as was the Nagasaki bomb. A gun-type device such as the one dropped on Hiroshima without being tested, would require more than twice as much uranium.

[2] The IAEA estimated, but was unable to verify, that as of May 15, 2022, Iran's uranium stockpile contained 3,491.8 kg of uranium in the form of uranium hexafluoride (UF6), 43.1 kg of which was enriched "up to" a level of 60% in the fissionable isotope U-235, 238.4 kg of which was enriched "up to" a level of 20% U-235, and 1,055.9 kg of which was enriched "up to" a level of 5% U-235. The U-235 isotope makes up about .7% of natural uranium; its concentration can be increased, or enriched, using centrifuges.

[3] Twenty kilograms of uranium in the form of UF6 enriched to 90% U-235 are assumed to be sufficient for one weapon. The uranium would need to be further processed into finished metal weapon components, which is assumed to cause about a 20% loss of material.

[4] According to pre-2016 production data from Natanz, Iran's IR-1 centrifuges have achieved an average annual output of about .8 separative work units, or SWUs, per machine. The IR-2m is based on Pakistan's P-2 centrifuge and is assumed in these estimates to have an operational output of 4 SWU (and a nominal output of 5 SWU). See Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)," Science and Global Security, Vol. 16, Nos. 1-2 (2008), p. 9. The SWU is the standard measure of the effort (work) required to increase the concentration of the fissionable U-235 isotope. See http://www.urenco.com/index.php/content/89/glossary.

[5] Iran's stockpile of enriched uranium is held at various enrichment levels and is sufficient in U-235 to fuel five nuclear warheads. Thus, these calculations assume that Iran would use this enriched stockpile in a dash to make weapons. The following table estimates Iran's stockpile as of May 15, 2022.

IRAN'S ESTIMATED STOCKPILE (5/15/22)	IF ENRICHED TO WEAPON GRADE (90% PRODUCT)	SWU REQUIRED	NUMBER OF NUCLEAR WEAPONS
33.6 kg up to 60% U-235 (~54%)	20 kg	95 SWU	One weapon (95 SWU)
9.5 kg up to 60% U-235 (~54%)	5.7 kg	27 SWU	
74.9 kg up to 20% U-235 (~18%)	14.3 kg	225 SWU	Two weapons (347 SWU)
104.7 kg up to 20% U-235 (~18%)	20 kg	315 SWU	Three weapons (662 SWU)
58.8 kg up to 20% U-235 (~18%)	11.2 kg	177 SWU	
223 kg up to 5% U-235 (~4.5%)	8.7 kg	360 SWU	Four weapons (1,199 SWU)
508.6 kg up to 5% U-235 (~4.5%)	20 kg	821 SWU	Five weapons (2,020 SWU)

These theoretical calculations are generated using a SWU calculator published by URENCO, a European uranium enrichment consortium. The calculations assume that 100 kg of 90% U-235 in the form of UF6 would be needed for an arsenal of five nuclear weapons. The tails are assumed to be 1% and because the IAEA describes the enrichment level as "up to" a percentage, a lower feed enrichment percentage is used for these calculations (included parenthetically).

With an output of .8 SWU annually, Iran's 32 cascades of IR-1 centrifuges at FEP (assumed to contain about 168 machines per cascade) would generate about 4,301 SWU per year, Iran's 1044 IR-1 centrifuges at FFEP would produce about 835 SWU per year, and Iran's six cascades of IR-2m centrifuges at FEP (assumed to contain about 174 machines per cascade) would generate about 4,176 SWU per year assuming an operational capacity of 4 SWU per machine. The IR-2m is based on Pakistan's P-2 centrifuge and is assumed in these estimates to have a nominal output of 5 SWU.

If Iran chose to produce enough enriched uranium for one weapon, it could do so by feeding uranium enriched up to 60% U-235 into either the cascades of IR-1 or IR-2m centrifuges at FEP. In either case, it would take the centrifuges at least 1.2 weeks to accomplish the necessary enrichment work (95 SWU). To reduce the time further would require feeding both the IR-1 and IR-2 cascades at the same time, an additional step Iran may not deem necessary in light of the short time frame.

[6] If Iran fed uranium enriched up to 60% U-235 and up to 20% U-235 into its IR-1 and IR-2m centrifuges being fed in production mode at FEP, at their estimated capacity of 8,477 SWU (see Note 5 above) they would take at least 2.1 weeks to accomplish the necessary enrichment work for two weapons (347 SWU).

[7] If Iran fed uranium enriched up to 20% U-235 into all of its IR-1 and IR-2m centrifuges being fed in production mode, at their estimated capacity of 9,338 SWU (see Note 5 above) they would take at least 3.7 weeks to accomplish the necessary enrichment work for three weapons (662 SWU).

[8] If Iran fed uranium enriched up to 20% U-235 and uranium enriched up to 5% U-235 into all of its IR-1 and IR-2m centrifuges being fed in production mode, at their estimated capacity of 9,312 SWU (see Note 5 above) they would take at least 6.7 weeks to accomplish the necessary enrichment work for four weapons (1,199 SWU).

[9] If Iran fed uranium enriched up to 5% U-235 into all of its IR-1 and IR-2m centrifuges being fed in production mode, at their estimated capacity of 9,312 SWU (see Note 5 above) they would take at least 11.3 weeks to accomplish the necessary enrichment work for five weapons (2,020 SWU).

[10] Iran has been operating six cascades of IR-2m centrifuges (approximately 1,044 machines) in production mode since November 2021. The IR-2m is based on Pakistan's P-2 centrifuge and is assumed in these estimates to have an operational output of 4 SWU (and a nominal output of 5 SWU). See Alexander Glaser, "Characteristics of the Gas Centrifuge for Uranium Enrichment and Their Relevance for Nuclear Weapon Proliferation (corrected)," Science and Global Security, Vol. 16, Nos. 1-2 (2008), p. 9.

[11] 3,000 IR-2m centrifuges, each with an operational output of 4 SWU, would produce approximately 12,000 SWU in one year. If about 4,000 SWU are needed to produce the 20 kg of 90% U-235 to fuel one weapon (assuming tails of .3% and a feed assay of .7% U-235) then it would take at least 4 months to produce the 4,000 SWU.

[12] The same 3,000 IR-2m centrifuges, producing an assumed 12,000 SWU per year, would produce the 20,000 SWU needed to fuel 5 weapons in approximately one year and eight months.

[13] Each centrifuge is assumed to require about one square meter (10.7 square feet) of space, the amount used in Iran's enrichment plant at Natanz. The ice surface of a National Hockey League rink is 200 feet long and 85 feet wide.

[14] 1,000 centrifuges at 10.7 square feet each would require about 11,000 square feet.

[15] "Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015) (GOV/2022/22)," International Atomic Energy Agency, May 30, 2022, paragraph 13.

[16] "Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015) (GOV/2022/22)," International Atomic Energy Agency, May 30, 2022, paragraph 17.

[17] "Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015) (GOV/2022/22)," International Atomic Energy Agency, May 30, paragraphs 22 and 23.
[18] "Verification and Monitoring in the Islamic Republic of Iran in Light of United Nations Security Council Resolution 2231 (2015) (GOV/2022/4)," International Atomic Energy Agency, March 3, 2022, paragraph 20.
[19] The 1,044 IR-1 centrifuges at Fordow generate about 835 SWU annually, if operated at their historic production rate of .8 SWU each. If this amount of work is used to enrich feed at about 4% enrichment to a level of about 20% enrichment, which Iran plans to do at Fordow, Iran would require 435 kg of about 4% feed to produce 82 kg of 20% product annually. To produce the 435 kg of about 4% feed from natural uranium, as Iran expects the IR-6 centrifuges to do, would require 2,295 SWU. Dividing the 2,295 SWU by the number of IR-6 machines in the two cascades yields about 6.6 SWU per machine for two cascades of 174 machines (the number used at Fordow for the IR-1 machines) or about 7 SWU for two cascades of 164 machines (the number used at Natanz for the IR-6 machines in production mode).
[20] Iran has claimed that the IR-6 centrifuge is ten times more powerful than the IR-1. The IR-6 is assumed in these estimates to have an operational output of 8 SWU (80% of the nominal output of 10 SWU). See Kiyoko Metzler, "UN Atomic Watchdog Raises Questions of Iran's Centrifuge Use," Associated Press, May 31, 2019.
[21] 3,000 IR-6 centrifuges each producing 8 SWU per year would produce in one year 24,000 SWU, or 2,000 SWU per month. Thus, it would take two months to produce the 4,000 SWU needed to fuel one weapon.
[22] 3,000 IR-6 centrifuges would produce the 20,000 SWU needed to fuel five weapons in about ten months.
[23] See Thomas B. Cochran and Christopher E. Paine, "The Amount of Plutonium and Highly Enriched Uranium Needed for Pure Fission Nuclear Weapons," (Washington, DC: Natural Resources Defense Council, revised April 13, 1995).
[24] Russia and Iran signed a nuclear fuel agreement in 1995. Under the agreement, Russia committed to supplying fuel for Bushehr for ten years and Iran committed to returning the spent fuel to Russia. Reportedly, the original 1992 nuclear cooperation agreement between Russia and Iran stipulated that Russia would supply fuel for the Bushehr reactor "for the entire lifespan of the nuclear power plant." See Mark Hibbs, "Iran's Russia Problem," Carnegie Endowment for International Peace, July 7, 2014.
[25] See the nuclear fuel cycle simulation system published by the IAEA (http://infcis.iaea.org/NFCSS/NFCSSMain.asp?RightP=Calculation&EPage=2&Re...).

Emirates successfully completes major tests to fully activate the last unit of Barakah Nuclear Power Plant

Source: https://atalayar.com/en/content/emirates-successfully-completes-major-tests-fully-activate-last-unit-barakah-nuclear-power

July 21 – **The Barakah Nuclear Power Plant in the United Arab Emirates is about to become fully operational.** The Emirates Nuclear Energy Corporation (ENEC) announced that it has completed the thermal performance test on Unit 4 of the Barakah Plant, located in the Al-Dhafra region. This marks an important step before the last of the four areas that make up the Emirati facility go into operation, after Unit 1, Unit 2 and Unit 3 successfully completed their final installation for commissioning.

During the thermal performance test of the fourth phase of the infrastructure, a full examination of the plant components in terms of thermal expansion and vibration

factors was completed, and the results showed that all systems perform to the highest standards of quality and safety under normal operating conditions.

In particular, **the test included pressure device safety valve testing, reactor cooling system flow measurement and main turbine system testing,** which confirmed that the plant's main components and systems function as designed and meet all requirements for normal operation, as reported by Al-Ain News.

This thermal performance test means a process of several weeks as up to 200 individual and integrated tests have to be performed to determine how the system performs in full operation. The so-called Hot Functional Testing (HFT) phase seeks to verify performance under normal operating conditions, without the presence of nuclear fuel assemblies in the reactor vessel. However, it also provides data on operation under less ideal conditions.

Sheikh Mohammed bin Zayed al-Nahyan, Crown Prince of Abu Dhabi, visits the Barakah Nuclear Power Plant.

Prior to the temperature assessment test, **ENEC also completed structural integrity and integrated leak rate tests of Barakah Unit 4.** The data provided by these tests confirmed the durability of the infrastructure of the fourth phase of the plant in terms of its ability to continue operating under normal and more challenging conditions.

In this regard, **Mohammed Ibrahim al-Hammadi, managing director and CEO of ENEC, said: "The completion of these tests at Barakah Unit 4 confirms the continuous progress in developing plants in accordance with local regulatory requirements and the highest international standards,"** as reported by Al-Ain News.

Al-Hammadi added: **"The work teams have applied all the lessons learned from the development of all the stations, resulting in an increase in completion efficiency while maintaining commitment to the highest international standards of quality and safety.** These tests are a major step towards the operational phase of the fourth station, and bring us closer to commercial operation of all Barakah stations, producing abundant, reliable and environmentally friendly electricity, as well as supporting the transition to environmentally friendly energy sources in the UAE, and enhancing energy security for the next 60 years. As a result, the Barakah plants play a key role in supporting the country's efforts to achieve climate neutrality goals by 2050," Al-Ain News specified.

Prior to the final implementation of Unit 4, ENEC had completed the relevant tests of Unit 3, including the safe and successful integration of the main power transformer and gas isolation line (GIB), an important test and key step for the proper operation of the plant. In addition to the main transformer and GIB, the auxiliary power transformers and excitation transformer of Unit 3 were safely and successfully energised in normal operating configuration a few months ago.

This is a clear commitment by the Gulf country to promote energy sources other than fossil fuels, which have been the mainstay of national revenues until now. Emirates is now seeking to diversify its economy and also to vary its energy sources so as not to rely solely on oil and natural gas and to improve its position in terms of environmental protection thanks to cleaner and more environmentally friendly energy sources.

The last unit of the Barakah Nuclear Power Plant began construction in 2015, three years after the start of work on Unit 1, and the development work has been carried out throughout these years without problems and with the strong support of the Emirati government, focused on reducing the carbon footprint of the national energy sector in order to achieve the long-awaited climate neutrality by 2050, as required by the United Nations.

Once fully operational, **the four units will supply 25% of the country's electricity consumption** and cut up to 22.4 million tonnes of carbon emissions per year, which is equivalent to the emissions of 4.8 million cars each year.

The Barakah plants are among the largest nuclear power plants in the world, with four APR-1400 advanced design reactors. In addition, all areas of Barakah are expected to contribute the most to reducing carbon emissions from the power and water sector in the Emirate of Abu Dhabi by 50%, in addition to producing more than 85% of the Emirate's clean and environmentally friendly electricity.

The Barakah Nuclear Power Plant thus becomes a global benchmark for new nuclear construction projects worldwide.
All four units have been under construction simultaneously over the past few years, a testament to the hard work being done on Emirati soil. This true feat of energy and construction in the Emirates was achieved through close cooperation with the prime contractor and joint venture partner, Korea Electric Power Corporation of South Korea (KEPCO), as well as expert teams from Nawah Energy Company and Abu Dhabi Transmission and Despatch Company (TRANSCO). The engineering challenge of this infrastructure is demonstrated by the number of people involved in the construction of the project, which amounts to 18,000.

Iran said building vast new underground tunnels to hold nuclear enrichment facility

Source: https://www.timesofisrael.com/iran-said-building-vast-new-underground-tunnels-to-hold-nuclear-enrichment-facility/

June 2022 – Iran is constructing a vast new network of tunnels at its Natanz nuclear site that could house a massive enrichment facility that would be impervious to bunker-busting bombs and cyberattacks, the New York Times reported Thursday.

This satellite image from Planet Labs PBC shows Iran's underground Natanz nuclear site, as well as ongoing construction to expand the facility in a nearby mountain south of Natanz. Iran, May 9, 2022. (Planet Labs PBC via AP)

The report said that the US and Israel had been monitoring construction at the site for several months, but had refrained from commenting on it publicly, with the exception of a brief remark made last month by Defense Minister Benny Gantz.

"At this very time, Iran is making an effort to complete the production and installation of 1,000 advanced IR6 centrifuges at its nuclear facilities, including a new facility being built at an underground site near Natanz," he said, speaking at a conference at Herzliya's Reichman University.
Gantz's public comments surprised both US and Israeli officials, the report said. Iran did not deny the accusation, having previously said it was constructing new facilities in response to attacks at the existing Natanz site, blamed on Israel.
Sattelite images published recently by research groups show that the new facility is close to the old center at Natanz, but buried far deeper under a mountain, in a similar manner to the Fordow plant. Efforts to attack such a site would require the most advanced bunker-busters, which Israel does not yet possess.
The report noted that the Americans and Israelis differ sharply over the seriousness of the implications of the construction.
Biden administration officials told the Times that they have been following the construction for more than a year and they were not especially alarmed.
They pointed out that the facility, which would be deep underneath a mountain, would not be ready for several years, giving the Americans time to deal with it either through diplomacy or force should the need arise.
They believe that the primary purpose of the new facility is to replace the centrifuge facility that was severely damaged in a sophisticated attack last year, blamed on Israel.

This photo released July 2, 2020, by the Atomic Energy Organization of Iran, shows a building after it was damaged by a fire, at the Natanz uranium enrichment facility some 200 miles (322 kilometers) south of the capital Tehran, Iran. (Atomic Energy Organization of Iran via AP)

And while it would not play a role in Iranian abilities to construct a nuclear weapon in the near future, Tehran was using its existence to pressure the US into concessions in talks over a return to the nuclear deal.
Talks between Iran and world powers in Vienna to revive the 2015 nuclear deal have stalled.
The nuclear deal collapsed four years ago when former US president Donald Trump withdrew the United States and imposed crushing sanctions on Iran. In the meantime, Iran has vastly expanded its nuclear work, while insisting that it is for peaceful purposes.
"The Iranians' highest priority is using the nuclear threat to gain concessions, economic and otherwise," Gen. Kenneth F. McKenzie Jr., the recently retired head of US Central Command, told the Times.
Israeli officials, however, view the site very differently.
They see it as further evidence of Iran's efforts to achieve nuclear weapons capabilities and justification for Israeli efforts to thwart the program, the Times said. The report said the construction could be behind what it called accelerated Israeli efforts to thwart the program, referencing several recent attacks on Iranian scientists and engineers blamed on Israel.

It also noted that construction of the new site began around the same time as the killing of the father of Iran's nuclear program Mohsen Fakhrizadeh, which has also been blamed on Israel.
In his recent speech, Gantz said Iran is just a "few weeks" from accumulating sufficient fissile material for a bomb.
"Iran continues to accumulate irreversible knowledge and experience in the development, research, production, and operation of advanced centrifuges," Gantz said.
"It stands just a few weeks away from accumulating fissile material that will be sufficient for a first bomb, holds 60 kg of enriched material at 60%, produces metallic uranium at the enrichment level of 20%, and prevents the IAEA from accessing its facilities," he added, before revealing the construction at Natanz.
The Times report quoted several Israeli officials as saying they believe Iran's ultimate objective is to use the facility to enrich uranium at a mass scale, using advanced new centrifuges.
American officials concede the new facility is quite large, and usually well protected, the Times said.
But while much of the West's focus was on Iran's nuclear program, General McKenzie warned that the major current threat came from Iran's ballistic missiles, cruise missiles and drones, which he called Tehran's "crown jewels."
"And that's where they've made huge strides in the last five to seven years," General McKenzie said, "where they now realistically have overmatch against their neighbors."

Chernobyl: The Lost Tapes | Official Trailer | HBO

Will We Survive The Biden Presidency?

Iran threatens to nuke NYC...

Source: https://andmagazine.substack.com/p/will-we-survive-the-biden-presidency

Aug 02 – Joe Biden says Ayman Zawahiri is dead, killed in a U.S. drone strike in Afghanistan. If true, the world is certainly a better place. It is not a safer one.

Zawahiri was not in any sense the operational commander of Al Qaida when killed. His death, balanced against the loss of Afghanistan and the worldwide debacle of American foreign policy under Biden, will mean nothing. Whatever plans Al Qaida was making yesterday to attack the United States are continuing today unabated.

Meanwhile, even as we stand on the brink of war with China, the Iranians are ramping up their rhetoric, signaling they are about to go nuclear and *threatening to use atomic bombs on New York City.*

An Iranian Revolutionary Guard Corps (IRGC) Telegram channel called 'Bisimchi Media' recently published a video saying that Iran will quickly complete the development of nuclear weapons capable of "turning New York into hellish ruins" if the United States "makes any stupid mistakes." The video was entitled "*When Will Iran's Sleeping Nuclear Warheads Awaken*".

"According to intelligence delivered to Israel by England's espionage organization, Iran has amassed sufficient material to build a nuclear bomb, and in case of a Western attack, the mission to execute the nuclear breakthrough, which is called Project Emad, was assigned to the secret facilities in Fordo. The Fordo nuclear facilities are located deep in the mountains, in the center of Iran, and they can withstand [an attack] by a "Bunker Buster," or even a nuclear bomb. This center guarantees Iran's atomic power, and it is equipped with all the infrastructure needed for a nuclear breakthrough.

> "According to the orders of the Islamic Republic of Iran's War Command Center, the Natanz facilities are very vulnerable to a possible attack by Israel and the West, but if a single missile hits these facilities, the Fordo facilities will go into battle readiness, and will execute the nuclear breakthrough project on their own, in a short time.
> "Another matter that makes America very cautious in its positions towards Iran is Iran's intercontinental missiles.
> "This technology was achieved with the help of the space program, and in case of a hostile measure by America, it gives Iran the ability to turn New York into a heap of rubble from Hell. This [video] was produced by Bisimchi Media."
> Bisimchi Media

It is a measure of the seriousness of this threat to note that Iran is now openly talking about the EMAD program, *which up until now it has claimed is a figment of the Western imagination.* All pretense of a peaceful purpose for Iran's nuclear work is now gone. They are quite clear. *They are about to field operational nuclear weapons.*

It is also well worth noting that, in effect, the Iranians have also now admitted that their "space" program was all along a cover for developing the capability to develop intercontinental ballistic missiles. They may or may not actually have the capability today to hit Manhattan with a missile. There is no question any longer about their intentions.

Perhaps the most significant thing about the Iranian threat to attack New York City, though, is that they made it at all. Under previous administrations, the ayatollahs would have thought twice about poking the bear. They most certainly would never have given Donald Trump any justification for firing back, not after Qasem Soleimani went to meet his maker.

Not anymore. There is no fear. There is no respect. The man in the White House is the mentally incompetent stooge of the Chinese Communist Party. We are betrayed at the highest possible level. The sharks are circling.

It is time to start asking ourselves – as a nation will we survive Joe Biden's Presidency?

Russian-held Ukraine nuclear plant 'out of control', IAEA chief warns

Source: https://www.scmp.com/news/world/europe/article/3187558/russian-held-ukraine-nuclear-plant-out-control-iaea-chief-warns

Aug 02 – The UN nuclear chief warned that Europe's largest nuclear power plant in Ukraine "is completely out of control" and issued an urgent plea to Russia and Ukraine to quickly allow experts to visit the sprawling complex to stabilise the situation and avoid a nuclear accident.

Rafael Grossi, director general of the International Atomic Energy Agency, said in an interview with Associated Press that the situation was getting more perilous every day at the Zaporizhzhia plant in the southeastern city of Enerhodar, which Russian troops seized in early March, soon after their February 24 invasion of Ukraine.

"Every principle of nuclear safety has been violated" at the plant, he said. "What is at stake is extremely serious and extremely grave and dangerous."

Grossi cited many violations of the plant's safety, adding that it is "in a place where active war is ongoing," near Russian-controlled territory.

The physical integrity of the plant hasn't been respected, he said, citing shelling at the beginning of the war when it was taken over and continuing information from Ukraine and Russia accusing each other of attacks at Zaporizhzhia.

There is "a paradoxical situation" in which the plant is controlled by Russia, but its Ukrainian staff continues to run its nuclear operations, leading to inevitable moments of friction and alleged violence, he said.

While the IAEA has some contacts with staff, they are "faulty" and "patchy," he said.

Grossi said the supply chain of equipment and spare parts has been interrupted, "so we are not sure the plant is getting all it needs". The IAEA also needs to perform very important inspections to ensure that nuclear material is being safeguarded, "and there is a lot of nuclear material there to be inspected," he said.

"When you put this together, you have a catalogue of things that should never be happening in any nuclear facility," Grossi said. "And this is why I have been insisting from day one that we have to be able to go there to perform this safety and security evaluation, to do the repairs and to assist as we already did in Chernobyl."

On Monday, US Secretary of State Antony Blinken accused Moscow of using the plant as a "military base to fire at Ukrainians, knowing that they can't and won't shoot back because they might accidentally strike a nuclear … reactor or highly radioactive waste in storage".

"That brings the notion of having a human shield to an entirely different and horrific level," he said.

A Russian firing position at the Chernobyl nuclear power plant in April. File photo: AP

The Russian capture of Zaporizhzhia renewed fears that the largest of Ukraine's 15 nuclear reactors could be damaged, setting off another emergency like the 1986 Chernobyl accident, the world's worst nuclear disaster, which happened about 110km (65 miles) north of the capital Kyiv.

Russian forces occupied the heavily contaminated site soon after the invasion but handed control back to the Ukrainians at the end of March.

Grossi visited Chernobyl on April 27 and tweeted that the level of safety was "like a 'red light' blinking". But he said on Tuesday that the IAEA set up "an assistance mission" at Chernobyl at that time "that has been very, very successful so far".

The IAEA needs to go to Zaporizhzhia, as it did to Chernobyl, to ascertain the facts of what is actually happening there, to carry out repairs and inspections, and "to prevent a nuclear accident from happening," Grossi said.

The IAEA chief said he and his team need protection to get to the plant and the urgent cooperation of Russia and Ukraine.

Each side wants this international mission to go from different sites, which is understandable in light of territorial integrity and political considerations, he said, but there's something more urgent and that is getting the IAEA team to Zaporizhzhia.

"The IAEA, by its presence, will be a deterrent to any act of violence against this nuclear power plant," Grossi said. "So I'm pleading as an international civil servant, as the head of an international organisation, I'm pleading to both sides to let this mission proceed." Grossi was in New York to deliver a keynote speech at Monday's opening of the long-delayed high-level meeting to review the landmark 50-year-old Nuclear Nonproliferation Treaty aimed at preventing the spread of nuclear weapons and eventually achieving a nuclear-free world.

Why Are Nuclear Weapons So Hard to Get Rid Of? Because They're Tied Up in Nuclear Countries' Sense of Right and Wrong

By Thomas E. Doyle, II

Source: https://www.homelandsecuritynewswire.com/dr20220805-why-are-nuclear-weapons-so-hard-to-get-rid-of-because-they-re-tied-up-in-nuclear-countries-sense-of-right-and-wrong

Aug 05 – Every five years, the nearly 200 member states of the Treaty on the Nonproliferation of Nuclear Weapons meet to review their progress – or lack thereof. After being postponed because of the COVID-19 pandemic, the monthlong conference is now meeting in New York and opened with a stark warning.

The world is "just one misunderstanding, one miscalculation away from nuclear annihilation," United Nations Secretary-General Antonio Guterres said Aug. 1, 2022, citing growing conflicts and weakening "guardrails" against escalation.

The treaty has three core missions: preventing the spread of nuclear weapons to states that do not have them, ensuring civil nuclear energy programs do not turn into weapons programs, and facilitating nuclear disarmament. The last review conference, held in 2015, was widely regarded as a nonproliferation success but a disarmament failure, with the five members that possess nuclear weapons failing to make progress toward eliminating their nuclear arsenals, as promised in previous conferences.

At the heart of this dispute are states' motivations for keeping nuclear weapons – often perceived as rooted in hard-nosed security strategy, by which morality is irrelevant or even self-defeating.

As a nuclear ethicist, though, I see these explanations as incomplete. To understand leaders' motives – and therefore effectively negotiate the elimination of nuclear weapons – other scholars and I argue we must acknowledge that policymakers express underlying moral concerns as strategic concerns. History shows that such moral concerns often form the foundations of nuclear strategy, even if they're deeply buried.

National Values

It is easier for many people to see how the nuclear abolitionist argument is fundamentally based in morality. The fear of nuclear winter – or even a less severe "nuclear autumn" – is rooted in the immorality of killing millions of innocent people and devastating the environment in long-lasting ways.

By contrast, a realistic and strategic approach to the value of nuclear weapons has dominated security discourse since the early Cold War era. This approach argues that the primary purpose of nuclear weapons is to deter adversaries from attacking vital national security interests. If an attack does occur, then nuclear weapons can be used to punish aggression in a proportional way and caution other adversaries, restoring nuclear deterrence.

Even so, according to political scientist Joseph Nye, the assistant secretary of defense for international security affairs under President Bill Clinton, a strategist may pose as a moral skeptic but "tends to smuggle his preferred values into foreign policy, often in the form of narrow nationalism."

Nationalism asserts the moral priority of one's own nation over others. Communities' deep-held beliefs are intimately woven into ideas about nationhood, security and prestige.

In the United States, for example, the moral underpinnings of American identity are deeply rooted in the idea of being "a city on a hill": an example the rest of the world is watching. Americans are anxious about losing their way, and many feel that their country was once a force for good in the world, but no longer. Thus, national survival is embraced as a moral value, and deterring or defending against aggression has strategic, political and moral overtones. Regardless of whether someone thinks these concerns are justified, it is important to recognize that, in their defenders' view, they go beyond strategy or sheer survival. They reflect societies' foundational ideas about what is wrong and right – their sense of morality.

Early Motives

So how are these moral concerns applied to the questions of nuclear weapons and their role in security strategy? It is worth remembering what motivated President Franklin D. Roosevelt to authorize the development of the atomic bomb: the genocidal evil of Nazi German aggression in World War II and the knowledge that Adolf Hitler had begun an atomic

bomb program. And when Nazi Germany had been defeated, the U.S. justifications for using atomic bombs on the Japanese cities of Hiroshima and Nagasaki centered on two kinds of moral concerns. The most frequently invoked was utilitarian: preventing a greater number of deaths in a land invasion of Japan. The second, not expressed as explicitly, viewed the atomic bombing as a kind of moral punishment for the Japanese invasion of Pearl Harbor and the brutal treatment of Allied prisoners of war.
In short, the motivations for the original atomic bomb program and its uses could not be described in solely "hard-nosed" strategic terms. As political philosopher Michael Walzer has argued, both morality and strategy are about justification: Both tell us what we should do or should not do, based on some set of values. And strategy is often used for decision-makers' moral aims, such as their goal to defeat a genocidal regime.

Morally Excusable?
Along with other scholars, I have argued that moral concerns also motivated the central role of nuclear deterrence policy during the Cold War. American policymakers portrayed Soviet communism, like Nazism, as a politics of brute force that had no regard for law or morals. Once the Soviet Union and China had acquired nuclear weapons, American analysts came to believe that communism represented an existential threat not only to U.S. security, but to liberal democracy in general. Walzer described such situations as "supreme emergency conditions," in which ordinary moral prohibitions against mass destruction are suspended to ensure what political leaders see as the highest value: national survival. This is self-preservation – but people often think about that, too, as a moral concern. Social norms against suicide, for example, imply that people have a moral duty to preserve their lives except under certain conditions, reflecting a belief that human life has intrinsic moral value. Walzer did not claim that using nuclear weapons, or even threatening their use, was morally justified. However, he suggested they might be necessary for national security, and therefore become morally excusable in supreme emergency situations. His argument has been very influential in government and academic circles. Many critics claim that it is always immoral to use nuclear weapons, since they cannot discriminate between soldiers and innocent civilians, including children, the elderly and the infirm. Moreover, the use of nuclear weapons cannot but bring social and environmental catastrophe, the kind that our darkest dystopian novels and films depict. And if it is immoral to use nuclear weapons, it is immoral to threaten to use them. But it is unsurprising that the leaders of the nuclear-weapon states are ultimately committed to the survival of their countries and peoples, even if others must pay an ultimate price. To fully appreciate nuclear motivations, we must understand the role of this kind of moral concern in their decision-making.

Thomas E. Doyle, II is Associate Professor of Political Science, Texas State University.

My message from Hiroshima

By António Guterres, Secretary-General of the United Nations.
Source: https://www.thejakartapost.com/opinion/2022/08/05/my-message-from-hiroshima-.html

Hopes float: A girl releases floating lanterns to mourn atomic bomb victims on the Motoyasu River beside the atomic bomb dome during the 74th anniversary of the atomic bombing in Hiroshima on Aug. 6, 2019. (Jiji Press/AFP)

Aug 07 – On Saturday, I proudly stood with Japan's Prime Minister, Fumio Kishida, and the people of Hiroshima in memory of an unprecedented catastrophe. Seventy-seven years ago, nuclear weapons were dropped on the people of Hiroshima and Nagasaki. Tens of thousands of women, children and men were killed in the blink of an eye, incinerated in a hellish fire. Buildings turned to dust. The cities' beautiful rivers ran with blood. Those who survived were cursed with a radioactive legacy, stalked by health problems, and subjected to lifelong stigma because of the nuclear bombing. I had the great honor of meeting with a group of those survivors — the hibakusha, whose numbers grow smaller each year.

They told me with unflinching bravery what they witnessed on that terrifying day in 1945. It is time for world leaders to be as clear-eyed as the hibakusha and see nuclear weapons for what they are. Nuclear weapons make no sense. They cannot deliver safety, protection or security. By design, they deliver only death and destruction. Three-quarters of a century have passed since mushroom clouds swelled above Hiroshima and Nagasaki. Since then, humanity has endured a Cold War, decades of absurd brinksmanship, and several terrifying near-misses that placed humanity within minutes of annihilation. But even during the depths of the Cold War, nuclear powers made significant reductions in their nuclear arsenals. There was widespread acceptance of the principles against the use, proliferation and testing of nuclear arms. Today, we are in danger of forgetting the lessons of 1945. A new arms race is picking up speed, with governments spending hundreds of billions of dollars to upgrade their stockpiles of nuclear arms. Almost 13,000 nuclear weapons are now held in arsenals around the world. Geopolitical crises with grave nuclear undertones are spreading fast, from the Middle East, to the Korean peninsula, to Russia's invasion of Ukraine. Once again, humanity is playing with a loaded gun. We are one mistake, one misunderstanding, one miscalculation away from Armageddon. Leaders must stop knocking on doomsday's door and take the nuclear option off the table for good. It is unacceptable for states in possession of nuclear weapons to admit the possibility of nuclear war, which would spell the end of humanity. By the same token, countries with nuclear weapons must commit to the "no first use" of those weapons. They must also assure States that do not have nuclear weapons that they will not use — or threaten to use — nuclear weapons against them, and be transparent throughout. Nuclear saber-rattling must stop. In the end, there is only one solution to the nuclear threat: not to have nuclear weapons at all. This means opening every avenue of dialogue, diplomacy and negotiation to ease tensions and eliminate these deadly weapons of mass destruction. We are seeing fresh signs of hope in New York, where the world has come together for the Tenth Review Conference on the Treaty on the Non-Proliferation of Nuclear Weapons. The Treaty is one of the main reasons why nuclear weapons have not been used since 1945. It contains legally binding commitments to achieve nuclear disarmament, and can be a powerful catalyst for disarmament — the only way to eliminate these horrendous weapons once and for all. And in June, members of the Treaty on the Prohibition of Nuclear Weapons met for the first time to develop a roadmap towards a world free of these doomsday devices. We can no longer accept the presence of weapons that hang by a slender thread over humanity's future.

It is time to heed the timeless message of the hibakusha: "No more Hiroshimas! No more Nagasakis!" It is time to proliferate peace. Together, step by step, let's wipe these weapons off the face of the earth.

EDITOR'S COMMENT: Why all speeches for disasters (natural and man-made) end with the same last sentence that is a wish far apart reality? No more school shooting! No more 9/11 or 7/7! No more wars! No more earthquakes, floods or wildfires! No more nuclear weapons! Until next time …

The myth that Hiroshima was necessary

By Peter van Buren

Source: https://www.spectator.com.au/2022/08/the-myth-that-hiroshima-was-necessary/

Aug 06 – If you think the falsehoods spilling out of Ukraine about casualties and atrocities are shocking, meet the greatest lie of modern history. August 6 marks the seventy-seventh anniversary of the nuclear destruction of Hiroshima and death of some 140,000 non-combatants. Yet the only nation in history to employ a weapon of mass destruction on an epic scale, against an undefended civilian population, shrugs off the significance of an act of immorality.

Beyond the destruction lies the myth of the atomic bombings, the post-war creation of a mass memory of things that did not happen. This myth has become the underpinning of American policy ever since, and carries forward the horrors of Hiroshima as generations pass.

The myth, the one kneaded into public consciousness, is that the bombs were dropped out of grudging military necessity, to hasten the end of the war, to avoid a land invasion of Japan, maybe to give the Soviets a good pre-Cold War scare. Nasty work, but such is war. As a result, the attacks need not provoke anything akin to introspection or national reflection. The possibility, however remote, that the bombs were tools of revenge or malice, immoral acts, was defined away. They were merely necessary and, because we won in the end, justified. That is the evolved myth, but it was not the way the atomic bombings were first presented to the American people.

Harry Truman, in his 1945 announcement of the bomb, focused on vengeance, and on the new power to destroy at a button push. "We are now prepared to obliterate more rapidly and completely every productive enterprise the Japanese have above ground in any city," said Truman. The plan put into play on August 6 — to force the Japanese government to surrender by making it watch mass casualties of innocents — speaks to a scale of cruelty previously unseen. It was fair: they'd started it, after all, and they deserved the pain. Imagine that idea cut loose in Ukraine.

Visitors at Hiroshima Peace Memorial Museum view a large scale panoramic photograph of the aftermath of the atomic bomb attack on Hiroshima (Getty Images)

The need to replace that justification with one of grudging military necessity, a tool for *saving* lives, grew out of John Hersey's account of the human suffering in Hiroshima, first published in 1946 in the *New Yorker*. Owing to wartime censorship, Americans knew little of the ground truth of atomic war, and Hersey's piece was shocking enough to the public that it required a formal response. Americans' belief that they're a decent people needed to be reconciled with the indecency of what had been done. With the Cold War getting underway, and with American leadership fully expecting to obliterate a few Russian cities in the near future, some nuclear philosophical groundwork needed to be laid.

And so the idea the bombing of Hiroshima as a "necessity" appeared in a 1947 article, signed by former secretary of war Henry Stimson, though actually drafted by McGeorge Bundy (later an architect of the Vietnam War) and James Conant (a scientist who helped build the original bomb). Dr. Conant described the article's purpose as countering Hersey's account at the beginning of the Cold War as "You have to get the past straight before you do much to prepare people for the future."

The Stimson article was the moment of formal creation of the Hiroshima myth. A historically challengeable argument was recast as unquestionable — drop the bombs or kill off tens of thousands or maybe even millions (the US regularly revised casualty estimates upwards) of American boys in a land invasion of Japan. It became gospel that the Japanese would never have surrendered, though of course surrender was in fact exactly what happened. Nonetheless, such lies were created to buttress a national belief that no moral wrong was committed, and thus there was no need for introspection by the United States.

No later opportunity to bypass reflection was missed. American presidents from Truman to Bush chose not to visit Hiroshima. The fiftieth anniversary of the bombing saw a moderately reflective planned exhibit at the Smithsonian turned into a patriotic orgy that only reinforced the "we had no choice" narrative. When Barack Obama became the first sitting president to visit Hiroshima in 2016, his spokespeople went out of their way to make clear he would be looking only forward with ally Japan, the mushroom cloud safely out of sight.

American foreign policy thus proceeded under a grim calculus that finds some acts of violence are morally justified simply because of who pulls the trigger, with much of the history of the next seventy-seven years a series of immoral acts allegedly servicing, albeit

destructively and imperfectly, the moral imperative of saving lives by killing. America's decisions on war, torture, rendition and indefinite detention could be explained in character as the distasteful but necessary actions of fundamentally good people against fundamentally evil ones. Hiroshima set in motion a sweeping, national generalization that if we do it, it is right.
We are, in fact, able to think we are practically doing the people of Afghanistan, Iraq, Syria, Yemen, Libya and Somalia a favor by killing some of them, as we believe we did for tens of thousands of Japanese who might have been lost in a land invasion of their home islands. There is little discussion because debate is largely unnecessary; the myth of Hiroshima says expediency wipes away concerns over morality. And with that neatly tucked away in our conscience, all that's left is to ponder where to righteously strike next. Donbas perhaps?
America's deliberate targeting of civilians, and its post-facto justifications, are clearly not unique, either in World War Two or in the wars before or since. Other nations, including Japan itself, added their own horror to the books, without remorse. But history's only use of nuclear weapons holds a significant place in infamy, especially on this August 6. America's lack of introspection over one of the single most destructive days in the history of human warfare continues, with 21st-century consequences.

The Unbearable Weight of Hiroshima and Nagasaki: Where We Stand on August 6 and 9, 2022

By H. Patricia Hynes
Source: https://www.juancole.com/2022/08/unbearable-hiroshima-nagasaki.html

Aug 06 – August 6 and 9 mark the 77th year since the United States dropped atomic bombs on the Japanese cities of Hiroshima and Nagasaki, annihilating instantly an estimated 170,000 women, men and children and sentencing tens of thousands more to eventual death from radiation poisoning and injuries.
American military leaders from all branches of the armed forces strongly dissented from the decision to use the bombs, some before August 1945, some in retrospect, for both military and moral reasons. On Armistice Day 1948, Army General Omar Bradley captured the soulless militarism ruling the US government: "Ours is a world of nuclear giants and ethical infants. We know more about war than we know about peace, more about killing than we know about living**."**
Who are the "ethical infants," the "we" who "know more about war than… about peace, more about killing than about living?"

Not the 122 Countries
that voted in 2017 to approve the United Nations Treaty on the Prohibition of Nuclear Weapons, despite heavy pressure by nuclear nations, foremost the United States, not to do so. By August 2022, 66 countries have ratified the Treaty; many more are in the process of doing so. Consider this a marathon for disarmament to outpace the current insane nuclear arms race in which all nine nuclear-armed countries are, in lockstep, upgrading their weapons.

Not the US Conference of Mayors
a hugely influential group, representing 1,400 US cities of more than 30,000 citizens, that in August 2021 unanimously adopted a resolution calling on Washington to embrace the Treaty on the Prohibition of Nuclear Weapons as a step toward finally ridding the world of weapons of mass destruction.

Not the Majority of the American Public
which, according to the 2020 Chicago Council Survey, believe that no country should be allowed to have nuclear weapons. These include majorities of Republicans (54%), Democrats (78%) and Independents (64%).

Not Climate Scientists
who recently committed civil disobedience, desperately warning that we have only a few years to stabilize emissions and then reduce them in order to avoid climate catastrophe. They were ignored by mainstream press and their western governments, which have focused exclusively on Russia's war against Ukraine. As a consequence of that war, the U.S. has undertaken new drilling for oil on federal lands, while it has been failing miserably to meet its goal of reducing climate change emissions 50% below 2005 emissions by 2030.

Not Veterans for Peace
who, while holding differing opinions about the roots of the ongoing war in Ukraine and the relative culpability of Russia, US and NATO, are unanimous in ending the conflict as soon as possible.
"*Many of us continue to suffer physical and spiritual wounds from multiple wars; we can tell hard truths. War is not the answer – it is mass murder and mayhem. War indiscriminately kills and maims innocent men, women and children. War dehumanizes soldiers and scars survivors for life. Nobody wins in war but the profiteers. We must end war or it will end us.*"

Not the World Food Program:
whose director David Beaseley rages against an unprecedented food crisis for hundreds of millions in Asia and Africa as a result of Covid, climate crisis, and the lack of grain and cooking oil from Ukraine and Russia. "We are facing hell on Earth…The best thing we can do right now is end the damn war in Russia and Ukraine and get the port open in Odesa."

Not the Bees
The bees
Do not stop
Collecting pollen
When humans
Murder each other
With guns.
The bees think:
How strange,
How low
On the evolutionary scale
Must those humans be,
That they haven't yet
Figured out
How to make honey
Or peace.
(Bees by Alden Solovy)

Not the Trees
which communicate, share nutrients and water, and act to protect each other from pests and other threats by releasing repelling chemicals. Trees connected in forests by underground networks of fungi live far longer lives than isolated trees.
Who, then, are the "ethical infants" who "know more about war than… about peace, more about killing than about living?"

The Masculinized, Militarized Nuclear Nations
among them Russia for its resort to war against Ukraine and US/NATO determined to bring Russia down by feeding the scourge of war with billions of dollars' worth of weapons to Ukraine.

The Weapons Industry
Public Citizen released a new report estimating that military contractors' contributions to US Congressional members in 2022 "could see a nearly 450,000% return on their investment."

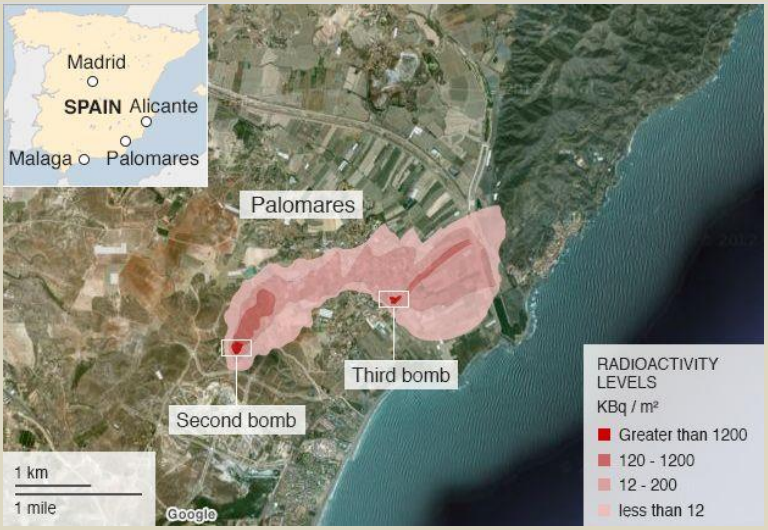
The upgrading of nuclear weapons by nine countries and morbid fantasy of a military solution to the Russian-Ukraine conflict risk life on Earth. Only determined diplomacy, only *ethical giants* can save us from that.

Pat Hynes, a former Professor of Environmental Health at Boston University, is a board member of the Traprock Center for Peace and Justice and a member of Women's International League for Peace and Justice. Her recently published book is *Hope, But Demand Justice*.

The lost nuclear bombs that no one can find

By Zaria Gorvett (senior journalist for BBC Future)
Source: https://www.bbc.com/future/article/20220804-the-lost-nuclear-bombs-that-no-one-can-find

Aug 04 – It was a mild winter's morning at the height of the Cold War.
On January 17, 1966, at around 10:30am, a Spanish shrimp fisherman watched a misshapen white parcel fall from the sky… and silently glide towards the Alboran Sea. It had something hanging beneath it, though he couldn't make out what it was. Then it slipped beneath the waves.
At the same time, in the nearby fishing village of Palomares, locals looked up at an identical sky and witnessed a very different scene – two giant fireballs, hurtling towards them. Within seconds, the sleepy rural idyll was shattered. Buildings shook. Shrapnel sliced towards the ground. Body parts fell to the earth.



A few weeks later, Philip Meyers received a message via a teleprinter – a device a bit like a fax that could send and receive primitive emails. At the time, he was working as a bomb disposal officer at the Naval Air Facility Sigonella, in eastern Sicily. He was told that there was a top secret emergency in Spain, and that he must report there within days.

However, the mission was not as covert as the military had hoped. "It was not a surprise to be called," says Meyers. Even the public knew what was going on. When he attended a dinner party that evening and announced his mysterious trip, its intended confidentiality became something of a joke. "It was kind of embarrassing," says Meyers. "It was supposed to be a secret but my friends were telling me why I was going."

For weeks, newspapers around the globe had been reporting rumours of a terrible accident – two US military planes had collided in mid-air, scattering four B28 thermonuclear bombs across Palomares. Three were quickly recovered on land – but one had disappeared into the sparkling blue expanse to the south east, lost to the bottom of the nearby swathe of Mediterranean Sea. Now the hunt was on to find it – along with its 1.1 megatonne warhead, with the explosive power of 1,100,000 tonnes of TNT.

An unknown number

In fact, the Palomares incident is not the only time a nuclear weapon has been misplaced. There have been at least 32 so-called "broken arrow" accidents – those involving these catastrophically destructive, earth-flattening devices – since 1950. In many cases, the weapons were dropped by mistake or jettisoned during an emergency, then later recovered. But three US bombs have gone missing altogether – they're still out there to this day, lurking in swamps, fields and oceans across the planet.

"We mostly know about the American cases," says Jeffrey Lewis, director of the East Asia Non-proliferation Program at the James Martin Center for Non-proliferation Studies, California. He explains that the full list only emerged when a summary prepared by the US Department of Defense was declassified in the 1980s.

Many occurred during the Cold War, when the nation teetered on the precipice of Mutually Assured Destruction (MAD) with the Soviet Union – and consequently kept airplanes armed with nuclear weapons in the sky at all times from 1960 to 1968, in an operation known as Chrome Dome.

"We don't know as much about other countries. We don't really know anything about the United Kingdom or France, or Russia or China," says Lewis. "So I don't think we have anything like a full accounting."

The Soviet Union's nuclear past is particularly murky – it had amassed a stockpile of 45,000 nuclear weapons as of 1986. There are known cases where the country lost nuclear bombs that have never been retrieved, but unlike with the US incidents, they all occurred on submarines and their locations are known, if inaccessible.

One began on 8 April 1970, when a fire started spreading through the air conditioning system of a Soviet K-8 nuclear-powered submarine while it was diving in the Bay of Biscay – a treacherous stretch of water in the northeast Atlantic Ocean off the coasts of Spain and France, which is notorious for its violent storms and where many vessels have met their end. It had four nuclear torpedoes onboard, and when it promptly sank, it took its radioactive cargo with it.

However, these lost vessels didn't always stay where they were. In 1974, a Soviet K-129 mysteriously sank in the Pacific Ocean, along with three nuclear missiles. The US soon found out, and decided to mount a secret attempt to retrieve this nuclear prize, "which was really a pretty crazy story in and of itself", says Lewis.

The eccentric American billionaire Howard Hughes, famous for his broad spectrum of activity, including as a pilot and film director, pretended to become interested in deep sea mining. "But in fact, it wasn't deep sea mining, it was an effort to build this giant claw that could go all the way down to the sea floor, grab the submarine, and bring it back up," says Lewis. This was Project Azorian – and unfortunately it didn't work. The submarine broke up as it was being lifted.

"And so those nuclear weapons would have fallen back to the sea floor," says Lewis. The weapons remain there to this day, trapped in their rusting tomb. Some people think the weapons remain there to this day, trapped in their rusting tomb – though others believe they were eventually recovered.

Every now and then, there are reports that some of the US' lost nuclear weapons have been found.

Back in 1998, a retired military officer and his partner were gripped with a sudden determination to discover a bomb dropped near Tybee Island, Georgia in 1958. They interviewed the pilot who had originally lost it, as well as those who had searched for the bomb all those decades ago – and narrowed down the search to Wassaw Sound, a nearby bay of the Atlantic Ocean. For years, the maverick duo scoured the area by boat, trailing a Geiger counter behind them to detect any tell-tale spikes in radiation.
And one day, there it was, in the exact spot the pilot had described – a patch with radiation 10 times the levels elsewhere. The government promptly dispatched a team to investigate. But alas, it was not the nuclear weapon. The anomaly was down to naturally occurring radiation from minerals in the seabed.
So for now, the US' three lost hydrogen bombs – and, at the very least, a number of Soviet torpedoes – belong to the ocean, preserved as monuments to the risks of nuclear war, though they have largely been forgotten. Why haven't we found all these rogue weapons yet? Is there a risk of them exploding? And will we ever get them back?

A shrouded object

When Meyers finally got to Palomares – the Spanish village where a B52 bomber came down in 1966 – the authorities were still looking for the missing nuclear bomb. Each night his team slept in tents in the village, which was freezing and damp. "It was just like an English winter," he says. During the day they did very little – it was a waiting game.
"It's a standard military thing, hurry up and wait," says Meyers. "We had to rush over and then we did nothing for two weeks. And then after that, the undersea exploration became very serious."
The search team enlisted the help of two ingenious inventions. One was an obscure theorem from the 18th Century invented by a Presbyterian minister-turned-amateur mathematician, which helps people to use information about past occurrences to calculate the probability of them happening again. They used this technique of "Bayesian inference" to decide where to look for the bomb, to help them search in the most efficient way possible and maximise their chances of finding it.
The second was "Alvin", a cutting-edge deep-ocean submarine able to dive to unprecedented depths. Like a rotund white shark, each day, it descended into the deep blue Mediterranean water with a human crew in its belly, and began a visual hunt.

Three missing US bombs

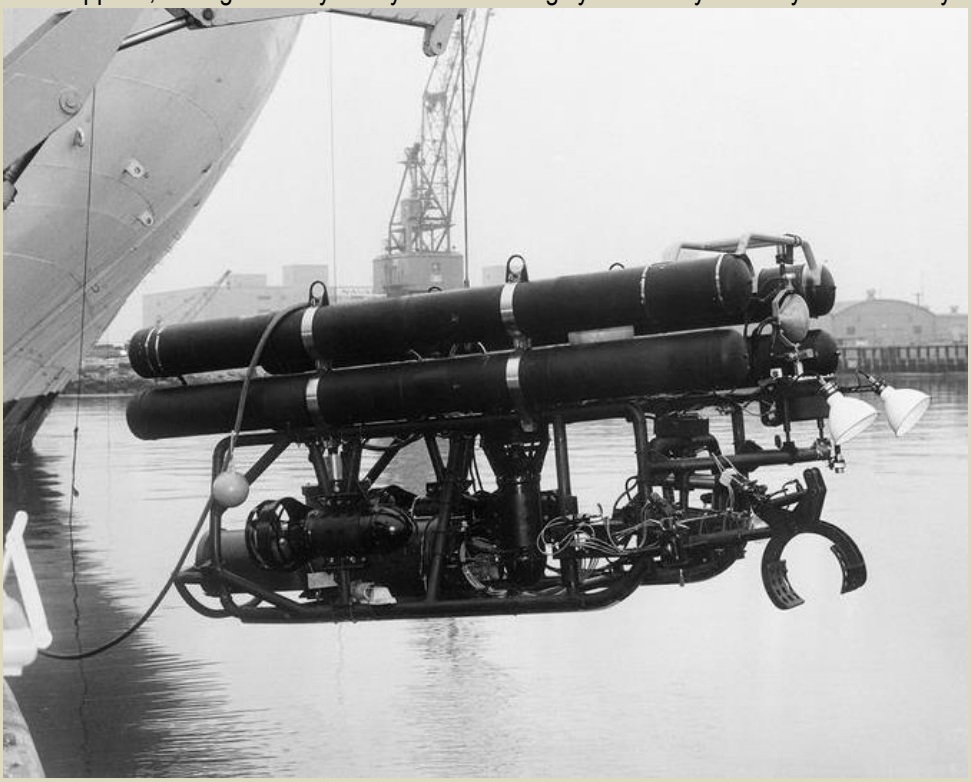
What? One Mark 15 thermonuclear bomb. Where? Tybee Island, Georgia (photo, right). When? February 5 1958. How? It was jettisoned to reduce the plane's weight for a safer landing.
What? One B43 thermonuclear bomb. Where? The Philippine Sea. When? December 5 1965. How? A bomber plane, pilot and nuclear weapon slipped off the side of a carrier boat, never to be seen again.
What? One B28FI thermonuclear bomb, second stage. Where? Thule Air Base, Greenland. When? 22 May 1968. How? A cabin fire forced the crew to eject, leaving the plane to crash with its nuclear payload onboard.
On 1 March 1966, the little sub finally spotted something: a track made by the bomb when it first hit the sea bed. Later images revealed an eerie scene – the rounded tip of the missing nuclear weapon, covered by a ghostly shroud – its white parachute, which had partially deployed when it dropped, tangling itself up with its precious cargo. This deadly tube of metal had somehow ended up resembling a person dressed up for Halloween in a bedsheet.
But the struggle was not over. Now it was Meyers' job to work out how to get this bomb off the ocean floor – where it sat 2,850ft (869m) deep. They improvised a kind of fishing line out of a few thousand feet of heavy duty nylon rope and a metal hook – the idea was to latch onto the device, and pull it up until it was close enough to the surface that a diver could go down and secure it more thoroughly. "That was the plan. It didn't work," says Meyers.
"It was all done very deliberately and cautiously and slowly," says Meyers. "So we just kind of waited around… we were anxious, wanting to see what do we do next when it comes up." They managed to hook onto the nuclear bomb, and started to hoist it out of the water. They had lifted it up off the bottom when disaster struck. The parachute, resuscitated from its sleep on the ocean floor, suddenly began doing what they do best – slowing down its cargo's speed, and making it harder to move.
"Do you realise that parachutes work just as well in water, as they do on land?" says Meyers.
Eventually, the parachute was pulling so hard on the line and hook that it simply snapped –

sending the nuclear bomb slowly gliding back down towards the bottom. This time, it ended up even deeper than before. (Little Alvin – with its human crew – only just managed to avoid becoming entangled and ending up on the bottom with it.)
Meyers was devastated. "It was extremely disappointing," he says. With the bomb now less accessible than ever, his improvised line wouldn't be long enough to catch it, so the task was handed over to another team, on another boat.
A month later they used a different kind of robotic submarine – a cable-controlled underwater vehicle – to grab the bomb by its parachute directly, and haul it up. It had shifted in its casing, so it couldn't be disarmed the usual way, via a special port in the side – alarmingly, the officers instead had to cut into the nuclear weapon. "[It would have been] kind of nerve wracking to drill a hole in a hydrogen bomb," says Meyers. "But they did it. They were prepared to do that."

A swampy mystery

Unfortunately, the three lost bombs still out there today did not meet with such successful recovery efforts. However, the risk of them causing a nuclear explosion is thought to be low.
To get to grips with why, it helps to look at how nuclear bombs work.
In September 1905, Albert Einstein placed his fountain pen on the pages of his scientific paper, and scribbled down an idea that would become the world's most famous equation. E = mc2, or energy equals an object's mass multiplied by the speed of light squared. It means that each atom that makes up the world can be exchanged into energy, and vice versa. If you can work out how to do this, the release of energy is so explosive, it's what powers the Sun.
Thirty-four years later, Einstein wrote to the US President, Franklin Roosevelt, to warn him that the Nazis were working on turning his theory into a weapon – and the rest is history. The Manhattan Project was rapidly formed, and in 1945 the US dropped its first nuclear weapon.
The bombs used on the Japanese cities of Hiroshima and – a few days later – Nagasaki, were the original, atomic kind. These involved smashing the atoms of radioactive elements against each other, to cause them to split up and create different elements. This "fission" reaction releases so much energy, it causes other atoms to split in turn, until you end up with a massive, runaway reaction. The first time they were ever tested, scientists weren't sure the reaction would ever stop – they considered the very real possibility that the world might end. (*Read more about the moments that could have destroyed humanity.*)
To achieve nuclear fission, atomic bombs usually involved a gun-like contraption that fired a hollow "bullet" of radioactive atoms such as uranium-235 into yet more uranium-235, or used conventional explosives to compress atoms of plutonium-239, until they started to split up. At Hiroshima and Nagasaki, these early weapons levelled the land for miles and killed hundreds of thousands of people, some of whom were vaporised in the blast zone and others who died of radiation burns or sickness in the days, months and years afterwards.
The next generation – the kind used in the 1950s and 60s, when the majority of the world's lost nuclear weapons were misplaced – were thousands of times more powerful. These were thermonuclear, or hydrogen bombs, and they involved a second nuclear reaction.
First there was the usual fission step as with atomic bombs, which would release staggering amounts of energy. This would then ignite a second core, this time containing isotopes of hydrogen – deuterium (heavy hydrogen) and tritium (radioactive hydrogen) – which smash together and release even more energy when they fuse to form helium and one free neutron.
This system left room for a number of safety devices.
Take the lost Tybee island bomb, which is still lying in silt somewhere in Wassaw Sound. On February 5, 1958, this 7,600-pound (3,400-kg) Mark 15 thermonuclear weapon was loaded onto a B-47 bomber, which was about to join another B-47 on a long training mission. The idea was to simulate an attack on the Soviet Union, substituting the US town of Radford, Virginia, for Moscow. The pilots set off from Florida and criss-crossed their way to their target, as a way of testing their ability to fly with the heavy weapons onboard for hours at a time.
It all went well, but on the way back to the base, the planes encountered a separate training mission in South Carolina. This group's plan was to intercept one of the B-47s – but there was a mix-up and they didn't spot the second one, which was carrying the nuclear weapon. In the ensuing crash, the B-47 carrying the nuclear bomb was damaged.
The pilot decided to ditch the nuclear bomb into the water, then make an emergency landing. The bomb dropped 30,000ft (9,144m) into the water off Tybee Island – and even this impact didn't detonate it. In fact, amazingly, none of the 32 broken arrow accidents have ever led to a detonation of nuclear components – though two have contaminated a wide area with radioactive material.
One possible factor in this lucky escape is a system of keeping the nuclear material needed for the fission reaction separate from the weapon itself. The capsule or "tip" – which in this case, consisted of plutonium – could then be added to the weapon at the last minute, when it was needed. This meant that, even if the weapon's conventional explosives went off when it was onboard, the radioactive material wouldn't get hot enough to actually do any atom-splitting.

Lewis also points out that, despite the Tybee bomb's long journey from the sky to the ocean, the latter will have cushioned the blow – this is the same reason space capsules usually have "splashdown" landings rather than descending onto land.
Later bombs also included features such as "one point safety" – a way of making sure nuclear devices didn't go off without being activated. In these weapons, the conventional explosives in a bomb might go off, but they wouldn't detonate the radioactive material because this is squeezed out before it can be compressed. "If the explosive goes off, you want it to go off in an uneven way, if that's not your goal – you want that plutonium to sort of squirt out," says Lewis.
As it happens, having so many safety features is highly necessary – mostly because they don't always work. In one case in 1961, a B-52 broke up while flying over Goldsboro, North Carolina, dropping two nuclear weapons to the ground. One was relatively undamaged after its parachute deployed successfully, but a later examination revealed that three out of four safeguards had failed.



In the end, the Palomares bomb was retrieved directly by a robotic submarine (Credit: Getty Images)

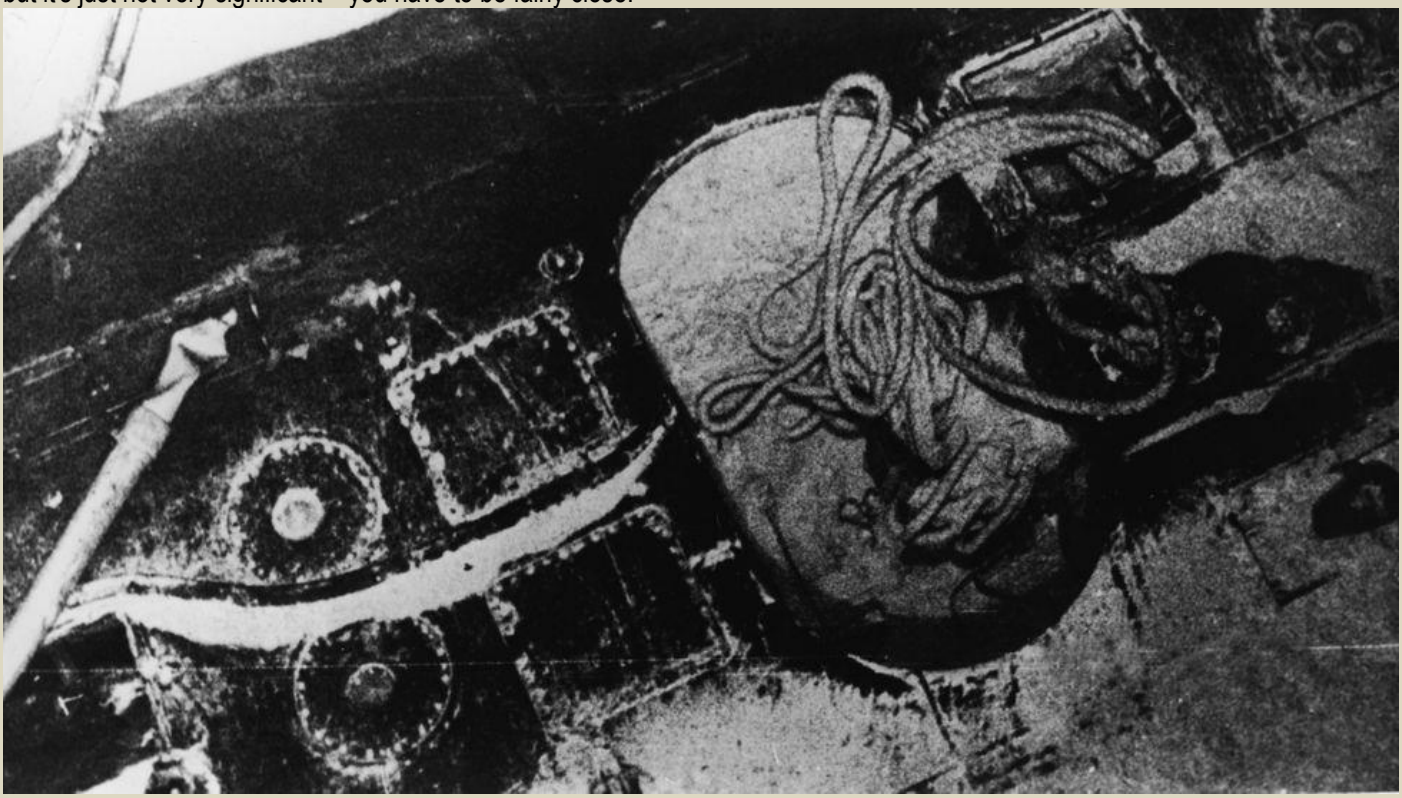
In a declassified document from 1963, the then-US Secretary of Defence summed up the incident as a case where "by the slightest margin of chance, literally the failure of two wires to cross, a nuclear explosion was averted".
The other nuclear bomb fell free to the ground, where it broke apart and ended up embedded in a field. Most parts were recovered, but one part containing uranium remains stuck under more than 50ft (15m) of mud. The US Air Force purchased the land around it to deter people from digging.
Some incidents are so baffling, they almost sound made up. Perhaps one of the most extraordinary occurred when a training exercise on the USS Ticonderoga went badly wrong in 1965. An A4E Skyhawk was being rolled to a plane elevator, while loaded with a B-43 nuclear bomb. It was a disaster in slow-motion – the crew on deck quickly realised that the plane was about to fall off, and waved for the pilot to apply the brakes. Tragically, he didn't see them, and the young lieutenant, plane and weapon vanished into the Philippine Sea. They're still there to this day, under 16,000 ft (4,900 m) of water near a Japanese island.

A confused picture

Despite nearly 10 weeks of searching, the Tybee island bomb was declared irretrievably lost on the 16th of April 1958. According to a receipt written by the pilot who dropped it, the weapon did not contain the capsule – it wasn't added before the training exercise. However, some people are concerned that this may not be correct. In 1966, the then-assistant to the Secretary of Defence wrote a letter in which he described the bomb as "complete" – i.e. containing its plutonium core. If this were true, the Mark 15 might still be capable of causing a full thermonuclear explosion.
Today the bomb is thought to be nestled under 5-15ft (1.5-4.6m) of silt on the seabed. In a final report on the weapon published in 2001, the Air Force Nuclear Weapons And Counterproliferation Agency concluded that if the conventional explosives inside are still intact, it could pose a "serious explosion hazard" to personnel and the environment – and is therefore best not disturbed, even by a recovery attempt.
But can a nuclear weapon explode underwater?
As it happens, it can. On 25 July 1946, the US detonated an atom bomb at the Bikini Atoll – a chain of postcard-perfect tropical islands surrounded by turquoise coral reefs, and beyond, the deep blue of the Pacific Ocean. They suspended the device 90ft (27m) below an assortment of ships filled with pigs and rats, and set it off. Several ships sank instantly, and the vast majority of the animals died – either from the initial blast or later of radiation

poisoning. One striking image from that day shows the giant white mushroom cloud rising up like an alien weather formation, in front of a palm-fringed beach.
As a result of this and other tests, the island chain became so radioactive that plankton glowed on photographic plates. It's still contaminated to this day – the people who once lived there have never been able to return, though like Chernobyl it has become an oasis for wildlife.

A permanent loss
Lewis thinks it's unlikely that we will ever find the three missing nuclear bombs. This is partly down to the same reasons they weren't found in the first place.
One is that they're usually located via a visual search – and this is extremely difficult.
When planes crash into the ocean, the black box is often found days or weeks later by officials looking to piece together what happened. This might give the impression that it's easy to find such objects in these vast swathes of water with modern technology. But they have a secret that helps this process along – an "underwater location beacon", which guides search teams towards them with a repeating electronic pulse.
The lost nuclear weapons came with no such equipment. Instead, teams must narrow down a search area, then scour the ocean bit by bit – a tedious and inefficient process, which requires human divers or submarines.
An alternative would be to look for spikes in radiation, as the retired military officer Derek Duke did in his search for the Tybee bomb. But this is also extremely tricky – partly because nuclear bombs are not actually particularly radioactive.
"They're designed not to be a radioactive threat to the people handling them," says Lewis. "So they do have a radioactive signature, but it's just not very significant – you have to be fairly close."



The nuclear submarine USS Scorpion, which sank with two Mark 45 torpedoes, has been underwater for 54 years (Credit: Getty Images)

In 1989, another Soviet nuclear submarine, the K-278 Komsomolets, sank in the Barents Sea off the coast of Norway. Like the K-8, it was also nuclear-powered, and it had been carrying two nuclear torpedoes at the time. For decades, its wreck has been lying under a mile (1.7km) of Arctic water.
But in 2019, scientists visited the vessel – and revealed that water samples taken from its ventilation pipe contained radiation levels up to 100,000 times higher than would normally be expected in sea water. However, this is unusual. It's thought that radioactive elements from its nuclear reactor – as opposed to its nuclear torpedoes – are leaking out through this

vent, possibly due to a rupture from when it crashed. Just half a meter (1.6ft) further away from the pipe, the isotopes were so diluted, radiation levels were normal.

For Lewis, the fascination with lost nuclear weapons isn't the potential risks they pose now – it's what they represent: the fragility of our seemingly sophisticated systems for handling dangerous inventions safely.

"I think we have this fantasy that the people who handle nuclear weapons are somehow different than all the other people we know, make fewer mistakes, or that they're somehow smarter. But the reality is that the organisations that we have to handle nuclear weapons are like every other human organisation. They make mistakes. They're imperfect," says Lewis.

Even at Palomares, where all the nuclear bombs that were dropped were eventually recovered, the land is still contaminated with radiation from two that detonated with conventional explosives. Some of the US military personnel who helped with the initial clean-up efforts – involving shovelling the surface of the soil into barrels – have since developed mysterious cancers which they believe are linked. In 2020, a number of survivors filed a class action suit against the Secretary of Veterans Affairs – though many of the claimants are currently in their late 70s and 80s.

Meanwhile, the local community has been campaigning for a more thorough clean-up for decades. Palomares has been dubbed "the most radioactive town in Europe", and local environmentalists are currently protesting against a British company's plans to build a holiday resort in the area.

The lost Palomares bomb had shifted in its casing, so deactivating it was risky (Credit: Alamy)

Lewis is confident that losses of the kind that occurred during the Cold War are unlikely to happen again, mostly because operation Chrome Dome was ended in 1968, and planes carrying nuclear bombs no longer fly around on regular training exercises. "Airborne alerts ended for reasons that must be obvious to us," he says. "In the end, the decision was made that it was too dangerous."

The exception to this progress is, of course, nuclear submarines – and even today, there are near-misses. The US currently has 14 ballistic missile submarines (SSBNs) in operation, while France and the UK have four each.

To work as nuclear deterrents these submarines must remain undetected during operations at sea, and this means they can't send any signals to the surface to find out where they are. Instead, they must navigate mostly by inertia – essentially, the crew rely on machines equipped with gyroscopes to calculate where the submarine is at any given time based on where it was last, what direction it was headed and how fast it was travelling. This potentially imprecise system has resulted in a number of incidents, including as recently as 2018 when a British SSBN almost bumped into a ferry.

Three Iran strategies that are guaranteed to backfire

By Michael Rubin

Source: https://www.washingtonexaminer.com/restoring-america/courage-strength-optimism/three-iran-strategies-that-are-guaranteed-to-backfire

Aug 04 – The Islamic Republic of Iran poses a grave challenge to both the United States and the region.

Two decades after exposure of Iran's then-covert nuclear enrichment program, Tehran is close to a nuclear weapon, even by its own admission . Its Revolutionary Guards prop up the Syrian regime, Hezbollah, the Houthis, and various Iraqi militias. The regime openly engages in hostage diplomacy. Meanwhile, U.S. Iran policy has become a political football, with partisanship trumping any honest assessment of what works and what does not.

But there are three strategies, sometimes openly embraced and sometimes percolating just below the surface in internal policy debates and think tanks, guaranteed to fail. If the U.S. truly cares about checking the Islamic Republic's growing threat and enabling the Iranian people to embrace a moderate future, then it is time for consensus about what not to do.

First, it is time to retire any support for the Mujahedin-e-Khalq , also known as the MEK. At best, the group is a creepy cult; at worst, it is a terrorist group. What it is not and has never been is popular or democratic. Maryam Rajavi, leader of the group and "president-elect" of its political front, is the closest thing Iranians have to the late American conspiracy theorist and huckster Lyndon LaRouche . Iranians living inside Iran might not agree on much, but they do despise the MEK based on its terrorism and past alliances with first Ayatollah Khomeini and then, after falling out with him, Saddam Hussein.

That the group sometimes reveals intelligence is no metric of its influence or infiltration within the Iranian system. First, its intelligence is often wrong. Second, even when right, it simply represents how the Israelis, Saudis, or perhaps even the CIA use the group to launder information to the public so that the real fingerprints of those who gathered it are not exposed. Any endorsement or embrace of the MEK is a gift to the Islamic Republic, as it allows the regime to rally an otherwise apathetic public around the flag.

Second, forget any division of Iran along ethnic lines. Iran is an ethnically diverse country: Persians, Azeris, Kurds, Arabs, Baluchis, Lors, and others. But it does not mean that it is an artificial state pulling apart at the seams. Whereas many states arose against the backdrop of ethnonationalism in the 19th or 20th centuries, the identity of Persian statehood predates that by millennia. Attempts to spark ethnic separatism in Iran by the Soviets after World War II or Iraq in 1979 failed, but in each case, the backlash resulted in a stronger Iranian dictatorship. True, some Azeris might chant slogans at soccer matches and Arabs rally against regime corruption, but in each case, the broader motivation is antipathy toward a corrupt regime rather than a desire for independence. Consider Tabriz: It may be ethnically Azeri, but it is also a former capital of Iran, the traditional seat of the crown prince, and the epicenter of Iran's constitutional movement. To bring Iran into the international community means winning over Iranians of all ethnicities and sects, not signaling to them that the goal is the destruction of Iran.

The final strategy guaranteed to backfire is endless diplomacy.

Partisans are wrong to say " Maximum Pressure " did not work. Such a claim, though, is not evidence that resourcing Iran's regime is wise. Because of the Revolutionary Guard's stranglehold over the economy, any windfall from sanctions relief strengthens the most reactionary elements of the regime. More importantly, engagement for its own sake ignores the Islamic Republic's motivations: both ideological and tactical. For the White House, diplomacy might be about the search for a win-win solution. For Iran, it is an asymmetric warfare strategy to distract the opponent while centrifuges spin and terrorist groups arm.

There is no magic formula to resolve disputes with Iran, nor are there shortcuts. It will take bipartisan solidarity, a credible military threat, maximum pressure, and a strategy to break the Revolutionary Guard's ironclad grip on society. But first, it is important to drop the strategies that do more harm than good.

Michael Rubin is a contributor to the Washington Examiner's Beltway Confidential. He is a senior fellow at the American Enterprise Institute.

Tehran Engages in Nuclear Games

By Seth J. Frantzman

Source: https://www.meforum.org/63419/tehran-engages-in-nuclear-games

Aug 01 – Iran has the technical capability to produce an atomic bomb, but it does not intend to do so, Atomic Energy Organization of Iran (AEOI) head Mohammad Eslami said Monday. He was speaking to a reporter from Fars News Agency, the Iranian media channel that is considered close to the Islamic Revolutionary Guard Corps.

His comments emphasized that the AEOI was in regular contact with the International Atomic Energy Agency (IAEA). Therefore, the comments, although they seem to present some kind of new bragging on behalf of the Islamic Republic, are ostensibly couched in terms of compliance with the Non-Proliferation Treaty, Iran says.

Iran's Sejjil 2 medium range ballistic missile (above) has a range of 2,000 km, or just over 1,200 miles

Under the terms of the so-called Iran deal, "Iran would limit its capacity and accept strict monitoring of its nuclear activities," Eslami said. Iran has shifted its policy since the US left the deal, openly enriching more uranium to higher levels. It continues to work on its long-range missiles and on satellite launch vehicles, technology that could potentially enable a nuclear weapon to be launched from a missile.

Eslami's point, however, was that Tehran has been at the receiving end of "false accusations."

"After withdrawing from the JCPOA, the Western side, in order to return to the JCPOA, is resuming the false accusations that were raised in the past," he said. "These accusations originate from the hypocrites and the Zionist regime, and they have been expressing these false issues for about 20 years."

Eslami said Iran turned off cameras monitoring its nuclear operations in response to these accusations. This seems a bizarre response to claims of "false" accusations. If they are false, why turn off the cameras?

The larger context

Eslami's comments come in the context of other ones by senior Biden administration officials.

Brett McGurk, the White House coordinator for the Middle East and North Africa, said reaching a deal with Tehran was now "highly unlikely," according to *Axios*. There is some interplay in the administration between this viewpoint and that of US Special Envoy for Iran Rob Malley. Overall, though, the administration keeps saying the window is closing.

Prof. Efraim Inbar, president of the Jerusalem Institute for Strategic Studies, responded to the announcement by the AEOI chief that Tehran is now capable of producing an atomic bomb.

"This is another provocative action on the part of Iran and is testimony to the limp-wristed policy of the West and the complete absence of deterrence," he said. "The statement by the AEOI strengthens the imperative for Israel to defend itself; in the current situation, there is no alternative to Israeli action to neutralize the Iranian nuclear threat."

First of all, this will require a strike on Iran's proxy, Hezbollah, to create deterrence, Inbar said. "Following that, Israel should prepare for continued action against the Iranian nuclear threat," he added.

Meanwhile, the head of Iran's Strategic Council on Foreign Relations, Kamal Kharazi, said Iran has the technical capabilities to build a nuclear bomb, but it has not decided to make one.

"It is no secret that we have the technical capabilities to manufacture a nuclear bomb, but we have not decided to do so," he said.

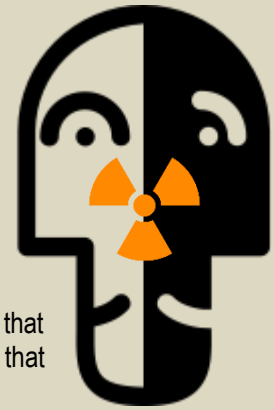
Kharazi, a senior adviser to Iranian Supreme Leader Ali Khamenei, made the comments to Al Jazeera. The "Zionist regime" was behind the "false" rumors, he emphasized.

Last week, Khamenei's office tweeted: "The Western powers are a mafia. The reality of this power is a mafia. At the top of this mafia stand the prominent Zionist merchants, and the politicians obey them. The US is their showcase, and they're spread out everywhere."
Beyond these comments are threats that were made on a video linked to the IRGC, which appeared on Telegram several days ago. It asked: "When will Iran's sleeping nuclear warheads awaken?" It concluded that the nuclear weapons could appear at any time, "if the US or the Zionist regime make any stupid mistakes."
The video said there is secret enrichment taking place at Fordow, allowing Iran to make weapons quickly if need be. What it actually means is that Tehran has enough highly enriched uranium to break out and have enough material to build a nuclear bomb. But how many, and has Iran ever even built one?
The Telegram video said Iran has ballistic missiles capable of "turning New York into hellish ruins." This sounds like the usual boasting and threats. Although Iran is improving its missiles, it would be hard for them to reach the United States.
Of more substance appears to be other comments by Eslami, arguing that the Iranian parliament's energy committee should create a comprehensive road map and laws for the nuclear industry so that the "nuclear development process is not damaged by the change of administrations," according to the website Iran International.
Overall, it's worth recalling that in May, Defense Minister Benny Gantz said Iran was just a "few weeks" from having enough fissile material for a bomb. It was installing 1,000 advanced centrifuges at Natanz as well, he indicated. In June, International Atomic Energy Agency Director-General Rafael Grossi said Iran was only a few weeks away from having a "significant quantity of enriched uranium."
The "weeks" and "months" time frame has been a key talking point for years. In February, McGurk and Malley both seemed to confirm a two-month time frame, according to Politico. A House Democrat was reported to have confirmed the "weeks" breakout time. Iran was also "weeks" away from a bomb in April.
But these time frames only refer to the "breakout period" for the Islamic Republic to have enough material for a nuclear weapon. Material must be put into a device.
However, for those worried about Iran's nuclear program, the real concern is that once it has enough material, it can blackmail the region, and any attempt to neutralize the material could be dangerous. This is why the time frame may not change over the months – because Tehran is also on the verge of producing enough material.
Iran's narrative is that it can build an actual weapon, but it keeps holding the region hostage by claiming that it needs to be blackmailed not to.

Seth Frantzman is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at *The Jerusalem Post*.

Nuclear weapons have no place in Iran's 'doctrine', says foreign minister

Source: https://www.rudaw.net/english/middleeast/iran/070820222



Aug 07 – Tehran is willing to continue cooperation towards establishing a zone in the Middle East free of weapons of mass destruction, said the Iranian foreign minister on Sunday, adding that nuclear weapons contradict Iran's "doctrine".
Iranian Foreign Minister Hossein Amir-Abdollahian held a phone call with United Nations Security-General Antonio Guterres, exchanging views on the latest developments in Iran's nuclear program and stressing the importance of reviving the 2015 nuclear deal.
"There is no place for nuclear weapons in the doctrine of the Islamic Republic of Iran, as they contradict our policies and beliefs," Iranian state media cited Amir-Abdollahian as saying in the phone call.
In regards to the talks to revive the Joint Comprehensive Plan of Action (JCPOA), the foreign minister stated that "the results of the negotiations depend on US' desire or lack of desire to reach an agreement," emphasizing that Iran has "a serious will" to reach a stable agreement.
The European Union has mediated talks between Iran and the US for over a year in hopes of reviving the JCPOA, under which Iran would significantly limit its nuclear program in return for sanctions relief, with no success.
A new round of talks began on Thursday in Vienna, with Russia's envoy to the talks, Mikhail Ulyanov, stating on Sunday the process towards restoring the deal was "moving in the right direction," as cited by AP.
For his part, Guterres emphasized the need to "remove nuclear weapons from the world," adding that they have made efforts toward closing down the Iranian nuclear file and have asked the European and American sides to exhibit flexibility during this stage of the talks towards restoring the 2015 nuclear deal.

In return for restoring the JCPOA, which former US President Donald Trump unilaterally withdrew from in 2018, Iran has demanded that the US lifts its sanctions on the country, including those on Iran's Revolutionary Guard Corps (IRGC), which the US has designated as a terrorist organization.

EDITOR'S COMMENT: A strange situation where both the West and Iran are either lying or telling the truth!

Atomic bomb survivors—A model for us in COVID-19 era

By Robert Jay Lifton

Source: https://thebulletin.org/2021/08/atomic-bomb-survivoers-a-model-for-us-in-covid-19-era/#post-heading

A vault within the Atomic Bomb Memorial Mound contains the ashes of Hiroshima victims cremated after the bombing. Remains of more than 800 have been identified but remain unclaimed. Thousands more remain unidentified. (Jeremy Carver / Creative Commons BY-NC-ND) https://flic.kr/p/8Ww79r

Aug 09 – Survivors of Hiroshima are a dying population. People who were 20 years old at the time of the bomb would now be 96. The survivors still alive were mostly children then, and they too are dying out. Does this suggest that the message of *hibakusha*, the original survivors, has come to an end? I do not think so.

Consider the message that Hiroshima survivors have brought to the world. A history professor I interviewed during my 1962 study of hibakusha — "explosion-affected people" — described how, soon after the bomb, he looked down at the city from a high suburb: "Hiroshima had disappeared. … I was shocked by the sight. … Hiroshima didn't exist — that was mainly what I saw — Hiroshima just didn't exist."

A physician, himself injured by the bomb, could not find words for what he witnessed: "I had to revise my meaning of the word destruction …. devastation may be a better word, but really I know of no word or words to describe the view from my twisted iron (hospital) bed."

Witnesses who cannot be silenced

Hiroshima survivors have traveled around the world to convey this message of what I have called imagery of extinction. They have sought to make known the sense of world-ending destruction that only they have experienced.

Hibakusha, then, are prophetic survivors. They warn of the nuclear revolution in destructiveness. Hibakusha have energized antinuclear movements everywhere in ways that inform our continuous struggles with the weapons. Their story was crucial for the recent United Nations decision declaring the very possession of nuclear weapons to be illegal. Their legacy can at times be ignored or repressed, but it cannot be completely silenced.

Because Hiroshima survivors are dying out, how can the legacy be sustained? That question arises with any large catastrophe, all the more so in connection with nuclear destruction. Much depends on future generations who embrace hibakusha narratives and then recreate them in ways that are relevant for their own historical moment. In that way the survivor legacy becomes generational, ever available to be recognized as a source of prophecy and potential wisdom.

This holds for new generations confronting any catastrophe. They can re-engage the legacy of the earlier event by bringing to it new images, moral imperatives and policies. The baseline for this generational reengagement is always the experience of actual survivors.

Today we are struggling with another survivor legacy: the COVID-19 pandemic. The pandemic has struck not just a particular city but the whole world, and has killed many times the number of people who died in Hiroshima. All of us who have stayed alive during this catastrophe can be considered survivors, though we do not necessarily use that term.

What is striking in our present catastrophe, however, is the refusal, for political reasons, of a large segment of the American population to acknowledge its full impact, or even its existence. Those who insist that there has been no catastrophe cannot experience themselves as survivors.

They also seek in many ways to interfere with the recognition of the lethal threat of the virus to everyone.

Learning from Hiroshima's survivors

In Hiroshima, many remained silent, but no one claimed that a catastrophe had not occurred. Hiroshima survivors seized upon their sense of catastrophe and found wisdom in disseminating its dimensions to the world. Americans today have much to learn from Hiroshima survivors. We, too, must embrace our own survivor state. In fact, that is beginning to happen. Groups such as COVID Survivors for Change and Survivor Corps are emerging and raising questions—not only about their or their family's illnesses, but also about the nature and source of the pandemic itself. COVID-19 could also produce prophetic survivors whose direct experience of catastrophe might provide the wisdom we require. Survivors could then become, as in Hiroshima, a vanguard of collective renewal.

Robert Jay Lifton is a psychiatrist and author, currently at Columbia University, whose books include *Death in Life: Survivors of Hiroshima*, which won a National Book Award, and most recently *Losing Reality: On Cults, Cultism, and the Mindset of Political and Religious Zealotry*.

What can a pandemic teach us about nuclear threats?

By Ted Lieu

Source: https://thebulletin.org/2020/08/what-can-a-pandemic-teach-us-about-nuclear-threats/#post-heading

Aug 07 – When Barack Obama became the first US president to visit Hiroshima in 2016, he stated: "Technological progress without an equivalent progress in human institutions can doom us." Those words ring true today. At the 75th anniversaries of the bombings of Hiroshima and Nagasaki, we stand in another moment of global chaos and profound loss.

Over 700,000 people worldwide have died from COVID-19, including over 160,000 in the United States. SARS-CoV-2 spread like wildfire in part due to global and domestic travel made far easier by technological progress. At the same time, failures in human institutions allowed the virus to escalate out of control in numerous places.

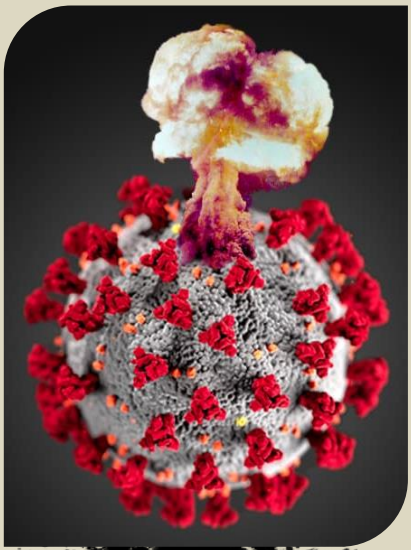


Illustration by Thomas Gaulkin. Coronavirus graphic via CDC; Maralinga nuclear test photo via InnoventionAustralia (CC BY 2.0)

The lessons learned from this pandemic make the case for re-thinking the United States' national security framework to decide which investments truly improve US national security and which seek to win yesterday's wars. Who would have thought that the equipment needed to fight an enemy that has already killed far more Americans than died in World War I was not the Trident missile or B-1 Bomber, but face masks and ventilators? Or that the heroes risking their lives this year are health care workers and grocery store employees?

The United States has already learned three important lessons from its failed pandemic response that should inform its nuclear strategy, so it doesn't repeat similar mistakes in the future: investing in prevention is key; experts' matter; and America needs to adjust to a new communications environment.

Investing in catastrophe prevention

Until 2017, both Democratic and Republican administrations understood the importance of preventing a pandemic. Before leaving office, the Obama administration set up the White House National Security Council Directorate for Global Health Security and Biodefense. In 2005, President George Bush spoke at the National Institutes of Health and said, "If we wait for a pandemic to appear, it will be too late to prepare." Indeed, one of the principal reasons for the existence of the Centers for Disease Control and Prevention, which was created in 1946, is "detecting and confronting new germs and diseases around the globe to increase our national security."

Unfortunately, the Trump administration eliminated the NSC Directorate for Global Health Security and Biodefense in 2018. The administration declined to renew funding for a federal pandemic detection program in 2019. The administration also proposed budget cuts to the CDC. And the Trump Administration ignored a step-by-step guide the Obama administration created on how to prevent a pandemic.

China's early actions—suppressing information about SARS-CoV-2 and providing misleading information about the virus—are indefensible. At the same time, the Trump administration's lack of preparation for the pandemic left the United States flat-footed when the virus—as a result of global air travel—started pouring into America from Europe. Even today, there is no national testing strategy, no national contact and tracing program, and no national pipeline for personal protective equipment, forcing hospitals and states to compete with one another to secure PPE, sometimes at exorbitant prices.

Prevention is and always has been the best strategy when it comes to disasters, whether they come in the form of disease or war. Unfortunately, the current administration has taken actions that increase, rather than decrease, the risks of nuclear war. From cuts and disarray at the State Department to withdrawing from arms control treaties to making it easier to use nuclear weapons, the last few years have been a disaster for nuclear conflict prevention.

The case for a unified national security budget—one that strikes the right balance among our diplomatic, informational, military, and economic instruments of power to prevent conflicts—has never been stronger. Instead, the budgets under the Trump administration have prioritized military spending over all other instruments of national power. We can already destroy the world several times over with our nuclear and conventional weapons. It is time to invest in our other instruments of national power.

Unfortunately, in the last few years, our diplomatic capacity has withered. As a member of the House Foreign Affairs Committee, I have seen how, under the Trump Administration, the US State Department has been gutted, as employees depart and positions go unfilled; morale has fallen; and several ambassadors and the Secretary of State have come under investigation for inappropriate or illegal behavior. We need to reverse course and re-invest in a large, professional, and ethical diplomatic corps.

We have also seen an unfortunate shift towards go-it-alone US nuclear policy that expands the risk of miscalculation and escalation. Withdrawing from nuclear arms control treaties and expanding the capabilities of our nuclear arsenal are destabilizing. The Trump administration's decisions to withdraw from Intermediate-Range Nuclear Forces (INF) Treaty last year, to announce its formal intent to withdraw from the Open Skies Treaty this year, and to lay the groundwork for allowing the New START Treaty to expire early next year all amount to a regressive policy that increases the chances of a nuclear conflict.

Similarly, the Trump administration's decision to produce new low-yield warheads increases the risk that nuclear weapons will be used. And the use of a low-yield nuclear weapon can easily escalate a conflict to an all-out nuclear war that cannot be won. That's one reason I and other members of Congress introduced the bicameral "Hold the LYNE Act" to prohibit low-yield nuclear weapons for submarine-launched ballistic missiles.

Instead of moving away from a prevention strategy, the United States needs to move toward one. Among the more obvious ways a catastrophic nuclear war could start is if a president launched a nuclear first strike. In October 2016, Sen. Ed Markey and I introduced the "Restricting First Use of Nuclear Weapons Act" to mitigate that possibility and to reassert the war making authority that the framers of the Constitution gave to Congress alone.

The current nuclear launch approval process gives the president the sole authority to decide whether and when to launch a nuclear first strike. No member of the cabinet, the judiciary, or Congress is required to be involved in that decision. And once the President orders the launch, the execution of the order would occur frighteningly fast.

The framers of the Constitution, however, went to great lengths to put checks and balances on the president. They created an entire judicial branch to check the president. They created a legislative branch to check the president. And then then gave the gravest power they knew at the time—the power to declare war—to Congress alone. There is no way the framers would have authorized one person to launch weapons that could kill hundreds of millions of people in less than an hour and not have called that war.

Our legislation enacts the vision of the framers and requires the president to get congressional authorization before launching a nuclear first-strike (except in cases when another country has already launched a nuclear weapon at the United States). Not only would our bill correct a constitutional defect, it would also reduce the incentive for other nuclear-armed countries to strike the United States.

Having served on active duty in the US Air Force, I have long understood that countries such as Russia and China have the capability to annihilate America with their nuclear weapons. One reason they don't use those weapons is their understanding that no matter how many missiles they launch, the United States has a robust second-strike capability that would annihilate them in return.

Mutually assured destruction relies on strengthening second-strike capabilities; a first-strike option is not only unnecessary, it is destabilizing. If these countries believe an unhinged president could rapidly launch a nuclear first strike, their calculation changes, and they are forced into a "use it or lose it" scenario with their weapons. Our legislation injects the crucial elements of time and approval by Congress to slow down any potential nuclear escalation.

The United States knew the risks and failed to prevent the outbreak of a novel coronavirus from becoming a deadly pandemic. It cannot fail to prevent a diplomatic or conventional military conflict from becoming a cataclysmic nuclear war. The United States needs to invest in diplomacy, to stop withdrawing from arms control treaties, and to curb the production of nuclear weapons. Buying new nukes doesn't make us safer; strengthened alliances and prioritized diplomacy do. There is strength in tackling problems before they arise, and America is living through what happens when prevention is underfunded or ignored.

The value of expertise

Another reason America leads the world in COVID-19 cases and deaths involves the failure of far too many people, including government officials, to listen to experts. Earlier this year, the Trump administration worked with medical experts and created a set of coronavirus guidelines for states to follow before they reopened businesses and other aspects of public life that had been restricted to slow the spread of COVID-19. What happened? Many states—and the president himself—ignored those guidelines. The president tweeted multiple times that various states should "liberate" themselves and reopen, even though none of those states met the reopening guidelines set forth by his own administration. As a result, COVID-19 cases and deaths started to spike again, and the virus continues to surge in many areas.

Medical experts have repeatedly told the American public to practice social distancing, wear masks in public, and avoid crowded indoor areas to help stop the spread of the virus. What happened? A number of Americans refused to wear masks in public, and the president spent those critical first months of the pandemic disparaging those who wore masks. It wasn't until recently that the president reversed himself and finally said that people should wear them. A number of Americans engaged in dangerous behavior, like going to bars, indoor parties, and a presidential indoor rally where social distancing was not observed and masks were not required. In many ways, this pandemic has taught us exactly what not to do in a nuclear-armed world where the Doomsday Clock says it is 100 seconds to midnight. We need to stop rejecting science. We need to prepare for worst-case scenarios. We need to listen to the experts screaming from the mountaintops that we're not doing enough. Earlier this year, some argued that a robust pandemic response would cause the public to think that the government was over-reacting. In the case of a potential nuclear conflict, there is no such thing as being over-prepared.

Experts in academia, in the private sector, in government, and at the *Bulletin of the Atomic Scientists* have provided numerous common-sense recommendations for how to prevent a nuclear conflict, from strengthening command and control systems to reducing nuclear proliferation. We should listen to them. If the American people choose a new president in November, one of the first orders of business should be to re-invest in the State Department, put the United States back into arms control treaties, and to stop the production of low-yield nuclear weapons. And of course, ensure the "Hold the LYNE Act" and the "Restricting First Use of Nuclear Weapons Act" become law.

Adjusting to a new communications environment

Technological progress is a double-edged sword. Obviously, it was technological progress that resulted in nuclear weapons. The ease of global and domestic travel made possible by technology—from comfortable, fast aircraft to online booking sites—is what swiftly turned the novel coronavirus into a worldwide pandemic. At the same time, it is science and technology that will one day give us a vaccine or drug therapy to stop the pandemic. In the area of communications, technology has advanced so rapidly that our institutions and citizenry have been caught off guard. For example, it can be difficult to know if a Facebook post was written by an American in your state—or a Russian agent in the

Kremlin. US officials have alleged that Russia is actively participating in disinformation campaigns about COVID-19 in America, as well as hacking COVID-19 research centers. And with the existence of deep-fake technology, it is nearly impossible for ordinary Americans to know if a video they are seeing is reality or fantasy.

False information about the virus—whether created intentionally or unintentionally—routinely shows up on multiple social media platforms. The president—with over 84 million Twitter followers—has repeatedly tweeted or retweeted misleading information about COVID-19. In our current communications environment, a lie disguised as fact or a manipulated video can reach hundreds of millions of people in seconds. Add the fact that high-profile social media accounts were recently hacked, and it is easy to imagine potentially dangerous situations when it comes to nuclear conflict. What happens if a hacker gains control of the president's Twitter account and posts a tweet that leads foreign leaders to believe the president ordered a nuclear first strike? Or what if the hacker uses Twitter's direct messaging function, so no one knows except the people who receive the direct message? What if someone posts a deep-fake video of North Korea launching a nuclear missile at Hawaii? What if Hawaii issues a nuclear missile alert from North Korea that instantaneously went to all cellphones? Oh wait, that last one happened. And it caused a lot of people in Hawaii to panic. Some cars reportedly sped up to 100 miles per hour after the alert was issued. Tourists in Kaneohe were reportedly taken up to a bunker in the mountains. Officials at the Sony Open PGA Tour golf tournament on Oahu evacuated the media center, while staff sought cover in the players' locker room. A man suffered a heart attack after saying what he thought were his last goodbyes to his children after the alert. And the 911 call system was overwhelmed, with many calls not being able to go through.

Technological advancements in communications have resulted in at least two consequences: one, information, whether true or false, can be distributed to a massive amount of people nearly instantaneously, and two, it is fairly easy to create false information that looks true. The first consequence will not be fixed, because there is often merit in being able to reach many people very quickly. Fixing the second consequence requires some combination of media literacy and better cyber security. Both consequences suggest that injecting more time and congressional authorization into nuclear situations is what is needed in our brave new advanced communications world.

Wake up!

America's failed response to the pandemic should serve as a wake-up call to our nation that we have become complacent in critical areas of national security. To the extent there was a nuclear component to the global war on terrorism, it was the fear of a terrorist network acquiring a nuclear weapon, smuggling it into the United States, and detonating it. With the 2017 National Security Strategy's shift to great power competition, we have now turned our attention back to two nuclear powers with advanced delivery systems and track records of brazen behavior. We cannot afford to wait before we invest serious diplomatic capital to ensure none of our conflicts with China or Russia escalate to nuclear war. Withdrawing from arms control treaties and buying easier-to-use nuclear weapons will not make us safer from nuclear conflict. Strengthening our alliances—our biggest competitive advantage over our adversaries—and showing up to lead coordinated diplomatic efforts will. At the same time, we can reduce the risk of nuclear conflict by requiring the president—any president—to seek authorization from Congress before launching a nuclear first strike.

We also need to listen to experts. To prevent a catastrophic disaster—whether a pandemic or a nuclear conflict—we need to stop rejecting facts and science. Unfortunately, the new world of instantaneous communications can make it more difficult to ascertain the truth. Government officials and the public need to adjust to this new environment. Lives are at stake.

Congressman Ted Lieu, in his third term in Congress, represents California's 33rd District. In his first term he was elected president of the Democratic Freshman Class by his colleagues; last term he was elected as a vice chair of the Democratic Congressional Campaign Committee; and this term he was elected to House leadership. Lieu serves on the House Foreign Affairs Committee and the House Judiciary Committee. Prior to Congress, he served nine years in the California State Legislature and one term on the Torrance City Council. He previously served on active duty in the United States Air Force and is a colonel in the Air Force reserves. He graduated with a B.S. and B.A. from Stanford and a J.D. *magna cum laude* from Georgetown University Law Center, where he served as editor-in-chief of the law review.

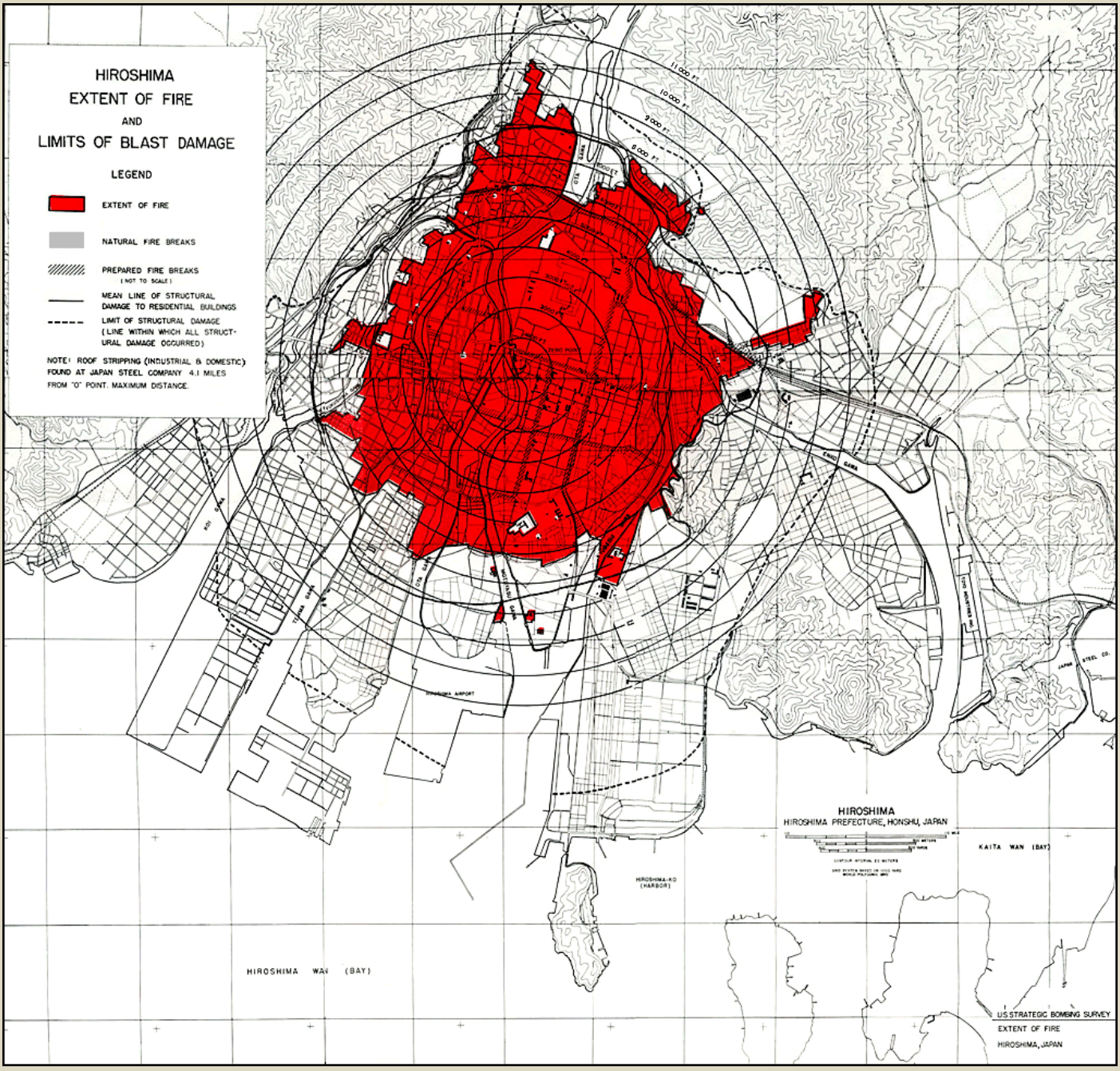
Hiroshima and COVID-19

By Robert Jay Lifton and Charles B. Strozier

Source: https://thebulletin.org/2020/08/hiroshima-and-covid-19/#post-heading

Aug 05 – We are always terrified by a deadly force that we cannot see or in any way perceive until it strikes. That was the kind of fear one of us (Lifton) encountered in survivors of the atomic bomb when he interviewed them in Hiroshima some decades ago—a fear of "invisible contamination." Their fear was based on their witness or experience of grotesque early

symptoms of radiation effects, a later increase in leukemia and other cancers, and the possibility of hereditary harm to subsequent generations.



Hiroshima blast and fire damage, US Strategic Bombing Survey map. Public domain.

With COVID-19 the dread involves a force that is everywhere and nowhere; the virus takes on an almost supernatural aura that in turn leads to bizarre conspiratorial explanations. It is very difficult to bring reason to a deadly force that is invisible.

Nuclear fear can be disseminated by the weapons themselves, by meltdowns in energy reactors, or by residual radiation effects in sites where the weapons were made or tested. Nuclear fear has become a model for large threats that endanger the human future. So when people encounter climate change, or now COVID-19, they find themselves associating back to nuclear images.

Indeed, such ultimate threats tend to merge in the mind as something on the order of world-ending apocalyptic dangers. When we (Lifton and Strozier) collaborated on a MacArthur Foundation study in the 1990s, entitled "Nuclear Fear in the American Self," we found a close interweaving of climate and nuclear anxieties so that psychological associations between them could occur within the same thought, sentence, or phrase. COVID-19 has entered that

apocalyptic realm and the fear of it has become amplified, along with anticipations of new and more extreme waves of this virus or other even more deadly viruses to come. To be sure, COVID-19 differs from radiation effects in its signature characteristic of what can be called *mobile contagion*. It spreads quickly and wildly and is easily transmitted by human contact. Since the virus can be present in people without symptoms, it creates a paranoid structure in which each of us is endangered by contact with anyone else and each of us poses a similar threat to all others. Among Hiroshima survivors there was no such physical contagion. Yet others avoided them and discriminated against them, experiencing them both as death-tainted and *psychologically contagious*. With COVID-19, each of us, as a potential victim, becomes to some degree death-tainted.

An important difference between nuclear and COVID-19 fear is the disparity in scientific knowledge about them. A lot is known about nuclear weapons, how to make them and what they do, because they are direct products of our technology. What is also known is the widespread psychic numbing they cause, as well as the antithetical meanings given them— either as sources of ultimate destruction that are dangerous to possess, or as necessary contributions to national respect, to "deterrence," and world peace.

In comparison, very little is known about COVID-19. There is still much ignorance about precisely what determines its spread and why it chooses certain areas and not others, about its differing symptoms and disease complexes, or its varying effects on age groups and people with particular prior conditions. Nor has COVID-19 been viewed as in any way beneficial, but there has been striking, politically-motivated negation of the virus and dismissal of its effects.

COVID-19 and nuclear fear both bring about universal death anxiety. With COVID-19 that has led also to various forms of profound dislocation. That dislocation may be geographic, as the more privileged among us flee from areas of high infection; it also extends to our way of living as we stay at home or socially distance ourselves, even from family and friends; to our work arrangements, which may collapse or be radically altered; and to excruciating decisions about teaching and learning and the function of schools. What we have lost is the relative safety of the pre-COVID-19 world. And we Americans are twice dislocated from national authority: from a president who has responded to the virus with extraordinary incompetence, cruelty, and corruption; and whose destructive approach to our institutions gravely endangers our political and psychological capacity to function as a democratic state.

With either threat, we have no choice but to call upon the remarkable capacity of the human species for adaptation. Such adaptation is by no means passive and must combine political will with scientific knowledge.

In the case of COVID-19, the American response so far has been egregiously inadequate. But that can change. American struggles for adaptation are increasingly informed, however painfully, by ubiquitous illness and enormous numbers of deaths. Holding to these physical truths about the virus we can break through the malignant normality the president seeks to impose—the brutal willingness to allow thousands, or hundreds of thousands of additional deaths in the service of economic recovery that would help him in the fall election. This policy meets with widespread public resistance. When people feel medically vulnerable and experience death anxiety, their strong psychological tendency is to turn to doctors for accurate information and appropriate policies, or to political leaders who hold to medical truths, however daunting.

Neither the virus nor nuclear threat are likely to soon disappear. But we as a species are capable of bringing to them the mind's capacity to embrace policies that hold back catastrophe and contribute to the continuity of human life.

Robert Jay Lifton is a psychiatrist and author, currently at Columbia University, whose books include *Death in Life: Survivors of Hiroshima*, which won a National Book Award, and most recently *Losing Reality: On Cults, Cultism, and the Mindset of Political and Religious Zealotry*.

Charles B. Strozier is a historian and psychoanalyst, emeritus professor at John Jay College of the City University of New York, and author of *Apocalypse: On the Psychology of Fundamentalism in America.*

Memorial Days: the racial underpinnings of the Hiroshima and Nagasaki bombings

By Elaine Scarry

Source: https://thebulletin.org/2020/08/memorial-days/#post-heading

Aug 03 – This past Memorial Day, a Minneapolis police officer knelt on the throat of an African-American, George Floyd, for 8 minutes and 46 seconds. Seventy-five years ago, an American pilot dropped an atomic bomb on the civilian population of Hiroshima. Worlds apart in time, space, and scale, the two events share three key features. Each was an act of state violence. Each was an act carried out against a defenseless opponent. Each was an act of naked racism.

The first two features—the role of the state and the impossibility of self-defense—probably require little elaboration. Each was an act of state cruelty: In one case, the agents of the

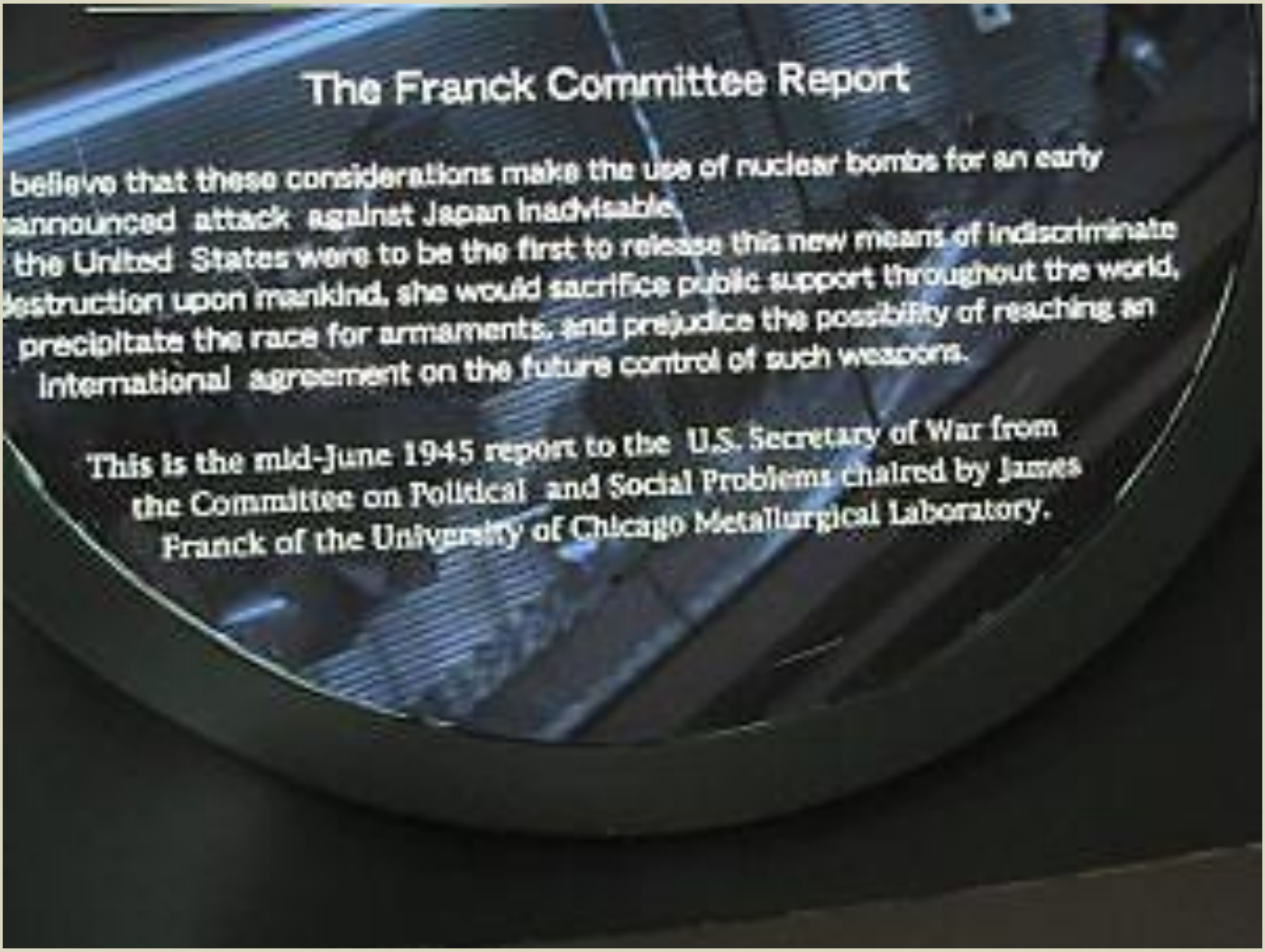
state acted on home ground and in the other, on foreign ground. Each was carried out against a defenseless opponent: George Floyd's hands were handcuffed behind him; he was not resisting arrest or putting the police officers at risk or even verbally challenging them; he used his voice merely to plead that he be permitted to breathe, then called out to his dead mother, whom he soon joined. Nor could the long line of executed black Americans who preceded George Floyd defend themselves: Breonna Taylor's work as an emergency medical technician entailed, on a daily basis, protecting both herself and her patients, but she could not, fast asleep in bed, carry out any self-defense when Louisville police, without warrant, burst through her doors after midnight and shot her eight times.

A barefoot boy waiting in line and staring ahead at a crematorium after the Nagasaki bombing, with his dead baby brother strapped to his back. Photo by US Marine photographer Joe O'Donnell

The now widely shared recognition that police racism within the United States is not just the practice of individual officers but is instead systemic entails the recognition that African-Americans, in their interactions with the police, have ceased to have the right of self-defense, the right that arguably underlies every other right. Persons of color in the United States—including Native Americans, whose rate of death at the hands of police is the highest of any racial group[1]— cannot defend themselves. Seeing that one is about to be slain, one may try to resist (to run, to refuse handcuffing, to flail out with arms or weapon), but that resistance will then be retroactively used to justify the slaying that was already underway. One's only choice is to comply or to resist—in other words, to be slain or to be slain.

Self-defense was not an option for any one of the 300,000 civilian inhabitants of the city of Hiroshima, nor for any one of the 250,000 civilians in Nagasaki three days later. We know from John Hersey's classic *Hiroshima* that as day dawned on that August morning, the city was full of courageous undertakings meant to increase the town's collective capacity for self-defense against conventional warfare, such as the clearing of fire lanes by hundreds of young school girls, many of whom would instantly vanish in the 6,000° C temperature of the initial flash, and others of whom, more distant from the center, would retain their lives but lose their faces.[2] The bombing of Hiroshima and Nagasaki initiated an era in which—for the first time on Earth and now continuing for seven and a half decades—humankind collectively and summarily lost the

right self-defense. No one on Earth—or almost no one on Earth[3]—has the means to outlive a blast that is four times the heat of the sun or withstand the hurricane winds and raging fires that follow.



Detail from the Nagasaki Atomic Bomb Museum. Photo courtesy of the author.

Is it accurate to designate self-defense the right underlying every other right? Freedom of speech matters for thousands of reasons, but at its most elementary, it matters because it increases one's chance of defending oneself and by this act, surviving. The same is true of the right of free press, the right of free assembly, the right to a fair trial, the right not to be subject to warrantless search and seizure: Each has a vast array of benefits, but the bottom line is that each amplifies the right of self-defense, the right to protect and thereby perpetuate one's own life. Centuries of political philosophers have asked, "What kind of political arrangements will create a noble and generous people?" Surely such arrangements cannot be ones where a handful of men control the means for destroying at will everyone on Earth from whom the means of self-defense have been eliminated.

The third link between Memorial Day 2020 and August 6 and 9, 1945 is the racism that made each event possible. Racism is a perceptual deformation that results in the judgement that people of a given skin color or ethnic derivation are not simply less deserving (of jobs, education, money, medical care, trust, responsibility, forgiveness, sympathy) but are, in a word, expendable. Lynch them, choke them, burn their faces off; we can do a follow-up study later.

When Americans first learned that the people of Hiroshima and Nagasaki had been collectively vaporized in less time than it takes for the heart to beat, many cheered. But not all. Black poet Langston Hughes at once recognized the moral depravity of executing 100,000 people and discerned racism as the phenomenon that had licensed the depravity: "How come we did not try them [atomic bombs] on Germany… . They just did not want to use them on white folks."[4] Although the building of the weapon was completed only after Germany surrendered on May 7, 1945, Japan had been designated the target on September 18, 1944, and training for the mission had already been initiated in that same month.[5] Black

journalist George Schuyler wrote: "The atom bomb puts the Anglo-Saxons definitely on top where they will remain for decades"; the country, in its "racial arrogance," has "achieved the supreme triumph of being able to slaughter whole cities at a time."[6] Still within the first year (and still before John Hersey had begun to awaken Americans to the horrible aversiveness of the injuries), novelist and anthropologist Zora Neale Hurston denounced the US president as a "butcher" and scorned the public's silent compliance, asking, "Is it that we are so devoted to a 'good Massa' that we feel we ought not to even protest such crimes?"[7] Silence—whether practiced by whites or people of color—was, she saw, a cowardly act of moral enslavement to a white supremacist.

Each of these three passages, and scores of others, are documented in Vincent Intondi's brilliant history, *African-Americans Against the Bomb*, which chronicles the repudiation by the Black community of nuclear arms from the 1940s up through President Obama's April 5, 2009 Prague speech: jazz saxophonist Charlie Parker, composer and pianist Duke Ellington, civil rights and gay activist Bayard Rustin, poet-novelist James Baldwin, playwright Lorraine Hansberry, civil rights leader Rev. Martin Luther King, and sociologist and pan-Africanist W.E. B. DuBois are among those who spoke out decisively and often. During these same decades, many white people also spoke out against the moral depravity of nuclear weapons, some even suffering terrible costs similar to those suffered by, for example, DuBois, who because of his ardent denunciation of the American nuclear arsenal was at various points arrested, accused of being an unregistered foreign agent, denied a passport, and eventually prompted to expatriate to Ghana.[8] But African-Americans, in addition to educating all who would hear about the moral depravity of the inflicted injuries, have also sought tirelessly to educate the country about the racial scaffolding that provides the gantry on which the missiles are launched.

Detail from the Nagasaki Atomic Bomb Museum. Photo courtesy of the author.

Some readers will recognize as self-evident the US addiction to white racial supremacy that was at work in the flattening of Hiroshima and Nagasaki and that today supports the country's prodigious nuclear arsenal, currently undergoing a 1.2 trillion dollar renewal.[9] But other readers—even some who perceive the moral turpitude of nuclear weapons and who work tirelessly for their dismantlement—may be reluctant to recognize that racism. After all, we

know nuclear weapons stand to eliminate all humans on Earth, not those of one or another race. Americans and Russians, who together possess more than 93 percent of the world's nuclear arsenal, have long been designated as one another's major opponent, and Russians are often loosely described as racially white (even though they, like the American people, are made up of many different ethnic groups). That nuclear war stands a high chance of being instigated by accident or by appropriation of the weapons by a hacker or nonstate actor may seem to make the conscious and unconscious racial biases of a United States president or nuclear command chain irrelevant.

But three lists—the list of geographies where US presidents have contemplated launching a first strike, the list of geographies where the United States has tested its bombs, and the list of countries that the United States condemns for their aspiration to acquire nuclear weapons—may, like avenues of insight radiating outward from Hiroshima and Nagasaki, help to make the racial underpinnings of the nuclear architecture unmistakable.

First, then, the geographies where we know presidents have contemplated first strikes. Eisenhower considered using an atomic weapon in the Taiwan Straits in 1954. The record of his statements in private meetings shows the presence of race, whether he was at any given moment explaining why he might use the weapon or instead why he might abstain from its use: "The President said that we must recognize the Quemoy is not our ship. Letters to him constantly say what do we care what happens to those yellow people out there."[10] Nixon tells us he contemplated ordering a first strike four times during his presidency. Although he did not name all four targets, we know one in 1969 was North Korea.[11] He contemplated striking North Vietnam in 1972.[12] Lyndon Johnson contemplated the launch of a nuclear weapon against China to prevent China from acquiring a nuclear weapon.[13] To this list may be added the times when US presidents have threatened a first strike, as when the George H.W. Bush administration during the first Gulf War informed Saddam Hussein that if he used chemical weapons, nuclear missiles were positioned to strike his country.[14]

Like the countries US presidents have chosen for a first strike, the US selection of nuclear testing sites indicates a belief that people of color are expendable. The painful instance of the Marshall Islands is succinctly summarized by *The Washington Post*'s Dan Zak: "[T]he United States tested 67 high-yield nuclear bombs between 1946 and 1958, resettling whole islands of Marshallese people, exposing many to radioactive fallout and bequeathing exile and ill health to ensuing generations."[15] One of the bombs was 15 megatons. Describing the total impact of the 67 tests, Zak reckons, "If their combined explosive power was parceled evenly over that 12-year period, it would equal 1.6 Hiroshima-size explosions per day."[16] The picture is not more heartening when one turns to tests carried out on US soil. On the arrival this summer of the 75th anniversary of the July 16, 1945 Trinity test in New Mexico, observers noted the racial distribution: "It should come as no surprise that the downwinders of Trinity were largely impoverished agricultural families, mostly Hispanic and Native."[17] As in New Mexico, so in Nevada. A study published in the medical journal *Risk Analysis* concludes, "Native Americans residing in a broad region downwind from the Nevada Test Site during the 1950s and 1960s received significant radiation exposures from nuclear weapons testing."[18]

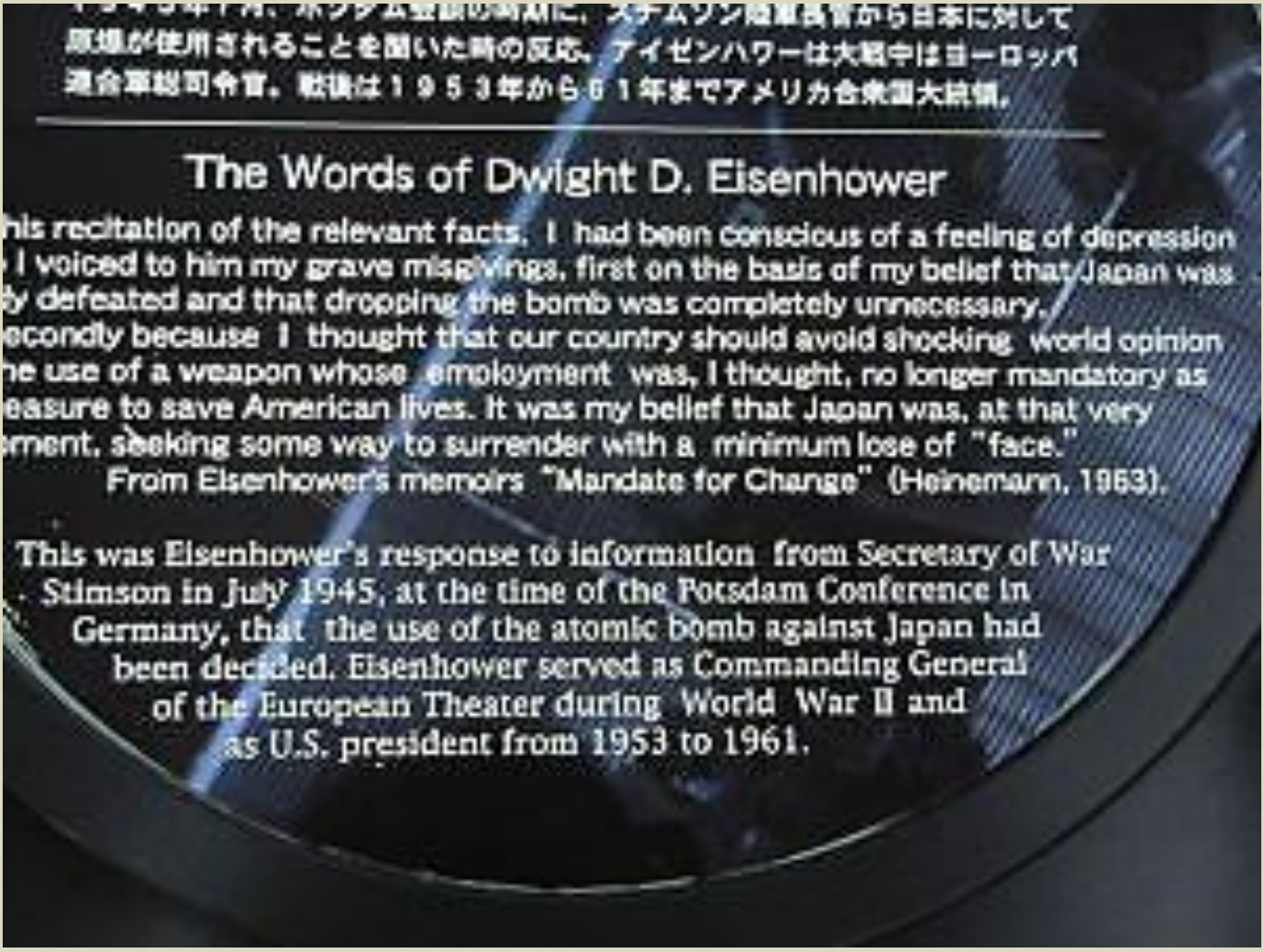
The third list is the sequence of countries we have condemned because their leaders and scientists have aspired to develop a nuclear weapon. The United States has treated these aspirants, in each case, people of color—Iranians, Iraqis, Libyans, North Koreans—as immoral, despite our own vast nuclear architecture and despite our 1995 statement at the International Court of Justice that our having a nuclear arsenal, threatening to use it, using it, and using it first do not violate international covenants such as the UN Convention on the Prevention and Punishment of the Crime of Genocide.[19] The United States sometimes bases its indignation toward nuclear aspirants on the fact that the acquisition of a nuclear weapon by yet another country will violate the Non-Proliferation Treaty (NPT); it righteously announces this violation while relentlessly overlooking the fact that it has for 50 years been in violation of that treaty, which requires, as one of its major pillars, that existing nuclear states dismantle their own arsenals.

A recent article in *The Atlantic* reports new neuroscience research suggesting that people holding positions of power may suffer brain damage, the incapacitation of mirror neurons that ordinarily enable one to comprehend the position of another person or people.[20] A country that has 6,000 nuclear weapons while savaging North Korea for having fewer than 30; a country that has 12 Ohio-class submarines each carrying the equivalent of 4,000 Hiroshima blasts while going to war against Iraq on false evidence that it might have material that could lead to a single nuclear weapon; a country that can't be bothered to commemorate August 6 and August 9 and the hundreds of thousands incinerated on those days, yet clucks and scolds about Iranian nuclear projects, imposes sanctions, and unleashes a Stuxnet digital worm that subverts Iran's uranium enrichment plant;[21] a country that persuades Libya to dispose of its nuclear materials and after it does so, swoops in to help assassinate the country's leader, might well appear to be a country whose governors—and perhaps, too, some in its population—no longer have functioning mirror neurons.

When this soul-destroying asymmetry is pointed out, the United States says, "Yes, but they (i.e., those people of color) may use them, while we (i.e., we white people in charge of the United States) will not use them," a manifestly incoherent statement since it is only the United States who has used them, and used them twice.[22] Extreme alarm incited by picturing nuclear weapons in the hands of yet-one-more country rarely kicks in when the United States distributes its own weapons to NATO allies, currently Germany, Belgium, Netherlands, Italy (Turkey, too, has US nuclear weapons, but many were removed after 2000 and those that remain have since 2016 become a source of mounting worry[23]). Since these

four countries are traditionally viewed as white-majority peoples, the danger of reckless use is apparently non-existent; the proliferation of the weapons to these countries does not, in the US view, violate the Non-Proliferation Treaty. In a feat of double think that might have startled even George Orwell, they calmly acknowledge that in the event of war (when the NATO sharing countries will be called upon to participate in the delivery of those weapons), the Non-Proliferation Treaty will cease to be in effect.[24]

So we return to the question: What kind of political arrangements will create a noble and generous people? What kind of arrangements will restrain a country from egregious mass killings in the future? Will enable that country to face responsibility for injuries it has in the past inflicted on home ground (on Native Americans and African Americans), and on foreign ground (the people of Hiroshima and Nagasaki)? Will help them to dedicate themselves to dismantling mis-trained and militarized police teams roving their cities and dismantling the nation's nuclear architecture? These accomplishments are momentous and difficult but surely also minimal if we aspire to one day become a great and good people.



Detail from the Nagasaki Atomic Bomb Museum. Photo courtesy of the author.

Langston Hughes voiced the opinion that until racial injustice on home ground in the United States ceases, "it is going to be very hard for some Americans not to think the easiest way to settle the problems of Asia is simply dropping an atom bomb on colored heads there."[25] While his statement was made in 1953, near the eighth anniversary of the Hiroshima and Nagasaki bombings, it remains equally relevant today, as we approach the 75th anniversary: Then, as now, the safety of the Korean people (among other peoples) was at issue. The cruelty daily inflicted on people of color in our own city streets acts as a mental rehearsal for carrying out large-scale slayings abroad. It keeps our capacity for cruelty limber; it dulls the mind and gives us practice in pronouncing the word "expendable."

Langston Hughes might have with equal accuracy noted the reverse. Our cruelty abroad hardens our hearts, enabling us to tolerate the spectacle of everyday racial injustice at home. Americans, seeing our country boast a vast nuclear architecture that has no other purpose

than the instant elimination from Earth of large civilian populations—the launch codes day and night casually tucked in our president's pocket—consciously or unconsciously absorb the power lesson, suffer the same brain deterioration, and now become dull-witted about whether Native American and Black lives any longer even matter.

A just state is a state that makes its population care to be just. Can a nuclear country inspire its population to be just? Doesn't that very nuclear architecture require its population to lose its perceptual acuity? If one keeps one's eyes on the monumental apparatus moment by moment, that will induce incapacitating shame and terror (as happened in the first two decades after Hiroshima and Nagasaki, when the horror of the weapons and, simultaneously, of racial injustice at home, was day by day on peoples' minds). Instead, vision has now contracted to a narrow band of bearable possibilities that, in its very narrowness, necessitates an ethical dumbing down.

If the charge of a self-imposed dumbing down seems fanciful, it may be helpful to consider recent critiques of the country's nuclear policy establishment. This establishment has the virtue –a virtue practiced by too few in the population – of remaining aware of the country's nuclear arsenal; but it does so by constricting its field of vision. Anthropologist Hugh Gusterson, a longtime observer of nuclear scientists and policy communities, in early 2019 described in the pages of the *Bulletin of Atomic Scientists* a large assembly in Washington's Brookings Institute that gathered to hear an all-star, five-person panel address "the Politics of New Start and Strategic Modernization." The five, he reports, delivered five nearly identical lectures, only debating "the semantics of whether [the] pairing of nuclear modernization and arms control should be characterized as the product of a 'consensus' or a 'coalition.'"[26] A related critique has been made by French political scientist Benoît Pelopidas, who describes, as his title announces, "Nuclear Weapons Scholarship as a Case of Self-Censorship in Security Studies." Despite the absence of any externally imposed prohibition on free discourse or constraints on argument, the community voluntarily contracts the frame of reference to bypass all normative considerations and to avoid contemplating the possibility of radical reordering of the world, such as by nuclear abolition. Two terms—"non-proliferation" and "deterrence"—are relentlessly used as tools to corral the discussion into a narrow perimeter of business-as-usual thinking that invalidates as unrealistic any alternative idea, thereby eliminating any sense of obligation to the future.[27]

The death of George Floyd has brought about, among many other outcomes, a commitment to change the nuclear policy arena. In the summer of 2020, a cascade of American foreign policy and national security institutions, including the *Bulletin of Atomic Scientists,* signed the statement authored by the Women of Color Advancing Peace, Security and Conflict and agreed to carry out a host of reforms, such as making sure institutions dedicated to peace and security "diversify our boards of directors and advisory committees," acknowledge the harmful effects of "microagressions" against people of color in the workplace, and "call out racism and share the burden of dismantling white supremacy."[28]

While the list of resolutions emphasizes changes in the workplace and governing boards of these institutions, it may be that these changes will in turn bring about a recognition of the place of racism in the very philosophies of international relations and nuclear weapons. The obligation to "call out racism and share the burden of dismantling white supremacy" should carry with it the obligation to recognize the racist foundation of the nuclear architecture itself (a northern hemisphere blanketed by nuclear states, a southern hemisphere blanketed by nuclear weapons-free zone treaties) and to dismantle it, beginning with the two states that hold 93 percent of all the weapons.

A mother and child, dressed in traditional clothing, sit on the ground amid rubble and burnt trees, Hiroshima, Japan, December 1945. On August 6, some four months previously, the United States had dropped an atomic bomb on the city–three days later a second one was dropped on Nagasaki. (Photo by Alfred Eisenstaedt/The LIFE Picture Collection via Getty Images)

Most nights during the summer of 2020, Black Lives Matter vigils take place, not only in cities but in small towns across the country. In Arlington, Massachusetts, for example, people stand, masked and at safe distances from one another, along the broad main avenue from 6 p.m. to 7 p.m., while a stream of bicycles and cars signal by waves and horns and thumbs up their affirmation of the signs: "Breonna Taylor." "Raychard Brooks." "George Floyd." "Say Their Names." "Not One More." "No Justice, No Peace." In the last 8-minutes and 46

seconds of the hour, people drop to one knee and only stand again when the church bells announce the closing of the hour. The posture is one inherited from decades of civil rights practice (initiated by Martin Luther King, Jr., then made new by Colin Kaepernick and black NFL players); the temporal duration is a direct reference to the killing of George Floyd, as though by duplicating the kneeling of the policeman we could back up and reverse its intent and its outcome. The posture expresses an array of feelings: sorrow at George Floyd's death, a counterfactual wish that it had not happened (let his breathing be restored), shame at not having collectively perceived the scale of the injuries for so long, and a commitment to reinvent a form of policing that nourishes and assists, rather than preys upon, our towns and cities.

Perhaps something like this same gesture could be carried out—in the privacy of one's home or on Main Street or in parks and spaces of public assembly—at 8:15 a.m. on August 6th and 11:02 a.m. on August 9. Carried out: out of sorrow for those slain and those hideously wounded, out of remorse for not having faced the injuries sooner, out of a shared commitment to dismantle the nuclear architecture so that we need only commemorate, and never again re-enact, what took place on those days. What would be an appropriate duration? Perhaps 53 seconds, the time interval between the moment the children of Hiroshima pointed to the B-29 in the blue sky and the moment a blinding flash of light melted their eyes and erased their world. Or perhaps the 100 seconds that the *Bulletin* designates as the window of time that now separates us from worldwide catastrophe.

Notes

[1] For a chart summarizing research by the Center for Disease Control and Prevention (CDC) on law enforcement killings of various racial groups from 1999 to 2015, see Elise Hansen, CNN, "The Forgotten Minority in Police Shootings," November 13, 2017. https://www.cnn.com/2017/11/10/us/native-lives-matter/index.html.

Another large study has shown "Native American males have 14 times as many fatal encounters [with police] as white males; Native American females have 38 times as many fatal encounters as white females." Matthew Harvey, The Center for Indian Country Development, "Fatal Encounters between Native Americans and the Police," March 2020. https://www.minneapolisfed.org/~/media/assets/articles/2020/fatal-encounters-between-native-americans-and-the-police/fatal-encounters-between-native-americans-and-the-police_march-2020.pdf?la=en

[2] John Hersey, *Hiroshima* (New York: Vintage, 1946, 1984; 2nd edition 2020), pp. 35, 181, 146, 167 168, 183-5, 191.

[3] I stipulate "*almost*" no one on Earth because the people of Switzerland, acting on an ethic of "equality of survival," have created fallout shelters for 114 percent of their population (as well as many hospitals and first aid stations hidden inside mountains); conceivably, some among them may survive. The United States has spent equally vast resources on a fallout shelter for a single person, the president, and his entourage—a miniature city carved out inside a mountain—but no shelter for the population. For the contrast between the Swiss and US shelter systems, see Elaine Scarry, *Thinking in an Emergency* (New York: Norton, 2011), pp.51-69; and for a detailed account of the U.S. shelter, see Garrett M. Graff, *Raven Rock: the Story of the U.S. Government's Secret Plan to Save Itself – While the Rest of Us Die* (New York: Simon and Schuster, 2017).

[4] Langston Hughes, "Here to Yonder: Simple and the Atom Bomb," *Chicago Defender,* August 19, 1945, cited in Vincent Intondi, *African Americans Against the Bomb: Nuclear Weapons, Colonialism, and the Black Freedom Movement* (Stanford, Ca.: Stanford University Press, 2015), p. 15.

[5] Richard Rhodes describes President Roosevelt's and Prime Minister Churchill's September 18-19, 1944 meeting at Roosevelt's Hudson Valley estate, Hyde Park, and "a secret aide-mémoire" that "recorded for the first time the Anglo-American position on the new weapon's first use." The document contemplates bombing multiple Japanese cities, with a warning coming only after the first city has been struck: "when a 'bomb' is finally available, it might perhaps, after mature consideration, be used against the Japanese, who should be warned that the bombardment will be repeated until they surrender." The fall 1944 training of the 509th Composite Group in Utah entailed visual targeting, something that puzzled the crews since they were used to "cloudy Europe" where visual identification of a target was seldom possible. (Richard Rhodes, *The Making of the Atomic Bomb* [New York: Simon & Schuster, 1986, 2012], pp. 537, 585).

[6] George Schuyler, "Views and Reviews," *Pittsburgh Courier,* August 18, 1945 and December 15, 1945, cited in Intondi, *African Americans Against the Bomb,* p. 14.

[7] Zora Neale Hurston, letter to Claude Barnette, July 21, 1946, published in *Zora Neale Hurston: A Life in Letters*, ed. Carla Kaplan (New York: Doubleday, 2002), p. 545, and cited in Intondi, *African Americans Against the Bomb,* p. 15.

[8] W.E.B. DuBois, *In Battle for Peace: the Story of My 83rd Birthday,* introd. Manning Marable (New York: Oxford University Press, 2007), pp. xxi, xxiii, xxv, 23, 26-27, 37, 48, 49, 137, 144.

[9] The Endowment for Human Development calculates that a billion dollars is a stack of hundred dollar bills 70 miles high, whereas one trillion dollars is a stack of hundred dollar bills 68,000 miles high or "more than one-fourth the way from the earth to the moon." https://www.ehd.org/science_technology_largenumbers.php

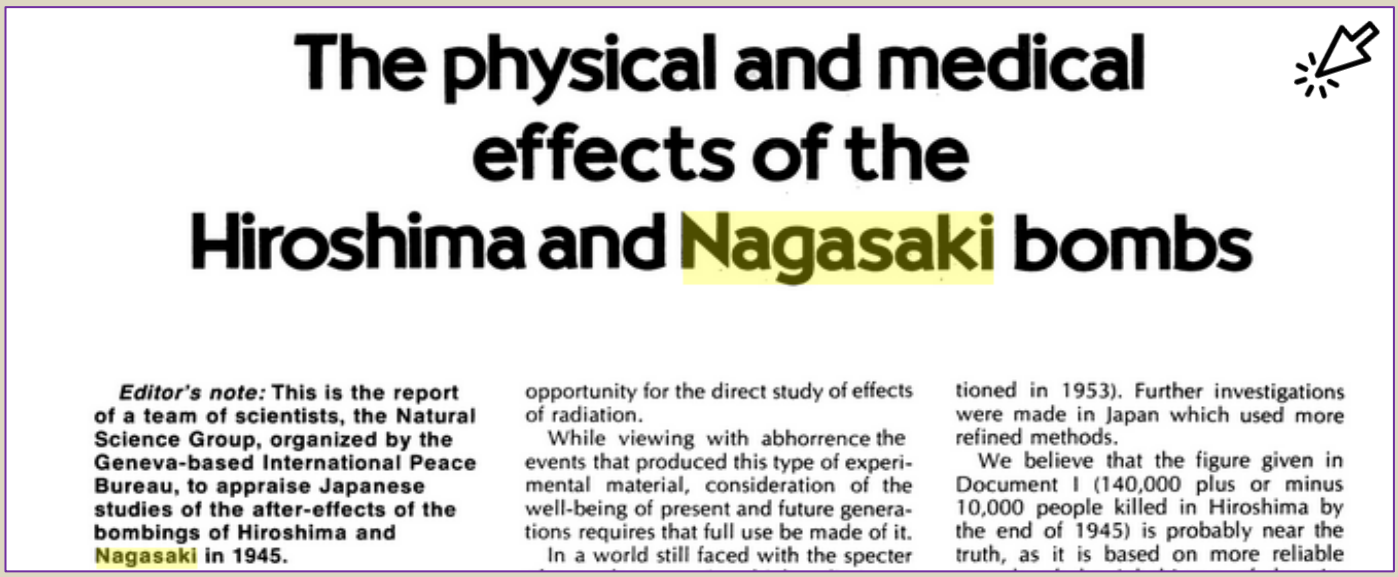
[10] *Foreign Relations of the United States*, 1952-54, vol. 14, p. 622. Eisenhower also considered using a nuclear weapon in 1959 in Berlin, a white population. I describe these events where presidents considered using an atomic weapon in *Thermonuclear Monarchy: Choosing between Democracy and Doom* (New York: Norton, 2014).

[11] "Memorandum: Secretary of Defense Laird to NSA Kissinger, June 25, 1969. Subject: Review of US Contingency Plans for Washington Special Action Group," Tab L, declassified October 2006 (Document 12, "How Do You Solve a Problem Like Korea," Electronic Briefing Book 322, National Security Archive, George Washington University). See also Chris McGreal, "Papers Reveal Nixon Plan for North Korea Nuclear Strike," *Guardian*, July 7, 2010.

[12] On Nixon's 1972 proposal to use nuclear weapons in North Vietnam, see Deb Riechmann, "Nixon Discussed Nuclear Strike in Vietnam," *Boston Globe*, March 3, 2002.
[13] On the release of documents showing Johnson's consideration of a pre-emptive strike in China, see Jim Mann, "U.S. Considered '64 Bombing to Keep China Nuclear-Free," *Los Angeles Times*, September 27, l998.
[14] Nick Pike, "Nuclear Threats during the Gulf War," Federation of American Scientist, February 19, 1998. Threats made by the United States and the United Kingdom included total destruction of the country: For example, British Foreign Minister Douglas Hurd warned against any action that would "provoke a response that would completely destroy that country." https://fas.org/irp/eprint/ds-threats.htm. For an account of U.S. and British threats against Iraq, as well as U.S. and British use of depleted uranium munitions against Iraq, see Joseph Gerson, *Empire of the Bomb: How the U.S. Uses Nuclear Weapons to Dominate the World* (Ann Arbor, Michigan: Pluto Press, 2007), p.217f.
[15] Dan Zak, "He saw a nuclear blast at 9, then spent his life opposing nuclear war and climate change," *Washington Post*, August 24, 2017. Available at: https://www.washingtonpost.com/local/he-saw-a-nuclear-blast-at-9-then-spent-his-life-opposing-nuclear-war-and-climate-change/2017/08/24/5b6d10e6-882e-11e7-a94f-3139abce39f5_story.html
[16] Dan Zak, "A Ground Zero Forgotten: The Marshall Islands, Once a U.S. Nuclear Test Site, Faces Oblivion Again," *Washington Post,* November 27, 2015. Available at: https://www.washingtonpost.com/sf/national/2015/11/27/a-ground-zero-forgotten/
[17] Joshua Wheeler, "It's Been 75 Years, and American Still Won't Admit a Nuclear Disaster," *New York Times,* July 16, 2020. The presence of Hispanic families is also noted by Maria Cramer, who writes, "Officials did not warn any of the residents — many of them ranchers, Navajos, Mexican settlers and their descendants who raised cattle and drank water from cisterns — about the test" ("'Now I Am Become Death': The Legacy of the First Nuclear Bomb Test," *New York Times,* July 15, 2020).
A 2010 study by the Center for Disease Control and Prevention (CDC) reports: "Different standards of safety were applied to informed project workers than to uninformed members of the public. Project workers knew enough to evacuate areas when high exposure rates were measured, or to take the necessary precautions to minimize exposure, but members of the public did not realize that changes in their behavior were prudent, and project staff did not call for evacuations or protective measures even though predetermined tolerances for exposure rate and projected total exposure had been exceeded." Addressing the racial composition of residents living near the test site, the report notes that General Leslie Groves stipulated "a 17 x 24 mile area on which no Native Americans lived." A chart summarizing the racial composition of nearby residents specifies the presence of whites and Hispanics but not Native Americans. CDC, "Final Report of the Los Alamos Historical Document Retrieval and Assessment (LAHDRA) Project," November 2010, pp. 10-3, 10-15, 10-50.
A wider perimeter, however, reveals the presence of many Native Americans. *Indian Country Today* states that the 19,000 people living within a 50-mile radius of the Trinity test site included 19 Pueblo communities, two Apache tribes, and several "chapters of the Navajo Nation." Tanya H. Lee, "H-Bomb Guinea Pigs! Natives Suffering After New Mexico Tests," *Indian Country Today,* March 5, 2014, https://indiancountrytoday.com/archive/h-bomb-guinea-pigs-natives-suffering-decades-after-new-mexico-tests-jpZAFe1gFEmRCGfiq42BDg
[18] E. Frohmberg, R. Goble, V. Sanchez, D. Quigley, "The Assessment of Radiation Exposures in Native American Communities from Nuclear Weapons Testing in Nevada," *Risk Analysis,* February 2000, pp. 101-111.
[19] Department of State and Department of Defense, "Written Statement of the Government of the United States," International Court of Justice, Hearings on the questions: "Is the threat or use of nuclear weapons in any circumstance permitted under international law?", 1995, p.33
[20] Jerry Useem, "Power Causes Brain Damage: How Leaders Lose Mental Capacities – Most Notably for Reading Other People – that Were Essential to Their Rise," *The Atlantic*, July/August 2020. The research —showing that people with power became "less adept at seeing things from other people's point of view" as well as "more impulsive, less risk-aware"—was carried out in separate studies by psychologist Dacher Keltner at UC Berkeley and neuroscientist Sukhvinder Obhi at McMaster University in Ontario.
[21] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History," *Wired,* July 11, 2011. See also the documentary film, *Zero Days*, directed by Alex Gibney, 2016.
[22] Anthropologist Hugh Gusterson calls this asymmetry in U.S. thinking "nuclear orientalism," the belief that other countries are "too infantile, too immature, and too irresponsible to be trusted with nuclear weapons." See his vividly illustrated lecture, "Democracy, Hypocrisy, First Use," at the Nov. 4, 2017 Harvard conference, "Presidential First Use: Is it Legal? Is it Constitutional? Is it Just?" , https://www.youtube.com/watch?v=zdLXKNivl9M&list=PL2SOU6wwxB0vZEgAvRotf9-INc9nA8t02&index=10&t=0s. To read a transcript (without visual illustrations), see *Public Books*, "Virtual Roundtable on Presidential First Use of Nuclear Weapons," February 26, 2018.
[23] See Hans Kristensen, "Urgent: Move US Nuclear Weapons Out of Turkey," Federation of American Scientists, October 16, 2019.
[24] "Questions on the Draft Non-Proliferation Treaty Asked by U.S. Allies Together with Answers Given by the United States," April 28, 1967, Tab A, connected to April 10, 1968 "Letter from the Under Secretary of State (Katzenbach) to Secretary of Defense Clifford," *Foreign Relations of the United States,* 1964-68, Vol. XI, Arms Control and Disarmament, p. 575.
[25] Langston Hughes, "Colored Asia Makes Highly Colored News These Days," *Chicago Defender,* August 15, 1953, p. 11, cited in Intondi, *African Americans Against the Bomb*, p. 31.
[26] Hugh Gusterson, "The Blinders on the U.S. Nuclear Policy Establishment," *Bulletin of Atomic Scientists,* January 8, 2019.
[27] Benoît Pelopidas "Nuclear Weapons Scholarship as a Case of Self-Censorship in Security Studies," *Journal of Global Security Studies,* 2016. Available at: https://spire.sciencespo.fr/hdl:/2441/7leam5bkng9j3binvavkneitle/resources/2016-pelopidas-nuclear-weapons.pdf
[28] Gayle Spinazze, WCAPS Statement: Standing Together Against Racism and Discrimination," *Bulletin of the Atomic Scientists*, June 10, 2020. As Rachel Bronson wrote in signing the statement, "The *Bulletin* recognizes racism as a threat to humanity and that national security cannot be advanced unless all citizens have strong personal security. . .. We acknowledge that we have much work to do

on this front to serve as an ally with communities of color, and those advocating change." Available at: https://thebulletin.org/2020/06/wcaps-statement-standing-together-against-racism-and-discrimination/

Elaine Scarry is the author of *Thermonuclear Monarchy: Choosing between Democracy and Doom* and *The Body in Pain: the Making and Unmaking of the World*. She is Cabot Professor of Aesthetics at Harvard University.



The physical and medical effects of the Hiroshima and Nagasaki bombs

Editor's note: **This is the report of a team of scientists, the Natural Science Group, organized by the Geneva-based International Peace Bureau, to appraise Japanese studies of the after-effects of the bombings of Hiroshima and Nagasaki in 1945.**

opportunity for the direct study of effects of radiation.

While viewing with abhorrence the events that produced this type of experimental material, consideration of the well-being of present and future generations requires that full use be made of it.

In a world still faced with the specter

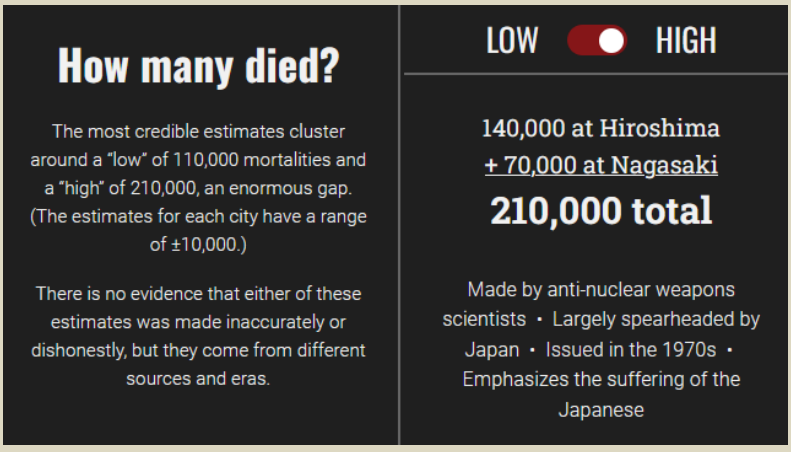
tioned in 1953). Further investigations were made in Japan which used more refined methods.

We believe that the figure given in Document I (140,000 plus or minus 10,000 people killed in Hiroshima by the end of 1945) is probably near the truth, as it is based on more reliable

Counting the dead at Hiroshima and Nagasaki

By Alex Wellerstein

Source: https://thebulletin.org/2020/08/counting-the-dead-at-hiroshima-and-nagasaki/



Aug 2020 – How many people died as a result of the atomic bombings of Hiroshima and Nagasaki? There is one thing that everyone who has tackled this question has agreed upon: The answer is probably fundamentally unknowable. The indiscriminate damage inflicted upon the cities, coupled with the existing disruptions of the wartime Japanese home front, means that any precise reckoning is never going to be achieved.

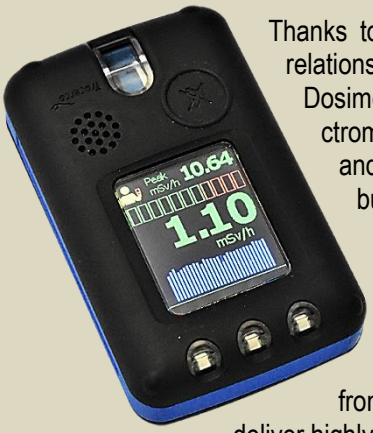
But beginning in 1945, people have tried to estimate the number of the dead and injured. The casualties from the first atomic bombings are not of mere historical interest. They are part of how we understand the effects of nuclear weapons today — for Hiroshima and Nagasaki, thankfully, remain the only instances of these weapons being used in warfare, and thus provide an invaluable "data set" upon which to base other understandings and simulations. The estimated casualties also play a nuanced role in the various narratives and arguments about the end of World War II.

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

Alex Wellerstein is an Associate Professor and Director of the Science and Technology Studies program at the Stevens Institute of Technology. His first book, *Restricted Data: The History of Nuclear Secrecy in the United States*, was published by the University of Chicago Press in April 2021.

Tracerco PED+ Simulator

Source: https://www.argonelectronics.com/tracerco-ped-simulator-cbrne-hazmat-training



Thanks to a combination of Argon's wealth of simulation experience and our relationship with Tracerco, the look, feel and response of the Personal Electronic Dosimeter (PED+) Simulator is extremely close to that of actual detector. PED+SIM responds to Radsim ele ctromagnetic sources that safely simulate ionizing radiation eliminating regulatory, environmental, and health and safety concerns for you and your students. You can use the simulation sources in the open or within buildings.

High impact radiation training

To ensure the ultimate training experience, all user interface components (display, indicators, switch panel, sounder and vibrator) are exactly the same as the real detector.

Response speed and characteristics when approaching and withdrawing from the simulation source are just like the real detector enabling you to deliver highly realistic source search / find training.

Simulated sensitivity enables the Tracerco PED+SIM to detect the Radsim GS4 simulation Gamma source at a free space distance of typically 200 feet (60 metres) distance line of sight.

Consistent, repeatable performance

Powerful proprietary signal processing ensures simulated readings are repeatable each time students revisit the same scenario location while also ensuring the readings observed on different simulators are within the accepted tolerances of actual detectors; all contributing to the provision of high quality, realistic training.

Even the effect of user body shielding to determine source position is realistically simulated so you can be certain your survey teams understand how to use and interpret their detector readings and alarms effectively.

Key features:

- Inverse square law (1/r2) response within real detector tolerance.
- Simulation of user body shielding for source location.
- Realistic representation of different shielding effects.
- Selectable units of measurement (Sv/hr, Rem, CPS).
- Same human interface as real Tracerco PED+.
- Configurable menu settings.
- Dose and dose rate alarm settings.
- Language selection.
- Same battery as real detector (approximately 36 hours standard operation, 150 hours operation in screen saver mode).
- No regular calibration.
- No preventative maintenance.

Time distance shielding

The PED+ training simulator enables the importance of time/distance shielding to be taught and demonstrated with ease; the activity of the simulated source realistically reduced depending upon the material between the simulation source and the simulated detector.

Extremely realistic inverse square law response allows the powerful protective combination of distance and shielding to be demonstrated enabling students to practice communication of recommendations and safety procedures without the regulatory, safety, environmental and cost restrictions associated with real sources.

Cost effective realistic training

No preventative maintenance, calibration or consumables (except batteries) are required ensuring whole life cost of ownership is minimal, expensive damage to real detectors is avoided and operational readiness is maintained.

PlumeSIM compatible

PED+SIM is compatible with PlumeSIM, Argon's proven Live Field and Tabletop CBRN exercise system. In use by many of the world's leading training facilities, PlumeSIM enables real time instrumented wide area tactical field and nuclear / HazMat / Chemical Warfare emergency response exercises to be conducted using single or multiple simulation device types that respond in the real time to simulated hazards.

The Diablo Canyon nuclear plant: assessing the seismic risks of extended operation

By Edwin Lyman

Source: https://thebulletin.org/2022/08/the-diablo-canyon-nuclear-plant-assessing-the-seismic-risks-of-extended-operation/

The Diablo Canyon nuclear power plant in Central California. Photo credit: marya from San Luis Obispo, USA via Wikimedia Commons, CC BY 2.0 license https://creativecommons.org/licenses/by/2.0/deed.en

Aug 15 – In 2016, Pacific Gas & Electric (PG&E) announced a historic agreement with labor and environmental groups to shut down the two-unit Diablo Canyon nuclear plant in California by 2025 and replace its roughly 2,200 megawatts of electricity with low- and zero-

carbon renewable energy, energy efficiency, and storage. Today, that agreement is in serious jeopardy after an academic study (underwritten in part by the nuclear industry), combined with a sustained and vocal public relations campaign waged by Diablo Canyon supporters (including a Tik-Tok influencer), have succeeded in raising doubts about the viability of the power replacement plan. Growing concerns about climate change-related impacts on the reliability of the electrical grid have also prompted California governor Gavin Newsom to reconsider his position and seek to keep the plant open, at least in the short term. The US Energy Department's Office of Nuclear Energy is also doing its part to keep Diablo Canyon open by relaxing the original financial qualification criteria and extending the application deadline by more than three months for its recently established Civil Nuclear Credit Program. This will make it possible for PG&E to apply for a first round of federal subsidies aimed at helping utilities keep nuclear power plants open.

Although there is some basis for the criticism that PG&E and the State of California are not acting quickly enough to ensure that enough carbon-free power will be available to replace all of Diablo Canyon's output, the California Public Utilities Commission's historic decision last year to procure 11,500 megawatts of clean energy resources by 2026, along with 4,000 megawatts of new capacity (mostly battery storage) added to the grid in the last year, should help address that concern. A recent analysis by Gridlab and Telos Energy also found that renewable energy could replace Diablo Canyon and supply 85 percent of California's electricity by 2030, while keeping the power on for its 40 million residents—even under stressful conditions such as low hydropower generation, retirements of fossil fuel-fired plants, and heatwaves similar to what caused rolling power outages in August 2020.

Nevertheless, the disagreement over the plant's future has become a proxy for the larger debate over what role nuclear power should play in addressing climate change, given its safety and security risks. If PG&E's original plan were to succeed, after all, it could undermine the nuclear advocates' argument that nuclear power is an irreplaceable asset in all circumstances.

But if Diablo Canyon is to remain open beyond 2025, PG&E will have to address a number of difficult issues. First, the company will have to prepare a new 20-year license renewal application and submit it to the US Nuclear Regulatory Commission (NRC) before the expiration of Unit 1's operating license in 2024. PG&E will also have to undertake extensive inspections and equipment upgrades that were indefinitely postponed after it made the decision to shut the plant, as discussed in a June 2022 meeting of the Diablo Canyon Independent Safety Committee. And finally, it must take a hard look at the vulnerability of the plant to earthquakes and consider the need to make seismic upgrades to minimize the risk to the public over the period of extended operation.

Conflicting information on the seismic question has been reported. A spokesperson for the California Public Utility Commission was quoted as saying that if PG&E were to resume the license renewal proceeding for the plant, it would need to make seismic upgrades. However, this statement is not consistent with the NRC's current position. Following a review conducted in the aftermath of the 2011 Fukushima accident in Japan, the agency concluded that no seismic upgrades at Diablo Canyon or any other US nuclear plants were necessary, because the health and safety risks to the public were acceptable. Since the NRC has sole authority over the radiological safety aspects of Diablo Canyon, this means that the plant owner will not have to spend a penny to strengthen its seismic protection, no matter what the state of California wants.

Arguably, however, the NRC is not doing enough to reduce the risk that a severe earthquake could cause a Fukushima-like core meltdown and radiation release at Diablo Canyon (or, for that matter, other seismically vulnerable nuclear plants in the country). The agency, as part of its drive to transform into a more "risk-informed" regulator, cites the low calculated radiological risk to the public from nuclear plant accidents to justify not taking action to increase safety across a wide range of areas, including seismic protection. But there's a major problem with this approach: Assessing the seismic risk involves understanding both the uncertainties associated with nuclear accidents and the even larger unknowns encountered in trying to predict earthquake behavior. These uncertainties raise doubts whether the seismic risks can be calculated with sufficient precision to support the NRC's complacency.

Although other nuclear plants are also seismically vulnerable, according to current information, the potential peak ground motion that the Diablo Canyon site may experience from an earthquake occurring every 10,000 years on average is far higher than any other US plant. But it is also important to consider this value in relation to the seismic standard that the plant was designed and built to meet and that is used as the basis for inspection and regulatory enforcement.[1] Diablo Canyon's seismic risk actually may be lower than some other US reactors because, given its location, it was originally designed with additional earthquake resistance. But that doesn't mean it is safe enough. Serious questions persist about whether Diablo Canyon's design basis and "current licensing basis" meet a high enough seismic standard to adequately protect the public.

This is an issue with a very long history, as detailed in a 2013 report by the Union of Concerned Scientists' former nuclear safety director Dave Lochbaum. Since that report, considerable additional information has been released about Diablo Canyon's seismic risks. A review of this new information clearly shows there are gaps in the seismic safety of Diablo Canyon that should be closed if the plant is going to continue to operate beyond 2025. If California decides to support license renewal, a portion of the "transition costs" that the Energy Department and the state may provide to PG&E to keep the plant operating should be allocated to reducing its vulnerability to earthquakes. The risk is not negligible, and the potential costs of an earthquake-induced

accident could, by our estimate, cause more than 10,000 cancer deaths and over $100 billion in damages.

NRC requirements for protection against earthquakes

The NRC's fundamental design criterion for protection of the current generation of nuclear power plants against earthquakes and other natural phenomena was first developed in the 1970s. The requirement is logical but challenging to meet: a nuclear plant applicant must design the "structures, systems, and components (SSCs) important to safety … to withstand the effects of natural phenomena such as earthquakes … without loss of capability to perform their safety functions." To implement this requirement, the agency specified how to determine the "design-basis" natural hazards that reactors are required to withstand. For earthquakes, the NRC defines a design-basis earthquake, otherwise known as a "safe shutdown earthquake" (SSE), as "that earthquake which is based upon an evaluation of the maximum earthquake potential considering the regional and local geology and seismology and specific characteristics of local subsurface material. It is that earthquake which produces the maximum vibratory ground motion for which certain structures, systems, and components are designed to remain functional." (Reactors licensed after 1997 use a somewhat different definition, as discussed below.)

Thus, the NRC requires reactor applicants to determine the characteristics of the safe shutdown earthquake, based on detailed seismological surveys and analyses, and then ensure that safety systems "remain functional" if such a quake occurs. In this case, functionality is defined as meeting the same relatively stringent requirements that must be met to protect against other design-basis accidents.[2]

Of course, it's always possible that a nuclear plant will encounter an earthquake more severe than the largest one that has occurred historically or is projected to occur at its location. In 2011, both the Fukushima Daiichi plant in Japan and the North Anna plant in Virginia experienced the most severe earthquakes in their recorded history. Seismological forecasting is far from an exact science. The goal of seismic design today is to choose a safe shutdown earthquake so that the probability that it will be exceeded over the facility lifetime is low—and if a larger earthquake does occur, that there is sufficient safety margin to prevent a disaster from occurring. North Anna was able to withstand a beyond-design-basis earthquake without safety being challenged, and even at Fukushima, the tipping point that led to disaster was not direct structural damage from the earthquake but flooding from the earthquake-generated tsunami. Nevertheless, there will always be a residual risk that a sufficiently destructive earthquake will cause a reactor meltdown.

One significant flaw in the standard methodology for analyzing earthquake impacts on nuclear plants is that it only considers the mainshock, and not the potential for aftershocks that could cause cumulative damage and potentially compromise plant safety, even if the plant survived the mainshock. This also has ramifications for scenarios in which operator actions that could be disrupted by aftershocks are needed to mitigate damage from the mainshock. Ignoring aftershocks has been identified as a potentially significant non-conservatism in seismic analysis—a gap that becomes more problematic as the size of the foreshock increases, given that "in general, the larger the mainshock, the larger and more numerous the aftershocks, and the longer they will continue." This is a particular concern for Diablo Canyon, considering its potential for large mainshocks.

Also at issue is how to address new information that emerges after a plant has already been built indicating that it is susceptible to larger earthquakes than were considered in the design—functionally rendering obsolete the safe shutdown earthquake documented in the plant's license. Based on the principle that the plant should be able to shut down and remain safe after such a quake, one might expect as a matter of course that the seismic design basis would be revised, and the plant's earthquake defenses strengthened accordingly.

But it can be costly or infeasible to extensively retrofit nuclear power plants to survive more powerful earthquakes. Diablo Canyon encountered this problem during construction in the 1970s, and in the last few decades new information and analyses have revealed that nearly every nuclear plant in the country faces more severe earthquakes than they were licensed to withstand. But the NRC's response, then as now, has been to settle for weaker measures with smaller safety margins, or—if it considers the associated increase in meltdown risk to be acceptable—even none at all. This approach leaves a big question mark about whether Diablo Canyon (not to mention the rest of the operating US nuclear fleet) is sufficiently well-protected against earthquakes.

But, given its seismic environment, this concern remains most acute for Diablo Canyon.

The complicated history of Diablo Canyon's seismic evaluations

One thing everyone can agree on is that the seismic issues at Diablo Canyon are very complex. As the NRC puts it:

[Diablo Canyon] has a unique and complex seismic design and licensing bases compared to other commercial nuclear power plants, in that it is composed of four seismic design response spectra used in the seismic design of Units 1 and 2 … Each spectrum is based on a different set of analysis assumptions … and different performance criteria.

In 1968, Diablo Canyon Unit 1 received a construction permit from the NRC's pre-1975 predecessor, the Atomic Energy Commission, under a different set of standards than the NRC's subsequent requirements described above.[3] Based on seismic studies, the safe-shutdown earthquake was taken to be one that could cause a peak ground acceleration of

0.4 times the acceleration of gravity (0.4g). But during construction of Unit 1, in 1973, a fault known as the Hosgri was discovered about three miles offshore from Diablo Canyon, and PG&E determined that an earthquake occurring on the Hosgri fault zone could cause a peak ground acceleration of 0.75 g—nearly twice the design-basis earthquake level originally estimated. Understandably, PG&E did not want to redefine the safe shutdown earthquake of the plant and retrofit the design to address this much greater hazard, given that construction was already underway.

In 1977, PG&E and the NRC reached an agreement on a special methodology, the Hosgri Evaluation, for addressing the new information.[4]

The Hosgri Evaluation methodology was not as conservative (that is, it provided smaller safety margins) than the earlier analyses. One major difference between the Hosgri Evaluation and the design-basis safe shutdown earthquake analysis: PG&E didn't have to assume that an accident (such as a pipe break or fire) occurred concurrently with a Hosgri Earthquake.[5] In other words, the Hosgri Evaluation assumed that all non-seismic safety and fire protection measures would work perfectly during the earthquake. As a result, PG&E has not evaluated whether plant piping and other key safety components would be able to survive, for example, the combined loads of both a Hosgri Earthquake and a concurrent loss-of-coolant accident. Simply put, the public is not as well-protected from a Hosgri Earthquake affecting Diablo Canyon as it is from the less severe safe shutdown earthquake originally estimated.

This was made abundantly clear when in 2011 PG&E proposed amending the Diablo Canyon license to redefine the SSE as the Hosgri Earthquake but later abandoned the request after some NRC staff opposed the amendment.[6]

Nevertheless, the NRC has allowed Diablo Canyon to keep operating without making seismic upgrades by accepting that the current licensing basis provides "reasonable assurance of adequate protection" of public health and safety—even though the Hosgri Evaluation methodology is a historical artifact that is inconsistent with the NRC's fundamental general design criterion for earthquake protection.

The confusion regarding the actual identity of Diablo Canyon's design-basis earthquake came to the fore when another fault—the Shoreline Fault—was discovered just off-shore of the plant site in 2008. Despite its proximity to the plant, PG&E showed that the ground motion at Diablo Canyon from an earthquake on the Shoreline Fault would be less than what the Hosgri fault might produce and argued that any impacts of a Shoreline earthquake would therefore be bounded by the impacts of a Hosgri earthquake. The NRC then agreed that no further actions were necessary.

An NRC inspector, Michael Peck, dissented, arguing that the discovery of the Shoreline Fault changed the Diablo Canyon seismic design-basis and SSE, and therefore the impacts of Shoreline Fault earthquakes should be analyzed using design-basis methodology. But NRC management rejected Peck's argument, reaffirming that PG&E could analyze the Shoreline Fault using the less conservative Hosgri Evaluation assumptions. Ultimately, the NRC settled the issue as part of its process for reevaluating external hazards following the March 2011 Fukushima accident in Japan, again concluding that the seismic risk is acceptable.

Fukushima seismic reevaluations

The 2011 Fukushima Daiichi accident showed the world what can happen when a nuclear plant experiences a natural disaster more severe than it was designed to handle. In response to the accident, the NRC convened a task force to evaluate whether its nuclear safety requirements needed to be strengthened. In its report, the task force noted that "available seismic data and models show increased seismic hazard estimates for some operating nuclear power plant sites" and recommended that the NRC "order licensees to reevaluate the seismic and flooding hazards at their sites against current NRC requirements and guidance, and if necessary, update the design basis and SSCs important to safety to protect against the updated hazards."

Although the NRC did accept part of the task force recommendation by directing all nuclear plants to "reevaluate the seismic and flooding hazards at their sites using present-day NRC requirements and guidance," it did not adopt the task force's proposed remedy: namely, that plants should update their design bases and harden their infrastructure to protect against reevaluated hazards that are more severe. Instead, the NRC made a weaker and more subjective request that licensees "identify actions that are planned to address plant-specific vulnerabilities associated with the reevaluated seismic and flooding hazard." The agency did not clearly define what those words actually meant until 2019, when it adopted a policy that has effectively allowed nuclear plant licensees to do *nothing* to address hazards that exceeded their design bases.[7]

The main new requirement that the NRC imposed on reactor owners in response to Fukushima was the acquisition of additional emergency equipment, known as "FLEX" (or, formally, Diverse and Flexible Coping Strategies). This included portable generators and diesel-powered pumps that could be used to keep nuclear fuel from overheating in the event of a long-term loss of electrical power—the root cause of the Fukushima meltdowns. However, the NRC allowed this additional equipment to be less robustly protected against design-basis external hazards than the installed plant safety equipment.

Even worse, the 2019 3-2 split decision by the NRC commissioners removed a proposed requirement that the FLEX equipment be protected *even to that lower level* against the reevaluated hazards that were being developed.

This is a huge problem. The hazard reevaluations revealed that most nuclear plants in the country faced floods and earthquakes greater than previously thought—meaning their design-basis protection levels are no longer compliant with the NRC's original siting requirements.[8]

In the case of earthquakes, the reevaluations found that 33 nuclear plant sites—about half the fleet—faced seismic hazards greater than their design bases. However, the NRC later decided that the exceedances were "significant" for only 20 sites. For these sites, the agency required that a "seismic probabilistic risk assessment," or SPRA, be performed. The assessment is a detailed calculation of the annual likelihoods that an earthquake could cause a reactor meltdown[9] and a containment failure or bypass that could rapidly lead to a large release of radioactivity.[10]

Diablo Canyon was among the plants with a reevaluated hazard significantly greater than the design basis safe shutdown earthquake and therefore had to submit a seismic probabilistic risk assessment for NRC review. But PG&E also determined that the reevaluated seismic hazard finalized in December 2015 (expressed as a "ground motion response spectrum,") also exceeds the Hosgri Earthquake in two frequency ranges (see Figure 1).[11]

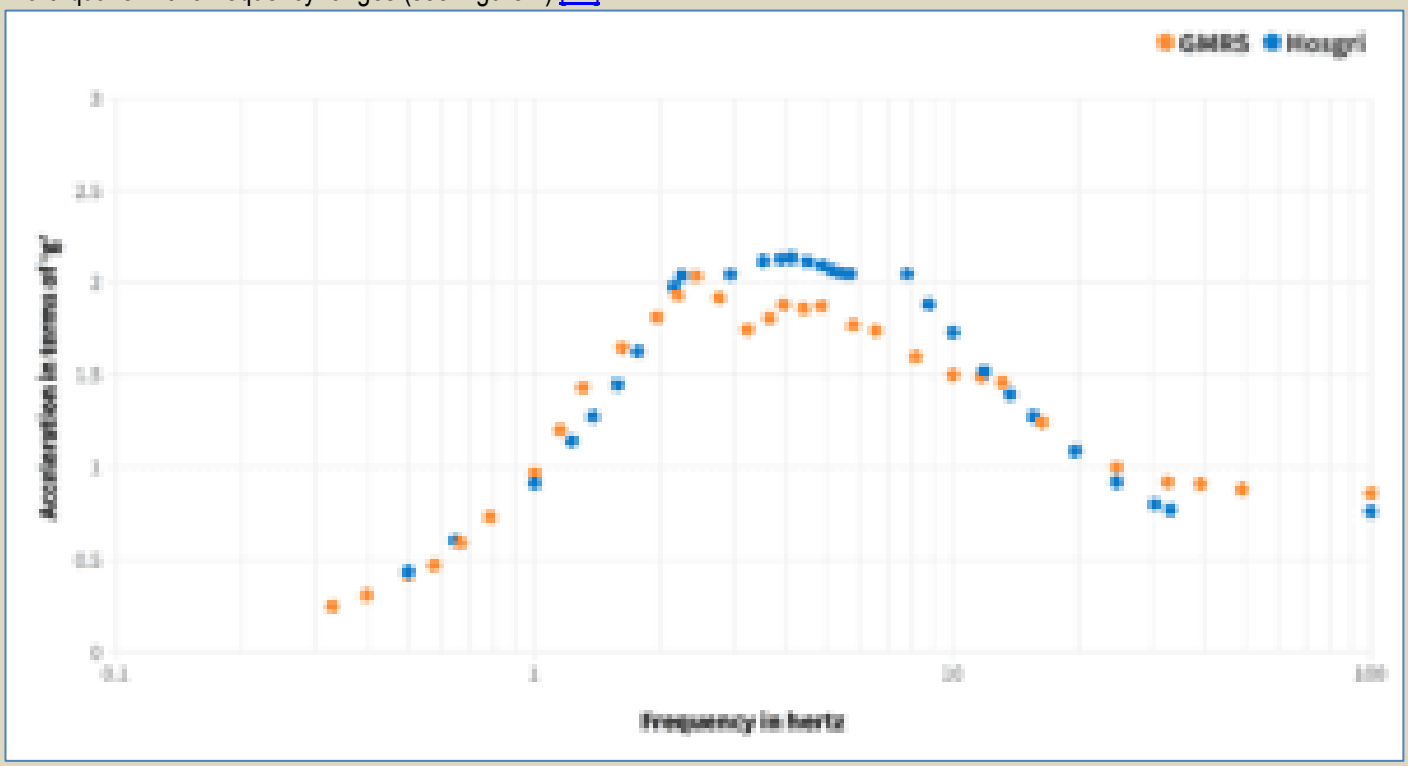


Figure 1: Comparison of Diablo Canyon post-Fukushima ground motion response spectrum with the Hosgri Earthquake spectrum (acceleration in "g's" versus frequency in hertz)

So PG&E could not argue that the earthquake defined by its post-Fukushima reevaluation was bounded by the Hosgri Evaluation and that, therefore, seismic modifications need not even be considered.

But are these new estimates significant for nuclear safety? According to PG&E, "no safety structures, systems and components required for safe shutdown are sensitive to ground motions at a frequency below 3 hertz," so Diablo Canyon's seismic vulnerability is not affected by the increased ground motion in this lower frequency range. However, at high frequencies, some components, such as electro-mechanical relays, could experience "chatter" as they are shaken, affecting critical safety equipment such as valves.[12] In this range, the 15-20 percent exceedance over the Hosgri ground motion could impact plant risk, although PG&E has asserted that "most relay chatter is acceptable …, is self-correcting, or can be recovered by operator action."

Nevertheless, PG&E's seismic probabilistic risk assessment, a rough indication of public risk, appears to show that the reevaluated hazard does increase the seismic core damage frequency.

Likelihood of earthquake-induced core damage at Diablo Canyon

The updated seismic probabilistic risk assessment PG&E conducted for Diablo Canyon was released in 2018.[13] The mean value from that assessment implies there is about a 1-in-35,000 chance per year on average that an earthquake will cause core damage in one of the units.

This seismic core damage frequency is roughly twice the value that PG&E had calculated earlier based on the original seismic hazard.[14] However, because of the complexity of these analyses, it is not clear if this increase is primarily due to the change in the seismic hazard or other modifications to the calculation.

Considering both reactors and an extended period of operation, a 1/35,000 per reactor-year risk translates into about a 1-in-800 chance on average that an earthquake would cause a core-melt accident at Diablo Canyon before it shuts down in 2045.[15] However, considering the uncertainties associated with the seismic hazard and the response of plant components, there is a five percent chance that the risk is more than 3.6 times larger.[16] This more conservative measure translates into a core damage risk of about 1-in-220 over 22 years, or about half a percent.

But the actual risk could be even higher. In its base case, PG&E assumed that following most earthquakes, plant workers would be able to carry out two manual actions from the Diablo Canyon FLEX program to prevent core damage. If no credit is given for these actions—a reasonable assumption given the challenges of a post-earthquake environment, including the aftershock potential—the seismic core damage frequency increases by nearly a factor of two, to nearly 1-in-100.

And accounting for other potential initiating events besides earthquakes—such as pipe breaks, internal fires, and floods— that could cause core damage, the estimate of the total core damage frequency rises above one percent.[17]

These estimates do not fully account for all the potential risks at Diablo Canyon. First, they assume that the two reactors are fully independent, which is not the case. In addition to having some shared safety equipment, Fukushima demonstrated that co-located reactors can influence each other, especially with respect to the operator actions needed to stabilize a damaged reactor. Thus, the likelihood that both reactors will experience core damage will be higher than the product of the likelihood of each reactor melting down independently.

Second, these estimates do not consider the potential that an accident will damage one or both of the spent fuel storage pools, which are outside of the reactor containment buildings. A severe earthquake could rupture a spent fuel pool liner and lead to a draindown of cooling water, which if not corrected could result in a zirconium fire and a large radiological release—potentially a much larger quantity of cesium-137 than in a reactor accident. A 2020 UCLA and PG&E analysis estimated that the likelihood of spent fuel becoming uncovered by cooling water following an earthquake was about 70 percent of the seismic core damage risk for each reactor.[18]

The best way to reduce the risk of a spent fuel pool fire is to transfer most of the densely packed stored spent fuel in the pools to dry storage casks. If the Diablo Canyon units are decommissioned, this will be accomplished within several years after the units are shut down. But the NRC insists that the risks of densely packed spent fuel pool storage are acceptable and has refused to require licensees to expedite spent fuel transfer to dry casks. If the reactors continue to operate, PG&E will have no regulatory mandate to procure and load the additional dry casks needed to thin out the pools, prolonging the period at which the spent fuel pools will pose undue risks.

Despite the fairly high risk of core damage that PG&E's seismic probabilistic risk assessment found, after reviewing the study the NRC took the position that the risks are acceptable and that "no modifications are warranted … because a potential cost-justified substantial safety improvement was not identified." And indeed, even if seismic core damage risk were eliminated entirely, it would reduce the total core damage risk by only about 25 percent. Still, the seismic core damage risk is significant in absolute terms, and it is likely that measures to reduce seismic risk would also be helpful in reducing the risks of other types of accidents. Given the potential consequences of a severe earthquake, we think these risks are unacceptable and that seismic upgrades would be necessary should PG&E decide to pursue license renewal of Diablo Canyon.

Consequences of a severe accident at Diablo Canyon

What is at stake if there were a seismically induced core damage accident at Diablo Canyon? PG&E's own 2015 Severe Accident Mitigation Alternatives (SAMA) analysis, which is required as part of nuclear plant license renewal applications, sheds some light on this question. In the most severe scenarios, the analysis considered—if the containment is breached early in the accident or bypassed due to a rupture of a coolant pipe outside of containment—up to 5,700 cancer fatalities within 50 miles would result, and the total economic cost (in 2015 dollars) would range from $12.2 billion to $33.4 billion ($15 billion to $41 billion in today's dollars). The consequences of spent fuel pool accidents, which are not included in such analyses, could be even more extensive and costly.

The potential radiological consequences of severe accidents are strongly dependent on the meteorological conditions. The Severe Accident Mitigation Alternatives analysis presents the mean values of the consequences obtained over a large number of different weather sequences. But more conservative values[19] are arguably more appropriate for use in risk studies. Based on studies I have performed for other nuclear plants, the peak consequences could exceed 10,000 cancer deaths and $100 billion in damages. These impacts are high enough to warrant further action to reduce the likelihood of a severe accident should taxpayers and ratepayers subsidize continued operation of Diablo Canyon.

Potential modifications to reduce seismic risk

In PG&E's initial 2009 license renewal environmental report and its 2015 revision, it evaluated a number of modifications to reduce the risk to the public from earthquakes. These included: reinforcing steam generator and reactor coolant system piping supports to prevent seismically induced steam generator failures that could cause core damage and potentially breach the containment, at a cost of $84 million per unit in 2009 dollars (about $115 million today; and installation of a seismically qualified response system that would be capable of providing all the functions needed to prevent core damage in the event of a severe earthquake, at a cost of $160 million per unit in 2015 dollars (about $200 million today).

But according to PG&E's calculations (as based on a methodology originally developed by the Nuclear Energy Institute), the risk reduction that could be achieved would not justify the cost of either of these modifications, giving the company an excuse not to carry them out.[20]

Aside from questions about methodology, some of PG&E's conclusions seem suspect in regard to logic. For example, the utility's analysis points out that "a significant portion" of the seismically qualified response system design is addressed by elements of the Diablo Canyon FLEX strategy. This raises a question: Why does the response system costs so much, if most of the elements in that system are already present at the plant? In 2015, PG&E argued that "the existence of the FLEX strategies would not reduce the PG&E implementation costs of the [Severe Accident Mitigation Alternatives] because PG&E must purchase the equipment whether it is for FLEX or for the license renewal effort."

But FLEX was bought and paid for several years ago and now represents a sunk cost. PG&E also points out that the actual cost of the seismically qualified response system could be higher because the FLEX equipment and strategies are not designed to cope with the damage from earthquakes greater than the so-called "safe shutdown earthquake." But only the incremental upgrade costs—above and beyond the existing FLEX system—should be considered in the cost-benefit analysis. In any event, it would be prudent to upgrade the protection of the FLEX portable equipment so it could survive a beyond-design-basis earthquake that damages the installed plant equipment. This is the approach that France took in its response to the Fukushima accident.

In its 2019 review of the Diablo Canyon seismic probabilistic risk assessment, the NRC also identified upgrades that could potentially reduce the radiological risk to the public from an earthquake at Diablo Canyon. One of these would entail strengthening the containments—the reinforced concrete domes over the reactors—at the power plant. PG&E's assessment determined that the four top seismic sequences causing core damage and early radiological release—representing nearly 40 percent of the risk of a large, "early" release of radiation—were due to failure of the containment's concrete shell.

Another significant danger that the seismic probabilistic risk assessment identified results from scenarios in which a pipe rupture allows radioactive material from the core to bypass the containment and leak directly to the environment. The NRC identified a modification to address this problem—routing all discharges from containment penetrations through a seismically hardened structure where effluents would be sprayed with water to scrub and condense them.

In both these cases, the NRC claimed that the cost of fixing the problem would exceed the benefit. However, the analysis underlying the agency's dismissal of seismic upgrades at Diablo Canyon is questionable.[21] In any event, if PG&E decides to reapply for a license renewal, it will have to update its Severe Accident Mitigation Alternatives analysis again. Significant changes have occurred since 2015 that could have a material impact on the results.[22] These changes would also affect the cost-benefit calculations that the NRC staff use to determine whether seismic backfits are justified, possibly leading to different results.

The cost of a seismic fix is not exorbitant

Regardless of the outcome of the dubious cost-benefit calculations, the price tag for the seismic modifications described above appears quite reasonable in absolute terms, even accounting for inflation—especially if PG&E is poised to receive hundreds of millions of dollars in federal and/or state subsidies. Although the NRC has taken a laissez-faire approach in response to the increased seismic risk documented at Diablo Canyon, the state of California does have the leverage to persuade PG&E to "voluntarily" make seismic upgrades at Diablo Canyon that could substantially reduce the risk to its population from a Fukushima-type accident. If California decides to support an extension to Diablo Canyon's lifetime, the state should:

- Convene an independent expert panel to make recommendations based on a review of the Diablo Canyon risk studies, the NRC's technical basis for rejecting all seismic upgrades, and the updated cost of such upgrades.
- Ensure that funds are allocated to expedite the transfer of spent fuel that has been out of the reactor for several years from Diablo Canyon's storage pools to dry casks. This is a critical defense-in-depth measure that would greatly improve safety over the period of extended operation.
- Fully resolve all other outstanding safety issues, including remediating the impacts of deferred maintenance identified by the Diablo Canyon Independent Safety Committee.

The Energy Department and the state of California should be concerned not only with PG&E's bottom line but also with making sure that all reasonable measures are taken to reduce the risk of Diablo Canyon's extended operation—whether or not the NRC requires them.

Notes

[1] Its peak ground acceleration of 0.86 times the acceleration of Earth's gravity (abbreviated as 0.86 g) is more than 60 percent greater than the second highest nuclear plant site, V.C. Summer in South Carolina. Although Diablo Canyon is among the 10 most seismically vulnerable plants in the US, it does not appear to be the one most at risk (based on the inherently uncertain risk calculations described above) even though it is located in the state with the most destructive earthquakes. Certain reactors in the Central and Eastern US may be more vulnerable—H.B. Robinson in South Carolina in particular—because they were designed to seismic standards that are now known to be inadequate in light of new information revealing that the seismicity in those regions was greater than originally thought.

[2] The requirements for so-called "safety-related" structures, systems, and components, including quality assurance, maintenance, and testing requirements, are intended to ensure they are highly reliable. With regard to seismic construction, the highest standards are known as Seismic Category I. The NRC details the criteria for Seismic Category I structures in its Standard Review Plan.

[3] A "design earthquake" with a peak ground acceleration of 0.2 g at 100 hertz (Hz) was chosen to represent the "maximum size earthquakes that can be expected to occur at [Diablo Canyon] during the life of the reactor," based on contemporary seismic studies. To add safety margin, this value was (somewhat arbitrarily) multiplied by 2 to arrive at a 0.4 g "double design earthquake," which was then taken as the design-basis earthquake. Subsequently, this value was equated to the SSE, and plant SSCs required to ensure plant safety following an SSE were designed to meet the highest seismic standard (then called Seismic Class 1).

[4] In doing so, the NRC took the position that the Hosgri Evaluation need not be considered to be part of Diablo Canyon's design basis, but rather part of its "current licensing basis"—which the NRC defines as the set of requirements "applicable to a specific plant and a licensee's written commitments for ensuring compliance with and operation within applicable NRC requirements and the plant-specific design basis (including all modifications and additions to such commitments over the life of the license) that are docketed and in effect."

[5] This is arguably inconsistent with the NRC's General Design Criterion 2, which stipulates that SSCs important to safety should consider "appropriate combinations of the effects of normal and accident conditions with the effects of the natural phenomena."

[6] PG&E asserted that this would be a mere administrative change because the NRC had already in effect accepted the Hosgri Earthquake as the SSE. However, documents UCS obtained under FOIA revealed that NRC staff did not agree, pointing out that PG&E had identified a "vast tally" of examples where the methodologies and acceptance limits used in the evaluation of structures and components for the Hosgri Earthquake deviate from current standards, and therefore "the proposed amendment explicitly reduce[d] the accepted inherent margins in the design for [the] SSE" and as such was "unacceptable from technical and regulatory perspectives." The situation is further complicated by the fact that Diablo Canyon was licensed before the current rules and standards for seismic design were promulgated. However, the position taken by the NRC staff in 2012, as revealed in the FOIA documents, was that if PG&E wanted to amend the license to establish the Hosgri Earthquake as the SSE it should conform to current evaluation standards and criteria.

[7] In the absence of NRC requirements, a number of nuclear plants, including Diablo Canyon, did voluntarily commit to making certain safety upgrades in response to the risks revealed in the seismic reevaluations. The modifications at Diablo Canyon were projected to have only a minimal (less than 5 percent) impact on risk. And in any event, the NRC cannot use its enforcement powers to ensure such voluntary actions are effectively implemented.

[8] In 10 CFR Part 100 Appendix A.

[9] The seismic "core damage frequency."

[10] The seismic "large early release frequency."

[11] At a frequency of 1-2 hertz and above around 25 hertz, with a peak acceleration of 0.86 g at 100 hertz compared to 0.75 g for the Hosgri Earthquake.

[12] Indeed, the loss of offsite power that both units of the North Anna plant experienced during the August 2011 earthquake was not caused by faults or gross damage to the electrical system but by spurious actuation of transformer relays caused by the high-frequency ground motion.

[13] PG&E estimated a point value of the seismic core damage frequency (SCDF) of 2.4×10^{-5} per reactor-year, and a mean value (over the uncertainty distribution) of 2.82×10^{-5} per reactor-year.

[14] The original calculation yielded a (point estimate) value of 1.45×10^{-5} per reactor-year.

[15] Estimating the cumulative risk of core damage by summing the point-estimate or mean annual core damage frequencies of different units and multiplying by a given time period

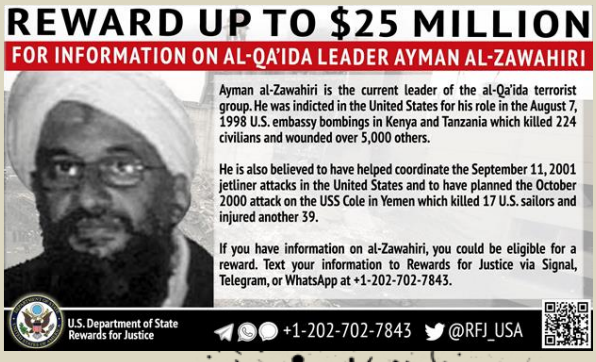
only yields a very crude approximation, yet this approach is used by the NRC (see, for example, NUREG-2201 (2016). To get a better estimate, uncertainty distributions must be fully and rigorously taken into account.
[16] That is, the 95th percentile risk is 1.02×10^{-4} per unit.
[17] The point-value contribution of other accident initiators is about 7×10^{-5} per reactor-year: nearly three times the point value of the seismic risk. Thus, the total (point value) risk of core damage at the Diablo Canyon site over 22 years from other events would be about 1-in-300, and the total (point value) site risk including seismic events would be about 1-in-250 if FLEX credit is assumed for the seismic events, and 1-in-200 if FLEX credit is not assumed. The 95th percentile value of the total core damage frequency would be more than three times larger, for a risk over one percent.
[18] That is, 1.74×10^{-5} per year for each pool.
[19] That is, based on a 95th percentile calculation.
[20] In any event the NRC does not have a requirement that licensees implement cost-justified Severe Accident Mitigation Alternatives as a condition for license renewal—a bad policy.
[21] First, the agency utilized older data from PG&E's 2009 SAMA analysis, even though updated data was available from PG&E's post-Fukushima seismic analyses and 2015 SAMA analysis. Second, it did not appear to have done any real calculations specific to Diablo Canyon, basing its conclusions on "NRC staff experience from SAMA analyses" and "engineering judgment." And finally, the NRC only summed the risk over seven years of operation: the remaining operating life of the plant under its current license, which would underestimate the total risk reduction by a factor of three in the event that the license is renewed for 20 years.
[22] First, the NRC has increased the so-called value of a statistical life that it uses for cost-benefit analyses for the first time in decades, resulting in an increase in the factor used to convert radiation exposure to monetary cost by a factor of 2.6 compared to the value that PG&E used in its 2015 analysis, and will adjust that value for inflation and real income growth. Second, the seismic core damage frequency PG&E calculated in its 2018 seismic PRA is nearly twice as high as the value used in 2015. Third, the off-site, non-farm property values used to estimate the economic damages caused by radiological contamination from a nuclear accident have increased substantially since 2015—home prices in California have risen at three times the rate of inflation. On the other side, the cost of the mitigation measures will also increase due to inflation. On balance, however, the increases in the equivalent monetary benefits of avoiding a nuclear accident are likely to make additional seismic upgrades cost beneficial.

Edwin Lyman is the Director of Nuclear Power Safety at the Union of Concerned Scientists. He earned a PhD in physics from Cornell University in 1992. He is a co-author (with David Lochbaum and Susan Q. Stranahan) of the book *Fukushima: The Story of a Nuclear Disaster* (The New Press, 2014). In 2018, he received the Leo Szilard Lectureship Award from the American Physical Society.

EDITOR'S COMMENT: Without being an expert, don't you think that the sea-wall in the article's photo is not enough to protect a nuclear power plant from a future earthquake-born tsunami? After the Fukushima disaster nobody took care of this issue worldwide but this is why the disaster started (plus installing emergency generators in the basement).

Why al-Zawahiri's death should focus attention on nuclear terrorism—foreign and domestic

By Scott Roecker and Nickolas Roth
Source: https://thebulletin.org/2022/08/why-al-zawahiris-death-should-focus-attention-on-nuclear-terrorism-foreign-and-domestic/



Aug 15 – The news that Ayman al-Zawahiri, the leader of the al-Qaeda terror group, was killed in a drone strike is not just a counterterrorism victory, but also a win for those seeking to prevent catastrophic nuclear terrorism. Al-Zawahiri's role in the September 11, 2001 attack on the World Trade Center is well known, but his role in supporting al-Qaeda's elaborate attempts to acquire a nuclear weapon is less well publicized.
The threat of nuclear terrorism is not hypothetical. Government officials over many decades have agreed that a relatively sophisticated, well-financed violent group could build a nuclear weapon if it acquired sufficient quantities of weapons-usable nuclear material. Also, there have already been successful attempts to sabotage of nuclear facilities. For example, in August 2014, an insider at the Doel-4 reactor in Belgium sabotaged one of the plant's turbines leading to the plant's shutdown for months. Al-Qaeda's nuclear program began in

1998 following Osama bin Laden's fatwa that called on Muslims to "kill the Americans and their allies—civilians and military" and his ascension as leader of the global Jihadist movement. Under the direction of al-Zawahiri—who served served as al-Qaeda's second in command when bin Laden was alive and advocated for destroying US "history, power balances, strategic and military doctrines, and global order"—al-Qaeda attempted to acquire nuclear weapons and considered targeting nuclear power plants in the United States. Bin Laden and al-Zawahiri specifically discussed nuclear weapons with two senior Pakistani scientists they tried to recruit. Public reports indicate the program went as far as conducting explosive tests in Afghanistan, consistent with the development of a nuclear weapon. Some might assume that al-Zawahiri's death and the decline of al-Qaeda over the past two decades means that nuclear terrorism threats are no longer a concern. Or people may think that the apocalyptic ideology and rhetoric that provided the justification for al-Qaeda's nuclear ambitions are unique to Islamic jihadism. Those would be wrong conclusions. This type of extreme, apocalyptic thinking exists among domestic terrorists in the United States today and needs more attention. There is a growing threat of politically motivated violent extremists in the United States, and some of those domestic extremists have ambitions similar to al-Qaeda's. These extremists, often known as accelerationists, view societal collapse as inevitable and seek to ignite a "total revolution" that would level the existing system of governance.

Brandon Russell, a former Florida National Guard member and co-founder of the accelerationist group Atomwaffen Division (which translates from German to "the nuclear weapons division"), was arrested in 2017 while heavily armed en route to the Turkey Point nuclear power plant. Several years before Ashli Babbitt was killed while storming the U.S. Capitol as part of a right-wing uprising on January 6, 2021, she was an employee of the Calvert Cliffs nuclear plant, where she exhibited violent behavior. Matthew Gebert, then a State Department employee, secretly headed a chapter of the white supremacist group The Right Stuff. In May 2018, while working for the State Department, Gebert said on a white nationalist podcast that "[w]e need a country founded for white people with a nuclear deterrent. And you watch how the world trembles." Although they were not backed by al-Qaeda's combination of apocalyptic ideology, resources, and technical sophistication and appeared unlikely to succeed, these people and incidents linked to them likely do not provide a complete picture of the threat. Like al-Zawahiri's nuclear ambitions, those demonstrated by domestic US terrorists underscore why policymakers should support programs and policies designed to protect nuclear facilities from theft and sabotage. In particular, the US government should redouble efforts to eliminate vulnerable nuclear weapons-useable material in any country or facility, at home and abroad, and increase funding for US programs that strengthen security at nuclear facilities worldwide.

Insider threats need to be reevaluated, as well. Although US nuclear facilities have elaborate programs to screen candidates and to monitor employees who could potentially pose a threat, there is reason to question whether those programs are sufficient to the threat. The January 6th attack on the Capitol revealed critical vulnerabilities in the US government's security systems. In response, the Biden administration released the first ever National Strategy for Countering Domestic Terrorism in June 2021. Since then, many departments within the US government, and in particular the Defense Department, have taken important steps to enhance monitoring of extremist activities amongst employees. Despite the clear need for action,, both commercial nuclear plants and government-run nuclear facilities responsible for weapons research, production, and deployment in the United States have not revealed what, if any, steps they have taken in recent years to enhance their protection against insider threats. Neither regulators nor political leaders have called for or required greater security. Ayman al-Zawahiri is dead, but the violence he perpetrated, the apocalyptic ideology he promoted, and the nuclear threat he posed lives on in a new generation of terrorists—here and abroad. As long as nuclear weapons and materials exist, governments must vigilantly defend against this threat and policymakers, like those in Congress, must provide the oversight and resources needed to adequately protect US nuclear facilities.

Scott Roecker is the vice president of Nuclear Materials Security at the Nuclear Threat Initiative (NTI). Before joining NTI, Roecker worked in the US government for more than 15 years at the National Security Council and National Nuclear Security Administration. **Nickolas Roth** serves as a senior director of Nuclear Materials Security at the Nuclear Threat Initiative. Previously, he was director of the Stimson Center's Nuclear Security Program and a senior research associate at the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs. His work has focused on nuclear security, US nuclear weapons policy, and arms control.

U.S.-Russia Nuclear War Could Leave 5 Billion Dead Due to Famine

Source: https://www.usnews.com/news/health-news/articles/2022-08-15/u-s-russia-nuclear-war-could-leave-5-billion-dead-due-to-famine

Aug 15 - Even a "small" nuclear war, far short of a global conflict, could kill much of the world's population due to starvation, a new study projects.

Any nuclear war would have obviously devastating effects in the places where it was waged — obliterating cities, instantly killing huge numbers of people, and contaminating local soil and water.

But the destruction would be expected to stretch far beyond those borders: It's believed the massive fires ignited by bomb blasts would launch soot high into the atmosphere, blocking sunlight and causing temperatures to plunge — a concept called nuclear winter. It would be akin to instant climate change, said Alan Robock, one of the researchers on the new study.

The effects on crops, fish and livestock worldwide could be catastrophic, but the extent would depend on how much soot is injected into the atmosphere.

So for the new study, Robock's team used computer simulations of six nuclear war scenarios. They estimated the impact of each on crops, wild fish and other food sources — and ultimately, the number of human lives lost to famine.

"The direct impact of nuclear war is devastating," said Robock, a professor of environmental sciences at Rutgers University in New Brunswick, N.J. "Our work is looking at what would happen to the rest of the world."

The researchers calculate that even a one-week regional war — between India and Pakistan, as an example — could kill more than 2 billion people worldwide. And while the bombs could instantly kill millions, the bulk of those deaths would actually happen in the following two years, due to starvation.

The greatest toll, though, would come from a wide-scale nuclear war between Russia and the United States and its allies. That, the study projects, could kill upwards of 5 billion people — again, largely from famine.

"No one has done this calculation before," Robock said. "No one has tried to calculate the numbers of people who would die."

As it stands, nine countries have nuclear arsenals: the United States, Russia, the United Kingdom, France, China, India, Pakistan, Israel and North Korea.

Back in the 1980s, Robock noted, the threat of nuclear war between the United States and the former Soviet Union was in the public consciousness, and there were widespread calls for disarmament.

But these days, he said, "most people think nuclear war will never happen. They have more-immediate concerns, like the price of gasoline."

"We want to make people aware of the danger," Robock said.

He is not alone. Earlier this month, U.N. Secretary-General Antonio Guterres warned that with geopolitical tensions rising — and nuclear arsenals growing and being modernized — humanity is "one misunderstanding, one miscalculation away from nuclear annihilation."

The new findings underscore the point that tensions between two nuclear-armed countries — even on the other side of planet — concern all of us, said Deepak Ray, a senior scientist at the University of Minnesota Institute on the Environment in St. Paul.

"Even a limited war would have widespread repercussions," said Ray, who wrote a commentary published with the study Aug. 15 in the journal *Nature Food*.

He noted that of all nuclear-armed countries, only two have made a "no first use" pledge: China and India. Ray said the world would be safer if all nuclear powers did so — though the existence of nuclear stockpiles would still pose a threat.

The study's projections are based in part on the reported number of weapons in each nuclear-armed nation's stockpile.
The researchers estimate that any atmospheric "soot injections" above 5 million metric tons would cause "mass food shortages" — even with mitigation measures, like reduced food waste and farmers switching to different crops.
A war between India and Pakistan alone could put anywhere from 255 million to over 2 billion people in danger of death from famine by end of the second post-conflict year — depending on the number of weapons used.
A U.S./Russia war would be more devastating. Assuming attacks in the United States, Russia, the United Kingdom, France, Germany, Japan and China, more than 5 billion people worldwide could die from starvation.
While the thought of such devastation might be overwhelming, Robock hopes the study serves as a call to action.
"You can write to your congressional representative and tell them you don't want another trillion dollars spent on nuclear weapons," he said. "You can tell them to spend it on health care, or food security. We don't need any more nuclear weapons."

Soot (Tg)	Number of weapons	Yield (kt)	Number of direct fatalities	Number of people without food at the end of Year 2
5	100	15	**27,000,000**	255,000,000
16	250	15	**52,000,000**	926,000,000
27	250	50	**97,000,000**	1,426,000,000
37	250	100	**127,000,000**	2,081,000,000
47	500	100	**164,000,000**	2,512,000,000
150	4,400	100	**360,000,000**	5,341,000,000
150	4,400	100	**360,000,000**	[a]5,081,000,000

The 5 Tg case scenario is from ref. [16] for an India–Pakistan war taking place in 2008; the 16–47 Tg cases are from ref. [18] for an India–Pakistan war taking place in 2025; and the 150 Tg case is from ref. [51], which assumes attacks on France, Germany, Japan, United Kingdom, United States, Russia and China. The last column is the number of people who would starve by the end of Year 2 when the rest of the population is provided with the minimum amount of food needed to survive, assumed to be a calorie intake of 1,911 kcal per capita per day, and allowing for no international trade; from Supplemental Information, Supplementary Table 5, the Partial Livestock case, in which 50% of livestock grain feed is used for human consumption, and 50% of livestock grain feed is used to raise livestock, using the latest complete data available for the year 2010. For 2010, the total population of the nations used in this study was 6,700,000,000. There are many other scenarios in which these amounts of soot could be produced by a nuclear war, and the scenarios we use are only meant to be illustrative examples. The last column is the case with the fewest number of deaths without international trade, and other cases are available in the Supplementary Information.
[a]Assuming total household waste is added to food consumption.

Are Attacks on Nuclear Plants Legal under International Law?

By Christoph Hasselbach (editor at *DW*)
Source: https://www.homelandsecuritynewswire.com/dr20220819-are-attacks-on-nuclear-plants-legal-under-international-law

Aug 19 – Since March, the Zaporizhzhia nuclear power plant in southern Ukraine has been under Russian occupation. Since late July, the largest nuclear plant in Europe has been shelled repeatedly, with Kyiv and Moscow blaming each other for the attacks. This has sparked fears of a nuclear disaster. Last week, the UN Security Council held an emergency meeting on the situation without getting any closer to a solution.
It is not the first time in this war that the question of nuclear safety and security has been raised. This is not only about the potential use of nuclear weapons — Russian President Vladimir Putin has openly expressed this thought — but also about nuclear power stations being used as military targets.

Geneva Conventions Regulate Conduct of War
What does international law say about this? The 1949 Geneva Convention and its subsequent Additional Protocols regulate the conduct of armed conflict and seek to limit its effects. Article 56 of the Additional Protocol (1) of 1977 pertains to the "Protection of works and installations containing dangerous forces" and explicitly mentions "dams, dykes and nuclear electrical generating stations."
Since the Russian Federation and Ukraine are both parties to the agreement and have not expressed reservations about the Additional Protocol (1), the regulations apply to both states.

And they are surprisingly detailed. In principle, according to paragraph 1, nuclear power plants "shall not be made the object of attack, even when these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population." Radioactivity is certainly what is meant here.
The issue here is one of the principles of international humanitarian law as consolidated by the Geneva Conventions: The difference between military and civilian targets. These provide for the "general protection of civilian objects, restricting attacks to military objectives."

Nuclear Power Stations Are Not Off-Limits

But paragraph 1 of the Additional Protocol (1) does not state that nuclear power plants are always off-limits, only to the extent that an attack "may cause the release of dangerous forces from the works or installations and consequent severe losses among the civilian population." In other words, if it is not expected to cause "severe losses among the civilian population," then it might be permitted under certain circumstances.

Russia publishes a map with results if Ukraine's Zaporizhzhya nuclear power plant explodes

Paragraph 2 suggests that a nuclear power plant could become an objective "if it provides electric power in regular, significant and direct support of military operations and if such attack is the only feasible way to terminate such support […]"
However, this is of course a matter of interpretation. In times of war, almost all nuclear power plants will provide electricity to civilians as well as to the military. It is hard to separate the two. But does this entail a "significant and direct support of military operations?" Thus, it is up to the discretion of the observer to evaluate whether a nuclear power plant is a legitimate military target or not.
It is also difficult to prove that an attack is "the only feasible way to terminate" support for acts of war. A potential aggressor has to deliberate and observe the principle of

proportionality: Does the military value clearly prevail? What impact would my actions have on the civilian population? And would there not be a less grave means of rendering a nuclear power plant inoperable? Such as destroying power lines so that electricity can no longer be supplied — without entailing the risk of causing radiation? That said, for a population in winter, a power supply disruption can also be grave.

Civilian Population Must Be Protected

But even if circumstances do justify an attack, the Additional Protocol states in paragraph 3 that in all cases "the civilian population […] shall remain entitled to all the protection accorded them by international law." A warring party would have to do everything possible to protect civilians from radiation, for example, by evacuating the surrounding areas before launching an attack on a plant.

Paragraph 5 is also relevant to Zaporizhzhya: "The Parties to the conflict shall endeavor to avoid locating any military objectives in the vicinity of the works or installations mentioned in paragraph 1." Ukraine accuses Russia of hunkering down at the power plant, effectively using it as a shield to avoid Ukrainian shelling. While Vladimir Rogov, a Russian-backed local official, claimed that Ukraine had launched artillery strikes using US-made howitzers near the power plant and in residential areas.

Qualifying the restrictions, however, the Additional Protocol also states: "Nevertheless, installations erected for the sole purpose of defending the protected works or installations from attack are permissible and shall not themselves be made the object of attack." Russia will surely depict its military as only acting defensively.

In conclusion: The states that have signed the Geneva Conventions and its Additional Protocols — and that includes Russia and Ukraine — have set a high bar for attacks on nuclear power plants. But they are not ruled out entirely, even if the circumstances, in which they are permitted, are very narrowly defined.

But in practice Article 56 of the Additional Protocol (1) is limited. It remains a matter of interpretation as to whether circumstances allow for a concrete case. Moreover, as a permanent member of the United Nations Security Council, Russia has a veto and can prevent any attempts by the body to sanction it for violating international law.

EDITOR'S COMMENT: Why do people continue to believe that war complies with international law?

Scientists simulate spread of radiation in case of accident at Zaporizhzhia Nuclear Power Plant

Source [+video]: https://www.pravda.com.ua/eng/news/2022/08/18/7363806/

Aug 18 – Based on the weather conditions observed on 15-18 August, in the case of an accident at the Zaporizhzhia Nuclear Power Plant (ZNPP), radioactive contamination would principally affect Ukraine, but it would also affect neighbouring countries. Such an accident would threaten not only Kyiv, but also the occupied territories of Donbas.

Details: Scientists of the Ukrainian Hydrometeorological Institute of the State Emergency Service of Ukraine and the National Academy of Sciences of Ukraine performed a simulation of the spread of radiation from a hypothetical accident at the Zaporizhzhia NPP under the meteorological conditions of 15-18 August 2022.

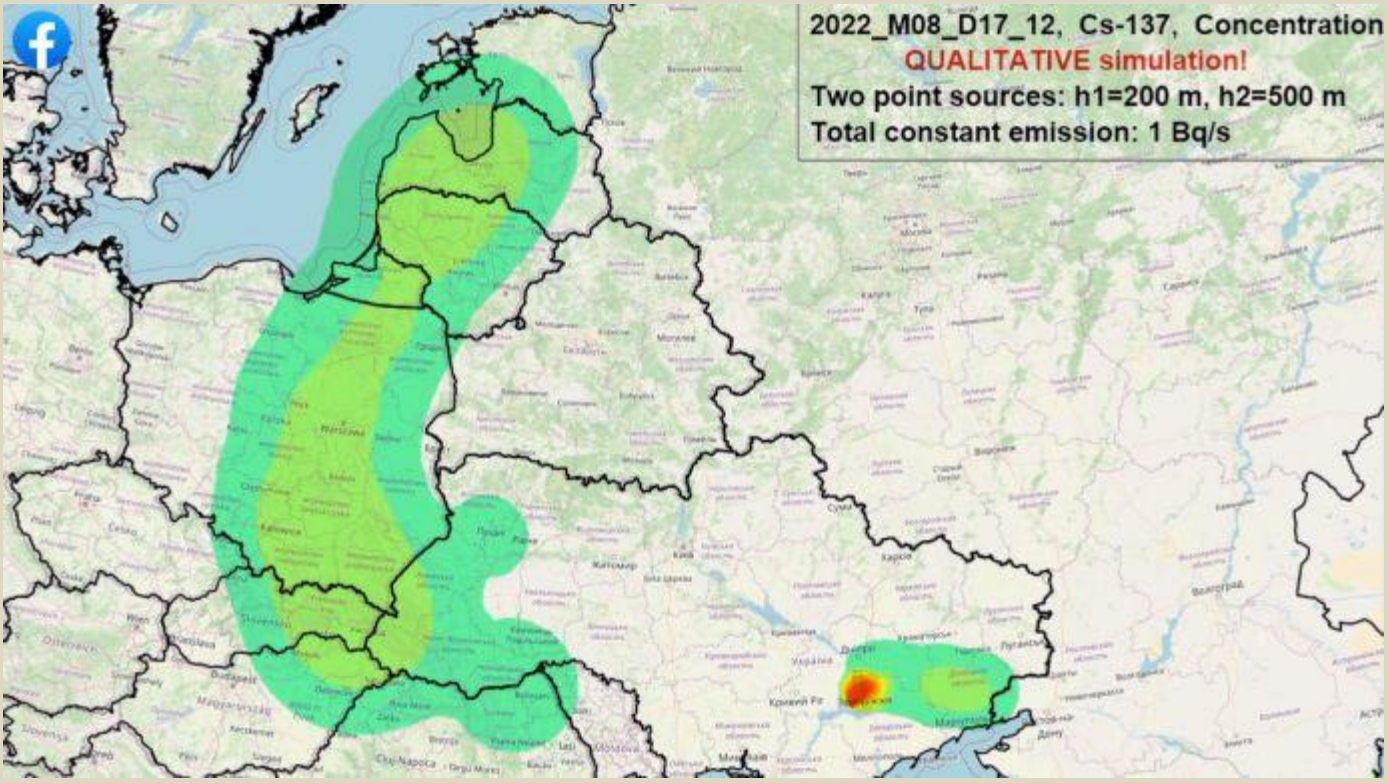
The results of modelling the atmospheric transfer and dispersion of radioactive Cs-137 aerosols were obtained using the Weather Research Forecasting (WRF) ARW version 4.3 forecasting meteorological model and the CALMET-CALPUFF version 6 atmospheric dispersion modelling complex.

The WRF forecast of meteorological conditions was calculated on the basis of GFS (global forecast data) with a spatial resolution of 0.5° and a time resolution of 3 hours. Radioactive emissions are given in the form of two-point sources at heights of 200m and 500m above the earth's surface, with a total stationary power of 1 becquerels/second (0.5 Bq/s for each sources). The following characteristics of the size distribution for radioactive aerosols were used: average diameter 1 μm, standard deviation 2 μm.

Given the impossibility of determining the exact characteristics of the source of emissions in the event of a hypothetical accident at the ZNPP, the results of numerical modelling should be interpreted only qualitatively and in relative terms.

Quote:

"According to the results of the calculations, during 15-18 August 2022, the highest concentrations of radioactive aerosols can be observed within the territory of Ukraine, especially in the zone closest to the emission source,
with a radius of 50-100 km in almost all directions from the ZNPP.
Significant concentrations of radionuclides could reach the city of Kyiv.
Partially radioactive impurities might also spread to the neighbouring states (the eastern part of Belarus, Poland, the Baltic States).



At the end of the simulated period, the main direction of radionuclide transport was eastward, as a result of which significant concentrations of radioactive aerosols could be observed over the occupied parts of Donetsk and Luhansk regions."

Deteriorating situation at Ukraine's largest nuclear power plant

By Dawn Stover

Source: https://thebulletin.org/2022/08/deteriorating-situation-at-ukraines-largest-nuclear-power-plant/

Aug 19 – Russian forces have occupied the Zaporizhzhia Nuclear Power Station in southern Ukraine for more than five months, placing the power plant's six nuclear reactors and its stores of radioactive spent fuel at unprecedented risk. The situation at the plant continues to worsen.

Russia and Ukraine, which blamed each other for earlier attacks on the plant, are this week trading fresh accusations and warning that another attack on the plant is coming soon.

Ukrainian military intelligence told NBC News that Russia had ordered most of the Zaporizhzhia plant's staff to stay home from work today. On its verified Facebook page, the Ukrainian intelligence directorate of the defense ministry claimed there is a "high likelihood" of a large-scale terrorist attack on the facility.

The Russian Ministry of Defense earlier accused the Ukrainian military of preparing to launch a terrorist attack on the Zaporizhzhia plant. The ministry acknowledged it is considering a shutdown of the plant in response to "negative developments."

Energoatom, Ukraine's state-owned nuclear utility, warned that shutting down the plant would make a radiation disaster scenario more likely. It would also cut off a significant source of electricity for Ukraine's grid.

At a US State Department briefing yesterday, department spokesman Ned Price said statements from Russian officials are "cause for concern because they fit squarely within the Russian playbook: accuse others of what it is you have done or what it is you intend to do." He said Russia "has engaged in a number of false flag operations" and that the United States would be watching the situation at the Zaporizhzhia power plant "very closely."

International intervention

In the Western Ukraine city of Lviv yesterday, Ukrainian President Volodymyr Zelensky met with UN Secretary General António Guterres and Turkish President Recep Tayyip Erdogan. It was the first meeting between Zelensky and Guterres since the Russian invasion of Ukraine began in late February.

On his official Telegram account, Zelensky wrote that he and Guterres paid "particular attention" at their summit to Russia's "nuclear blackmail" at the Zaporizhzhia plant. Zelensky called on the United Nations to "ensure the security" of Zaporizhzhia, which is the largest nuclear power plant in Europe. Guterres said he is "gravely concerned" about potentially "suicidal" damage to the plant. However, it is unclear what the United Nations can do to help.
In response to a Russian accusation that the UN Secretariat has canceled or blocked a visit by the International Atomic Energy Agency (IAEA) to the plant, the Secretariat clarified that it has no authority to block any IAEA activities. (The IAEA, which has made repeated and increasingly urgent requests for a visit, reports to the United Nations, but it is an autonomous organization.)
The Secretariat said it would support any IAEA mission to Zaporizhzhia and has "in Ukraine" the logistics and security capacity to do so. Russia has said it will allow an IAEA visit to the plant, but the Russians want the mission to travel to the plant through Russian-occupied territory and have claimed it would be too dangerous for an international mission to approach from Kyiv. A Russian-controlled route is unacceptable to Ukrainian officials, who worry that it could be seen as a tacit acknowledgement by the IAEA that Russia now "owns" the plant.

The specter of Chernobyl (and Fukushima)
After the summit in Lviv, Erdogan warned about the potential for "another Chernobyl." An anonymous worker at the Zaporizhzhia plant used similar language on Tuesday, telling ABC News: "If something happens to the spent fuel storage, the consequences could be the same as Chernobyl." Mistakes made by plant operators during a test caused a reactor at the Chernobyl nuclear power plant to go out of control in 1986, resulting in an explosion and fire that released large amounts of radiation into the atmosphere. While the reactors at the Zaporizhzhia plant are a different type than the flawed design used at Chernobyl, the chances for operator error are rising as the occupation drags on. Ukrainian employees of the state-owned nuclear utility Energoatom continue to run the plant, but they are working in an extremely stressful environment, and are constantly under Russian observation and suspicion.
Operator error is only one of the risks facing the nuclear plant. Another possibility is more akin to the Fukushima nuclear reactor meltdowns than to Chernobyl: If the Zaporizhzhia plant were to face an extended loss of electrical power because of an accidental or intentional attack, the plant operators might not be able to continue pumping cool water into the reactor cores and spent-fuel storage pools to prevent radioactive fuel from overheating.

A militarized zone
An agreement between Ukraine and Russia on grain exports, mediated by Erdogan, raised hopes that a similar agreement could be negotiated to halt military activities in and around the Zaporizhzhia site. Guterres called for establishment of a demilitarized zone around the plant, but Russia rejected the idea, saying the Russians need to "protect" the plant from provocations and terrorist attacks. Zaporizhzhia is not the only nuclear power plant caught in the crossfire between Russia and Ukraine. Earlier this week, Russia accused "Ukrainian saboteurs" of blowing up six towers supporting high-voltage power lines that transmit electricity from the Kursk Nuclear Power Plant in western Russia, near the border with Ukraine. Fierce fighting continues in the vicinity of the Zaporizhzhia plant. In an address on Saturday, Zelensky said Ukraine would target Russian soldiers shooting at, or from, the plant. The plant is located on the south side of the Dnipro River, and Russia has been firing artillery shells and rockets at Ukrainian-controlled towns on the river's north side. On Thursday, CNN reported, the Russian defense ministry issued a statement insisting that "weapons, especially heavy ones, are not placed on the territory of this [nuclear] station" and said it was ready to present high-resolution satellite images to the IAEA as proof.

Dawn Stover is a contributing editor at the Bulletin. A science writer based in the Pacific Northwest, her work has appeared in *Scientific American*, *Conservation*, *Popular Science*, *New Scientist*, *The New York Times*, and other publications. One of her articles is included in the *2010 Best American Science and Nature Writing*, and another article was awarded a special citation by the Knight-Risser Prize for Western Environmental Journalism.

Experts weigh in on the risk of disaster at a Ukrainian nuclear power plant

By François Diaz-Maurin
Source: https://thebulletin.org/2022/08/experts-weigh-in-on-the-risk-of-disaster-at-a-ukrainian-nuclear-power-plant/

Aug 19 – Since Russian forces shelled and seized the Zaporizhzhia Nuclear Power Plant in early March, the plant has become a focal point of nuclear concern. Shelling and explosions have continued, with Ukraine and Russia blaming each other. Russian forces are using the plant as a military base to conduct night shelling of the Ukraine-controlled city of Nikopol,

located just across the Dnieper River. In a video address last week, Ukrainian President Volodymyr Zelensky promised to target "every Russian soldier who either shoots at the plant, or shoots using the plant as cover."

Generating units at the Zaporizhzhia Nuclear Power Plant are illuminated at night in southeastern Ukraine on July 9, 2019. There is growing concern that the ongoing war in Ukraine could lead to serious damage at Europe's largest nuclear power plant. Ukraine and Russia accuse each other of the shelling of the nuclear power station, a sprawling facility on Russian-occupied ground that continues to function as the war rages around it. File photo by Dmytro Smolyenko/Ukrinform/Abaca/Sipa USA (Sipa via AP Images)

The worsening situation at the Zaporizhzhia plant, one of the 10 biggest nuclear plants in the world and Europe's largest, prompted heightened alarm last week on both the United Nations and the International Atomic Energy Agency (IAEA), the UN's nuclear watchdog. Addressing the UN security council on August 11, IAEA Director General Rafael Mariano Grossi called again for the IAEA to conduct a mission to assess the safety of the plant. "This is a serious hour, a grave hour," Grossi told the security council from his Vienna office.

Following Grossi's warning, UN Secretary-General Antonio Guterres called for the establishment of a demilitarized zone at the Zaporizhzhia plant. Guterres was soon joined in his call by 42 countries—including the United States, Japan, the United Kingdom, Turkey, as well as the European Union—urging Russia to immediately withdraw its military forces from the plant and its immediate surroundings. On Monday, Ukrainian President Zelensky also called for the immediate withdrawal of Russian troops from the territory of the Zaporizhzhia NPP "without any conditions." It did not take long, however, for Russia to reject these calls. A Russian diplomat even struck a warning note, saying it would be too dangerous for an IAEA mission to inspect the Zaporizhzhia plant by passing through the capital city of Kyiv.

Despite fears of a new nuclear disaster at the Zaporizhzhia plant, there has been no indication of elevated radiation levels at the plant. According to the Ukrainian state nuclear company Energoatom, however, the early-August missile attack that hit the plant's dry spent fuel storage area damaged three radiation monitoring sensors, impairing the ability to detect any increase in radiation levels in the area. Only an IAEA inspection would be able to confirm the damage.

On August 12, a US senior military official held a background briefing saying: "In Zaporizhzhia, no particular updates on the nuclear power plant. It is under Russian control

and I'd just point you to the IAEA's comments [that] there's no immediate threat to nuclear safety." The senior military official added,"[B]ut that could change at any moment." On the same day, IAEA Director General told the Associated Press the situation at the Russian-controlled Zaporizhzhia plant "has been deteriorating very rapidly." Grossi qualified the military activity at the plant as "very alarming."

Map of southern Ukraine identifying the Zaporizhzhia nuclear power plant, Russian-occupied areas and key cities. Inset shows location of Ukraine's four operating nuclear plants (yellow) and the Chernobyl plant (red), fully decommissioned in 2000. (Source: Institute for the Study of War and AEI's Critical Threats Project. Map: Thomas Gaulkin / OpenStreetMap)

The state of alarm certainly is fueled by the confusion surrounding the plant's safety, the extent of the Russian military equipment inside, and ultimately Russia's goal in attacking the plant.

Many observers seemed in the dark as to what Russia's endgame is with the plant. Ukrainian presidential advisor Mykhailo Podolyak told the *Kyiv Independent* that "Russian troops are shelling the Zaporizhzhia Nuclear Power Plant to cut Ukraine's south from electricity and blame it on the Ukrainian Armed Forces." "The goal is to disconnect us from the (plant) and blame the Ukrainian army for this," Podolyak added on Twitter. The BBC earlier reported Ukraine's defense ministry as saying that a high-voltage power line had been damaged following the early-August shelling.

According to the *Wall Street Journal*, Ukrainian leaders, international nuclear power experts, and the plant's workers all confirmed that there seemed to be a deliberate attempt by Russia to isolate the Zaporizhzhia plant from Ukraine's remaining territory by cutting its power lines. To add to the confusion, the *Kyiv Independent* reported intelligence information from Ukraine's defense ministry that Russian troops are preparing a false-flag operation, disguising Russian self-propelled artillery as Ukrainian. It is not clear at this point what such an operation would target besides the power lines.

Talking to the *Bulletin*, Olexi Pasyuk, a nuclear power expert and deputy-director of Ecoaction, a Ukrainian nongovernmental organization, went out on more of a limb in his opinion: "I think the Russians have a very clear understanding of what they do at the ZNPP. For now, they are interested to keep it running to provide electricity for occupied territories. The question is what they will do when they withdraw."

This is where the situation could really get dangerous. The lack of power supply can lead to a loss of cooling and a meltdown.

Rod Ewing, a professor of nuclear security at Stanford University, sees four vulnerabilities that need to be considered at the Zaporizhzhia plant. He told the *Bulletin*: "the reactor themselves, spent fuel [storage] pools, the supporting equipment such as backup generators, and the operating personnel."

Zaporizhzhia's six VVER reactors each have a containment structure consisting of an approximately one-meter-thick reinforced concrete wall. (VVER reactors are pressurized, light-water-cooled and -moderated reactors similar to Western pressurized water reactors.) "Modern weapons, such as bunker busters, can be expected to penetrate containment and cause an exposure of the core," says Ewing. But for Pasyuk, there is no need to penetrate the containment building to damage the reactors—not even destroy the cooling system. Rather, Pasyuk says, one most probable scenario potentially leading to a disaster at the Zaporizhzhia plant would be a "loss of external power combined with human error."

Another nuclear power expert, M.V. Ramana of the University of British Columbia, confirms this assessment in a statement to the *Bulletin*: "There is, of course, natural concern about a missile or rocket damaging one of the nuclear facilities at the Zaporizhzhia plant. There is also the concern that the electricity supplied to the plant is interrupted and the plant loses all backup means to generate electricity, which could mean a meltdown even without any direct attack on the plant. A final concern is that the operators at the plant, professional though they might be, must be exhausted and stressed out, and thus capable of errors. Such errors can be disastrous, as we have seen at Three Mile Island and Chernobyl—accidents that started without any external trigger. The last two possibilities can occur at any nuclear power plant anywhere in the world, even in the absence of war and military attacks."

Notwithstanding the shelling, Ukrainian operators have continued working at the plant—often at gunpoint and under constant fear—"to make sure there is no Chernobyl-style disaster," one of them told *Reuters*. Referring to the accrued risk of human error, Pasyuk said, "the plant's staff has been working under stress for over five months, while [we know] human error is an important factor in nuclear accidents."

Ewing echoed this view. "One cannot expect that the operating personnel, held as prisoners, will be able to meet the expected standard for the safe operation of the reactors," Ewing said.

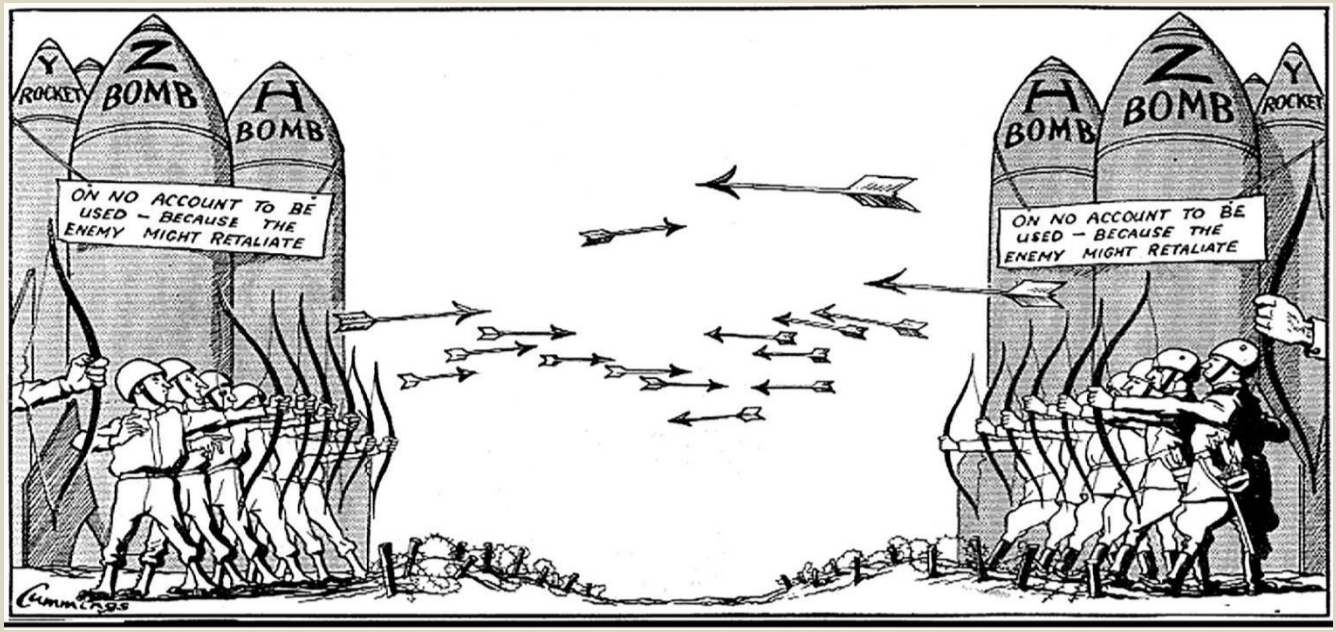
For his part, physicist Robert Rosner noted that an additional complicating factor is the presence of the fog of war, saying: "[M]y read is that neither side wants to disclose what's actually going on: the West, because it's helpful to blame the Russians for destructive actions at a nuclear site, the Russians because they are good at blaming the Ukrainians via their repeated 'false flag' actions."

Rosner also noted that in his opinion, the real concerns come in two flavors: the stress of the nuclear power plant's operating staff working under such conditions, and a simple military mistake. "The Russians have brought in quite a few poorly trained combat forces, and these have already demonstrated poor judgment, both in the early days of attacking the Zaporizhzhia power complex and their behavior at Chernobyl. In both cases, I think what happened was the result of poor command control, and in the context of an environment where a lot of highly radioactive material is stored in a relatively poorly protected manner, e.g., in the storage pools. That is very worrying—a mistake there could lead to a major radioactive material release. And that possibility is unfortunately the most likely, and most damaging, outcome of poor Russian command control."

The international community continues to insist on the importance of the IAEA being able to conduct its mission at the Zaporizhzhia plant. But not all nuclear power experts agree that it is the most effective way to prevent a disaster. "There is no need to visit the site to understand that the risk is high and that Russia already breaks IAEA resolutions and even the protocol of the Geneva Conventions that forbids these actions," says Pasyuk. "This is time for the IAEA and the UN to amend the Laws of War and make it a war crime to attack civilian nuclear facilities, similar to the restrictions to attacking hospitals," suggests Ewing. But how to get a UN or IAEA resolution if Russia is a member state?

As a sign of the helplessness of the international community about the fate of the Zaporizhzhia nuclear plant, the director-general of the World Health Organization, Tedros Adhanom Ghebreyesus, said at a press briefing on Wednesday that the world may be "sleepwalking into a major disaster … even a nuclear war."

François Diaz-Maurin is the associate editor for nuclear affairs at the Bulletin of the Atomic Scientists. Previously, Diaz-Maurin was a MacArthur Foundation Nuclear Security Visiting Scholar at the Center for International Security and Cooperation (CISAC), Stanford University, and a European Commission's Marie Sklodowska-Curie Fellow. He has been a scientific advisor to members of the European Parliament on nuclear issues, and he is a founding member of the Emerging Leaders in Environmental and Energy Policy network (ELEEP) of the Atlantic Council, Washington D.C. and the Ecologic Institute, Berlin. Prior to joining academia, Diaz-Maurin spent four years as a research engineer in the nuclear industry in Paris, France and Boston, MA. There, he worked on the safety design of new reactors and of a treatment plant to vitrify Hanford's tank waste from WWII and Cold War nuclear weapons production. Diaz-Maurin received multi-disciplinary training in civil engineering (B.Sc./M.Sc., University of Rennes 1, 2004/2007, both with distinction), environmental and sustainability sciences (Ph.D., Universitat Autònoma de Barcelona, 2013, summa cum laude and "Extraordinary Ph.D." Award), and nuclear materials, geochemistry of radionuclides and nuclear security (postdoctoral training, Stanford University, 2017–2019).



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

The street cleaners of Mogadishu: Doing Somalia's riskiest job

By Hamza Mohamed

Source: https://www.aljazeera.com/news/2022/7/21/street-cleaners-the-women-doing-mogadishus-riskiest-job

At night or early morning, female street cleaners say they do not like to wear high visibility jackets as that can attract robbers [Hamza Mohamed/Al Jazeera]

July 21 – It is an hour before sunrise in downtown Mogadishu. The Somali capital is fast asleep with eerie silence hanging in the warm salty air blowing from the Indian Ocean.

Apart from a small group of women wearing dark-coloured clothes and flip-flops on Maka al-Mukarama road in the heart of the city, there is no other soul in sight. With few street lights working, the women blend almost perfectly into the pre-dawn darkness.

Each is carrying a plastic broom, a shovel and sack, and works about 300m (984 feet) away from the other. They barely make any sound as they get to work.

"It is best not to be seen for your own safety," one of them, 50-year-old Maryan Salad Mohamed, told Al Jazeera. "We do our best not to be seen and even better if no one hears us. There are many dangers when you do our job."

Maryan and the others are street cleaners working for the city's local authority – one of the most dangerous jobs in the Somali capital.

"Before I leave the house I pray. You don't know if you will come back alive," the mother-of-seven, told Al Jazeera in a low, soft voice.

There is no official count for the number of street cleaners who have lost their lives in the line of duty. But for years, the city has lost dozens of street cleaners due to Improvised Explosive Devices (IEDs) hidden in rubbish left on the side of the streets.

In August 2008, at least 21 female street cleaners were killed on the same stretch of the street following an explosion that also left 46 others, mostly women street cleaners, wounded. In August 2014, an explosion left four female street cleaners dead and seven others injured in that same district of Mogadishu.

And in a gruesome attack in February 2019, unknown gunmen shot dead nine street cleaners, including six women at a location some 15km (9 miles) from the city centre.

Authorities blamed the al-Qaeda-linked armed group al-Shabab for the deadly blasts.

The group, which wants to impose a strict interpretation of Sharia law in Somalia, is fighting the country's Western-backed government. It has often planted IEDs on the side of the roads to take down passing government officials or African Union peacekeeping troops in the country.
But it has denied government claims they are behind the attacks or that street cleaners are the goal.
"We do not target anyone for cleaning the streets of Mogadishu, in fact cleaning the streets is an act of charity that is welcomed by Islam," the group told Al Jazeera in a statement on July 5.
"Mogadishu's street cleaners are killed by the same troops who frequently target the Tuk-tuk drivers of Mogadishu, and everyone knows who those are. They are the apostate militia and their foreign crusaders," the statement added.

'No other option'

Most of them are widows who lost their husbands during the country's 30-year-old civil war and are their families' breadwinners. On any given day, there are at least 450 of them cleaning the streets of the Somali capital, according to the local city authority.
The highest earners take home $150 a month. Some receive food rations in exchange for the work and many work on a voluntary basis hoping to secure a job if and when one comes up.
A short distance away, Hawo Ali Hassan, an eight-year veteran of the streets is going through empty boxes left on the side of the road gently with two fingers.
Hawa says she doesn't like her "very risky" job but has to do it to put food on the table for her large family.
"I would not recommend anyone to do it. You can die at any moment. I work seven days a week because I have to support my children and blind husband," the mother of 10 children said.
Her husband became blind after a mortar landed near where he was working 10 years ago.
"I have no other option. I'm a mother. I will do anything to support my children. Yes, it is risky but I will take any risk for them," the 58-year-old added as she moved to the next pile of rubbish that needed clearing.

Relatives of the street cleaners lost in the line of duty are still coming to terms with the tragedy.
"I still remember receiving a phone call from my brother-in-law telling me my grandmother has been killed," Hodma Abdishakur Hassan told Al Jazeera.
"She was blown up near Medina police station. She was just starting her shift. Her lower body was blown to pieces. She was alive first but died of the injuries a few hours later. She was not just my grandmother but was also raising me and my two other siblings," Hodma added, tears dripping on her black niqab. Fay Mohamed Hassan was 70 years old when she was killed in November 2011 and earning $120 a month, Hodma added. Two other female cleaners lost their lives in the same explosion.

Easy targets

IEDs are not the only threat the street cleaners face on a daily basis.
"We are easy target for robbers. Most of us have [been] robbed of mobile phones and valuables. If you work late at night or early morning then you will most likely get robbed. And they are very violent. It is why none of us want to wear high viz jackets because it will attract robbers," Maryan said.
The local authority says they are doing their best to protect their staff.
"We have stopped them from working night shift for safety reasons," Hussein Abtidoon Warsame, the deputy head of sanitation for Mogadishu municipality told Al Jazeera.

"We have started hiring male staff to deter thieves from targeting female staff. But it is not easy to find male staff because men don't want to do cleaning work," he added.
Hussein, who himself was badly injured in an attack claimed by al-Shabab and moves with the help of a walking stick, says government pays the hospital bills of those injured in the line of work.
"Sadly, we can't afford to give compensation if someone dies. We don't have the money. But we will give the position to family members if they wish [to] take up the work," he added.
For the women going out every morning to keep Mogadishu clean, it is a risk they are long accustomed to.
"We have no one to protect us but God. In our line of work, we fear people. Not stray dogs or wild animals," Maryan said.

US Navy robotic minesweeper ship declared operational

Source: https://newatlas.com/military/us-navy-robotic-minesweeper-ship-declared-operational/

Aug 03 – Robotic ships have officially joined the US Navy. The Program Executive Office, Unmanned and Small Combatants (PEO USC) announced on July 22 that the Navy's **Unmanned Influence Sweep System (UISS)** uncrewed minesweeper has been awarded Initial Operating Capability (IOC).
The announcement that the UISS has reached the state where it is at least minimally ready for deployment is a major advance in the Navy's program of introducing uncrewed ships into the fleet as a way to not only shield humans from going into harm's way, but also as a means of reducing costs while increasing capabilities.
The IOC declaration comes after the formal testing of the system and the delivery of the supporting logistics and training materials for the minesweeping mission package. According to the PEO, this marks a significant milestone in the push to produce a hybrid crewed/uncrewed fleet for the Navy.
Developed by Textron Systems, the UISS is a self-propelled, semi-autonomous surface vessel that can seek out undersea mines acoustically and magnetically. When it is fully operational, it will replace the Navy's Avenger-class minesweeping ships and MH-53E Sea Dragon helicopters and will operate from a variety of ships to keep sea lanes, fleet operating areas, straits, choke points, and amphibious landing sites clear of mines.

The UISS is diesel driven with **a maximum range of 87 miles (140 km) and can operate at sea for over 20 hours.** It can also tow about 4,000 lb (1,814 kg) at a speed of 20 kt (23 mph, 37 km/h). Payloads include side-scan sonar, gap-filling sonar, forward sonar, non-lethal weapons, mine neutralization systems, and intelligence, surveillance, and reconnaissance (ISR) sensors. These will allow it to simultaneously detect, locate, and classify bottom, moored, close-tethered, and volume-moored mines.
"UISS's declaration of IOC is a monumental achievement for the Navy's Mine Countermeasures (MCM) Mission Package (MP)," said Capt. Godfrey "Gus" Weekes, LCS Mission Modules (PMS 420) Program Manager. "Over the years, the program has worked tirelessly to mature and field the UISS system that will keep the Navy's most valuable asset, our sailors, safer by keeping them out of the minefield. With this declaration, the program is inching closer toward system-wide IOC for the MCM MP."

Drones Approved for Aerial Inspections of Power Facilities

Source: https://www.homelandsecuritynewswire.com/dr20220804-drones-approved-for-aerial-inspections-of-power-facilities

Aug 04 – Since the Virginia Tech Mid-Atlantic Aviation Partnership was designated by the Federal Aviation Administration (FAA) as an official drone test site in 2013, its research has helped shape drone integration in the U.S.
In the process, it has carved out new opportunities for companies that see new ways to use the technology that stretch the boundaries of current regulations. One of the latest wins is a waiver from the FAA that gives Dominion Energy, one of the region's largest energy companies, permission to use drones to inspect power-generation facilities in seven states.
Drones have become a popular tool for inspections of bridges, buildings, and other structures because high-resolution aerial imagery is a convenient alternative to an assessment that could be time-consuming or dangerous to do in person. What makes this particular waiver so valuable for Dominion is a feature that's widely coveted but still relatively rare: It doesn't require the operator to be able to see the aircraft the whole time it's being flown.

Keeping the drone within "visual line of sight" is a standard requirement written into drone regulations to reduce the risk of collision with low-flying crewed aircraft such as helicopters and small planes. Breaking this barrier and flying beyond visual line of sight has become a central priority in the drone industry because of the efficiencies that accrue when an operator has the flexibility to cover longer distances or — more relevantly for this type of work — maneuver around corners or behind obstacles.

Dominion will conduct its inspections with an aircraft from U.S. drone manufacturer Skydio with sophisticated, autonomous obstacle avoidance capabilities. That feature allows the drone to be safely flown in close proximity to structures. Virginia Tech helped Skydio and Dominion make the case to the FAA that flying close to structures on the facility kept the drone out of the way of other potential air traffic, making the risk of collision so low that the FAA could safely waive the requirement for the pilot to see the drone or for an additional crew member to constantly scan the airspace.

"Two major goals of our research are helping firms like Dominion develop safe, practical ways to use drones to enhance their operations and helping drone companies like Skydio find opportunities to leverage the power of their technology to enable new kinds of operations," said Tombo Jones, the test site's director. "This waiver achieves both of those things."

Spearheaded by Dominion's uncrewed aicraft systems program in partnership with Skydio's regulatory affairs team and Virginia Tech, the project unfolded under the umbrella of the FAA's BEYOND program. That federal initiative focuses on enabling drone operations beyond visual line of sight in situations — such as infrastructure inspection — where drones can offer significant advantages that will only be fully realized with those more ambitious flights.

The Virginia Tech Mid-Atlantic Aviation Partnership leads Virginia's BEYOND team in collaboration with the Virginia Innovation Partnership Corporation. Dominion's infrastructure inspection project is one of three applications the team is tackling, along with residential package delivery with Wing and insurance inspections with State Farm.

The waiver request, developed by Skydio's regulatory affairs team, covers more than 40 of Dominion's facilities in Connecticut, Georgia, Indiana, North Carolina, South Carolina, Virginia, and West Virginia. These facilities undergo routine inspections, and using a drone to do them avoids having to send an inspector up scaffolding, down walls, or into areas with high temperatures or other hazards. Adding the ability to fly beyond line of sight upgrades that safety advantage with a dramatic increase in efficiency: Now, the pilot can potentially conduct an entire facility inspection from a single location, sometimes even in a single flight, rather than traveling from place to place to keep the drone in view. Dominion Energy first deployed drones in 2014, focusing primarily on identifying electrical transmission line defects. Since then, Dominion has expanded its drone program to include approximately 50 drones and drone pilots serving multiple operational business segments. At power generation facilities, Dominion Energy drones take volumetric measurements and assess construction progress, provide surveying and mapping services, and inspect infrastructure.

"A 20-minute inspection by a battery-powered drone will increase safety for our colleagues, who will no longer need to rappel down the side of a structure, as well as save time during inspection-related preparations," said Nate Robie, the manager of Dominion Energy's unmanned systems program. "As a pioneer in beyond visual line of sight drone use, Dominion Energy contributes to a safer, greener future as well as potentially lowering operations and maintenance costs, which ultimately benefits our customers."

Developing regulations that would allow flights beyond visual line of sight to become routine and scalable, instead of permitted on a case-by-case basis through individual waivers and exemptions, is the focus of significant effort across the drone industry and at the FAA. Programs such as BEYOND provide real-world examples of strategies for conducting operations like this in ways that are practical, beneficial, and, crucially, safe. "This pivotal approval brings Dominion Energy, Skydio, and the entire drone industry one step closer to advanced drone operations at scale," said Jenn Player, Skydio's director of regulatory affairs. "When it comes to scaling beyond visual line of sight operations, having an intelligent drone makes all the difference, and Skydio was proud to support Dominion Energy in obtaining this waiver that enables them to inspect critically important power facilities."

The test site, Dominion, and Skydio all served on an advisory committee convened by the FAA last year to develop recommendations for rulemaking on operations beyond visual line of sight. The committee submitted its recommendations to the FAA last spring.

"The overwhelming majority of economically viable drone operations will require flying beyond visual line of sight," Jones said. "It's the key to reaching the tremendous potential that we all recognize is there. There's still a lot of research and testing that needs to be done to get to that point, but operations enabled by waivers like this one give us a window into what the future could look like."

Netherlands: More self-made explosives used in attacks on houses

Source: https://nltimes.nl/2022/08/03/self-made-explosives-used-attacks-houses

Aug 03 – Criminals are shifting from hand grenades to improvised explosives when attacking houses and vehicles in the Netherlands, according to the Ministry of Defense's Explosive Ordinance Disposal Service (EOD). The number of incidents involving self-made bombs using, for example, fireworks is on the rise, while incidents with hand grenades are plummeting, EOD Major Peter said to NOS.

Last year, the EOD responded to 11 incidents of self-made explosives attached to homes or cars. This year, the counter is already at 17. On the other hand, incidents involving hand grenades dropped from 14 last year to only four so far this year.
Major Peter, who asked that his surname be withheld given the nature of his work, can't give an exact cause for the shift. The EOD pointed out that in the past, self-made explosives were mainly used for things like ATM bombings, the number of which has decreased in the past months due to investments by banks and the police to boost security around the machines. It may also be that hand grenades are harder to come by. Grenades mainly come from the Eastern Bloc, according to the major.
The EOD is concerned about the development. Improvised explosives are extra dangerous to defuse. "We have a manual for a hand grenade, and there is quality control on it," said Peter. "If people manufacture an explosive themselves, then the question is how it works."

Extreme Drought in Italy Reveals Hidden Bomb Submerged in River Since WWII

Source: https://www.sciencealert.com/intact-wwii-era-bomb-discovered-in-italy-s-river-po-following-extreme-drought

Aug 09 – Fishermen discovered the American-made bomb on July 25, near the northern Italian village of Borgo Virgilio, near the city of Mantua, according to Reuters.
The bomb appeared to have been submerged there for more than 70 years.
However, water levels in the River Po – which stretches east-west across northern Italy and is the country's longest river – have diminished significantly this summer, following multiple heat waves that hit many parts of Europe (including Italy) with record high temperatures.
According to military experts, the bomb weighed nearly 1,000 pounds (450 kilograms).
After evacuating the roughly 3,000 civilians who live in the village's vicinity, military experts cut the bomb's fuse and moved the device to a quarry about 30 miles (45 kilometers) away.
There, the bomb was destroyed in a controlled detonation. There were no injuries or damages reported from the controlled explosion.
This summer has seen much of the Northern Hemisphere hit with extreme heat waves, which are predicted to become more and more common as a result of ongoing climate change.

In late June, Rome reported its highest recorded temperature ever, at 105 degrees Fahrenheit (40.5 Celsius), according to *The Washington Post*.
During the June heat wave, Rome's Tiber River dried up so much that the ruins of an ancient bridge built during the reign of Emperor Nero (who ruled as the fifth emperor from CE 54 to 68) became plainly visible on the river bottom.
The bridge ruins only appear during long periods of drought, experts told Live Science.
Because of the ongoing drought, Italy declared a state of emergency last month for areas surrounding the River Po, where roughly one-third of Italy's agricultural production takes place, according to Reuters. (The state of emergency had nothing to do with the bomb).
The region is suffering the worst drought seen in roughly 70 years.

Who Dropped Thousands Of Antipersonnel 'Butterfly' Mines On Donetsk? (UPDATE: UK Blames Russia)

By David Hambling (South London-based technology journalist, consultant and author)
Source: https://www.forbes.com/sites/davidhambling/2022/08/04/who-dropped-thousands-of-antipersonnel-butterfly-mines-on-donetsk/

Aug 04 – Thousands of miniature PFM-1 'butterfly' mines rained down on a built-up area of Russian-occupied Donetsk on the night of July 27, according to local news and social media. One Twitter video shows motorists driving down a street which has become a minefield, with mines exploding under their tires. In another, frightened pedestrians pick their way along the sidewalk avoiding the explosive hazards. The big question is who is responsible for this attack – though for local residents demining their neighborhood may be a more urgent issue.

Each plastic antipersonnel mine, known as PFM-1, Lepestok ("Petal"), Butterfly or Green Parrot, contains 37 grams of explosive, enough to blow off a foot. They became notorious after the Soviets used them extensively in Afghanistan, often injuring curious children. There have been reports of butterfly mines use in the current conflict – see our previous report here — but little evidence. The volume of images and videos from Donetsk suggest a definite, deliberate, large-scale attack on a civilian area. News reports mention people injured but there have been no numbers or reports of deaths yet.

The mines seem to have been delivered by a Uragan ("Hurricane") 220mm multiple rocket launcher. One image shows a mine container which failed to open properly. One rocket delivers 312 mines, and the launch vehicles fires rockets in salvoes of sixteen, scattering thousands of mines over an area over half a mile across, leaving one mine every thirty feet or so.

The mines are sensitive to pressure, either a single contact such as being trodden on or the cumulative effect of being handled. They are often picked up by people not realizing what they are. A video from Donestsk shows a woman taking one out of her handbag — she had picked it up show workmates, assuming it was bomb shrapnel.

The mines are relatively easy to spot, though they may lie hidden in grass. But dealing with this number of mines in a heavily populated area is a challenge. A local news report shows a bomb-disposal crew using a plastic water bottle cut in half on the end of a pole to scoop up mines into a heap so several can be blown up together. Another team uses a road roller to run over the mines and explode them.

Some soldiers not trained in bomb disposal adopt more casual, more hazardous approaches to demining. Videos show them setting off mines by throwing tires or bricks on to them, or even hitting a mine with a long stick. This is possible because, unlike many types of mine, the PFM-1 is purely a blast weapon and does not throw out shrapnel. There is (relatively) little risk to someone two meters away, but messing with explosives is always dangerous and experts advise against it.

Some of the mines are also in inaccessible locations; a bomb disposal team located several on the flat roof of a shop. They could remain there for some time before strong wind or rain disturbs them and produce enough cumulative force to trigger an explosion. In Afghanistan, butterfly mines have maimed people after lying inert for years.

Ukraine became a state party to the Mine Ban Treaty in 2006, but still has stockpiles of millions of butterfly mines. Russia also has the mines and has not joined the treaty, but is still bound by humanitarian law which outlaws deliberate attacks on civilian population with no military objective. This was purely a terror attack, intended to frighten and inure the civilian population, with no military justification.

Human Rights Watch has closely monitored the war in Ukraine and documented previous instances of landmine use. But at present they cannot say who is responsible.

"We are not commenting on these specific allegations at this point since it is impossible to independently verify or attribute the reporting," HRW Associate Arms Director Mark Hiznay told me. "We note that similar allegations have sporadically surfaced from Russian sources about the use of this weapon since the beginning of the war. "

HRWs previous report on these allegations concluded in June that there was "no credible information that Ukrainian government forces have used antipersonnel mines," while they also reported that Russia had used POM-3s, a different types of air-dropped anti-personnel mine, in the Kharkiv region.

Determining whether the attack was carried out by Ukrainian forces, or whether it was a 'false flag' attack or even friendly fire by Russian forces or local militia, as some have suggested, is likely to be difficult. While munitions often have serial numbers or manufacturer's codes stamped on them indicating the date and place of production – and markings can be seen on some of the mines – this may not be conclusive. In any case, deminers are usually more concerned with safety than the challenge of gathering forensic evidence.

"We clear landmines to make local people safe and we mostly do so in ways that render them unidentifiable," a spokesman from demining NGO HALO Trust told me.

There may also be evidence in the form of radar or other tracks of rocket launches in the area. These may show the location that the rockets were fired from and so indicate which side was responsible if not the actual unit. As in the case of the missile that downed Malaysia Airlines flight MH17 such evidence is likely to be contested. But it might still be possible to bring the perpetrators to justice – eventually – and discourage such attacks on civilians in the future.

Update 9th August: The UK Ministry of Defence Intelligence Update appears to blame Russia for the attacks, stating that "In Donetsk and Kramatorsk, Russia has highly likely attempted employment of PFM-1 and PFM-1S scatterable anti-personnel mines. Commonly called the 'butterfly mine', the PFM-1 series is deeply controversial, indiscriminate weapons." They add that "in the Soviet-Afghan War ... they allegedly maimed high numbers of children who mistook them for toys."

EDITOR'S COMMENT: When the British blame Russians for the butterfly bombs then it is almost certain that Ukrainians did it.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Officials are racing to protect the absolutely most important hacking targets

Source: https://www.washingtonpost.com/politics/2022/07/28/officials-are-racing-protect-absolutely-most-important-hacking-targets/

July 28 – **Welcome to The Cybersecurity 202!** How do *you* feel about the "improbable hacker character" as a plot cliche? They're at least … kind of fun, right?

There's momentum for identifying and safeguarding the most crucial U.S. infrastructure

Congress and the Biden administration are moving on parallel tracks to whittle down the list of U.S. hacking targets to no more than a few hundred **they say need extra protection because attacks on them would have dire ramifications for national security, health, public safety or the economy.**

It's an idea floated among cybersecurity policy wonks for a few years, but it's now making substantial progress on Capitol Hill and at the Department of Homeland Security. Still, some in industry harbor fears of how Congress in particular might apply the concept to them.

Their argument: While the U.S. has for decades maintained 16 categories of the most "critical" infrastructure that the federal government prioritizes for protection — like chemical plants, pipelines and government facilities — the concept has its limits.

"We have diluted the definition of critical infrastructure to [include] a lot of different things that can argue that they're critical infrastructure, and it makes it harder to take a risk-based approach," **Bob Kolasky**, a former Cybersecurity and Infrastructure Security Agency official who worked on the project there, told me.

As CISA Director **Jen Easterly** likes to say, "If everything's a priority, nothing's a priority."

"We need to have a way when there's a really bad day to figure out how to allocate government resources and focus to understand cascading impacts of an attack on one set of infrastructure, because we know you can't just think about one sector," she said in our interview this week. "You have to think cross-sector."

- **The congressionally created, bipartisan Cyberspace Solarium Commission helped kick off the rethink** with a 2020 recommendation about what it called "systemically important critical infrastructure," or "SICI." Under the commission's proposal, the federal government would compile a list, then institute both "benefits and burdens" to help or prompt infrastructure owners to improve their defenses.
- As legislation establishing SICI into law has yet to advance, **CISA has moved forward on its own ongoing compilation of such infrastructure,** which it instead calls "primary systemically important entities" or "PSIEs" (pronounced "Pisces").

Examples of entities likely to fall under the designation — whatever the final name — are big banks, sprawling information technology firms and major suppliers of electrical power.

150 to 300 organizations

Rep. **Jim Langevin** (D-R.I.), who was a Solarium commissioner, this month won approval for an amendment to the House's annual defense policy bill that offers a modified version of what the commission proposed. **Federal agencies would initially identify up to 150 organizations to label as especially critical, swiftly share threat information with them and study possible security goals for them to meet.** Entities labeled as such would have to report to the government on their most important digital assets and their supply chain security practices.

Financial services lobbying groups complained about earlier versions of the idea, saying it would force heavily-regulated banks to comply with duplicative demands from agencies. In response, Langevin's amendment included a provision to determine whether reports submitted elsewhere would suffice for DHS's purposes.

Some industry officials remain unpersuaded by Langevin's effort.

"Collaborative partnerships between industry and government must be formed to mitigate significant cyberattacks, but the current SICI effort has not fully addressed this," said **Matthew Eggers**, vice president of cybersecurity policy at the U.S. Chamber of Commerce. "Also, many business policy objectives, including legal liability protections and express national preemption, are left out of the amendment."

One banking industry official, speaking on the condition of anonymity because they are still reviewing the language of Langevin's proposal, said: "We don't have a report that we share with regulators that could just be handed over to CISA. It would basically duplicate and add yet an additional layer of government reporting to what we already do that introduces risk without providing a clear benefit."

Another industry official, speaking on the condition of anonymity as they continued to review the Langevin amendment, criticized the bill's proposed studying of performance goals. "Everybody who writes bills has been around the policymaking process for a while [and] knows that studies are a precursor to developing requirements," they said.

Easterly, meanwhile, says CISA is looking on its own at a list of between 150 to 300 entities. They're in a "decomposition" process to divide up "primary" entities and "other" entities that serve crucial national functions like distributing goods or managing hazardous materials, she said. Entities on the primary list could receive benefits such as threat intelligence, incident response or CISA teams who could hunt for vulnerabilities, she added.

Next steps

CISA has some authority to meet the goals of the concept, but it's more limited without Congress, according to Kolasky, who now works at supply chain risk-management company Exiger.

Langevin is still huddling with industry over the language and teaming with Sen. **Angus King** (I-Maine), another Solarium commissioner, to include his provisions in the Senate's version of the defense bill, Langevin told me.

"The consequences of our inaction could be severe," Langevin said.

The keys

U.S. lawmakers signal that they plan to further scrutinize spyware

Foreign spyware poses national security and privacy risks, House Intelligence Committee Chairman **Adam B. Schiff** (D-Calif.) said at a hearing, **CyberScoop**'s Suzanne Smalley reports. "Schiff suggested more action will be coming from the committee, saying he believes the U.S. needs to put a 'greater emphasis on this' and 'respond to this threat with urgency,'" Suzanne writes.

- Microsoft, meanwhile, says Austrian firm DSIRF was behind spyware used to target "law firms, banks and strategic consultancies in countries such as Austria, the United Kingdom and Panama," Reuters reported. Microsoft also said it had patched a previously-unknown vulnerability used by DSIRF. DSIRF didn't respond to Reuters's requests for comment.

European investigators have found evidence that some European Commission staffers were hacked with Pegasus, E.U. Justice Commissioner **Didier Reynders** said in a letter to European lawmaker **Sophie in 't Veld** obtained by **Reuters**'s Raphael Satter. Apple warned Reynders last year that his phone may have been hacked with Pegasus, Reynders wrote in the letter. It's not clear who was responsible for the hacks and the investigation is ongoing, Reynders reportedly wrote.

- Reynders didn't respond to Reuters's request for comment. NSO told the outlet that it would cooperate with a European investigation. "Our assistance is even more crucial, as there is no concrete proof so far that a breach occurred," an NSO spokeswoman told Reuters. "Any illegal use by a customer targeting activists, journalists, etc., is considered a serious misuse."
- In 't Veld is the rapporteur of a European committee investigating Pegasus and other spyware. Last week, the committee said 14 European governments have purchased technology from NSO. Officials in Hungary, Poland and Spain are being — or already have been — questioned about their use of Pegasus, Reynders reportedly wrote in the letter.
- Reynders's letter emerged just after a Greek member of the European Parliament, **Nikos Androulakis**, said he had been informed by European investigators that he had been targeted with another type of spyware called "Predator." It's not clear who was behind the hacking attempt, but a European Commission spokesperson told Euractiv that "any attempts by national security services to illegally access data of citizens, including journalists and political opponents, if confirmed, is unacceptable."

Lawmakers in Canada are also going to investigate how Canadian police use spyware, Politico's Maura Forrest reports. It comes after the RCMP last month disclosed that it has used spyware in criminal investigations, Politico previously reported. The RCMP says it only uses hacking tools in serious cases and gets approval from a judge.

- The lawmakers want to know if the RCMP use NSO spyware, Forrest reports. They plan to hold two days of hearings in the country's parliament next month.

Three senators call for new cybersecurity standards for federal data centers

Bipartisan legislation unveiled today would task federal officials to come up with new cybersecurity guidelines for federal agencies' data centers. The bill is being introduced by Sen. **Jacky Rosen** (D-Nev.), Senate Homeland Security Committee Chairman **Gary Peters** (D-Mich.) and Sen. **John Cornyn** (R-Tex.).

The legislation calls for officials to consult with the director of CISA and the national cyber director in creating cybersecurity requirements, according to a copy of the legislation obtained exclusively by The Cybersecurity 202.

"The sensitive information stored on federal systems cannot be left open to vulnerabilities like cyberattacks or natural disasters," Cornyn said in a statement. "This legislation would help secure federal data and encourage optimization, which will save taxpayer dollars and protect Americans who entrust their information to the federal government."

Tallinn Workshop Report

ECCRI EUROPEAN CYBER CONFLICT RESEARCH INITIATIVE

Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far)

Monica Kaminska, James Shires, and Max Smeets

Monica Kaminska is a postdoctoral researcher at The Hague Program on International Cyber Security at the Institute of Security and Global Affairs, University of Leiden.
James Shires is an assistant professor in Cybersecurity Governance at the Institute of Security and Global Affairs, University of Leiden.
Max Smeets is the director of ECCRI and a senior researcher at the Center for Security Studies (CSS) at ETH Zurich.

Deep Learning Is Not Immune to Cyber Attacks – What Can We Do?

Source: https://i-hls.com/archives/115259

July 29 – While deep learning algorithms may be looking promising for identifying and characterizing cybersecurity intrusions, various attacks can cause them to provide inaccurate information, or even upset their entire plan of operations. Research shows that cybercriminals have been developing new attacks against different deep learning systems, such as those used for image analysis and natural language processing. Previous research has shown the efficacy of various adversarial approaches in causing deep neural networks (DNNs) to deliver untrustworthy and inaccurate predictions. Researchers from the cyber security company Citadel have recently shown that current deep learning-based solutions for identifying certain cyberattacks, such as DDoS DNS, have substantial weaknesses and vulnerabilities. Certain attack techniques are capable of creating corrupted data that DNNs would misclassify, therefore delivering false information. The Citadel researchers developed a DNN capable of detecting cyber-attacks, and then assaulted it with adversarial data to trick the DNN into arriving at false conclusions. The findings of these experiments clearly showed that a DNN can be deceived by malicious attacks and ignore or falsely report on DDoS DNS attacks. DDoS DNS amplification attacks use weaknesses in DNS servers to magnify requests sent to them, eventually flooding them with data and taking the servers down. These assaults have the potential to significantly impair internet services provided by both large and small multinational corporations. According to Marktechpost.com, the work of this Citadel team of researchers may inspire the creation of more effective technologies for detecting DDoS DNS amplification assaults in the future, which can recognize and categorize hostile data.

New Cyber Attack Can Unmask Anonymous Users

Source: https://i-hls.com/archives/115227

July 27 – Researchers from the New Jersey Institute of Technology have discovered a way to use basic functions of the internet to identify who visits a certain website, with the user being able to detect that they are being hacked. This is a huge warning against a novel technique that attackers could use to de-anonymize website visitors and gain information regarding the personal and digital lives of the visitors.
The findings show how an attacker who tricks someone into loading a malicious website can determine whether that visitor controls a particular public identifier, like an email address or social media account, thus linking the visitor to a piece of potentially personal data.
Wired.com explains that when you visit a website, the page can capture your IP address, but this doesn't necessarily give the site owner enough information to individually identify you. Instead, the hack analyzes subtle features of a potential target's browser activity to

determine whether they are logged into an account for an array of services, from YouTube and Dropbox to Twitter, Facebook, TikTok, and more. Plus, the attacks work against every major browser, including the anonymity-focused Tor Browser. Reza Curtmola, one of the study authors and a computer science professor at the New Jersey Institute of Technology elaborates that "If you're an average internet user, you may not think too much about your privacy when you visit a random website, but there are certain categories of internet users who may be more significantly impacted by this, like people who organize and participate in political protest, journalists, and people who network with fellow members of their minority group. And what makes these types of attacks dangerous is they're very stealthy. You just visit the website, and you have no idea that you've been exposed." Curtmola goes on to say that this form of an attack can aid law enforcement in identifying the users of underground extremists or activists, even if these users use pseudonyms. This poses a real privacy concern for active online users and exposes one of the vulnerabilities of the digital world that goes deep into the design of hardware, which makes changes and improvements much more elaborate and difficult.

Russian Hackers Target U.S. HIMARS Maker in 'New Type of Attack': Report

Source: https://www.newsweek.com/russian-hackers-target-us-himars-maker-report-ukraine-russia-1729502

Aug 01 – Russian hackers have launched "a new type of attack" on American military company Lockheed Martin, which makes the M142 High Mobility Artillery Rocket System (HIMARS) that the U.S. has supplied to Ukraine, a pro-Moscow news website said.
The Kremlin-supporting Life website reported that the cyberattack by the Killnet and Killmilk hacker groups took place at 7 a.m. on Monday. The groups said the rocket systems - credited by the Ukrainians with shifting the balance in the war against Russia - had been responsible for thousands of deaths.
"The notorious HIMARS multiple launch rocket systems, supplied to Ukraine by the aforementioned military-industrial corporation, allow the criminal authorities of the Kiev regime to kill civilians, destroy the infrastructure and social facilities of the still temporarily occupied Ukraine," the hackers said in a statement reported by Life.

US soldier walk past an M142 High Mobility Artillery Rocket System (HIMARS) launcher vehicle, during the "African Lion" military exercise in the Grier Labouihi region in southeastern Morocco on June 9, 2021. Russian hackers have reported launched a cyberattack on American military company Lockheed Martin, the maker of the HIMARS. Fadel Senna/AFP/Getty

The hackers said Lockheed Martin "is the actual sponsor of world terrorism, is responsible" for thousands of deaths. *Newsweek* has contacted Lockheed Martin for comment. *Newsweek* did not see evidence that Lockheed Martin sponsors terrorism.
A Russian military expert claimed on state television on July 28 that Russia had come up with a "secret development" that allows it to hack into the HIMARS systems.

On July 22, members of Killnet said: "We are using a new type of attack, we have no equal in this area. This is a new technology that we are using for the first time against the world's largest arms manufacturer—Lockheed Martin," Life reported at the time.
Lockheed Martin's website describes it as a global security and aerospace company.
The HIMARS have been supplied to Ukraine by the United States, and the weapons have been touted as "a gamechanger" by senior Western military officials. The U.S. has promised Ukraine up to sixteen of the units, which can be mounted to a standard U.S. Army M1140 truck frame.
Each HIMARS can carry six GPS-guided missiles that can be reloaded in about a minute with a small team consisting of only a driver, gunner and launcher section chief.
The range of the weapons is 80km (50 miles), almost double the ranger of M777 howitzers, another Western-made weapon that Ukraine has been using against Russian forces since May.
A HIMARS can fire in similar ranges to conventional multiple launch rocket systems, at targets up to 300 km away.
On July 22, a senior U.S. defense official said that Ukraine had used HIMARS to destroy more than 100 "high value" Russian targets in recent weeks.
Ukraine says it has used the weapons to strike dozens of Russian ammunition depots, command-and-control sites, and other targets such as critical bridges in the Kherson region.
Kyiv has been mounting a counter-offensive to re-take the southern area that fell to the Russians in early March. Ukrainian forces have retaken dozens of villages and towns along the border and are pushing towards Kherson's eponymous regional capital, the region's military governor Dymtro Butrii has said.
Russia is moving large numbers of troops to the region and other areas in the south, Ukraine's deputy head of intelligence said on Monday.
Kherson is strategically important in the conflict because it connects to the Crimean Peninsula, Ukrainian land that Russia annexed in 2014.

New Ransomware Discovered Due to Cyber Attack on Albania

Source: https://i-hls.com/archives/115441

Aug 06 – New piece of ransomware discovered following the cyber attack on the Albanian Government. The Albanian government announced mid-July that it was forced to shut down some public online services due to a cyberattack. Mandiant, a cyber security company, has investigated the incident, which led to the discovery of a new piece of ransomware. Mandiant researchers came across the ransomware after it had been uploaded from Albania to a public malware repository a few days after the cyberattack was launched. The ransomware has been named Roadsweep.

Securityweek.com reports that while the researchers could not confirm that the ransomware was indeed used in the attack, the malware encrypts files on compromised systems and then drops a ransom note suggesting that its target is the Albanian government. The cybersecurity firm also spotted a website and Telegram channel named 'HomeLand Justice', which took credit for a ransomware operation aimed at the Albanian government. The site implied that it had been run by Albanian citizens unhappy with their government. However, this entity's focus appeared to be an Iranian opposition organization designated as a terrorist group by the US Department of State.

Following a thorough investigation, the researchers were able to determine that the Roadsweep ransomware shared code with a back door named Chimneysweep that allows its operators to take screenshots, log keystrokes and steal files.

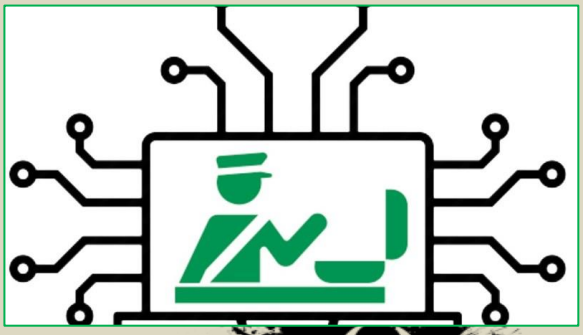
Moreover, it appears from within the country uploaded to a public malware repository a sample of a wiper malware that Mandiant has named Zeroclear. While the cybersecurity company was unable to confirm that this malware was used in the disruptive operation, Zeroclear was previously used by Iran-linked threat actors for disruptive activities in the Middle East.

Mandiant researchers also believe other NATO members could be targeted in similar operations.

Borders and cyber-threats: how safe are we?

By Petros Chatzis and Eliana Stavrou

Source: https://border-security-report.com/borders-and-cyber-threats-how-safe-are-we/



July 27 – In the recent decades, the border landscape has dramatically evolved, from the traditional geographical related boundaries, which defined national sovereignty territories, towards a critical infrastructure, involving checks and surveillance and falling under law enforcement jurisdiction. Nations rely upon well-controlled borders, especially due to the interchanges of globalization and the increasing demand for movements, using all technological advances. On the other hand, the interdependence of cyber and physical areas and the heavy reliance on technology have greatly expanded the attack surface, giving more opportunities to malicious actors to attack borders. Due to the criticality of the borders, the impact from

a cyberattack could be far-reaching. This article highlights the importance of the topic, presenting a list of cyber-threats and threat actors relevant to borders' control management operations.

To effectively protect border control management operations, one must first obtain a clear view of the different assets that take part in this complex infrastructure and then identify the cyber-threats that can jeopardize their operation. Border control increasingly relies on databases, large information systems and algorithms, which are stored in the cloud or controlled by third-parties. In parallel, the systems become more and more interconnected and interdepended, thus any failure to one of them could have a cascading effect to the others. Moreover, the heterogeneity of the different systems contributes to the complexity of the border control management infrastructure, which may consist of components of different types and origin, e.g., the manufacturers of cameras, sensors and operating system. The advanced interconnectivity of systems, people, and processes along with the heavy reliance on smart technologies increase the exposure to cyber-threats, such as personal data breach and disruption of services, which could have a serious impact, resulting even in harming national security and sovereignty.

Existing cyber-attacks against the borders, reveal the reality and the dimension of the problem.

The following list of examples is indicative and not exhaustive, aiming to demonstrate the range of cyber-attacks that can be executed against the borders:

- 2021. Belarus: Hackers claim to have accessed full database of those crossing the country's borders (Woollacott, 2021).
- 2021, Ukraine: Border control was hit with data-wiping malware, slowing refugee crossing (Alspach, 2022).
- 2019, USA: CBP Says Thousands of Traveler Photos Stolen in 'Malicious Cyber-Attack' (Levin, 2019).
- 2017, Taiwan: Since 2011, Taiwan used biometric e-Gates allowing fast-track passport control at main airports. It is suspected that the system had been compromised by a foreign government, due to a pre-installed 'backdoor' by the manufacturer (Everington, 2017).
- 2015, USA: Drug traffickers invested in spoofing and jamming the GPS systems of the border surveillance drones (Thompson, 2015).

These examples are indicative of the different threats that the borders face which extend the traditional "physical" threats, for example a person by-passing the border control by hiding in a vehicle or the use of a look-alike passport. Also, it needs to be taken into consideration that cyber-threats are not limited to intentional malicious actions, but extended also to non-malicious actions, like human errors, systems' misconfigurations or natural disasters (ENISA, 2021).

There are various threat taxonomies developed for different critical infrastructures. Specifically for the border control infrastructures, the relevant threat categories could be summarized as follows:

• Natural and social phenomena can cause serious disruptions in the functioning of the society, and it is a category where the border management agencies do not have direct control such as the "push and pull" factors, e.g., a war situation causing mass migration movements. Other examples falling under this category are natural disasters, e.g., a fire destroying the border assets, a pandemic or even climate conditions such as strong winds not allowing the UAV surveillance flight. Disinformation or fake news is also a recent trend e.g., mass movements of people have been recently encountered trying to abolish border controls.

• **Third-party failures** are a great threat due to the interdependencies between border control management and third parties, which could seriously disrupt the border functions and assets; for example, a disruption caused by the internet service provider, errors or delays by companies to provide passenger or crew lists.

• **System failures & outages**, especially related to hardware and software failures, communication disruptions or even false alerts, e.g., a false alert of a database, could mean that an innocent person might be perceived as a threat.

• **Human errors** include all range of unintentional human activities which could harm the efficiency of border control processes and harm a range of assets. Fatigue could result to data-entry errors, non-compliance with security policies could lead to exposure of sensitive data, improper use of equipment could damage it and use of non-secure equipment might become a target of a malicious actor.

• **Malicious actions:** The core element of these threats is the intentional character and the aim, such as the disruption, destruction and unauthorized access to assets. Three subcategories are identified, in particular: a) Insider threats are caused by the border staff with malicious motivation, e.g., a) Corrupted officer misusing his data access rights to sell information, b) Physical attacks take place with traditional "physical" methods and tools, without reliance on technology, such as vandalism, sabotage and theft of assets, and c) Cyber-attacks are those targeting the ICT systems, in particular:

- Malware which is a generic term for software that has a malicious purpose, e.g., ransomware, trojan horses, virus, and spyware. Unpatched systems could be easily become target of an attacker. Malware could be also installed due to negligence of the users in a variety of border systems, from PCs to remote border control assets.
- In Denial of Service (DoS) attacks the attackers block access from legitimate users and could be conducted by cyber-criminals to disrupt functions, e.g., the access to travel authorization systems, possibly requested as a service by criminals.

- Penetration attacks is a broad category for describing all those attacks involving breaking into systems and networks by using known vulnerabilities of hardware and software assets, including interception and network attacks. Such attacks can take place at the borders considering the vast reliance on wired and wireless networks, e.g., drones, remote cameras and radio communication devices, possibly to steal sensitive data.
- Social engineering is defined as the act to influence a person to take action against their personal or organization's interest, including disclosure of confidential information (Sutton, 2017). A typical attack type is 'phishing' which is the process of attempting to obtain personal information, e.g., credentials from a target, using techniques like mass emails, which entice recipients into clicking a 'legitimate' website but in fact they end up in a phishing website (Computer Security Fundamentals 4th Edition, 2019). Border guards could be deceived by social engineering attacks, so that malicious actors can gain further access to a range of systems or even the border databases. Such attacks could be also addressed to other relevant stakeholders, such as third-party service providers, persons with access to the database servers, airport and port staff, as a way to gain cyber access to the border systems.
- Advanced Persisted Threats (APTs) are sophisticated and focused network attacks in which an individual or a group gains access to a network and stays undetected over a long period of time. APT groups may obtain open-source intelligence or use social engineering methods and perform monitoring of a specific target, aiming at high-value information in companies and governments, usually in a long-term campaign involving different steps, and they are potentially funded by governments (Chain, Desmet, & Huygens, 2014).

The list above provides a broad categorization and description of threat types mainly affecting border control infrastructures. Moreover, threat types should not be seen in isolation but, sometimes complementing or even overlapping each other, e.g., APTs might use sophisticated malware as a main tool for their attack, whilst social engineering attacks may be the first step before spreading malware.

The coherent overview of the cyber-threat landscape should certainly incorporate the different threat actors as well. Gaining a good understanding of the threat actors and their motives is essential to prioritize decision-making and effectively address the relevant threats. In terms of threat actors, there are those that unintentionally impact assets and those that have a malicious intent. Unintentional human errors can be caused by a variety of factors, e.g., lack of sufficient training, lack of a proper security policy in place, lack of skills or negligence. This dimension does not only apply to the custom officers or border guards but also to the wider border community, e.g., airport and port staff, service providers, etc. On the other hand, there are several threat actors with a malicious intention, in particular: a) Insiders motivated mostly by financial gains, for example corrupted border guards. b) Irregular travelers are all those persons trying to enter/exit the borders without fulfilling the legal requirements, e.g., by presenting fake documents. c) Nation States is a main category of threat actors as they have the adequate resources for sophisticated attacks, while they can use advanced technology and methods.

Main motive is espionage, seeking to gain access to sensitive information, such as personal data and commercial information. In the frame of a warfare, their motive could be even harming national security or disrupting critical infrastructure. d) Criminals and criminal groups are largely driven by financial gain and try to exploit different vulnerabilities to achieve their target. Examples of criminal groups include migrant smugglers, drug and weapon dealers. e) Cyber-criminals are all malicious actors using cyber techniques, usually in an attempt to generate money for example by selling personal data in the dark-web. In addition, these actors could offer their services to criminal groups to facilitate their illegal cross-border activities. f) Terrorists may use the borders for illegally trafficking small arms, weapons, and explosives (UNCCT, 2018), whilst illegal border crossing could be part of a plan for a terrorist attack. g) Activists are driven by the willingness to affect the political or social change and some of the respective groups are exclusively dedicated to a struggle against border controls, e.g., the "no borders" movement.

It is common that synergies are established among the different threat actors. Some examples are:

- Nation States could "instrumentalize" the migration flow as a part of their political agenda, whilst borders can be a favorable target for long-term espionage campaigns undertaken by cyber-criminals.
- An organized crime group might facilitate irregular travelers, using the classified information provided by insiders.
- A cyber-criminal can be used by traditional criminals for accessing patrolling information or gaining access to the surveillance equipment.

Of course, threat actors are highly flexible and can constantly adjust their attack strategies, for example, a malicious actor can easily target another border post, if the one initially targeted is well secured.

Cyber-threats are a modern challenge for the border infrastructures and specific actions are required to reduce the vulnerabilities and mitigate the impact of a cyber-attack. Border control shall be considered a "critical infrastructure" requiring a multifaceted security approach: staff trainings, focused risk assessments, enhanced information exchange and strengthened collaboration with the private sector. It is also important to keep privacy and fundamental rights as essential parameters of every policy, since these aspects need to be well protected.

Technology solutions could also help amplify security states in borders. Absolute security cannot be guaranteed, however, a holistic security approach focusing on enhancing awareness and preparation of people, implementing appropriate technologies and processes would assist in minimizing risks and protecting the operation of border control infrastructures (Chatzis & Stavrou, 2022).

Petros Chatzis, is a Specialist – Border Management.
Eliana Stavrou is Assistant Professor in Cybersecurity and Course Leader of MSC Cybersecurity, University of Central Lancashire, Cyprus.

It's Time to Move Past the Password!

Source: https://i-hls.com/archives/115510

Aug 10 – Even in such a developed and still advancing digital world like ours, we still don't seem to be able to ditch passwords. Undenounced to most of the population, passwords pose a much bigger security threat to the user than other more nefarious looking tools. They provide little to no protection against even common cyber security attacks. Despite a seemingly endless string of hacks, attacks, breaches, and breakdowns — 81% of hacking-related breaches are caused by password issues.

Since passwords have become so standard it is almost impossible to get rid of them. As a result, digital experts have advised the use of MFA, or multifactor authentication. According to darkreading.com, most organizations and many consumers recognize the need to move beyond password-only authentication. Yet two-factor authentication (2FA) and even many MFA techniques were never designed for today's sophisticated digital frameworks. Design, usability, and functionality are all critical. There's a need to convince people to move beyond a basic password and adopt MFA, but it's also critical to deploy higher grade MFA methods while moving to password less.

The reasons for this reticence are at least partly rooted in the nature of today's online world. For better or worse, people expect Web pages to load instantaneously, and they seek access to accounts without any latency — even when dozens of APIs and servers around the world are required for a transaction.

Yet it's also clear that MFA frameworks can be a big hassle. Oftentimes, it's necessary to request a text code or pull out a phone and open an authenticator app from Google or Microsoft and type in a code. Meanwhile, physical tokens offer stellar security — but they can be difficult to set up and use.

"There are too many companies giving too little thought to how to implement more advanced MFA and password-less systems," says Jason Casey, CTO for authentication vendor Beyond Identity. "You can't build a security architecture without considering design and usability. As the level of friction goes up, participation goes down."

The Medical Field Must Increase Cyber Security

Source: https://i-hls.com/archives/115683

Aug 19 – A recent report done on cyber security in healthcare concluded that the increased access to data creates more opportunities for security vulnerabilities in the medical device sector. Medical analysts state that the healthcare, pharma, and medical device sectors are particularly susceptible to cyberattacks. Devices like insulin pumps, heart pacemakers, inhalers, and wearables track patient data in real-time and even transmit to the user's phone, making the data immediately accessible to both the patient and their doctor. The more medical devices become connected to each other via remote medicine, the harder it will be to ensure the security of private patient information.

"Medical history cannot be changed, unlike identification and credit card information, making it invaluable to hackers and resulting in high costs for healthcare data breaches," said medical analyst at GlobalData, Ashley Clarke. Clarke informs that hackers can use healthcare information to create fake insurance claims, buy and sell medical equipment, or acquire illegal prescription medications.

Futureio.tech stressed that according to reports of breaches by the U.S. Department of Health and Human Services Office of Civil Rights, over 41 million individuals in the US were affected by healthcare data breaches in 2021.

"This change in technology means that medical device companies and their business associates are now responsible for increasingly large amounts of sensitive electronic patient data and have fallen prey to a significant amount of data breaches in recent years," said Clarke.

Without securing all components of the cybersecurity value chain, medical device companies will remain a primary target for hackers Clarke adds that "It's crucial for companies to invest in a variety of technologies such as chip-based security, network security, and cloud security, at every stage of the product development to ensure patient information is safeguarded. Older legacy devices may be unable to receive security patches, but new devices should have a security update plan in place for their entire device lifecycle."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS

Flood the Zone with Cheap Drones

Source: https://www.lawfareblog.com/flood-zone-cheap-drones-0

Attack drone Aralez Davaro

July 22 – The U.S. government has provided substantial support to the Ukrainian military since the Russian invasion, including supplying Ukraine with sophisticated rocket systems, artillery pieces, surface-to-air missiles, and a host of other items totaling billions of dollars. With the war in Ukraine entering a sustained phase, the U.S. should not only maintain this stream of aid to Ukraine but also develop and provide new systems specifically tailored to the nature of the ongoing conflict.

In particular, the U.S. military can design and manufacture low-cost suicide drones (also known as "loitering munitions") for transfer to the Ukrainian military. A suicide drone is a small drone that can be remotely controlled to crash into a target, giving a precision-strike capability to anyone who can launch such a drone. This could both support Ukrainian forces and serve as a valuable exercise for the U.S. military's own innovation capabilities.

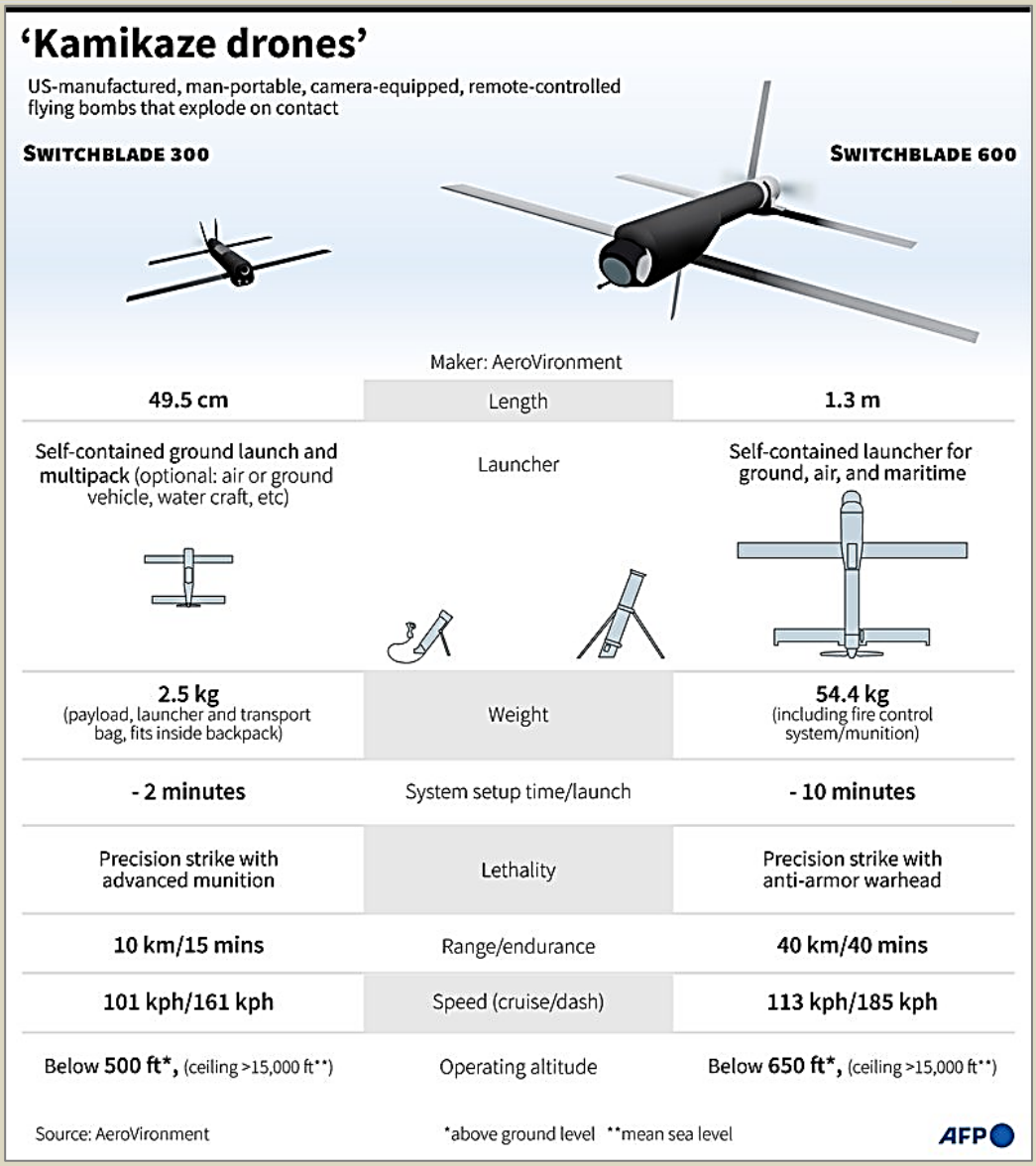
The continuing footage provided by small drones in the Ukraine area suggests an exploitable problem with Russian electronic warfare capabilities. These small drones are remote controlled, and the Russians seem to be neither effectively jamming nor attacking the drones' controllers with artillery fire. This suggests a stunning deficiency in Russian military operations, one that the Ukrainian military—with quickly deployed foreign systems—should be able to further exploit.

The U.S. has already begun to supply "low cost" Switchblade drones—small suicide drones with an explosive payload. The payload in these drones is not much, roughly equivalent to a 40 millimeter (mm) grenade. The U.S. military has agreed to deliver 700 Switchblade 300s, which at an estimated $6,000 each, represents an investment of over $4 million. The

Switchblade itself is fairly sophisticated: It is launched from a portable tube launcher, and, after a target is selected, it flies into the target and explodes just before impact.

Switchblade drones

But the key aspect is that a small explosive warhead, a mere 200 grams for a 40 mm grenade (just 33 percent heavier than a baseball), is remarkably effective when combined with the precision of a drone. Consider a long-ranged howitzer weapon and its crew. An artillery shell with 10 kilograms of explosive that lands 100 meters from the target will do less damage to personnel and equipment compared to a simple grenade delivered by a drone to explode on top of the gun's breech.
But "low cost" by U.S. military standards is still too expensive for supporting Ukraine in a war where Russia is firing 60,000 artillery shells per day. The Ukrainian military needs systems that are actually low cost, not "low cost" by our standards. It needs suicide drones that cost $500, not $6,000.
Given the permissive electronic warfare environment, it is reasonable to crash develop and deploy, en masse, such inexpensive systems with a range of more than 4 kilometers and a lethal payload equivalent to that of the Switchblade. A $10 million budget could then flood Ukraine with 19,000 easy-to-use suicide drones (at roughly $500/drone) and 1,000 ground stations (at roughly $500/station). Basically 10 times the drones for the same amount of money. Such a design need not rely on outside contractors but could use in-house U.S. military expertise to design and build.



How can one design such drones?
One begins with an airframe. The Switchblade uses a custom airframe in order to be launched from a tube. But if the operators are willing to throw the drone into the air by hand or use a giant rubber band, there are much cheaper alternatives.
The design would start with a medium-sized model airplane, such as this polypropylene foam fixed-wing design ($200), which is made out of the same material you find in car bumpers and can easily carry a grenade's worth of payload.
Such drones need power, but a rechargeable high-capacity battery costs just $60. This should provide sufficient endurance for a half hour of flight. It then becomes simply a matter of developing a control system. Later on one could add some low-cost autonomy (something I'm working on myself in my new start-up). But if the U.S. wants to ship something today, it should be purely human controlled.
The components necessary for human control already exist, such as this long-range receiver with basic stabilization ($40). Stabilization routines make the drone remarkably easy to fly, as it operates under the same "fly-by-wire" logic present in a modern airplane: Instead of the inputs directly controlling the drone, it translates "pilot intent." This also means a loss of communication can put the drone into a mode where it just continues to fly in a straight line. If the operator lines up a drone on

a nonmoving target, subsequent jamming from an adversary won't stop the drone's impact. Thus any jamming must be accomplished before the operator lines up for an attack.
To complete the system, add a camera ($50) and a video transmitter ($50)—which allows the pilot to see from the drone's viewpoint. Then 3D print an internal frame and add whatever $10 servo (a small electrically controlled motor) is needed to arm the explosives. Hit the drone with a coat of sky-blue spray paint, install the warhead, and the drone is complete. Total cost, excluding the warhead, should be roughly $500. Now all that is needed is a ground station to control the drone—which would include a standard hobby radio ($200), a transmitter module ($65), a video receiver ($90), and a battery charger ($70).
Such a system would require almost no training: The airframe is easy to assemble in the field (just attach the wings, pair the receiver, power the drone, and arm the warhead); it is hand launched; and the stabilization routines in the receiver make it easy to fly. A few hours of training should be sufficient (especially given the video-game reflexes of the modern generation). And existing drone simulation software can be modified to further enhance training.

Initially in the rush to field systems, it makes sense to use standard transmitters. But in the long run, this represents a vulnerability: A radio transmitter can be detected and targeted. Subsequent revisions need to make some changes. Fortunately the design of the radios will make revisions to the transmitters relatively easy, as the actual transmitter that broadcasts the controls is a distinct component and can therefore be swapped out without too much trouble.
When making operational improvements to the transmitter, instead of installing the transmitter module directly in the radio, it would be necessary to design and fabricate a relay module. This would consist of two pieces—one in the radio and one connected to the transmitter—linked by a long wire. This way the soldier's transmitter would be a significant distance from the drone itself, reducing the ability of a competent adversary to direct accurate fire onto the transmitter.
Designing drone systems in this way is clearly not "military grade" engineering. Instead it is cheap and, truth be told, janky engineering. But an enemy soldier is no less dead if the 200 gram explosive payload is delivered by something cobbled together from the hobby market rather than built through quality engineering. The goal is simply to effectively deliver the payload to the target as cheaply as possible.

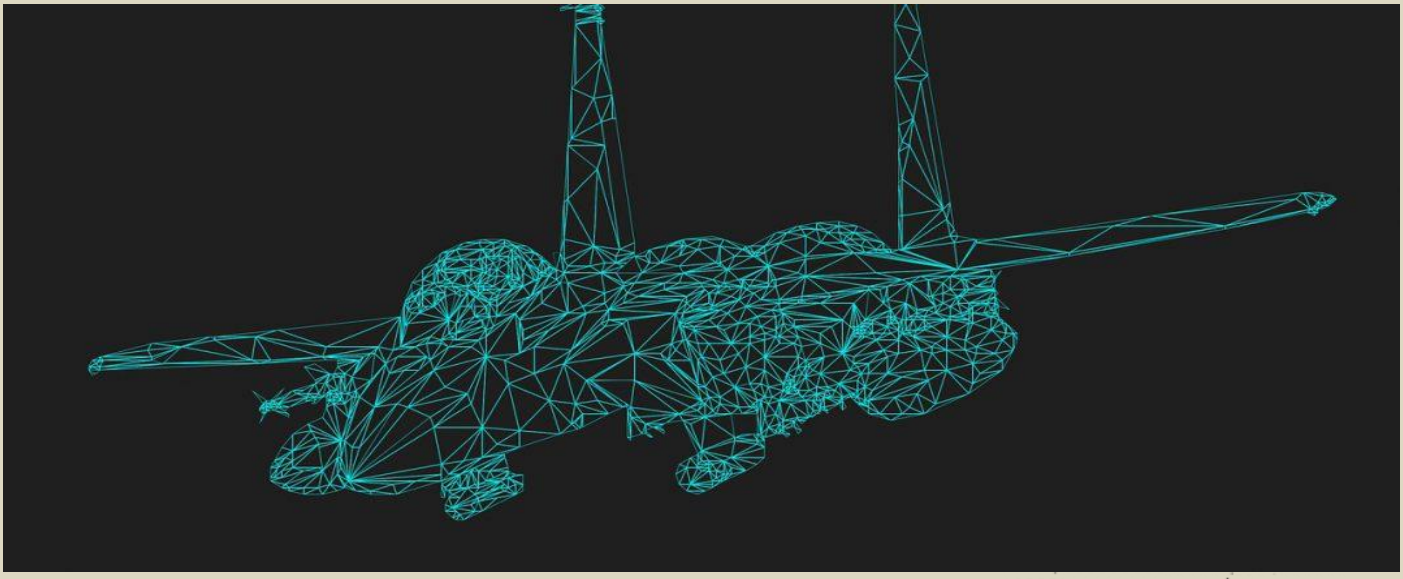
Who should design and build these systems?
Once military contractors get involved, the price multiplies exponentially. This would eliminate the cost savings and probably increase the time to market. Fortunately, however,

the U.S. military has the resources to design and build such drones in house without needing to rely on contractor support.
For example, the Air Force has a series of innovation labs at bases throughout the country. One such lab at Travis Air Force Base, the Travis Spark Lab, has the necessary resources and internal expertise—including experience with small drones and additive manufacturing. Additionally, the military academies could use this as an exercise for their senior engineering students, all of whom should be up to this task. Provide this as an assignment to the personnel at Travis and the cadets at the Air Force Academy in Colorado Springs, give each team a $20,000 prepaid credit card to order the necessary materials, and they could probably be flying in a week, refined in two, and shipping in three. Even better it could be a contest: Four Teams (Travis, Colorado Springs, the Military Academy at West Point, and the Naval Academy at Annapolis), Three Weeks, One Mission. By the end there would almost certainly be at least one if not four fieldable systems. Then to continuously refine the systems, the U.S. should settle into a repeating cycle of design, produce 500, and ship to Ukraine. This would not only act to support Ukraine with a substantial number of otherwise unavailable precision resources, but it would also serve as a test and—hopefully—demonstration that the U.S. military's innovation labs have the capacity, in house, to provide capabilities at a price that no contractor could match.

All that would be left to do would be monitoring and improving the airframes and the electronics based on tests and feedback from the Ukrainian customer base. Changes might include encrypting transmitters to prevent hijacking, switching airframes to deal with supply chain limitations, the addition of optional **psychological effects** (such as a version of a Stuka's siren), switching from an integrated warhead to a design using a reloadable 40 mm grenade launcher, or other changes as driven by customer demand.
The ability of such drones likely won't last forever. If Russia is willing to deploy broad-spectrum electromagnetic (EM) jamming (which would most likely disrupt their own small drones), it can stop the attack. Quick EM triangulation could identify the transmitters as well, though the transmitters should eventually be placed well away from the actual controllers using relay modules—w hich would largely negate the threat posed by EM triangulation. But until Russian forces bolster their EW capabilities, they would face a swarm of lightweight drones.

Super Hornet and UAVs – Controlling Swarms Right from The Cockpit

Source: https://i-hls.com/archives/115162

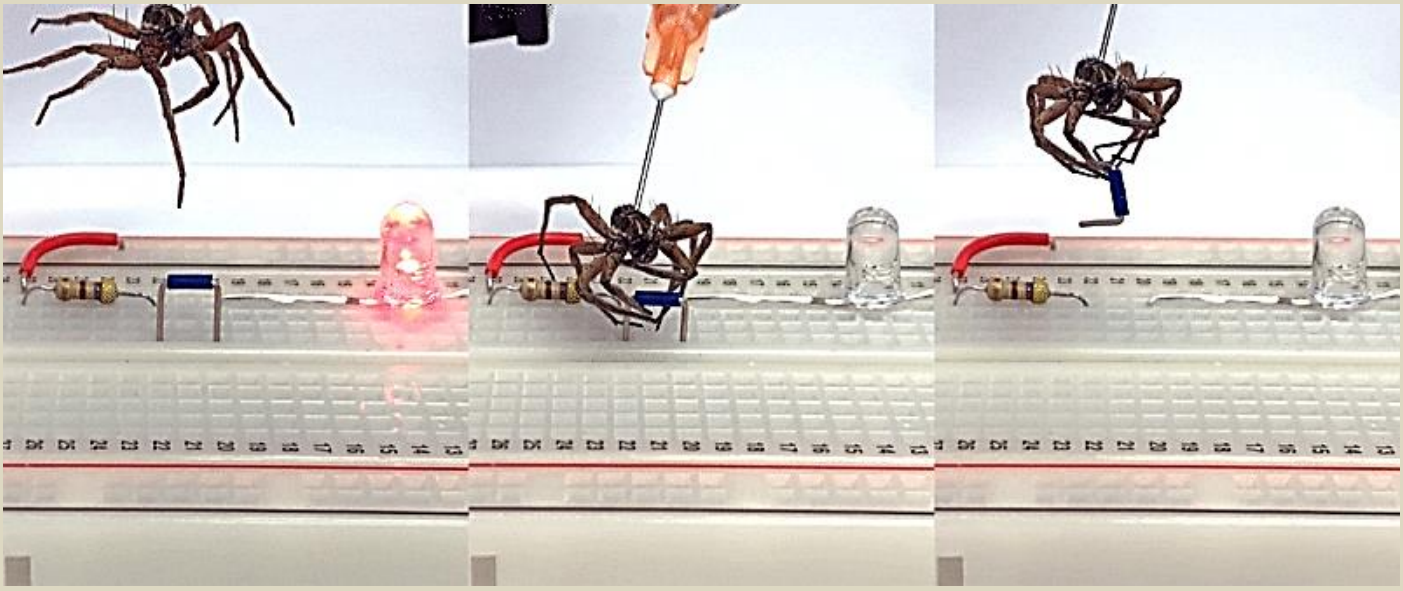


July 24 – The Pentagon has proclaimed time and time again that it seems as though manned-unmanned teaming, collaboration between piloted planes and autonomous

drones/robotic wingmen, as a key component of future warfare. Recent news has only facilitated this point of view.
As of late, the US Navy and its industry partners recently conducted several flight tests that demonstrated the ability of manned F/A-18 Super Hornet fighter jets to team with unmanned aerial vehicles (UAVs). This is one of the Navy's steps to a manned-unmanned future. Fedscoop.com reports that a series of four flight tests recently conducted by the F/A-18 and EA-18G Program Office (PMA-265) at Naval Air Warfare Center Weapons Division, California, successfully demonstrated the ability of a Block III Super Hornet to command and control three drones, according to a Naval Air Systems Command (NAVAIR) press release.
"During the flight tests, F/A-18 pilots entered commands into a third-party tablet instructing the UAVs to perform various maneuvers used in combat missions. The tablet was connected to the Block III's adjunct processor, which transmitted these commands to the UAVs. The UAVs successfully carried out all commands given by the pilots," Navy representatives proclaimed. The press release did not identify what types of UAVs took part in the tests or what combat maneuvers they performed.
These new experiments act to further develop and refine technologies that could potentially be incorporated into Navy platforms, and over platforms around the world. The analysis of the data captured in these trials is crucial to the teaming of manned and unmanned vehicles. "Future fighter pilots will be the quarterback of the skies, orchestrating commands and controlling UAVs from the integrated Block III touch-screen cockpit," said Mark Sears, Boeing vice president and program manager of F/A-18 and EA-18G programs. "Block III Super Hornet is the bridge to the future and is a risk reducer for the Navy that is delivering on teaming, networking and interoperability now."
"As part of a Joint All-Domain Command and Control network, teams of UAV conducting ISR missions led by the latest Super Hornets equipped with network-enabled data fusion and advanced capabilities would provide warfighters across the Joint Force with significant information advantage," Scott Dickson, Boeing's director for multi-domain integration, said in a press release.

Dead Spider Becomes Robot Gripper: It's Necrobotics!

Source: https://hackaday.com/2022/08/01/dead-spider-becomes-robot-gripper-its-necrobotics/



The process of making necrobiotic grippers with wolf spider carcasses. Credit: Preston Innovation Laboratory, Rice University

Aug 01 – Robot arms and grippers do important work every hour of every day. They're used in production lines around the world, toiling virtually ceaselessly outside of their designated maintenance windows.
They're typically built out of steel, and powered by brawny hydraulic systems. However, some scientists have gone for a smaller scale approach that may horrify the squeamish. They've figured out how to turn a dead spider into a useful robotic gripper.
The name of this new Frankensteinian field? Why, it's necrobotics, of course!

Working With Nature

Scientists and engineers have long held reverence for the achievements of the natural world. Tiny insects are capable of feats far exceeding those of our greatest robots, and can operate independently for days or weeks without ever needing to be plugged in. The intricate mechanical systems of spiders and beetles are beyond even our finest engineering to date.

Spiders are particularly impressive. They have eight legs of surprising strength, especially given their weight and power requirements. Rather than try to create something to match these capabilities from scratch, a group of researchers at Rice University decided to simply hack the spiders themselves.

Spider legs only have muscles for retraction, while extension is achieved via a hydraulic mechanism. In the spider's body, a chamber filled with blood expands and contracts to control the movements of the creature's legs. Each leg has a valve that allows the spider to control their movement individually. After death, all these valves open up and the spider's hydraulic system loses pressure. This is what causes a spider's legs to curl up after death.

The researchers realised that they could tap into this hydraulic system to extend and contract the spider's legs at will. With a dead spider, all the individual leg valves typically fail open, so control is limited to extending or contracting all the legs at once. This causes the dead spider to act like a robot gripper, just like you might see on a skill tester arcade machine.

Researchers worked with wolf spiders, and began by euthanizing them in cold temperatures. A needle was then inserted into the spider's body, and sealed with glue. This allowed the hydraulic passages inside the spider to be pressurized with air to extend the legs. Releasing the pressure lets the legs contract again into the curled-up position.

Testing and Applications

The dead spiders are surprisingly robust. In testing, the group was able to get over 1,000 open-close cycles out of a single spider carcass. Some wear and tear was notable at the higher end of this range, which the team believes is primarily due to the dehydration of the spider body. Research is ongoing as to whether this problem can be solved with special polymeric coatings to keep the body from drying out. Lifting power was also impressive. Wolf spider bodies were reliably able to lift 130% of their own body weight. Some bodies would exceed this figure by a great amount, too. Of course, variability is to be expected when working with a carcass as an engineering material.

The team believes that dead spiders could serve as useful actuators for small-scale pick-and-place tasks. Demonstration from the team included using a spider gripper to pull a jumper out of an electronic breadboard. Other examples involved moving small objects and even lifting another spider. The benefit of the necrobotic gripper is that the spider's eight legs are good at gripping objects of odd shapes and sizes. The team also cite the renewable nature of the necrobotic gripper. "The spiders themselves are biodegradable," said Daniel Preston, assistant professor of Mechanical Engineering at Rice University. "We're not introducing a big waste stream, which can be a problem with more traditional components," he adds.

However, the necrobotic grippers as shown do have some limitations. A usable service life of 1,000 cycles is relatively low for a robotic gripper, particularly one to be used in a mass-production environment. There's also a lot of variability in dead spider bodies that isn't seen with regular engineered robotic components. Additionally, while the spider carcasses themselves are biodegradable, the needles, glues, and plastic fittings are not. Plus, the production of spider grippers is time-consuming, fiddly work. Then there's the significant investment required in spider husbandry facilities.

The Future For Necrobotics

The research is compelling, and shows off reliable control of a stable spider carcass after death. It's also much simpler than other insect-robotics projects that use electrodes inserted into cockroach brains for control. There's no need to manipulate a living creature's brain, or fight against its natural instincts to make it complete a given task.

However, the research would raise ethical hackles for some. It's less troubling than electronically enslaving living beings, perhaps. Regardless, humans have always had strong feelings around the proper treatment and respect of mortal remains. Using spiders is likely to draw far less condemnation than if the same research were carried out with a mouse or hamster, for example. Try the same feat with a cat or a dog, and you might expect your lab to be closed with remarkable haste.

Just to be clear, we don't think you'll be using a spider-based pick-and-place any time soon. But work in the field of necrobotics will likely teach us a lot about how the bodies of animals and insects work. They may also guide the development of our own robotic or biomechatronic creations. In any case, the quest for knowledge often presents us with strange and meandering paths to follow. And sometimes, just sometimes… those paths are covered in spiders.

AUDROS tech would keep captured drones from falling on people's heads

Source: https://newatlas.com/drones/audros-drone-capture-system/

Aug 05 – There are now a number of systems in which "good" drones are used to disable "enemy" drones, such as those conducting spying missions. A new system takes a safer approach to the task, in that the captured drones don't simply plummet to the ground.

In many existing drone-vs-drone systems, the defending drone shoots a net at the enemy drone. The latter drone's propellers then get tangled in the net and stop spinning, causing the aircraft to fall to the earth. *Hopefully*, it won't hit anyone (or any cars, buildings, etc) when it lands.

The AUDROS setup's Eagle One octocopter, with its captured quarry – Dronehub

The European AUDROS (AUtonomous DROne System) project is developing a less risky alternative.
In the current version of the system, an **Eagle One octocopter** (made by Czech company Fly4Future – photo below) is based out of a battery-charging docking station (made by Polish company Dronehub).

When an approaching enemy drone is detected, the Eagle One autonomously takes off, flies to that drone's location, positions itself above that drone, then releases a row of dangling cords which are deployed from two-fold-out booms on its underside. The enemy drone's propellers get caught in those cords, just as they would in a net. Because the cords are still attached to the Eagle One, however, the captured drone stays hanging beneath it until it lands.
It should be noted that in at least one existing drone-netting system, the net stays attached to the defending drone by a tether after being shot out, so the captured drone doesn't just fall to the ground. That said, because the Eagle One has two booms' worth of cords, it can capture *two* drones per flight. By contrast, most net-shooting drones have only one net, so they have to return to their base after bringing down just one other drone.
The system was recently successfully tested in the Czech Republic, in close cooperation with the Czech prison service – one possible application of the technology would be to keep drones from being used to smuggle items into or out of prisons. Along with Fly4Future and Dronehub, other partners in the AUDROS project include Czech companies BizGarden and GINA Software.

Robots Will Take Over These Five Sectors

Source: https://i-hls.com/archives/115481

Aug 08 – The advancements in technology and rise in developments of artificial intelligence, virtual reality systems and more are sure to have a massive impact on our world. Many of these ripple effects will be advantageous, while some might be more malicious. According to cybernews.com, many workers worry about the risks of automation and whether it could mean the end of their employment. The rise of automated skills and roles will sweep up large parts of the workforce in its wake – but it'll take a little while to do so. There are several sectors that might feel the automation take over effects sooner than others, 5 to be exact.

First is the **customer service industry**. The recent COVID-19 pandemic has showcased to many of us that replacing human staff in the service industry was surprisingly easy and efficient in harsh economic times. The less human intervention, the better. However, total replacement is still largely in its early days.

Retail. Besides the great shift online, seeing us spend far more of our cash on online purchases than in person, we're also seeing smaller movements that indicate how important automation is going to be to the future of retail.

Transport. Automation already taking place in the driving seat is a signal of things to come. Transport drivers are one of the groups of workers most at risk of seeing their jobs replaced by automated alternatives because of the great strides already occurring in the field of transport.

Cargo. Loading and unloading shipping containers is partly done by humans and partly by robots, but the robots are winning. As they become more precise and able to understand where to place items, the role of humans in the system becomes less useful, and with it, the risk of automation rises.

Wait staff. Many restaurants already use robot waiters who deliver food to your table. It's a prediction of what's to come for the human staff working alongside them because wait staff in restaurants have been singled out as among the most at-risk group of employees.

How Do Israeli Troops Chat with Robots?

Source: https://i-hls.com/archives/115495

Aug 09 – The IDF has always been at the forefront of integrating technology with its martial tactics, and this development is no different. A new system, named Casper, will soon allow Israeli troops to talk to drones. Utilizing voice command technology, the soldiers will be able to use voice commands to communicate with unmanned systems. So far, the system can only understand Hebrew.

A representative of the Directorate of Defense Research and Development said the system is about voice dialogue between humans and machines. "It's called Casper, and we wanted the system to be a member of the team: a hybrid team of human and nonhuman operating and working together," the official told Defense News. "To make this happen, we needed the

drone as a team member so I can say 'go forward' or 'cover me,' and the drone can say it observes an objective 90 degrees from us, for example," the official added.

The official said 80% of the technology's capabilities involve controlling a drone's basic abilities, such as lifting off and flying to a certain height, while the remaining 20% is focused on commanding a drone to investigate or detect targets.

"We understood that we needed a new approach of operating systems on a battlefield," the official said, noting that these kinds of voice commands already exist in the civilian world. "On a battlefield, you need to be aware of surroundings, you need to look forward and have your hands on a weapon and not on a control [screen]."

The official added that the new technology is meant to make it easier for forces to identify and investigate targets, as well as close the sensor-to-shooter loop — the time it takes for different systems to communicate with each other.

The system is expected to be operational within the next several years.

EHang Announced Completion of EH216F's Technical Examination by NFFE

Source: https://www.ehang.com/news/798.html

July 2021 -- EHang Holdings Limited (Nasdaq: EH) ("EHang" or the "Company"), the world's leading autonomous aerial vehicle ("AAV") technology platform company, today announced it has successfully completed the technical examination of its EH216F AAV, the firefighting model, by the China National Fire-Fighting Equipment Quality Supervision Testing Center ("NFFE") as entrusted by the Company. The NFFE is a national firefighting equipment quality examination agency under the Ministry of Emergency Management ("MEM") of the People's Republic of China. Its nationwide responsibilities include standards development, centralized management, and technical guidance for firefighting equipment products, including firefighting unmanned aerial vehicles ("UAVs").

The NFFE's technical examination is widely used in the firefighting equipment markets and the MEM system and considered the cornerstone of quality for firefighting products in China. EH216F's successful completion of the technical examination certifies that it conforms to the firefighting UAV standards and requirements by the NFFE and we believe it will further enhance customer confidence and promote the recognition and adoption of EHang's high-rise firefighting solutions in the commercial markets in China and further abroad.

The NFFE conducted a comprehensive 10-month technical examination on EH216F and 52 different types of tests were completed in areas such as flight control functions, hovering and return accuracy, high/low altitude flights, electromagnetic compatibility, wind resistance, high/low temperature adaptability, vibration/shock resistance, radiant heat resistance and smoke performance.

EH216F undergoing the wind resistance test

EH216F was officially launched in July 2020. With key advantages in autopilot, quick response and cluster management, EH216F is designed to address pain points in urban high-rise firefighting and become a valuable complement to the existing firefighting system. This firefighting AAV model demonstrates the commercial capabilities of EHang's AAV technology in practical scenarios such as aerial firefighting and emergency rescues.

EDITOR'S COMMENT: This would be an excellent solution for the under-construction 200m high Riviera Tower, Athens, Greece [photo, right] – the tallest skyscraper by the Mediterranean Sea.

About EHang

EHang (Nasdaq: EH) is the world's leading autonomous aerial vehicle (AAV) technology platform company. Our mission is to make safe, autonomous, and eco-friendly air mobility accessible to everyone. EHang provides customers in various industries with AAV products and commercial solutions: air mobility (including passenger transportation and logistics), smart city management, and aerial media solutions. As the forerunner of cutting-edge AAV technologies and commercial solutions in the global Urban Air Mobility (UAM) industry, EHang continues to explore the boundaries of the sky to make flying technologies benefit our life in smart cities. For more information, please visit www.ehang.com.

Future Ballistic Missile Submarine Concept Unveiled At Russian Arms Expo

Flying Unmanned Submarine Developed in China

Source: https://i-hls.com/archives/115520

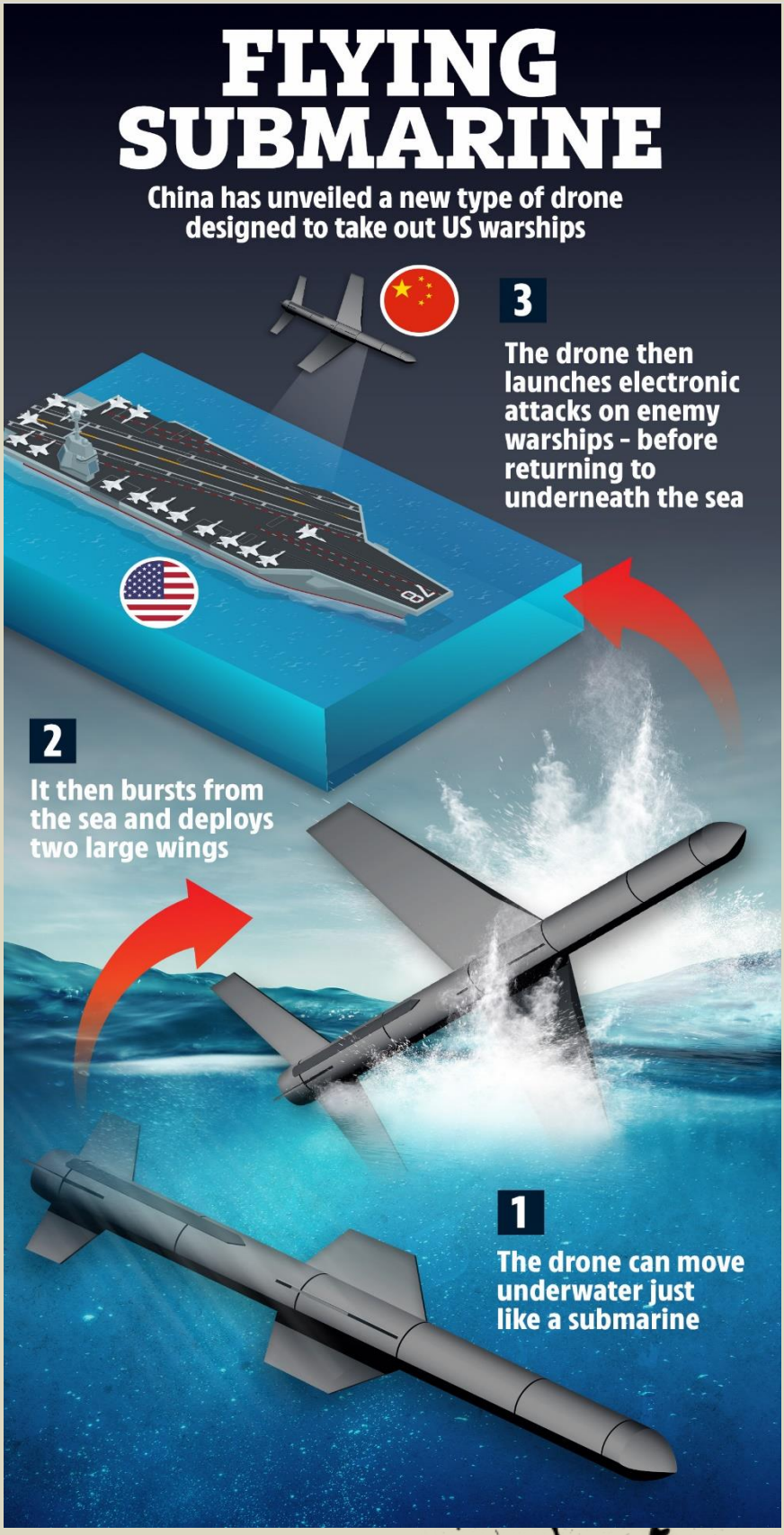
Aug 10 – A research team of scientists from eastern China have developed a prototype submarine drone that can fly at very high speeds. It is capable of carrying out both civilian and military activities, according to the researchers, and consumes little energy when in fixed wing mode.

The South China Morning Post reports that this unmanned drone is driven by four propellers that allow it to approach an underwater target slowly and linger in that area for a long time. Two large wings that fold over its back can extend when the drone reaches the surface of the water, allowing it to fly at a speed of 120km/h, about twice as fast as an ordinary drone powered by rotor blades.

It is possible that China has been developing numerous types of "transmedia vessels" that could travel in both air and water, supposedly for military applications. It is said that some even reached hypersonic speed. This type of transmedia vessel is one of the cheapest, most effective methods to cripple the defense system of an aircraft carrier fleet. The average defense system of a modern warship will not be able to detect this system as it can go underwater when detected by radar and resurface to dodge sonar. This flying unmanned submarine targets strikes accurately and effectively and is sure to become of use to the China's Navy.

The unmanned drone is equipped with an airbag that can be filled with water to adjust buoyancy so it can stay at a given depth without making noise with its propellers. When cruising in water with its wings folded, its streamlined body resembles that of a typical submarine, allowing for less drag and higher mobility.

According to the research team, the biggest challenge occurred during takeoff. If the vessel rises directly out of the water, the take-off process is unstable because of surface waves and the drone's simultaneous interaction with air and water. To fix this, they developed a complex control mechanism so that the submarine can glide on the waves before lifting.

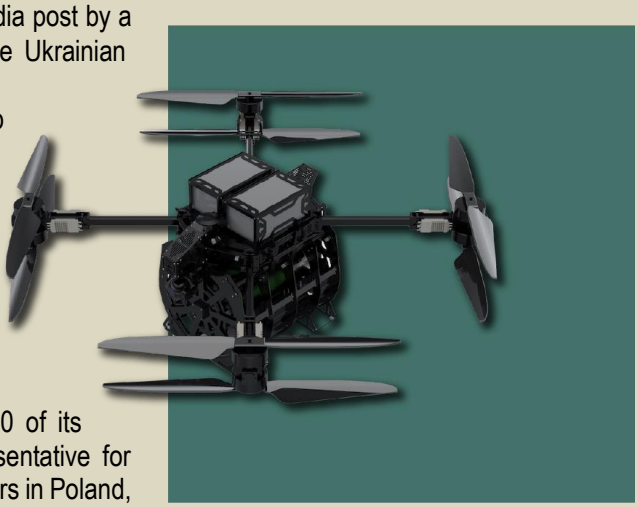


Taiwan's Revolver 860 combat drones being used by Ukrainians

Source [+video]: https://www.taiwannews.com.tw/en/news/4630475

Aug 18 — Taiwan-made Revolver 860 combat drones are reportedly being used by Ukrainian forces on the battlefield against Russian troops.

On Wednesday (Aug. 17), Oryx reported that Revolver 860 Armed VTOL UAV's have been sold to Poland and subsequently transferred to Ukraine. In June, CM Media (信傳媒) cited a social media post by a military enthusiast showing that the Revolver was being used by the Ukrainian military to carry eight mortar shells to be dropped on enemy troops.



The Revolver 860 military combat rotor drone can carry a payload of up to 42 kilograms, enabling it to carry up to eight 60-millimeter mortar rounds. It can stay airborne for 20 to 40 minutes with its four arms and eight propellors, depending on weight and wind conditions.

When CM Media contacted the Keelung-based manufacturer DronesVision for comment, given the "complex and changeable international situation," it only disclosed that it has buyers in Poland, which later delivered its products for combat in Ukraine and "should have already participated in battles."

When asked on Thursday (Aug. 18) to comment on claims that 800 of its Revolver 860 UAVs had been sent to the Ukrainian army, a representative for DronesVision told Taiwan News that the company only ships to customers in Poland, and it cannot comment on where those firms may later send the drones as it has signed non-discloser agreements with its clients. The spokesperson did say that customers in Poland have purchased the company's full range of UAV products. The representative said that purchases of the drones picked up in Poland in March, shortly after Russia invaded Ukraine, and have steadily increased since. According to the company contact, while direct shipments of its products to Ukraine have been severed due to the war, the number of drones ordered and the number of companies placing orders from Poland have steadily increased over the past five months.

●▶ **Read also:** AR-1 Assault Rotor Weaponized Drone and TR-2 Tactical Rotor Long Endurance Drone

Do armed drones reduce terrorism? Here's the data.

By Joshua A. Schwartz and Matthew Fuhrmann

Source: https://www.washingtonpost.com/politics/2022/08/18/drone-alqaeda-terrorist-attack/

Hellfire missiles onto an MQ-1C Gray Eagle

Aug 18 – At 6:18 a.m. on July 31, a CIA drone fired the two Hellfire missiles that killed al-Qaeda leader Ayman al-Zawahiri, a former deputy to Osama bin Laden. Since 9/11, the United States has conducted over 14,000 drone strikes like this against suspected terrorist targets. Countries such as Iran, Turkey, Nigeria and Egypt have also acquired armed drones and conduct their own strikes. But do armed drone operations reduce terrorism, or do they actually make countries more vulnerable to it?

To find out, we analyzed patterns of terrorism in 18 countries — every country that has fielded armed drones to date. The evidence reveals that obtaining armed drones reduces the amount of terrorism a country experiences. Armed drones may raise ethical concerns but appear to be an effective counterterrorism tool.

What drone pessimists believe

Some analysts argue that the use of drones increases terrorism for two main reasons.

First, drones can cause "blowback" among civilian populations, when drones kill or psychologically terrify noncombatants and violate countries' sovereignty. For example, data collected by the Bureau of Investigative Journalism suggests that U.S. drone strikes have killed up to 2,220 civilians since 2010, including up to 450 children. Blowback from drone strikes could motivate civilians to directly aid terrorist groups by joining them, providing material support or even carrying out lone-wolf attacks.

Second, drones may increase terrorism by empowering lower-level militants with a greater preference for violence. Drone strikes often target terrorist leaders — like Zawahiri — rather than rank-and-file members. This means a successful strike can have an unintended consequence: undermining the control that leaders have over their subordinates. So a drone strike can potentially backfire because lower-level militants are often younger and have a more limited understanding of the strategic pitfalls of attacking civilians, in comparison to the more experienced bosses they replace.

What drone optimists argue

Alternatively, drone optimists argue that drones decrease terrorism for two main reasons.

First, drones can disrupt terrorist groups by increasing the security risk to militants, making it harder for them to operate. For example, fear of drone strikes can cause terrorists to restrict their movements, reduce their communications, close their training camps, and become more distrustful of allies and potential recruits.

Second, drone strikes may degrade terrorist groups by physically removing leaders and key operators from the battlefield. Highly skilled individuals that can build bombs, fly planes, speak multiple languages, forge documents and avoid detection are critical to carrying out terrorist attacks.

What does the research say?

Most of the evidence on drone effectiveness, to date, comes from scholarship about the U.S. drone program. However, armed drones have proliferated rapidly around the world over the past decade. It's now possible to analyze the counterterrorism impact of armed drones beyond just the U.S. context. To do so, we've studied the full universe of cases: all 18 countries that acquired armed drones between 2001 and 2019, and the 11 countries that conducted drone strikes against any target during this period. We also examined the longer-term (yearly) impact of drones on terrorism. Some drone pessimists believe that the negative effects of drones only materialize in the long-term. But previous research focuses on the short-term (monthly, weekly or even daily) impact of drones on terrorism, which leaves analysis on the longer-term strategic impacts of drones unclear. We surveyed open-source materials to identify which countries fielded armed drones and when they obtained this capability. Using the Global Terrorism Database, we measured the number of terrorist attacks and deaths from terrorism in those 18 countries each year.

Next, we used statistical analysis to compare the rates of terrorism that these countries experienced in years before and after adopting armed drones. Our analysis accounts for other factors that could mask the true relationship between armed drones and terrorism, such as regime type, periods of civil war, GDP per capita, U.S. counterterrorism aid, and terrorism in neighboring countries.

Yes, armed drones do appear to decrease terrorism

Across statistical tests, we find evidence that armed drones decrease terrorism. According to our main analysis, obtaining armed drones leads to about six fewer terrorist attacks and 31 fewer deaths from terrorism annually. This translates to a 35 percent reduction in attacks and a 75 percent decrease in fatalities per year. However, these numbers fluctuate based on various modeling choices — which means we are more confident that drones decrease terrorism than we are about the specific amount by which it declines.

Most broadly, our study suggests that there is indeed a compelling counterterrorism rationale for utilizing armed drones to enhance national security. Although armed drone operations can be costly — for example, by causing civilian casualties — our findings strengthen the case that the benefits exceed the costs. However, the decision of when, how or even whether to employ armed drones remains a difficult one. For example, drone strikes specifically — and leadership targeting, more generally — may be less effective depending on the particular terrorist group's organizational structure and ideology. Drones are by no means a panacea and may not always be a net positive for the world. For the United States, our study implies that a strategy to combat terrorism "from over the horizon" using long-range technology such as drones could be effective. Skeptics of this strategy point out that withdrawing from Afghanistan makes conducting drone operations more challenging. As political scientists Sarah Kreps and Paul Lushenko wrote here at TMC last year, successful drone strikes require accurate and timely intelligence to identify targets, and this information can be difficult to collect from a distance. Yet the successful drone strike that killed Zawahiri demonstrates that the United States can conduct over-the-horizon operations to combat terrorism, even after withdrawing from Afghanistan.

For the world more generally, our results indicate that the military utility of armed drones makes acquiring this technology attractive to other countries. That means we should expect proliferation to continue apace.

Joshua A. Schwartz is a Grand Strategy, Security, and Statecraft Postdoctoral Fellow at the Massachusetts Institute of Technology and the Harvard Kennedy School.
Matthew Fuhrmann is a Professor of Political Science and Presidential Impact Fellow at Texas A&M University.

New Drone Can Sense Threatening Gases

Source: https://i-hls.com/archives/108633

Aug 18 – A drone-based micro-sensor technology will identify explosives from the air. Professor Otto Gregory of the College of Engineering at the University of Rhode Island has developed drone deployed sensors that can identify explosive materials, particles from a potentially deadly virus, and illegal drugs at the part-per-quadrillion level – single-molecule detection.

"The platform is broad-based, so you can apply it to lots of different venues, with lots of different end-users," said Gregory.

The research is largely funded by the Department of Homeland Security, as well as by other government agencies. "This project started as a DARPA-funded project mainly to look at toxic gases — threats that would be used in gas warfare, and when I say gases, chemical weapons," said Gregory on GoLocal LIVE (golocalprov.com).

Gregory said the directive from the federal funding agencies was to look at "threats that could be put on airplanes, put in public transportation venues, subways trains — all those venues that were targets."
Gregory said the Department of Defense may be interested in using it to monitor wounds in soldiers. If a soldier or first responder suffered an open wound from shrapnel, Gregory's sensors could help determine if the wound became infected. The development can also detect roadside improvised explosive devices (IEDs).
According to Gregory, the U.S. Coast Guard has shown an interest in using the technology to "sniff out" illegal drugs being smuggled into the United State aboard ships.
"By decreasing the thermal mass of the sensor, we've decreased the amount of power required to run the sensor," said Gregory. "We started with a thermal mass on the order of grams. Now the thermal mass of our sensor is on the order of micrograms."
He says one of the keys to making a device as small and powerful as Gregory's is to find the right battery. "We have partnered with a company that makes very thin, low-mass batteries in Colorado called ITN Energy Systems," Gregory said. "They make lithium batteries that are no thicker than a piece of paper. The process has been about finding the right partners, which helps us improve our catalysts and improve our sensor platform."

The Future of Drones – Beyond Visual Line of Sight

By Mark Andrews (Soliton Systems, Live Streaming Consultant)
Source: https://border-security-report.com/the-future-of-drones-beyond-visual-line-of-sight/

Aug 01 – As drones become almost ubiquitous in their usage for law enforcement and other public agencies, what advances are likely to come with their continued deployment?
Drones and UAVs (Unmanned Aerial Vehicles) are used for a variety of operational or situation awareness applications from evidence gathering, looking for missing persons, coordinating rescues, surveillance, and crowd control. Monitoring with drones is often used as a low-cost replacement for helicopters.
Outside of public safety drones are also heavily used in other industrial applications, for example in the energy industry they are used for inspection of powerlines, pipelines and windmills and in agriculture they are utilized for measuring the health of plants on large farms.
The one major restriction of drones currently is that they must be with the eyesight of the operator, restricting how far a drone can travel and restricting how effective a tool it can be, for example with border control and the potential thousands of kilometers that is required for coverage from a single location. But with so much adoption of drones across many industries, it is only natural that they will move onto the next generation of evolvement – in this case drones that can fly Beyond Visual Line of Sight (BVLOS).
One of the major considerations for utilizing BVLOS is the issue of safety and the risk of collision with other Unmanned Aerial Vehicles (UAV's), aircraft, buildings, and even trees. There are many initiatives being worked on to address this. Flying commercial drones is highly regulated, especially when it comes to even allowing companies who want to develop BVLOS drones being given permission to test. These regulatory authorities such as the Federal Aviation Administration (FAA) in the US and the European Union Aviation Safety Agency (EUASA), with the guidance of The Royal Netherlands Aerospace Centre, are responsible for issuing permits to develop BVLOS drones in tightly controlled environments. The majority of permit requests for the BVLOS to the FAA are currently rejected.
BVLOS of drones is not new, Amazon have spent a small fortune since 2012 in developing delivery drones and the military has been using UAVs for many years for surveillance and delivering ordnance. The big difference is that these drones are used for payloads with differing requirements – BVLOS for border control ideally need a real-time "eye-in-the-sky" for monitoring, surveillance and evidence gathering though these requirements are expected to evolve.

How do we make BVLOS drones safe to operate from a remote teleoperations center?
One strategy is the BVLOS Sense and Avoid. This is a detect and avoid system, also known as sense-and-avoid, where drones can detect obstacles and then make rapid adjustments to their flight plan to avoid a collision. Collison avoidance technologies such as LiDar, acoustic sense & avoid, ultra-low latency live video, and radar are all technologies that are being developed. These outputs from the drone can be used by AI technology, either locally or remotely, to automatically detect and avoid obstacles.
A second technological breakthrough with a BVLOS drone is to have a flight view of the onboard camera that can be used for real time manual navigation from a remote location. This allows the drone to be manually flown from a faraway position which would open a whole range of new possibilities for the use of drones. New technology with ultra-low latency that can live stream over multiple cellular networks while controlling the drone from a remote location is changing how drones can be used effectively in the fight against illegal border crossing.

In both cases security is paramount – any chance of a hacker either controlling the drone or intercepting the live stream must be mitigated against.

What are the applications for BVLOS?

The possibility of BVLOS drones is going beyond how drones are used today. Imagine the border control agents being able to monitor vast areas of country without the need for regular relocation. The ability to implement a missing person search or a mountain rescue can be much more effective with BVLOS then they are today with line-of-sight drones.

It is expected that once firmer regulations are enacted, the market will continue to open to new players and applications with BVLOS drones becoming routine. It is expected a new sky control system, or an Unmanned Traffic Management (UTM) system, an air traffic control equivalent for drones, will be put into service that will ensure drones and UAV's can interact and operate safely, especially over busy cities. This will include a range of exciting new possibilities such as urban air mobility (UAM). UAM will include vehicles like air taxis, which can revolutionize travel and will advance enormously how taxi services are operating today. UAM vehicles will have practical applications with point-to-point low-altitude air-travel, such as lowering the time of commutes, journeys to airports. It will also allow the delivery of emergency personnel and first responders into areas that are difficult to access, either through natural disaster or war, and then using the same drone technology, it will evacuate people and onto hospital as required.

Initiatives such as Fast Forward 2020 is a three-year collaborative research project that will develop a new Urban Air Mobility (UAM) ecosystem to demonstrate safe drone deployment in urban cities and its integration into Smart City infrastructure with the feedback utilized to create the necessary regulations. With many companies and universities involved, researchers are looking at technology beyond current levels including the implementation of new 6G infrastructures. Such initiatives really demonstrate how much is yet to be done and the growth-potential there is within the drone industry.

Live Streaming with Drones

A major element of BVLOS technology is the live stream from the onboard camera for remote control. These cameras typically have low levels of power and high reliability, but importantly they require an ultra low latency connection from the drone to its remote operator. And by low latency BVLOS datalinks would ideally need to perform below 100ms end-to-end. This must include all the video encoding and decoding that is normally a part of the process of any live video stream.

Typical latency for streaming is over a second, and with satellite connected drones this can be multiple seconds and the video can be compromised. Having latency below 100ms, especially for an untethered device such as a BVLOS drone, that would normally rely on either cellular or satellite communication, is especially challenging. RF (radio frequency) is another form of communication that has a low delay but relies on line-of-sight which becomes impractical with BVLOS drones.

The live streams generated from the drone are also used as real-time surveillance. The ability to capture video in ultra high definition (UHD) offers a new range of surveillance applications where AI is utilized for video surveillance to spot anomalies over vast areas.

Ideally drones can fly autonomously with data gathered from onboard instruments and sensors. Typically, these UAVs have long-range telemetry, as well as a command-and-control link with the user ground control station. It is using these secure data IP links that an encrypted live stream and return remote control can be sent and received.

With both the FAA and the EUASA already allowing some restricted BVLOS operations to take place, albeit in very specific and regulated circumstances, as technology evolves further it is expected that this industry will evolve quickly. The sights of drones carrying passengers flying over our heads, as often seen in futuristic science fiction movies, could arrive quicker than you think.

International CBRNE INSTITUTE

AI - NEWS

C2BRNE DIARY

Chess robot breaks seven-year-old's finger during tournament in Russia

Source: https://www.theverge.com/2022/7/25/23276982/chess-robot-breaks-childs-finger-russia-tournament

Photo by Gao Yuwen/VCG via Getty Images

July 25 – A chess robot broke the finger of a seven-year-old boy playing in a tournament in Russia, according to reports from local news outlets (seen via *The Guardian*).

The incident happened last week at the Moscow Chess Open, where the robot was hired to play competitors. Video of the incident (below) shows the machine is a standard industrial robot arm customized to move pieces on three chess boards simultaneously.

"The robot broke the child's finger. This, of course, is bad," Sergey Lazarev, President of the Moscow Chess Federation, told Russian news agency TASS (translation via Google Translate).

Said Lazarev: "The robot was rented by us, it has been exhibited in many places, for a long time, with specialists. Apparently, the operators overlooked it. The child made a move, and after that we need to give time for the robot to answer, but the boy hurried, the robot grabbed him. We have nothing to do with the robot."

It's not clear what explanation —if any — the robot's creators have offered for this accident, but such incidents are not unusual in scenarios where robot engineers have failed to properly consider safety protocol around humans.

In most industrial environments, robots are essentially unseeing operators. They move along set paths at set times, and often lack sensors to recognize or respond to nearby humans. In other words: if you move into their path, they won't know you're there.

This sort of blind collision has been the cause of many robot fatalities. The first such incident is generally thought to have taken place in 1979, when Ford factory worker Robert Williams was crushed by a robot arm. The US Department of Labor logs these deaths, which tally roughly one fatality a year, though the statistics vary based on different companies' definition of a robot. For example, is a conveyer belt a robot? Or a molding machine?

In the case of the chess robot, it seems the device was designed only to identify and move chess pieces — not respond to the appearance of a human hand in its playing area.
"There are certain safety rules and the child, apparently, violated them. When he made his move, he did not realize he first had to wait," Sergey Smagin, vice-president of the Russian Chess Federation, told a Telegram-based news channel Baza, according to *The Guardian*.
However, it's more accurate to say that the robot's designers violated safety rules by creating a machine that could inadvertently hurt humans. A number of basic features could have prevented the accident — from placing a camera above the chess board that disables the robot's movement if foreign objects appear in frame, to limiting the force that can be output by the robot's arm.
Although footage of the incident is distressing, according to Lazarev the child was soon recovered enough to continue to play. "The child played the very next day, finished the tournament in a cast, and the volunteers helped to record the moves," Lazarev told *TASS*. "The robot operators, apparently, will have to think about strengthening protection so that this situation does not happen again."

'Killer Robots': Will They Be Banned?

By Nina Werkhäuser (DW journalist)
Source: https://www.homelandsecuritynewswire.com/dr20220725-killer-robots-will-they-be-banned

July 25 – These aren't the drones that deliver your online order. Loaded with cameras, sensors, and explosives, their mission is to drive themselves to a target with an algorithm in the driver's seat. They destroy themselves along with the target, leaving behind just a pile of electronic detritus.
Increasingly, these sorts of weapons are the stuff of a manufacturer's promotional materials rather than science fiction movies. From today, a United Nations conference of 80 countries gathers in Geneva to debate whether to ban them or at least regulate them more strictly.

Machines Killing Humans
Autonomous weapons are, as their name suggests, able to select and attack targets on their own. That is unlike piloted drones and other weapons, which a human operator directs from afar. Arms manufacturers are taking advantage of the latest advances in artificial intelligence and machine learning to develop them.
The UN conference calls them "lethal autonomous weapons systems." Critics call them killer robots. They can take the form of drones, land vehicles, or submarines.
Some countries want autonomous weapons banned, arguing that an algorithm should never decide over life and death. Other countries want autonomous weapons regulated, with more or less binding rules of engagement that include some role for human decision-making.

Big Powers in the Way

The UN has been meeting twice a year since 2014 to debate the issue. The United States, Russia, and China are the loudest opponents of an outright ban on autonomous weapon systems or binding rules to govern their use.

Russia blocked the last meeting, which was scheduled for March, by refusing to accept the agenda. At that point, Russia's invasion of Ukraine was a few weeks old.

Autonomous War Crimes

"If an autonomous weapon makes a mistake and possibly commits a war crime, who's responsible?" asks Vanessa Vohs, who researches autonomous weapons at the German Armed Forces University in Munich.

For Vohs, accountability is one of several open questions.

The Geneva gatherings do not appear to be close to answering many of them, and Russia's war in Ukraine has added to the uncertainty. For some, it is more evidence to ban autonomous weapons. Others see the war as another sign that doing so is hopeless.

"There is evidence of Russia using autonomous weapons in this conflict," said Ousman Noor, who works for the Campaign to Stop Killer Robots. The NGO wants to see these weapons banned. "That could lead to the acknowledgment of urgently needing to regulate these weapons before they get sold the world over."

The US has reportedly sent the Ukrainian army several tactical unmanned "kamikaze" drones that can find their own target and explode on impact.

AI experts have long warned of the ease of producing small, armed drones in large numbers, which any IT student could program. "Without the need of a person to service these weapons, you can dispatch tens of thousands, if not millions, of them," Stuart Russell, an AI researcher, told DW. "We're creating weapons with the potential of being deadlier than an atomic bomb."

More Money for German Armed Drones

The war in Ukraine has motivated countries to spend more on their militaries, including investing in the latest weaponry. The additional 100 billion euros ($102 billion) that Germany is borrowing to top up its defense budget may go partly to buying fleets of armed drones or other advanced weapons systems that use AI.

Observers at the Geneva talks have said Germany's representatives there have so far remained reluctant to take a clear position. Few believe the multilateral discussion will result in a ban or any binding rules.

With reports of autonomous weapons already being deployed on the battlefield, there is an increasing sense of urgency to find a solution.

"That's why we need new rules," Vohs said. "Before we find ourselves in an apocalyptic scenario when something really goes wrong."

AI Will Be a Double-Edged Sword in Future Cyber Conflicts

By Max Smeets

Source: https://nationalinterest.org/blog/techland-when-great-power-competition-meets-digital-world/ai-will-be-double-edged-sword-future

April 2022 – "Artificial Intelligence and machine learning … [are] foundational to the future of cybersecurity. We have got to work our way through how we're going to deal with this. It is not the *if*, it's only the *when* to me," Adm. Mike Rogers, former chief of the National Security Agency and U.S. Cyber Command, remarked in an interview. During his presidency, Barack Obama shared his concerns about an attacker using artificial intelligence (AI) to access launch codes for nuclear weapons. "If that's its only job, if it's self-teaching and it's just a really effective algorithm, then you've got problems," Obama said.

AI opens up a set of new risks and opportunities for the military and intelligence community. It is, however, important to be more precise about how AI applications impact different types of military and intelligence activities. Discussing the use of AI in cyber operations is not about whether technology or humans will be more important in the future. It is about how AI can make sure developers, operators, administrators, and other personnel of cyber organizations or hacking groups do a better job. It is essential to understand some of the key applications of AI in future cyber conflicts—from both the offensive and defensive perspectives.

How AI Can Help the Attacker

There are several ways in which hackers can benefit from AI techniques to conduct cyber operations more effectively. First, AI technology might help in finding exploitable vulnerabilities. Finding unknown vulnerabilities is often done through a dynamic process called "fuzzing" in which an operator automatically inputs massive amounts of data, called fuzz, to uncover "response exceptions," or potential signs of vulnerabilities. AI will improve these fuzzing techniques. Researchers at the Pacific Northwest National Laboratory have already demonstrated that AI-based fuzzing, complemented with conventional fuzzing techniques, is faster and more effective than conventional fuzzing alone.

Second, AI might allow for more effective forms of social engineering. Spam emails can be automatically tailored to a target's profile. Similarly, chatbots fed with large amounts of personal data of users could engage in long conversations and gain a target's trust. AI applications will further enable the creation of so-called deepfakes, which are created by combining existing videos or images and overlaying other images. Deepfake apps and improvements in facial recognition software have brought the inexpensive and easy creation of content within anyone's reach—someone can simply download several facial images of a person, process them into a 3D image, and then use them in a deepfake video. It is not hard to conceive of a future in which deepfake bots will be able to masquerade as real people in live video chats to steal credentials or other information. One poorly executed application, a deepfake purporting to show Ukrainian president Volodymyr Zelenskyy capitulating to Russia, has already been seen in the Russo-Ukrainian War.

Third, AI techniques allow for the generation of malicious malware samples that can avoid detection by simulating the behavior of legitimate applications. For example, Maria Rigaki and Sebastian Garcia demonstrated that it is possible to avoid detection through the adoption of a Generative Adversarial Network, which models network traffic behavior that mimics a traffic profile, such as a Facebook chat.

Fourth, AI techniques may allow malware to spread itself more effectively. The Trojan downloader Emotet provides a glimpse of how AI-enabled propagation can operate faster than human directed operations. First identified in 2014, Emotet was originally designed as a banking malware that spread through spam emails. Over the years, Emotet has evolved, and its most recent versions are suspected to utilize machine learning to make Emotet more effective in targeting victims. "Despite attacking and compromising thousands of devices daily, it is surprisingly effective in avoiding researcher machines, honeypots and botnet trackers," researchers from ESET note. "To achieve this, Emotet collects the telemetry of its potential victims and sends it to the attacker's C&C server for analysis. Based on these inputs, the malware not only picks the modules that are to be included in the final payload but also appears to distinguish real human operators from virtual machines and automated environments used by researchers," they continue. Emotet seems to be able to automatically distinguish between legitimate processes and artificial ones, subsequently allowing it to select relevant payloads—a process that would take a significant amount of time and resources if done manually.

Finally, perhaps the most significant developments will be on the back end, infrastructure side of cyber capability development. For example, AI-powered data analytics are expected to improve the collection, translation, and manipulation of data. This will reduce the need for linguists and make the jobs of analysts much easier.

Toward a Better Cyber Defense

While AI technology can have significant upsides for attackers, we should equally recognize the potential for AI to aid cyber defense. There will be AI applications for both the detection and response to cyberattacks. On the detection side, we can expect a (further) move away

from so-called signature-based detection, which relies on a set of static rules that must be constantly updated. It will be flexible detection that captures what a baseline network looks like and will be able to spot any changes that appear abnormal. Even if these systems will still not be perfect and may show false positives, they can make first passes through data and reduce the need for human analysis.

AI might also facilitate intelligent responses to adversarial cyber activity. In 2016, DARPA organized the Cyber Grand Challenge, the world's first all-machine competition to create automatic defensive systems capable of discovering, proving, and patching software flaws on a network in real-time. The automated defense system that was crowned winner of the challenge, ForAllSecure's Mayhem, was unable to beat a team of human operators at a later event. Nevertheless, DARPA's event was a proof of concept for autonomous cyber defense, demonstrating how automated systems can find security flaws and develop and deploy solutions in real-time. The U.S. Defense Innovation Unit Experimental (DIUx) launched a project following the event in order to determine if commercial "cyber reasoning" could be deployed to detect and remediate previously unknown vulnerabilities in weapon systems.

Finally, particularly for the more responsible states that worry about collateral damage, some AI techniques—such as those used to further develop self-propagating malware, also known as worms —will have to be used with great caution. If worms do not have clear boundaries on where they are allowed to go, it increases the risk of indiscriminate targeting and uncontrolled propagation.

Jon Lindsay and Erik Gartzke note that "cyber operations alone lack the insurance policy of hard military power, so their success depends on the success of deception." AI provides novel opportunities for the attacker to mislead the enemy more effectively and efficiently. It can improve the attackers' ability to find vulnerabilities, exploit the human factor, and deliver malware. But it equally provides new opportunities to quickly uncover acts of deception. Ultimately, AI cuts both ways.

Max Smeets is a Senior Researcher at the Center for Security Studies (CSS) at ETH Zurich and Director of the European Cyber Conflict Research Initiative. He is the author of *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force* (Oxford University Press & Hurst, 2022) and co-editor of *Deter, Disrupt or Deceive? Assessing Cyber Conflict as an Intelligence Contest* (Georgetown University Press, 2023), with Robert Chesney.

New AI Detects Anomalies in Oil and Gas Industry

Source: https://i-hls.com/archives/115291

July 30 – A US Robotics company is adding new artificial intelligence anomaly detection capabilities to its autonomous Scout System drone. A leading US provider of private wireless data, drone and automated data has announced that the new containment capabilities will enable oil and gas customers to minimize environmental risks, clean-up costs, fines, and litigation expenses.

Suasnews.com reports that the loss of containment analytics feature will accelerate early detection and location of crude oil leaks before they become critical to customers by providing frequent, autonomous inspections of oil and gas pumpjacks, heater treaters, tanks, pipes, pumps, and more via the autonomous Scout System. Autonomous drones have become a crucial component to ensuring safety and conducting regular inspections within the oil and gas industry. "On the heels of our announcement of new high-resolution RGB and thermal camera payloads, American Robotics continues to enhance our offerings for current and future customers in the oil and gas industry," said Reese Mozer, co-founder and CEO of American Robotics. "This analytics feature is the first to be announced from our industry-optimized product roadmap put in place early last year. We have worked closely with our customers to define these requirements on route to fleet deployments, and we are grateful for their partnership." A recent Market Research Future report predicted that the market size for drones in the oil and gas industry is projected to be worth over $23 billion by 2027.

AI, Autonomy, and the Risk of Nuclear War

By James Johnson

Source: https://warontherocks.com/2022/07/ai-autonomy-and-the-risk-of-nuclear-war/

July 29 – Will emerging technologies like AI increase the risk of nuclear war? We are in an era of rapid disruptive technological change, especially in AI. Therefore, the nascent journey to reorient military forces to prepare for the future digitized battlefield is no longer merely speculation or science fiction. "AI technology" is already fused into military machines, and global armed forces are well advanced in their planning, research and development, and, in many cases, deployment of AI-enabled capabilities.

AI does not exist in a vacuum. In isolation, AI is unlikely to be a strategic game changer. Instead, it will likely reinforce the destabilizing effects of advanced weaponry, thereby increasing the speed of war and compressing the decision-making timeframe. The inherently destabilizing effects of military AI may exacerbate tension between nuclear-armed powers, especially China and the United States, but not for the reasons you may think.
How and to what degree does AI augmentation mark a departure from automation in the nuclear enterprise, which goes back several decades? How transformative are these developments? And what are the potential risks posed by fusing AI technology with nuclear weapons? While we can't answer these questions fully, only by extrapolating present trends in AI-enabling capabilities can we illuminate the potential risks of the current trajectory and thus consider ways to manage them.

The Emerging AI-Nuclear Nexus
It is worth considering how advances in AI technology are being researched, developed, and, in some cases, are deployed and operational in the context of the broader nuclear deterrence architecture — early-warning and intelligence, surveillance, and reconnaissance; command and control; nuclear weapon delivery systems; and non-nuclear operations.

Early-Warning and Intelligence, Surveillance, and Reconnaissance
AI machine learning might, in three ways, quantitatively enhance existing early-warning and intelligence, surveillance, and reconnaissance systems. First, machine learning, in conjunction with cloud computing, unmanned aerial vehicles (or drones), and big-data analytics, could be used to enable mobile intelligence, surveillance, and reconnaissance platforms to be deployed in geographically long ranges, and in complex, dangerous environments (e.g., contested anti-access/area-denial zones, urban counterinsurgency, or deep-sea) to process real-time data and alert commanders of potentially suspicious or threatening situations such as military drills and suspicious troop or mobile missile launcher movements.
Second, machine-learning algorithms could be used to gather, mine, and analyze large volumes of intelligence (open-source and classified) sources to detect correlations in heterogeneous — and possibly contradictory, compromised, or otherwise manipulated — datasets. Third, and related, algorithmic processed intelligence could be used to support commanders to anticipate — and thus more rapidly preempt — an adversary's preparations for a nuclear strike. In short, AI could offer human commanders operating in complex and dynamic environments vastly improved situational awareness and decision-making tools, allowing for more time to make informed decisions with potentially stabilizing effects.

Nuclear Command and Control
Compared to intelligence and early-warning systems, the impact of AI is unlikely to have a material impact on nuclear command and control, which for several decades have synthesized automation but not autonomy. As we have seen in these pages, algorithms that underlie complex autonomous systems today are too unpredictable, vulnerable (to cyber attacks), unexplainable (the "black-box" problem), brittle, and myopic to be used unsupervised in safety-critical domains. For now, there is a broad consensus amongst nuclear experts and nuclear-armed states that, even if the technology permitted, AI decision-making that directly impacts nuclear command-and-control functions (i.e., missile-launch decisions), should not be pre-delegated to AIs. Whether this fragile consensus can withstand mounting first-mover advantage temptations in a multipolar nuclear order is less certain. Whether human commanders — predisposed to anthropomorphize subjects, cognitive offloading, and automation bias — can avoid the temptation to view AI as a panacea for the cognitive fallibilities of human decision-making is also unclear. The question, therefore, is perhaps less *whether* nuclear-armed states will adopt AI technology into the nuclear enterprise, but rather *by whom, when, and to what degree*.
Nuclear and Non-Nuclear Missile Delivery Systems
AI technology will likely affect the nuclear weapon delivery systems in several ways. First, machine-learning algorithms may be used to improve the accuracy, navigation (pre-programed guidance parameters), autonomy ("fire-and-forget" functionality) of missiles, and precision — mainly used in conjunction with hypersonic glide vehicles. For example, China's DF-ZF maneuverable hypersonic glide vehicle is a dual-capable (nuclear and conventionally armed) prototype with autonomous functionality.
Second, it could improve the resilience and survivability of nuclear launch platforms against adversary countermeasures such as electronic warfare jamming or cyber attacks — that is, autonomous AI-enhancements would remove the existing vulnerabilities of communications and data links between launch vehicles and operators.
Third, the extended endurance of AI-augmented unmanned (i.e., unmanned underwater vehicles and unmanned combat aerial vehicles) platforms used in extended intelligence, reconnaissance, and surveillance missions — that cannot be operated remotely — can potentially increase their ability to survive countermeasures and reduce states' fear of a nuclear decapitation. This is especially the case in asymmetric nuclear dyads, such as United States-Russia, India-Pakistan, and United States-China. AI and autonomy might also strengthen states' second-strike capability — and thus deterrence — and even support escalation management during a crisis or conflict.

Conventional Counterforce Operations

AI could be used to enhance a range of conventional capabilities, with potentially significant strategic implications — especially strategic non-nuclear weapons used in conventional counterforce operations. Machine learning could increase the onboard intelligence of manned and unmanned fighter aircraft, thus increasing their capacity to penetrate enemy defenses using conventional high-precision munitions. Moreover, increased levels of AI-enabled autonomy might allow unmanned drones — possibly in swarms — to operate in environments hitherto considered inaccessible or too dangerous for manned systems (e.g., anti-access and area denial zones, or deep-water and outer space environments). The 2021 Azerbaijani-Armenian war and the recent Ukrainian-Russian conflict have demonstrated how smaller states can integrate new weapon systems to amplify their battlefield effectiveness and lethality.

Machine-learning techniques could materially enhance missile, air, and space defense systems' ability to detect, track, target, and intercept. Though AI technology has been integrated with automatic target recognition to support defense systems since the 1970s, the speed of defense systems' target-identification — because of the limited database of target signatures that an automatic target recognition system uses to recognize its target — has progressed slowly. Advances in AI and particularly generative adversarial networks could alleviate this technical bottleneck, generating realistic synthetic data to train and test automatic target recognition systems. Besides, autonomous drone swarms might also be used defensively (e.g., decoys or flying mines) to buttress traditional air defenses.

AI technology is also changing how (both offensive and defensive) cyber capabilities are designed and operated. On the one hand, AI might reduce a military's vulnerability to cyber attacks and electronic warfare operations. AI cyber-defensive tools and anti-jamming capabilities — designed, for example, to recognize changes to patterns of behavior and anomalies in a network and automatically identify malware or software code vulnerabilities — could protect nuclear systems against cyber intrusions or jamming operations.

On the other hand, advances in AI machine learning (notably an increase in the speed, stealth, and anonymity of cyber warfare) might enable identifying an adversary's "zero-day vulnerabilities" — that is, undetected or unaddressed software vulnerabilities. Motivated adversaries might also use malware to take control, manipulate, or fool the behavior and pattern recognition systems of autonomous systems such as the Project Maven — for example, using generative adversarial networks to generate synthetic and realistic-looking data poses a threat to both machine learning and rules-based forms of attack detection. In short, AI technology in the nuclear domain will likely be a double-edged sword: strengthening the nuclear systems while expanding the pathways and tools available to adversaries to conduct cyber-attacks and electronic warfare operations against these systems (e.g., AI-augmented "left of launch").

Finally, advances in AI technology could contribute to the physical security of nuclear weapons, particularly against threats posed by third-party and non-state actors. Autonomous vehicles (e.g., "anti-saboteur robots") could be used, for example, to protect states nuclear forces, patrol the parameter of sensitive facilities, or form armed automated surveillance systems (e.g., South Korea's Super Aegis II robotic sentry weapon that includes a fully autonomous mode), along vulnerable borders. AI technology — in conjunction with other emerging technologies such as big-data analytics and early-warning and detection systems — might also be harnessed to provide novel solutions to support nuclear risk and non-proliferation efforts; for example, removing the need for "boots on the ground" inspectors in sensitive facilities to support non-interference mechanisms for arms control verification agreements.

The 2025 "Flash War" in the Taiwan Straits

How might AI-powered capabilities intensify a crisis between two nuclear-armed adversaries? Consider the following fictional counterfactual: On the morning of Dec. 12, 2025, political leaders in Beijing and Washington authorized a nuclear exchange in the Taiwan Straits. Independent investigators into the 2025 "flash war" expressed sanguinity that neither side deployed AI-powered "fully autonomous" weapons nor intentionally violated the law of armed conflict.

In an election dominated by the island's volatile relations with Communist China in 2024, President Tsai Ing-wen, and in another major snub to Beijing, pulled off a sweeping victory, securing her third term for the pro-independence Democrats. As the mid-2020s dawned, tensions across the Straits continued to sour, as both sides — held hostage to hardline politicians and hawkish generals — maintained uncompromising positions, jettisoning diplomatic gestures, and inflamed by escalatory rhetoric, fake news, and campaigns of mis/disinformation. At the same time, both China and the United States deployed AI to support battlefield awareness, intelligence, surveillance, and reconnaissance, early-warning, and other decision-support tools — to predict and suggest tactical responses to enemy actions in real time.

By late 2025, the rapid improvements in the fidelity, speed, and predictive capabilities of commercially produced dual-use AI applications, persuaded great military powers not only to feed data-hungry machine learning to enhance tactical and operational maneuvers but increasingly to inform strategic decisions. Impressed by the early adoption and fielding by Russia, Turkey, and Israeli of AI tools to support autonomous drone swarms to outmaneuver and crush counterterrorist incursions on

their borders, China synthesized the latest iterations of dual-use AI, sacrificing rigorous testing and evaluation in the race for first-mover advantage.

With Chinese military incursions — aircraft flyovers, island blockade drills, and drone surveillance operations — in the Taiwan Straits marking a dramatic escalation in tensions, leaders in China and the United States demanded the immediate fielding of the latest strategic AI to gain the maximum asymmetric advantage in scale, speed, and lethality. As the incendiary rhetoric playing out on social media — exacerbated by disinformation campaigns and cyber intrusions on command-and-control networks — reached a fever pitch on both sides, a chorus of voices expounded the immediacy of a forced unification of Taiwan by China.

Buoyed by the escalatory situation unraveling in the Pacific — and with testing and evaluation processes incomplete — the United States decided to bring forward the fielding of its prototype autonomous AI-powered "Strategic Prediction & Recommendation System" (SPRS) — supporting decision-making in non-lethal activities such as logistics, cyber, space assurance, and energy management. China, fearful of losing the asymmetric upper hand, fielded a similar decision-making support system, "Strategic & Intelligence Advisory System" (SIAS), to ensure its autonomous preparedness for any ensuring crisis.

On June 14, 2025, at 06:30, a Taiwanese coast guard patrol boat collided with and sank a Chinese autonomous sea-surface vehicle conducting an intelligence recon mission within Taiwan's territorial waters. On the previous day, President Tsai hosted a senior delegation of U.S. congressional staff and White House officials in Taipei on a high-profile diplomatic visit. By 06:50, the cascading effect that following — turbo-charged by AI-enabled bots, deepfakes, and false-flag operations — far exceeded Beijing's pre-defined threshold, and thus capacity to contain.

By 07:15, these information operations coincided with a spike in cyber intrusions targeting U.S. Indo-Pacific Command and Taiwanese military systems, defensive maneuvers of orbital Chinese counter space assets, automated People's Liberation Army logistics systems were activating, and the suspicious movement of the PLA's nuclear road-mobile transporter erector launchers. At 07:20, U.S. SPRS assessed this behavior as an impending major national security threat and recommended an elevated deterrence posture and a powerful demonstration of force. The White House authorized an autonomous strategic bomber flyover in the Taiwan Straits at 07:25.

In response, at 07:35, China's SIAS notified Beijing of an increased communication loading between U.S. Indo-Pacific Command and critical command and communication nodes at the Pentagon. By 07:40, SIAS raised the threat level for a preemptive U.S. strike in the Pacific to defend Taiwan, attack Chinese-held territory in the South China Seas, and contain China. At 07:45, SIAS advised Chinese leaders to use conventional counterforce weapons (cyber, anti-satellite, hypersonic weapons, and other smart precision missile technology) in a limited preemptive strike against critical U.S. Pacific assets including U.S. Air Force Base, Guam.

Chinese military leaders, at 07:50, fearful of an imminent disarming U.S. strike and increasingly reliant on the assessments of SIAS, authorized the attack — which SIAS had already anticipated and thus planned and prepared for. At 07:55, SPRS alerted Washington of the imminent attack and recommended an immediate limited nuclear strike to compel Beijing to call off its offensive. After a limited U.S.-China atomic exchange in the Pacific, leaving millions of people dead and tens of millions injured, both sides agreed to cease hostilities.

In the immediate aftermath of the deadly confrontation — lasting only a matter of hours — killing millions and injuring many more, leaders on both sides were dumbfounded about what caused the "flash war." Both sides attempted to retroactively reconstruct a detailed analysis of decisions made by SPRS and SIAS. However, the designers of the algorithms underlying SPRS and SIAS reported that it was not possible to explain the decision rationale and reasoning of the AI behind every subset decision. Besides, because of the various time, encryption, and privacy constraints imposed by the end military and business users, it was impossible to keep retroactive back-testing logs and protocols. Did AI technology cause the 2025 "flash war"?

Human Solutions to the Machine Problem

In the final analysis, the best way to prepare for the AI-nuclear future may be to adhere to a few basic principles to guide the management of nuclear weapons in their interactions with emerging technology. First, nuclear weapon systems should avoid being unduly complex, entangled, or overcomplicated. Second, these systems must be fortified and robust enough to withstand traditional threats and increasing new threats emerging in the digital domain. Third, nuclear weapons must be disentangled and, where possible, distinctly separate (both physically and doctrinally) from non-nuclear capabilities and command, control, communications, and intelligence systems. If this principle was followed it would likely rule out the existence of the kind of dual-use systems described in the "flash war" vignette.

Towards these lofty ends, AI could also support defense planners' design and run wargaming and other virtual training exercises to refine operational concepts, test various conflict scenarios, and identify areas and technologies for potential development. For instance, AI-machine learning techniques — modeling, simulation, and analysis — might complement counterfactuals and low-tech table-top wargaming simulations to identify contingencies under which nuclear risk might arise. As

Alan Turing wrote in 1950: "We can only see a short distance ahead, but we can see plenty there that needs to be done."

James Johnson is a lecturer in strategic studies at the University of Aberdeen. He is also an honorary fellow at the University of Leicester, a non-resident associate on the European Research Council-funded Towards a Third Nuclear Age Project, and a mid-career cadre with the Center for Strategic Studies Project on Nuclear Issues. He is the author of *Artificial Intelligence and the Future of Warfare: USA, China & Strategic Stability*. His latest book project with Oxford University Press is *AI & the Bomb: Nuclear Strategy and Risk in the Digital Age*.

AI in the IDF: Israeli Troops Speak with Their Drones

By Seth J. Frantzman

Source: https://www.meforum.org/63417/ai-in-the-idf-israeli-troops-speak-with-their

Aug 01 — Israel is working on a system that will enable ground forces to use voice commands for unmanned systems.

Technology development efforts have taken place over the last two years as part of a broader process of developing new tools for the Israel Defense Forces.

Israel's Casper drone system allows troops to use voice commands to communicate with drones

An official with the Defense Ministry's Directorate of Defense Research and Development said the system is about voice dialogue between humans and machines.

"It's called Casper, and we wanted the system to be a member of the team: a hybrid team of human and nonhuman operating and working together," the official told Defense News, speaking on the condition of anonymity due to security reasons. This kind of partnering is often called manned-unmanned teaming, or MUM-T.

"To make this happen, we needed the drone as a team member so I can say 'go forward' or 'cover me,' and the drone can say it observes an objective 90 degrees from us, for example," the official added.

The directorate's voice command system is being designed for use with a variety of unmanned systems, but it can currently only understand Hebrew.

The official said 80% of the technology's capabilities involve controlling a drone's basic abilities, such as lifting off and flying to a certain height, while the remaining 20% is focused on commanding a drone to investigate or detect targets.

We needed the drone as a team member so I can say 'go forward' or 'cover me,' and the drone can say it observes an object 90 degrees from us, for example.

"We understood we need a new approach of operating systems in a battlefield," the official said, noting that these kinds of voice commands already exist in the civilian world. "On a battlefield, you need to be aware of surroundings, you need to look forward and have your hands on a weapon and not on a control [screen]."

The official added that the new technology is meant to make it easier for forces to identify and investigate targets and well as close the sensor-to-shooter loop — the time it takes for different systems to communicate with each other. "I can tell Casper to go investigate and close the loops once we have the real-time, accurate augmentation and the drone and the human on the same C4I system, [with] common language and the same map."

The directorate is at the end of the first development phase and has employed about 20 commands to get there. The system is projected to be operational within the next several years.

The technology will first head to special units — "early adapters," as the official put it — with the hope the larger ground force will take up the technology. The ministry has said this incremental approach is simply a building block toward larger manned-unmanned teaming that the IDF hopes to widely adopt in the future.

Local defense company Elbit Systems is already working on a government program called Edge of Tomorrow, which combines new technology to improve situational awareness. These technologies include augmented reality, artificial intelligence and other aspects of

digitization for dismounted forces. This voice command effort, developed by Thirdeye Systems, could represent the next step for Edge of Tomorrow

"On the battlefield, a few seconds can be the difference between life and death, between mission accomplishment and mission failure," Bradley Bowman, senior director of the Center on Military and Political Power at the Foundation for Defense of Democracies, told Defense News. "Voice commands that eliminate the need to look down at a tablet can save vital time and increase soldier situational awareness. That will save lives."

We are now in a dramatic change in concept [with] the way we are giving tools to the local commanders, from the battalion level, all the way from brigade to company level.

Retired Maj. Gen. Eitan Dangot, a former military secretary under three Israeli defense ministers who is now a senior fellow at the Jerusalem Institute for Strategy and Security, said the IDF has sought to improve its maneuver abilities for ground forces, especially to confront threats in urban areas. He noted this stems from lessons learned during the 2014 conflict in Gaza as well as anti-tank threats Israel faced in the 2006 war in Lebanon.

"We are now in a dramatic change in concept [with] the way we are giving tools to the local commanders from battalion level, all the way from brigade to company level, giving them opportunities to increase their area of fighting by ... identifying targets when they need fire support — fire that comes from other vehicles," he told Defense News.

The next step, the defense directorate official said, depends on several factors, such as determining "what is the right asset for the mission. Will it be a robot or drone or human being doing this all the time? [We need to] understand operational limits and abilities. This will require a strong AI engine to divide the resources and aim at the right place at the right time."

Bowman said these advanced technologies will have broader ramifications.

"That's one of the big ideas behind the U.S.-Israel Operations-Technology Working Group," he said, referring to a bilateral effort to provide troops with advanced capabilities to outmatch any potential enemy. "The U.S. is too often painfully slow at going from concept to fielded combat capability. In the intense military technology competition with China, I worry we will pay a higher price if we don't expedite this process and get capabilities to our troops more quickly. Working more closely with Israel can help address this perennial Pentagon problem."

The U.S. is too often painfully slow at going from concept to fielded combat capability. Working more closely with Israel can help address this problem.

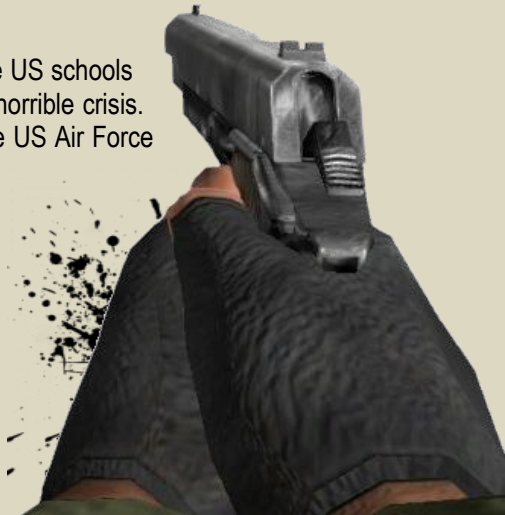
He noted that Congress authorized the creation of the working group, which was established between the U.S. Defense Department and Israeli Defense Ministry last November.

"The Israelis are among the best in the world in some areas that are central to the generational American military modernization effort that is underway. They are strong on drones and counter-drone technology. They are obviously strong on AI and missile defense. The combatants who can close that kill chain the quickest will accomplish their missions and return home to their families.

Seth Frantzman is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at *The Jerusalem Post*.

US Air Force Tests AI and Drones to Stop Shooters

Source: https://i-hls.com/archives/115389



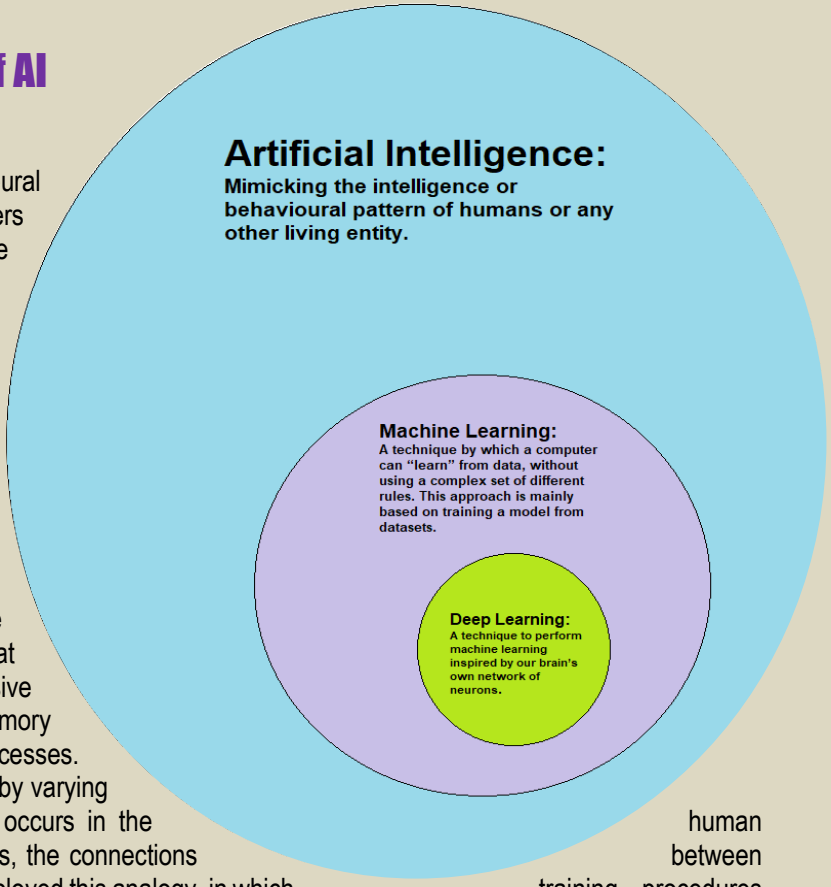
Aug 03 – It is a difficult fact to admit that the US is amid a shooter epidemic. More and more US schools and institutions are increasing their security measures and looking for ways to combat this horrible crisis. Not only are private and government facilities taking part in this effort, so is the military. The US Air Force has begun testing a system that utilized artificial intelligence (AI) and drones on several bases to aid in putting a stop to the active shooter phenomenon.

The system will be built off previous AI gun-detection software that is already in use in security camera systems across several Air Force bases, allowing it to deploy drones or

robots to combat a potential active shooter. The drones or robots will use non-lethal means aimed at disorienting a shooter, including sirens and strobe lights.
"The entire idea behind the platform is being able to take a robot and ultimately impede, disorient an active threat on an installation before they can do any more damage," ZeroEyes Senior Vice President of Government Solutions JT Wilkins, whose company is developing the technology for the government, told National Defense.
According to research, up to 85 percent of active shooters expose their weapons two to 30 minutes prior to firing their first shot. Once detected, this period of time could give the robots an opportunity to intervene ahead of a violent incident. The most crucial part is the ability to detect these weapons and send in a robot until relevant personnel arrive at the scene. Though the system uses AI and drone technology, it is not fully autonomous. After detecting a potential weapon, a human must verify and review the positive warnings. The robots and drones are not being tested to replace human intervenes such as security or the police, but act as support to first responders
The trial period of the system is expected to last 15 months and that the system will be available for use by government and private sectors alike.

Analog Deep Learning – The Future of AI

Source: https://i-hls.com/archives/115431



Aug 05 – How can you train increasingly complicated neural network models faster with less materials? Some researchers suggest investing in a new branch of artificial intelligence called 'analog deep learning'. Analog deep learning promises faster processing with far less energy consumption. Researchers have developed a network of analog artificial "neurons" and "synapses" that can do calculations similarly to a digital neural network by repeating arrays of programmable resistors in intricate layers. Then, this network may be trained using complex AI tasks like image recognition and natural language processing.
Marktechpost.com writes that there are two main reasons due to which analog deep learning is faster and more efficient than its digital version. The main factor is that computations are carried out in memory, preventing massive amounts of data from being repeatedly transported from memory to a processor. Analog processors also carry out parallel processes.
Analog machine learning can be possible with a processor by varying the electrical conductivity of protonic resistors. Learning occurs in the human brain due to the strengthening and weakening of synapses, the connections between neurons. Since its inception, deep neural networks have employed this analogy, in which training procedures are used to design the network weights.
Additionally, analog deep learning can endure extremely powerful, pulsed electric fields. The resistor can successfully run for millions of cycles without failing since protons do not harm the material, making it a million times faster. Moreover, it can function efficiently at ambient temperature, making it appropriate for integration into computing devices.

Indian Army deploys AI-based system to reduce manual surveillance at borders

Source: https://pragnews.com/national/indian-army-deploys%20-based-system

Aug 06 – The Indian Army has been installing AI-based surveillance systems on its western and northern borders in order to improve capabilities.
In addition to installing AI-based surveillance systems at borders, sources in the defense establishment have stated that "They are utilizing it to maintain watch on real-time social media monitoring, pattern identification, and prediction of opponent courses of action, etc."

"Real-time monitoring software powered by AI has been used in counter terrorism operations to gather intelligence. Eight places in the Northern and Southern Theater now have an AI-based suspicious vehicle recognition system installed "said a source.
According to some, artificial intelligence (AI) can significantly increase the asymmetry of military operations.

The employment of AI is expected to change current war fighting paradigms. Applications for artificial intelligence (AI) can be used for surveillance and detection, real-time social media monitoring, pattern identification, and predicting the next move of an opponent, among other things.
The Indian Army has been working closely with Indian academia, Indian business, and the DRDO to realise challenging AI-based initiatives.
To address this, the Military College of Telecommunication Engineering has built an AI Lab where AI projects have undergone thorough internal testing before being delivered to a production agency for deployment. On the western and northern frontiers, the Indian Army has placed several AI-Powered Smart Surveillance System units. The unit can process heterogeneous inputs from gadgets like handheld thermal imagers and PTZ cameras.
This has significantly decreased the need for manual monitoring. There are eight spots in the Northern and Southern Theaters where an AI-based suspicious vehicle recognition system has been installed. Real-time monitoring software powered by AI has been used in counter terrorism operations to gather intelligence.

Artificial Intelligence Isn't That Intelligent

By Harriet Farlow

Source: https://www.homelandsecuritynewswire.com/dr20220808-artificial-intelligence-isn-t-that-intelligent
Aug 08 – Late last month, Australia's leading scientists, researchers and businesspeople came together for the inaugural Australian Defense Science, Technology and Research Summit (ADSTAR), hosted by the Defense Department's Science and Technology Group. In a demonstration of Australia's commitment to partnerships that would make our non-allied adversaries flinch, Chief Defense Scientist Tanya Monro was joined by representatives from each of the Five Eyes partners, as well as Japan, Singapore and South Korea. Two streams focusing on artificial intelligence were dedicated to research and applications in the defense context.
'At the end of the day, isn't hacking an AI a bit like social engineering?'
A friend who works in cybersecurity asked me this. In the world of information security, social engineering is the game of manipulating people into divulging information that can be used in a cyberattack or scam. Cyber experts may therefore be excused for assuming that AI might display some human-like level of intelligence that makes it difficult to hack.
Unfortunately, it's not. It's actually very easy.
The man who coined the term 'artificial intelligence' in the 1950s, cybernetics researcher John McCarthy, also said that once we know how it works, it isn't called AI anymore. This explains why AI means different things to different people. It also explains why trust in and assurance of AI is so challenging.
AI is not some all-powerful capability that, despite how much it can mimic humans, also thinks like humans. Most implementations, specifically machine-learning models, are just very complicated implementations of the statistical methods we're familiar with from high school. It doesn't make them smart, merely complex and opaque. This leads to problems in AI safety and security.
Bias in AI has long been known to cause problems. For example, AI-driven recruitment systems in tech companies have been shown to filter out applications from women, and re-offence prediction systems in US prisons exhibit consistent biases against black inmates.
Fortunately, bias and fairness concerns in AI are now well known and actively investigated by researchers, practitioners and policymakers.
AI security is different, however. While AI safety deals with the impact of the decisions an AI might make, AI security looks at the inherent characteristics of a model and whether it could

be exploited. AI systems are vulnerable to attackers and adversaries just as cyber systems are.
A known challenge is adversarial machine learning, where 'adversarial perturbations' added to an image cause a model to predictably misclassify it.
When researchers added adversarial noise imperceptible to humans to an image of a panda, the model predicted it was a gibbon.
In another study, a 3D-printed turtle had adversarial perturbations embedded in its surface so that an object-detection model believed it to be a rifle. This was true even when the object was rotated.
I can't help but notice disturbing similarities between the rapid adoption of and misplaced trust in the internet in the latter half of the last century and the unfettered adoption of AI now.
It was a sobering moment when, in 2018, the then US director of national intelligence, Daniel Coats, called out cyber as the greatest strategic threat to the US.
Many nations are publishing AI strategies (including Australia, the US and the UK) that address these concerns, and there's still time to apply the lessons learned from cyber to AI. These include investment in AI safety and security at the same pace as investment in AI adoption is made; commercial solutions for AI security, assurance and audit; legislation for AI safety and security requirements, as is done for cyber; and greater understanding of AI and its limitations, as well as the technologies, like machine learning, that underpin it.
Cybersecurity incidents have also driven home the necessity for the public and private sectors to work together not just to define standards, but to reach them together. This is essential both domestically and internationally.
Autonomous drone swarms, undetectable insect-sized robots and targeted surveillance based on facial recognition are all technologies that exist. While Australia and our allies adhere to ethical standards for AI use, our adversaries may not.
Speaking on resilience at ADSTAR, Chief Scientist Cathy Foley discussed how pre-empting and planning for setbacks is far more strategic than simply ensuring you can get back up after one. That couldn't be more true when it comes to AI, especially given Defense's unique risk profile and the current geostrategic environment.
I read recently that Ukraine is using AI-enabled drones to target and strike Russians. Notwithstanding the ethical issues this poses, the article I read was written in Polish and translated to English for me by Google's language translation AI. Artificial intelligence is already pervasive in our lives. Now we need to be able to trust it.

Harriet Farlow is a deputy director in the Australian Department of Defense and a Ph.D. candidate in cybersecurity, focusing on adversarial machine learning.

AI autopilot could let autonomous aircraft fly in busy airspaces

Source: https://newatlas.com/aircraft/ai-autopilot-autonomous-aircraft-crowded-airspaces/

Aug 09 – While pilots commonly use an autopilot when cruising at high altitudes, they typically switch to manual control when entering crowded lower airspaces. However, what if the plane *has* no pilot? Well, a new AI autopilot system for busy airspaces may be the answer.
Currently being developed by researchers at Carnegie Mellon University, the system was trained on data collected at Pennsylvania's Allegheny County Airport and Pittsburgh-Butler Regional Airport.

In a test of the artificially intelligent autopilot, both it (left) and a human pilot (right) controlled virtual aircraft in the same simulated airspace – Carnegie Mellon University

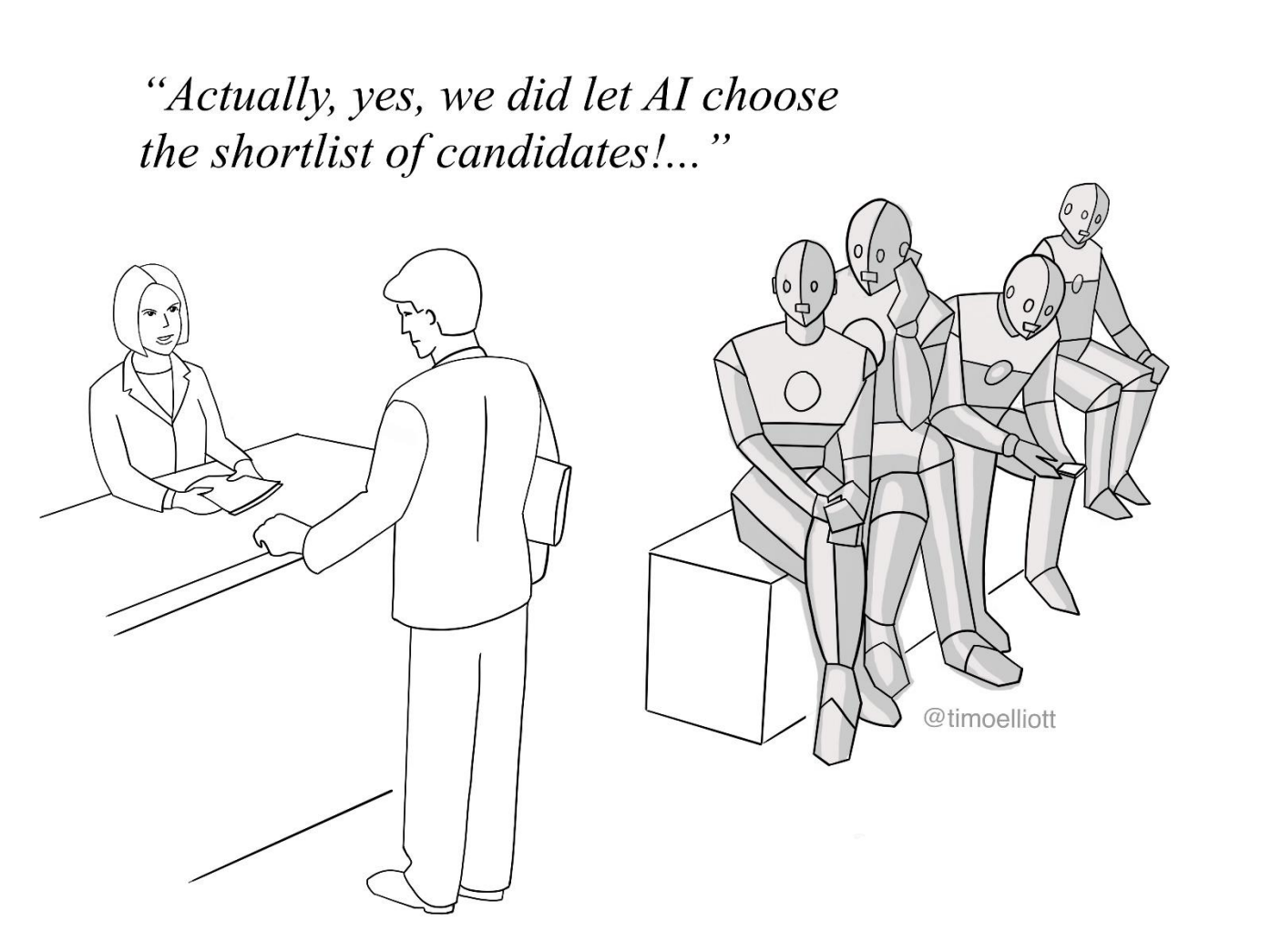
Along with utilizing the autonomous aircraft's existing instrumentation – and information provided by local air traffic controllers – it incorporates six cameras and a computer vision system. According to the scientists, the latter setup allows it to visually spot nearby aircraft much as a human pilot would do. The system is able to subsequently track those aircraft and

predict their trajectories, taking action to avoid collisions when necessary. It can reportedly even understand plain-language spoken radio communications from other pilots or airports, responding with a synthetic speech system of its own.

Although the technology has yet to be tested on an actual airplane, it has been trialed in a setup that involved two linked flight simulators. In that setup, a human-piloted one virtual aircraft, while the AI system piloted another in the same airspace. It was found that the AI was able to successfully avoid collisions with human-piloted aircraft, even when the pilot had little experience at flying a plane.

The scientists hope that once developed further, the system could be applied to autonomous aircraft such as air taxis or delivery drones.

"This is the first AI pilot that works in the current airspace," said team member Assoc. Prof. Sebastian Scherer. "I don't see that airspace changing for UAVs [unmanned aerial vehicles]. The UAVs will have to change for the airspace."

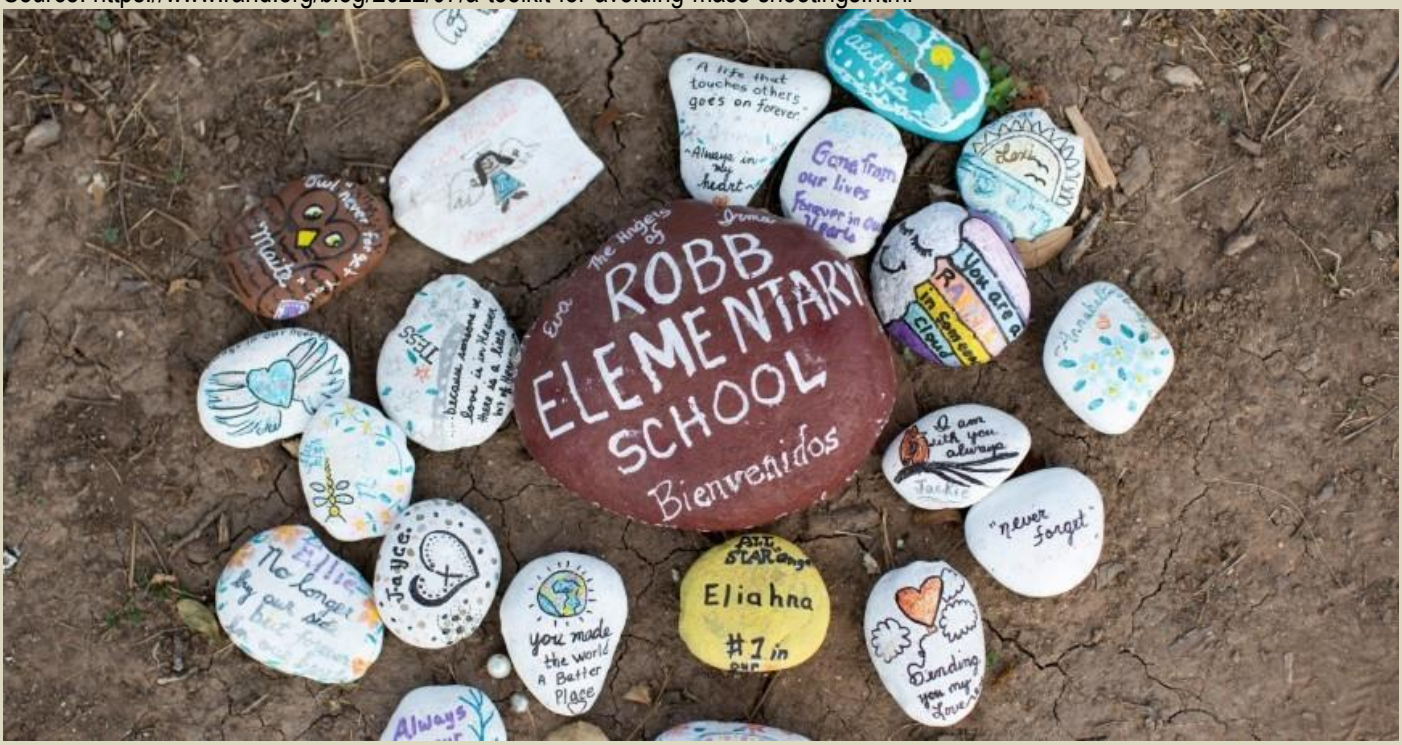



International
CBRNE
INSTITUTE
C2BRNE
DIARY
CBRNE-Terrorism
Newsletter
W
M
O
D
EMERGENCY
RESPONSE

A Toolkit for Avoiding Mass Shootings

By Richard H. Donohue and John S. Hollywood

Source: https://www.rand.org/blog/2022/07/a-toolkit-for-avoiding-mass-shootings.html



Painted stones are placed at a memorial outside Robb Elementary School in Uvalde, Texas, July 13, 2022 | Photo by Kaylee Greenlee Beal/Reuters

July 14 – Independence Day celebrations come to a tragic ending; a simple trip to the grocery store and a day at school turn deadly. These recent events in Highland Park, Illinois, Buffalo, New York, and Uvalde, Texas, have once again brought the issue of mass shootings to the forefront of the national conversation. Policymakers took some steps aimed at helping reduce gun violence with the recent passage of a bipartisan law, but there are some additional clear, concrete steps communities, policymakers and law enforcement could take today to help protect society from mass attacks.

For the last two years, our team analyzed over 600 cases related to mass attacks, including over 300 that were stopped in advance. We reviewed reports and resources related to these events, and interviewed dozens of subject matter experts to learn more about effective (and ineffective) prevention and response strategies.

From all of this, we developed an online educational toolkit, funded by the National Institute of Justice, to provide practical strategies and guidance on deterring, mitigating, and responding to mass attacks. Our research highlights three top ways we can mitigate and/or respond to mass attacks right now: through proactive prevention, relentless follow-up, and diligent preparation and training.

Proactive Prevention

Of the cases we examined, more than half were foiled in advance of a mass attack. Almost two-thirds of the clues leading to foiling mass attacks came from the public, with the most important warning signs being serious intentions and preparations to carry out attacks. Examples of intentions to kill include describing (often online) how they are inspired by past attacks or an extremist cause to kill, or describing how they feel they have no choice or are compelled to kill.

Clues related to planning attacks include showing off weapons they want to use, studying how to kill, compiling arsenals of weapons without a benign explanation, and site probing. Just recently, a tip reporting overhearing a plot led to stopping a mass shooting at a Fourth of July celebration in Richmond, Virginia.

Awareness and the simple reporting of alarming behavior is the first step in preventing a mass attack.

Awareness and the simple reporting of alarming behavior is the first step in preventing a mass attack. There is a need for more-detailed public education on reporting that provides more information on what the most concerning signs are, how to report them, and why members of the public should report.

Without engaging community members, the first link necessary to preventing mass attacks can be broken. Prevention needs to be linked in and across communities, tying together resources from schools, to the private sector and to law enforcement, among others. Mental health support systems are vital—as is trust in law enforcement to assist citizens. The latter is especially challenged in today's environment; it is incumbent on police agencies to foster trust and be accountable for their actions.

Relentless Follow-Up

Once warning signs have been reported, follow-up is critical across community networks. Communities must build prevention teams to tie together information and resources ahead of time, and not wait for an attack to happen.

Warning signs, tips, and threats should be assessed by community-based teams and shared with other communities, as well as state- and federal-level partners as necessary. Within teams, each case needs to be led by a single point of contact to lead the assessment and follow-up, ensuring that agreed-to actions are completed. Information simply cannot be left in the field and balls cannot be dropped.

Diligent Training, Preparation

People and communities need to be trained and educated on what they can do to respond to attacks. This includes, but goes well beyond, the "run, hide, fight" we—and our children—have become accustomed to. Advance planning and training are required of all agencies and partners who will jointly respond to mass attacks. This is not just for law enforcement—it is also for fire, EMS, emergency management, and for owners and security managers responsible for protecting public locations.

Diligent training isn't limited to responding to an event in the minutes it unfolds. Being prepared and having resources to support the community after a mass attack (or other tragedy) is key. This includes being prepared to offer mental health and emotional support for first responders, victims, and survivors and the critical need for effective communications skills.

Supporting Mass Attack Defenses

More support, best practices development, and education for both the multi-agency threat assessment and response teams may help avoid new tragedies.

In order to foster the prevention and mitigation efforts, there needs to be institutional support. Even though mass attacks are rare, communities can't wait to put these elements together. Federal resources are available. Individual agencies or municipalities can work together to increase their ability to fund and staff efforts, and can leverage existing threat assessment and emergency response–planning efforts

Policymakers could provide key support, as well. First, there could be a need to build on "See Something, Say Something" to provide the public more details on what is most important to look for and how to report it. Second, education and support on detecting, reporting, and assessing suspicious gun acquisition attempts could help, as trying to build up arsenals is a key detectable part of mass shootings plots. Third, law enforcement officers may need guidance on how to conduct the wellness checks that provide the initial contact, evaluation, and support for a person reported to be at risk.

Finally, more support, best practices development, and education for both the multi-agency threat assessment and response teams may also help avoid new tragedies. Providing this support, and resourcing the needed preparation, could help to realize the wisdom of one of our interviewed experts: "Heroes are made because they prepare for an incident."

Richard H. Donohue is a policy researcher and **John S. Hollywood** is a senior operations researcher at the nonprofit, nonpartisan RAND Corporation.

Mass Attacks Defense Toolkit

Preventing Mass Attacks, Saving Lives

The Mass Attacks Defense Toolkit can help reduce casualties from mass shootings and other violent attacks

●▶ Start now

Funded by the National Institute of Justice

RAND Corporation researchers created this toolkit to help reduce the likelihood of mass shootings and other public attacks, and reduce the casualties of completed attacks. Whatever your role or level of experience, this toolkit can make you a better defender against mass attacks.

After studying 600 mass attack events and plots, interviewing dozens of experts, and reviewing hundreds of references, the team identified the Mass Attacks Defense Chain, a series of defenses that work together to reduce the probability of mass attacks and their impacts.

What Preparedness & Response Leaders Need in the New Normal

By Catherine L. Feinman

The past few years have challenged emergency preparedness and response professionals around the world. Events that have been called unprecedented, record-breaking, or once-in-a-lifetime are becoming commonplace. Just a few defining events that spurred changes in preparedness efforts include the 9/11 attacks in 2001, Hurricane Katrina in 2005, Hurricane Harvey in 2017, and the COVID pandemic that began in 2019. Today's leaders need to be forward-thinking, equipped with the right tools, and prepared to manage the inevitable uncertainties that lie ahead. Leadership frameworks and industry traditions may need to change to better plan for, mitigate, and manage emergencies and disasters that occur in combination or that span large geographical areas.

July 2022, Domestic Preparedness Journal

Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the Domestic Preparedness Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Disaster intelligence: developing strategic warning for national security

By Chad M. Briggs, Miriam Matejova and Robert Weiss

Intelligence and National Security | Published online: 17 Mar 2022

Source: https://www.tandfonline.com/doi/abs/10.1080/02684527.2022.2043080?journalCode=fint20

The growing occurrence and intensity of disasters pose complex risks to national security, yet intelligence agencies do not possess the expertise to identify and assess emerging hazards effectively. Greater cooperation with experts outside the intelligence community, particularly scientists and local experts with valuable information, can allow effective warnings in advance of catastrophic events. This article makes an argument for strategic disaster intelligence, using two cases of major earthquakes and tsunamis to illustrate both disaster warning failures and opportunities for more effective disaster and risk mitigation.

Chad M. Briggs holds a PhD in political science from Carleton University in Canada, and currently serves with the US State Department. Briggs has previously worked on climate, disaster, and conflict issues in Alaska, Ukraine, Kosovo, and was Minerva Chair and Professor of Energy and Environmental Security with the US Air Force. Also, previously a senior intelligence advisor for the US Department of Energy, Briggs has developed environmental scenario planning methods that translate scientific data into risk and threat assessments. He has published on disaster planning, climate security, post-conflict reconstruction, public health, and hybrid/cyber warfare. (All views expressed are those of the author alone and do not necessarily reflect the official positions of the US State Dept. or the federal government.)

Miriam Matejova is an assistant professor in political science at the Faculty of Social Studies, Masaryk University and a fellow at the Norman Paterson School of International Affairs, Carleton University. She holds a PhD in political science from the University of British Columbia. She has published articles on energy and environmental security, global environmental activism, foreign intelligence, and international conflict management.

Robert Weiss is a Professor of Natural Hazard in the Department of Geosciences at Virginia Tech. He directs the Virginia Tech's Center for Coastal Studies, the graduate education program in Disaster Resilience and Risk Management, and the Academy of Integrated Science in Virginia Tech's College of Science. He has authored and co-authored over 60 publications on the impact of coastal hazards, especially tsunamis.

Evacuating Outside the Lines

Source: https://www.homelandsecuritynewswire.com/dr20220801-evacuating-outside-the-lines

Aug 01 — Scientists from the Division of Policy and Planning Sciences at the University of Tsukuba studied ways to make flood evacuations more efficient by allowing for routes that cross municipal boundaries. They estimate that the nearest shelter for 24% of citizens in Japan are actually located in another city, and that optimizing response plans this way can reduce evacuation time by 14%. This work may significantly improve public safety and overall preparedness for natural disasters. The increasing intensity of flooding around the world may lead to the need for wide-area evacuations from at-risk areas, even across administrative boundaries. In extreme cases, everyone in a certain region must be evacuated to a designated shelter. However, under the current disaster response system, the responsibility for creating evacuation plans falls primarily on city-level governments, and the effects of evacuation to shelters across municipal borders had not been investigated. Now, scientists at the University of Tsukuba have found that, by comparing the required evacuation time to available shelters with or without the restriction that people stay within their own city, a significant increase in efficiency occurs if cross-boundary evacuation is allowed. To do this, they compared intra- and cross-boundary evacuation routes in Japan, selecting all 733 cities with flooding risk based on the expected inundated area data, then using census data to map the population density of the country with a 500-meter grid. "While faster in many instances, our plan will likely require intermunicipal cooperation or coordination by higher levels of government, such as prefectures," first author Professor Sunyong Eom says. In any case, moving out of the immediate area of flooding is often a necessity. It can be expected that about 30% of the designated shelters would be in areas also impacted by inundation, so they cannot be safely used. Thus, evacuees would have to find alternative shelters further away. However, the team noted that the option of cross-border evacuations may not improve efficiency in all situations. They identified certain bridges and railway crossings that might become bottleneck points that cause longer evacuation times compared with intra-boundary routes during a mass evacuation in heavily populated cities.

Another finding relates with the spatial range of intermunicipal cooperation required for effective cross-border evacuation. Even though there is an increasing need to prepare for these routes, the complicated relationships between many cities may pose an obstacle to intermunicipal evacuation plans. Their findings can provide information to promote effective cooperation by identyfing the cities that have to participate. "Our work represents a first step towards understanding the improvement in disaster response that is possible when certain constraints are lifted," author Professor Michitaka Umemoto says. The current research was limited to people evacuating on foot. Future studies may include other modes of transportation, such as private cars or mass transit, and would help to inform local and central governments on updating existing evacuation guidelines.

Technical innovations in the fields of fire fighting and rescue

By John Retsios

Text in Greek

Source: https://www.fire.gr/egkyklopaideia/epistimoniki-arthrografia/technologikes-kainotomies-ston-choro-tis-pyrosvesis-kai-tis-diasosis/

John Retsios is a trainer in the area of individual protection and an expert on CBRN/HAZMAT equipment.

Prediction of Human Movement During Disasters Allows More Effective Emergency Response

Source: https://www.homelandsecuritynewswire.com/dr20220811-prediction-of-human-movement-during-disasters-allows-more-effective-emergency-response

Aug 11 – The COVID-19 pandemic, bigger and more frequent wildfires, devastating floods, and powerful storms have become unfortunate facts of life. With each disaster, people depend on the emergency response of governments, nonprofit organizations, and the private sector for aid when their lives are upended. However, a complicating factor in delivering that aid is that people tend to disperse with such disasters.

In research recently published in *The Proceedings of the National Academy of Sciences*, a team led by Jianxi Gao, assistant professor of computer science at Rensselaer Polytechnic Institute, and Qi "Ryan" Wang, associate professor of civil and environmental engineering at Northeastern University, formulated a method to predict human movement during large-scale extreme events with the goal of enabling more effective emergency responses. The model also revealed great disparity in movement among different economic groups.

"Despite many possible variables, we found that changes in human mobility behavior during various extreme events exhibit a consistent hyperbolic decline," said Gao. "We call it 'spatiotemporal decay.'"

Typically, people's movements follow predictable patterns. When an extreme event disrupts the pattern, scientists refer to it as a "mobility perturbation." For example, people may stop commuting to work, or they may change their route, or even evacuate to a shelter. Not only do these mobility perturbations cause challenges when delivering aid, but they also lead to financial, medical, and quality of life repercussions. The nature, extent, and duration of mobility perturbations vary widely.

Gao's team tracked the anonymous movements of 90 million people in the United States over the course of six large-scale disasters including wildfires, tropical storms, winter freezes, and pandemics in order to develop a unified model.

"Our model reveals the underlying uniformity across variables by incorporating heterogeneity across space and over time," said Gao. "We found strong regularities in how much mobility behavior changes following extreme events and in how fast mobility behavior returns to normal, allowing us to predict complex human behaviors during large-scale crises."

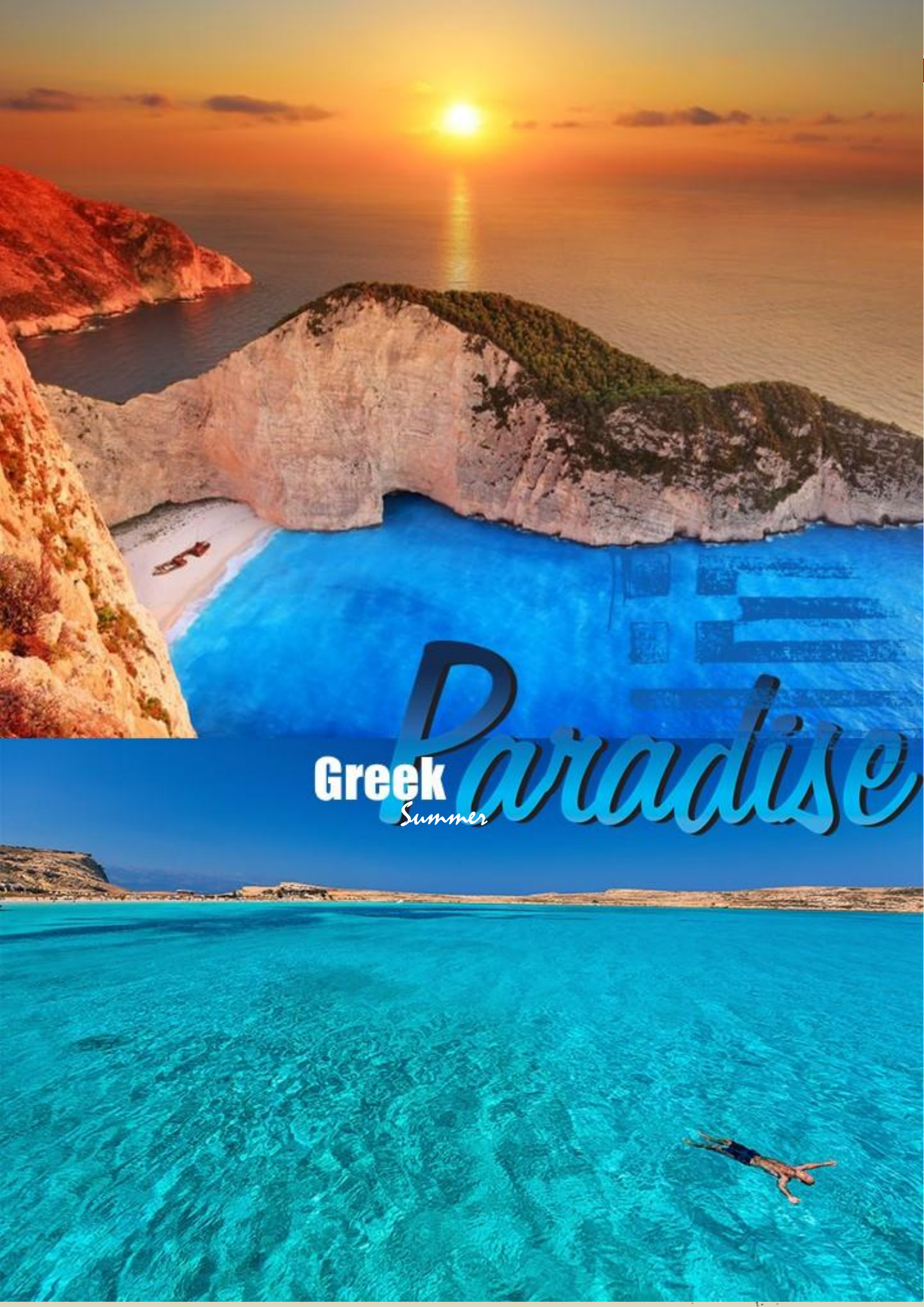
Gao's team found that people living close to the nucleus of the crisis – ground zero, or where a storm hits - limit their mobility significantly and quickly. Those living further away do not alter their movement patterns as drastically. This is what is referred to as 'spatial decay.' Over time, mobility patterns either return to normal, inch towards normal, or become even more perturbed. The team accounted for these variables by considering 'temporal decay,' as well.

When the team applied the model to the COVID-19 pandemic, it revealed great differences in movement among economic groups, which may help to explain the different infection rates. People from wealthy areas were more able to immediately reduce their mobility and maintain that change longer. People living in lower income areas exhibited a faster and greater hyperbolic decay.

"In other words, wealthier people were able to socially distance," Gao said. "Lower income people were forced to return to work."

"If events of recent years have taught us anything, it is that we must do our best to prepare for crises," said Curt Breneman, Dean of the Rensselaer School of Science. "This work by Dr. Gao and his team can inform enhanced and proactive emergency response planning to mitigate future extreme events. It also shines a light on persistent social inequities that we must find new ways to address."

Gao explained his research in this video.


Greek
Summer
Paradise

Because international CBRNE First Responders need a common roof!

https://www.ici-belgium.be/