CBRNE DIARY

Dedicated to Global First Responders

ICI International CBRNE INSTITUTE

09\23

Libya

September 2023

PART B

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

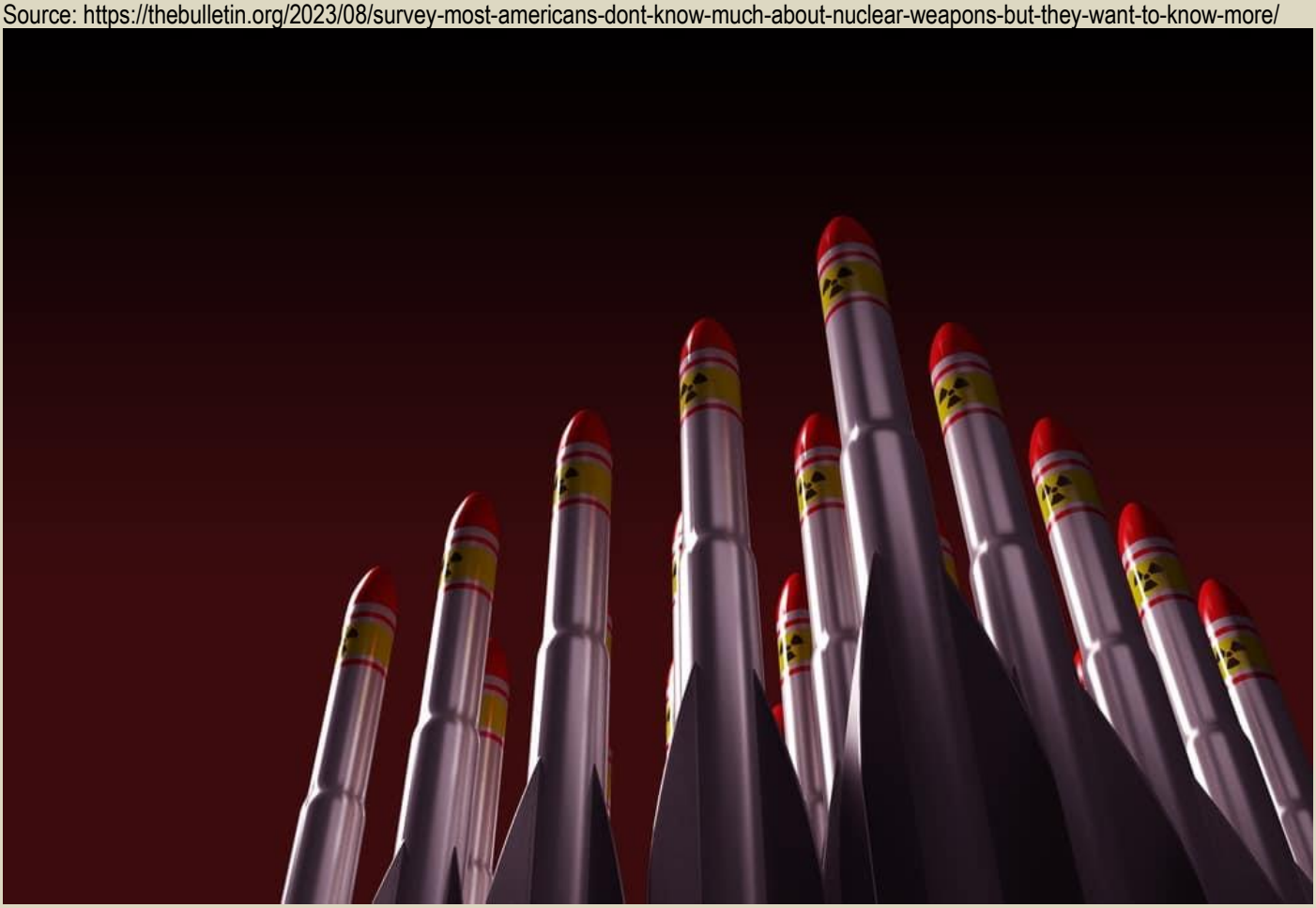
DIRTY R-NEWS

C2BRNE DIARY

Survey: Most Americans don't know much about nuclear weapons. But they want to know more.

By Dina Smeltz, and Sharon K. Weiner

Source: https://thebulletin.org/2023/08/survey-most-americans-dont-know-much-about-nuclear-weapons-but-they-want-to-know-more/



Aug 23 – For younger generations, the recent rollout of Christopher Nolan's Oppenheimer film might raise existential issues surrounding nuclear weapons. In fact, the prospect of the use of nuclear weapons seems more realistic now than it has for decades. Besides Russia's nuclear threats throughout the war against Ukraine, China's nuclear build-up raises concerns about a potential arms race with the United States and potentially other countries in Asia. In this context, the United States is undergoing an extensive—and expensive—nuclear modernization process, which may well force nuclear issues back onto the front pages for the American public.

But how ready are Americans to reengage with nuclear issues? A recent joint Chicago Council-Carnegie Corporation survey among the American public shows that Americans are fairly mixed in their views about nuclear weapons. A limited percentage of Americans say they are familiar with US nuclear weapons policy, their costs, their effects, and other issues related to the US nuclear weapons arsenal. But regardless of their age, most Americans today do not consider themselves familiar with nuclear issues.

A complex array of nuclear beliefs

Many Americans—especially younger and non-white Americans—don't think nuclear weapons make a difference to US national security or say they don't know enough to give an opinion. Moreover, relatively few Americans are interested in flexing their agency or getting more involved in making US nuclear policy beyond voting for a candidate who shares their views on nuclear policy.

On the one hand, Americans lean toward positive assessments of US nuclear policy. A majority believe nuclear weapons are either very or somewhat effective at preventing conflict between the United States and other countries (63 percent). Almost half (46 percent) are at least somewhat confident that the US missile defense system will protect them in the event of a nuclear war. And Americans who say they are familiar with nuclear deterrence (40 percent of the overall sample) overwhelmingly think it has been effective at preventing a nuclear attack on the United States (88 percent of those familiar with deterrence).

On the other hand, just under half the public think nuclear weapons make the United States safer (47 percent). When combined, almost as many say that nuclear weapons don't make a difference (24 percent) in making the country safer or that they don't know enough about nuclear weapons to express a view (19 percent). On this question, there are significant differences between age groups, racial groups, and partisan affiliations. Only among Americans over the age of 45 does a majority say that the US nuclear arsenal makes the country safer (55 percent); a plurality of younger Americans say they don't make a difference. White Americans are more likely than other racial groups to say nuclear weapons make the country safer, largely because Hispanic and African Americans are more likely to say they do not know enough to express a view. And Republicans (61 percent) are more convinced than Democrats (45 percent) that nuclear weapons make the United States safer.

While lacking familiarity about US nuclear weapons policy, a majority (60 percent) of the US public also say they are interested in learning more. When they are asked in an open-ended question to specify what they would like to learn more about, the responses fall into three broad categories: basic questions about how nuclear weapons operate (24 percent), the effects of nuclear weapons when they are deployed (22 percent), and more details about US nuclear weapons policy (18 percent). An additional 42 percent of people who want to know more did not offer a specific response about what topics or issues they would like to explore.

Where Americans go for information about nuclear weapons

Television is the most popular source for nuclear weapons information for those 30 and over. Social media plays that role for Gen Z, a finding that tracks with where these groups go for most of their news in general. Very few turn to government for more information. Across all age demographics, 9 percent or fewer say they turn most often to the US government for information about nuclear weapons policy. Very few turn to academics or activists to get information about nuclear issues.

Who are the most trusted sources of information on nuclear issues? Government is once again toward the bottom of the list. Six in 10 respondents say they distrust Congress for information about nuclear issues (63 percent). Party identification and age demographics don't make a difference; many people are skeptical of information about nuclear weapons from Congress.

While trusted more than Congress, the president (56 percent distrust), elicits more partisan division, with 76 percent of Republicans and 37 percent of Democrats skeptical of the president as a source of information, likely a reflection of a Democratic president in the Oval Office now. However, there is more partisan agreement around discomfort with the issue of sole authority. Sixty-two percent of Americans report being somewhat or very uncomfortable with the US president having the sole authority to launch a nuclear strike.

Even though few citizens turn to them for nuclear weapons information, the highest marks on trust go to academics, with 58 percent of respondents saying they place a great deal or fair amount of trust in academics as a source of information on nuclear issues. A close second is the military—56 percent place some or a great deal of trust with the military on nuclear issues.

Will Americans become more involved?

Respondents to our survey said they should be more involved; six in 10 say the American people should be more influential in US nuclear policy. But, somewhat discordantly, most don't want to be more involved personally, with just 21 percent saying they would like to be more involved. Just shy of 40 percent are comfortable with their current level of involvement in US nuclear policy. A third (34 percent) report they have no desire to get involved in this area. This response rises to 43 percent among those between the ages of 18 and 29.

Some have argued that today's nuclear weapons debate has become too technical and distant, perhaps making the topic less tangible and accessible for most Americans. The fears surrounding the potential use of nuclear weapons related to the war in Ukraine and the Oppenheimer film clearly have stirred some interest among the general public. But it is unclear how long that interest may last. While a minority, the 21 percent who responded in our survey that they want to be more involved could, if they did so, make a real difference in at least the American nuclear weapons debate. But the varied responses to our survey suggest that today's Americans struggle, like Oppenheimer did, to reconcile conflicting senses: Nuclear weapons provide some security, but if ever used, they would inflict a terrible cost on the entire world.

Dina Smeltz is a senior fellow at the Chicago Council of Global Affairs. She oversees the Council's well-known annual survey of American attitudes toward foreign policy and has authored and co-authored many of the analyses based on that work. She also directs the Council's collaboration with Russian, Mexican, Canadian, Australian, and East Asian research organizations. Smeltz has published commentary on public opinion and international issues in *The Washington Post*, *Foreign Affairs*, *POLITICO*, *RealClearWorld*, *Foreign Policy*, and the Council's survey blog (*Running Numbers*). As the director of research in the Middle East and South Asia division (2001-2007) and analyst/director of the European division (1992-2004) in the Bureau of Intelligence and Research at the US State Department's Office of Research, Smeltz conducted over a hundred surveys in these regions and regularly briefed senior government officials on key research findings.

Sharon K. Weiner is a senior resident fellow in the International Peace and Security program of the Carnegie Corporation of New York. While serving in this role, Weiner will take a leave of absence from her position as an associate professor at American University's School of International Service. At American University, her teaching, research, and policy engagement are at the intersection of organizational politics and U.S. national security. Her work also focuses on civil-military relations and nuclear weapons programs and nonproliferation. Previously, Weiner served as a program examiner with the White House's Office of Management and Budget, where she was responsible for budget and policy issues related to nuclear weapons and nonproliferation. She has worked for the Armed Services Committee of the US House of Representatives and has held research positions at the Los Alamos National Laboratory and at Princeton University's Program on Science and Global Security. Weiner holds a PhD in political science from MIT's Security Studies Program.

EDITOR'S COMMENT: Are we talking about **these Americans**?

Japan Pushes The Button on Fukushima Water Dump, Despite Backlash

By Mathias CENA, AFP

Source: https://www.sciencealert.com/japan-pushes-the-button-on-fukushima-water-dump-despite-backlash

Key switch operations for the initial discharge of wastewater at the Fukushima Daiichi nuclear power plant. (Tokyo Electric Power Company)

Aug 15 – Japan began releasing wastewater from the crippled Fukushima nuclear plant into the Pacific Ocean on Thursday, prompting a furious China to ban all seafood imports from its neighbour.

The start of the discharge of around 540 Olympic swimming pools' worth of water over several decades is a big step in decommissioning the still highly dangerous site 12 years after one of the world's worst nuclear accidents.

Live video provided by plant operator TEPCO showed two engineers clicking on computer mouses and an official saying – after a countdown – that the "valves near the seawater transport pumps are opening".

Japan has repeatedly insisted the wastewater is treated and will be harmless, a position backed by UN atomic watchdog the International Atomic Energy Agency (IAEA).

The IAEA said on Thursday that new on-site tests had confirmed the levels of radioactive tritium in the water being discharged were safe.

But China has warned the release will contaminate the ocean, and immediately responded Thursday by blasting Japan as "extremely selfish".

It then banned all Japanese seafood imports "to comprehensively prevent the food safety risks of radioactive contamination" – with Japan hours later demanding China lift the ban.

North Korea's foreign ministry likewise criticised the release, urging Japan to call it off.

Local fishermen in Japan have also voiced opposition.

About 10 people held a protest near Fukushima on Thursday and around 100 others gathered outside TEPCO headquarters in Tokyo. "It's like dumping an atomic bomb in the ocean. Japan is the first country that was attacked with an atomic bomb in the world, and the prime minister of the country made this decision," said Kenichi Sato, 68, in Tokyo.

Multiple meltdowns

Three reactors at the Fukushima-Daiichi facility in northeastern Japan went into meltdown following a massive earthquake and tsunami that killed around 18,000 people in 2011.

Since then, TEPCO has collected 1.34 million cubic metres of water that was contaminated as it cooled the wrecked reactors, along with groundwater and rain that has seeped in.

Japan says that all radioactive elements have been filtered out except the tritium, levels of which are harmless and lower than what is discharged by operational nuclear power plants – including in China.

Environmental group Greenpeace says that the filtration process is flawed. China and Russia have suggested the water be vaporised and released into the atmosphere instead.

But Japan's analysis is backed by most experts.

"When released into the Pacific, the tritium is further diluted into a vast body of water and would quickly get to a radioactivity level which is not discernibly different from normal seawater," said Tom Scott from the University of Bristol.

TEPCO will carry out four releases of the treated water from Thursday until March 2024.

The first will last about 17 days, though it is expected to take around 30 years for all of the wastewater to be discharged.

With around 1,000 steel containers holding the water, TEPCO has said it needs to clear space for the removal of highly dangerous radioactive nuclear fuel and rubble from the three wrecked nuclear reactors.

Sushi safety

Even before Thursday's release, China had banned seafood imports from 10 of Japan's 47 prefectures and imposed radiation checks.

Hong Kong and Macau, both Chinese territories, followed suit this week.

China on Thursday extended its import ban to cover all of Japan, while Prime Minister Fumio Kishida told reporters that Tokyo had demanded Beijing "immediately eliminate" the ban, calling for "science-based discussions".

Analysts said that while China may have genuine safety concerns, its strong reaction is also motivated at least in part by its economic rivalry and frosty relations with Japan.

The South Korean government, which is seeking to improve ties with Japan, has not objected, although many ordinary people are worried and there have been scattered protests.

On Thursday, police arrested more than 10 people who tried to enter the Japanese embassy in Seoul.

South Korean Prime Minister Han Duck-soo said there was "no need to be excessively concerned" about the plan.

Han also criticised what he called a "politically driven" campaign using "fake news" to fan fears.

Social media posts in China and South Korea have included false claims about the release, including doctored images of deformed fish with claims they were linked to Fukushima.

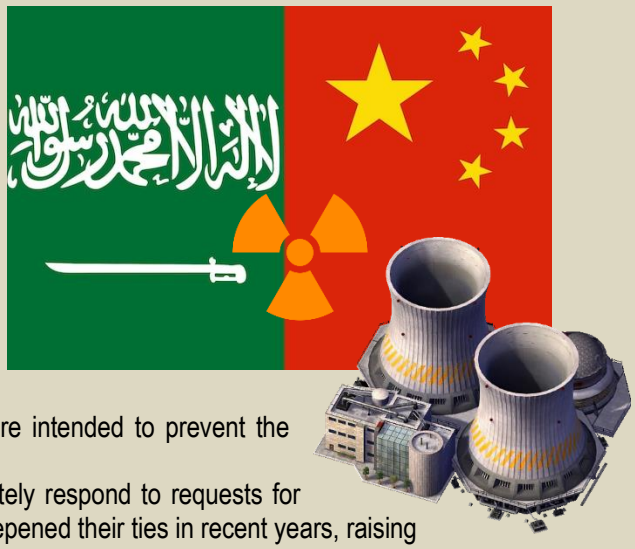
'Future generations'

People in the Japanese fishing industry also oppose the release, concerned that governments and consumers will shun their seafood.

"I am worried about the future," protester Ruiko Muto, 70, told AFP in Miharu near the power plant.
"We can't pass on the responsibility of what happened during our generation to the generation of our children and to future generations."

Saudi Arabia considering Chinese bid to build nuclear plant, report says

Source: https://www.aljazeera.com/economy/2023/8/25/saudi-arabia-considering-chinese-bid-to-build-nuclear-plant-report-says



Aug 25 – Saudi Arabia is considering a Chinese bid to build a nuclear power plant in the kingdom amid frustration over the United States' stipulations for supporting Riyadh's quest for nuclear power, the Wall Street Journal has reported.
China National Nuclear Corporation (CNNC), a state-owned firm, has proposed the construction of a nuclear plant near the border with Qatar and the United Arab Emirates, the newspaper reported on Thursday, citing unnamed Saudi officials.
Saudi officials hope the Chinese bid will push US President Joe Biden's administration to loosen its conditions for aiding the kingdom's nascent nuclear industry, including commitments not to enrich uranium or mine their own uranium deposits, the newspaper said.
China is unlikely to require Riyadh to adhere to such requirements, which are intended to prevent the proliferation of nuclear weapons, the newspaper said.
CNNC and the foreign ministries of China and Saudi Arabia did not immediately respond to requests for comment made by the Reuters news agency. Saudi Arabia and China have deepened their ties in recent years, raising concern in Washington. Chinese President Xi Jinping visited the kingdom in December and the two countries in June announced investment deals worth $10bn during the two-day Arab-China business summit in Riyadh.
Xi, whose country is the world's biggest energy consumer, has pledged to pursue a "pattern of multi-faceted energy cooperation" with Gulf countries. China has in recent years sought to export its nuclear energy industry overseas.
In 2019, a senior Chinese official said Beijing could build as many as 30 overseas nuclear reactors through its "Belt and Road" infrastructure drive over the following decade.
Beijing has also ramped up its diplomatic presence in the region, including brokering a deal earlier this year that normalised relations between Saudi Arabia and Iran after years of hostilities.
Saudi Arabia, one of the world's biggest oil producers, has for years explored the development of a domestic nuclear energy industry to reduce its dependence on fossil fuels.
The kingdom generates almost all of its power needs from oil and natural gas, according to the US Energy Information Administration.

There should be no Saudi uranium enrichment

By Victor Gilinsky
Source: https://thebulletin.org/2023/08/there-should-be-no-saudi-uranium-enrichment/

Aug28 – There is increasing talk of a United States-brokered "grand bargain" on Middle East security, the core of which would be normalization of ties between Israel and Saudi Arabia. It isn't clear what motivates Joe Biden to press for this deal now. The obvious goal would involve the eternal search for peace in the Middle East, but there are hints that such a bargain may have more to do with keeping the Saudis out of China's orbit. One thing we know, Biden's lieutenants are lobbying hard in the Senate for acceptance of some version of far-reaching demands from the Saudi crown prince, Mohammed bin Salman, among them access to uranium enrichment technology that would ostensibly provide fuel for future Saudi nuclear power plants. Indeed, enrichment is a step in the production of nuclear reactor fuel. It is also a vital part of one of two paths to the atomic bomb.
As always, the "realists" argue that we can't be too fastidious about our partners. If we refuse to accommodate Saudi nuclear aspirations, then Russia and China will step in, and we will have less influence in the Middle East. But the record of "realistic" foreign policy is not so great, either. Indulging the crown prince in his illicit quest is just too dangerous.
The crown prince hasn't been shy about revealing how he may use a civilian nuclear power project. In a 2018 CBS News interview he said, "Saudi Arabia does not want to acquire any nuclear bomb, but without a doubt if Iran developed a nuclear bomb, we will follow suit as soon as possible." Will he wait for that

development? He made no mention of working through the international system to prevent an Iranian bomb. He wants a nuclear power program on a hair trigger, ready to convert quickly to a nuclear weapon program.

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.

That isn't of course the polite version of the crown prince's plan. He says he wants to use domestic uranium, of which the Saudis claimed to have large deposits, to fuel civilian nuclear power reactors. He wants to produce fuel domestically, ergo he needs to acquire enrichment technology. But despite Saudi claims, there are no significant uranium deposits in the country. Recent reports reveal that the teams of geologists sent to search for it have turned up empty-handed. That hasn't, however, caused the crown prince to lose interest in enrichment, which is itself a revealing fact about his intentions—and his reliance on American cupidity. To cope with what the Saudis regard as excessive suspicion of others, they have suggested they are open to accepting some modest additional oversight arrangements, which they cynically expect Congress to accept after members engage in some ritual handwringing.

You would think the Saudi insistence on inclusion of enrichment, no matter how restricted, would be a non-starter for a US-Saudi "123" agreement for nuclear cooperation. (Compliance with Section 123 of the Atomic Energy Act is essential for any significant US-Saudi nuclear trade.) But such common sense is a thin reed to lean on when it comes to Washington nuclear politics. Powerful lobbies have been pushing for years for sale of power reactors in the Middle East and for generous subsidies to allow this to happen. The departments of Energy and State will be supporting this, too, claiming that international "safeguards" would be effective in preventing misuse of civilian nuclear facilities. The official line on nuclear energy is still Atoms for Peace, as it has been since President Eisenhower's 1953 speech. Recall that George W. Bush said even Iranian power reactors, by themselves, were perfectly legitimate.

The problem is that hardly anyone in Congress has any real understanding of nuclear technology. The members are swept off their feet by promises of safe, non-carbon producing energy sources, especially when nuclear proponents use adjectives like "small" and "modular" and "advanced." Congressional discussions on international aspects seldom get beyond "restoring America's competitive advantage in nuclear energy."

There is also little understanding of the limitations of international "safeguards," the inspection system of the International Atomic Energy Agency (IAEA). (Is there any realistic recourse if the Saudis break the rules?) It is indicative of Saudi Arabia's attitude toward the IAEA that it has used every stratagem to

minimize its safeguards responsibilities. The minimization strategy does not violate IAEA requirements, yes, but a country anxious to demonstrate its nuclear bona fides should be more forthcoming in its nonproliferation cooperation.
The 2008 US-India civil nuclear agreement is an eternal warning about how American international nuclear policy can go off the rails when the president and Congress are swept away by visions of gaining an ally against China *plus* the prospect of dozens of power reactor sales. That agreement ran a truck through the Non-Proliferation Treaty, and none of the sales of nuclear power plants materialized.
The Saudis know Americans can be made to swallow principle—they recently succeeded in humbling the US president on human rights and oil prices—and so are unlikely to soften their stance on inclusion of enrichment in a 123 agreement. The White House will be looking for a formula that accepts it, but adds some restriction, or appearance of restriction, or another sweetener, perhaps related to Palestinian rights, that would allow members of the House and Senate to go along with inclusion of enrichment in a US-Saudi agreement.
Who would stand in the way? Not the Republicans: They love the Saudis. The one possibility is if Israel balks at any deal that includes Saudi enrichment. Opposition Leader Yair Lapid told Democratic Party lawmakers visiting Israel recently that he opposes a potential Israel-Saudi Arabia normalization deal that allows Riyadh to enrich uranium because it would harm Israel's security. But the Israeli government's response—that is, Prime Minister Netanyahu's—has been ambiguous.
Somebody needs to stand up. Not only should the United States say no to Saudi enrichment, but Washington should also rethink the entire notion of nuclear power reactors in Saudi Arabia. Such reactors, coupled with a reprocessing facility to extract plutonium from used fuel, which the Saudis will surely want as well, provide the other path to a bomb, a plutonium bomb.
With its constant threat of wars, the Middle East is no place for nuclear reactors. Nuclear reactors in the region have been targeted in aerial attacks a dozen times. The safety issues that followed the capture by the Russians of the Zaporizhzhia power reactors in Ukraine should teach us something, too. Nuclear reactors do not belong in regions of potential conflict.
The ultimate argument against a US-Saudi nuclear deal is the crown prince himself, who is in line to be king and for practical purposes already is. He is a liar and a gruesome killer. Saudi Arabia, for all its modern trappings, is a primitive state with no effective checks on his powers. The king makes the laws, rules by decree, and is the chief judge. He has powers the British king gave up in the 13th century. Saudi Arabia has a long way to go before it will be a safe place for nuclear energy.

Victor Gilinsky is a physicist and was a commissioner of the US Nuclear Regulatory Commission during the Ford, Carter, and Reagan administrations.

Ms. Nuclear Energy Is Winning Over Nuclear Skeptics

By Poornima Apte
Source: https://www.homelandsecuritynewswire.com/dr20230829-ms-nuclear-energy-is-winning-over-nuclear-skeptics

Aug 29 – First-year MIT nuclear science and engineering (NSE) doctoral student Kaylee Cunningham is not the first person to notice that nuclear energy has a public relations problem. But her commitment to dispel myths about the alternative power source has earned her the moniker "Ms. Nuclear Energy" on TikTok and a devoted fan base on the social media platform.
Cunningham's activism kicked into place shortly after a week-long trip to Iceland to study geothermal energy. During a discussion about how the country was going to achieve its net zero energy goals, a representative from the University of Reykjavik balked at Cunningham's suggestion of including a nuclear option in the alternative energy mix. "The response I got was that we're a peace-loving nation, we don't do that," Cunningham remembers. "I was appalled by the reaction, I mean we're talking energy not weapons here, right?" she asks. Incredulous, Cunningham made a TikTok that targeted misinformation. Overnight she garnered 10,000 followers and "Ms. Nuclear Energy" was off to the races. Ms. Nuclear Energy is now Cunningham's TikTok handle.

A Theater and Science Nerd
TikTok is a fitting platform for a theater nerd like Cunningham. Born in Melrose, Massachusetts, Cunningham's childhood was punctuated by moves to places where her roofer father's work took the

family. She moved to North Carolina shortly after fifth grade and fell in love with theater. "I was doing theater classes, the spring musical, it was my entire world," Cunningham remembers. When she moved again, this time to Florida halfway through her first year of high school, she found the spring musical had already been cast. But she could help behind the scenes. Through that work, Cunningham gained her first real exposure to hands-on tech. She was hooked.

Soon Cunningham was part of a team that represented her high school at the student Astronaut Challenge, an aerospace competition run by Florida State University. Statewide winners got to fly a space shuttle simulator at the Kennedy Space Center and participate in additional engineering challenges. Cunningham's team was involved in creating a proposal to help NASA's Asteroid Redirect Mission, designed to help the agency gather a large boulder from a near-earth asteroid. The task was Cunningham's induction into an understanding of radiation and "anything nuclear." Her high school engineering teacher, Nirmala Arunachalam, encouraged Cunningham's interest in the subject.

The Astronaut Challenge might just have been the end of Cunningham's path in nuclear engineering had it not been for her mother. In high school, Cunningham had also enrolled in computer science classes and her love of the subject earned her a scholarship at Norwich University in Vermont where she had pursued a camp in cybersecurity. Cunningham had already laid down the college deposit for Norwich.

But Cunningham's mother persuaded her daughter to pay another visit to the University of Florida, where she had expressed interest in pursuing nuclear engineering. To her pleasant surprise, the department chair, Professor James Baciak, pulled out all the stops, bringing mother and daughter on a tour of the on-campus nuclear reactor and promising Cunningham a paid research position. Cunningham was sold and Backiak has been a mentor throughout her research career.

Merging Nuclear Engineering and Computer Science

Undergraduate research internships, including one at Oak Ridge National Laboratory, where she could combine her two loves, nuclear engineering and computer science, convinced Cunningham she wanted to pursue a similar path in graduate school.

Cunningham's undergraduate application to MIT had been rejected but that didn't deter her from applying to NSE for graduate school. Having spent her early years in an elementary school barely 20 minutes from campus, she had grown up hearing that "the smartest people in the world go to MIT." Cunningham figured that if she got into MIT, it would be "like going back home to Massachusetts" and that she could fit right in.

Under the advisement of Professor Michael Short, Cunningham is looking to pursue her passions in both computer science and nuclear engineering in her doctoral studies.

The Activism Continues

Simultaneously, Cunningham is determined to keep her activism going.

Her ability to digest "complex topics into something understandable to people who have no connection to academia" has helped Cunningham on TikTok. "It's been something I've been doing all my life with my parents and siblings and extended family," she says. Punctuating her video snippets with humor — a Simpsons reference is par for the course — helps Cunningham break through to her audience who love her goofy and tongue-in-cheek approach to the subject matter without compromising accuracy. "Sometimes I do stupid dances and make a total fool of myself, but I've really found my niche by being willing to engage and entertain people and educate them at the same time."

Such education needs to be an important part of an industry that's received its share of misunderstandings, Cunningham says. "Technical people trying to communicate in a way that the general people don't understand is such a concerning thing," she adds. Case in point: the response in the wake of the Three Mile Island accident, which prevented massive contamination leaks. It was a perfect example of how well our safety regulations actually work, Cunningham says, "but you'd never guess from the PR fallout from it all."

As Ms. Nuclear Energy, Cunningham receives her share of skepticism. One viewer questioned the safety of nuclear reactors if "tons of pollution" was spewing out from them. Cunningham produced a TikTok that addressed this misconception. Pointing to the "pollution" in a photo, Cunningham clarifies that it's just water vapor. The TikTok has garnered over a million views. "It really goes to show how starving for accurate information the public really is," Cunningham says, " in this age of having all the information we could ever want at our fingertips, it's hard to sift through and decide what's real and accurate and what isn't."

Another reason for her advocacy: doing her part to encourage young people toward a nuclear science or engineering career. "If we're going to start putting up tons of small modular reactors around the country, we need people to build them, people to run them, and we need regulatory bodies to inspect and keep them safe," Cunningham points out. " And we don't have enough people entering the workforce in comparison to those that are retiring from the workforce," she adds. "I'm able to engage those younger audiences and put nuclear engineering on their radar," Cunningham says. The advocacy has been paying off: Cunningham regularly receives — and responds to — inquiries from high school junior girls looking for advice on pursuing nuclear engineering.

All the activism is in service toward a clear end goal. “At the end of the day, the fight is to save the planet,” Cunningham says, “I honestly believe that nuclear power is the best chance we’ve got to fight climate change and keep our planet alive.”

Poornima Apte, a free-lance writer and editor, draws on her mechanical engineering and materials scientist background for her technology writing.

Radioactive German pigs affected by unexpected source of contamination

Source: https://newatlas.com/science/radioactive-pigs-contamination/

The radioactive contamination of wild boars in Germany and Austria has led to an overpopulation issue in some areas, as their meat is considered unsafe for human consumption

Aug 30 – Free-roaming boars in the woods of Austria and Germany have levels of radioactivity that makes their meat unsuitable for eating. Once thought to be the result of the Chernobyl nuclear power plant accident, new research points to another, darker, source of contamination.

When the Chernobyl nuclear power plant accident occurred in 1986, it represented "the largest uncontrolled radioactive release into the environment ever recorded for any civilian operation," according to the World Nuclear Association. Radioactive material spewed into the air for 10 days, finding its way into the ecosystem and the food chain. Two of the chief contaminants from the accident were radionuclides **cesium-135 and cesium-137**.

Even though wildlife in the 4,200-sq-km (1,621-sq mi) human exclusion zone eventually rebounded, ongoing radioactive contamination of animals with cesium still continues, although it has lessened in many animals.

Not so with the wild pigs in Germany and Austria. In what's become known as the "wild boar paradox," their levels of radioactivity still remain high enough to exceed regulatory limits for human consumption. To find out why this is, researchers from Leibniz University in Germany and the Vienna University of Technology worked with hunters in Southern Germany to collect wild boar meat.

Upon examining the meat with a gamma-ray detector and mass spectrometry, they were able to determine specific ratios of the two forms of cesium. These ratios revealed that, while some of the contamination did come from Chernobyl, another important source of the radioactivity was global nuclear weapons tests carried out in the 1960s. The cesium released by those tests found its way into food sources for the boar, including underground truffles, which is why their overall levels of radioactivity still have not returned to safe levels.

The study revealed that 88% of the samples they tested were still too radioactive to consume and that in some cases, the contamination from weapons testing alone was enough to make the meat unsafe. Overall, the researchers found that between 10 to 68% of the contamination came from weapons tests instead of Chernobyl. This led them to conclude that decades-old nuclear weapons testing has been an underreported source of radiocesium contamination in the pigs, and that the mix of radioactive materials from multiple sources is more persistent and dangerous than from one source alone.

"Once released, radiocesium will remain in the environment for generations and impact food safety immediately and, as shown in our study, for decades," write the researchers in a paper published in the journal, *Environmental Science & Technology*.

"Any additional releases will cause further accumulation and mixing with older sources, making it necessary to understand the underlying mechanisms of the biogeochemical cycling of radiocesium. For example, the impact of soil properties on mixing of different radiocesium sources has not yet been understood sufficiently. Consequently, more efforts are still needed to better understand the sources, inventories, environmental fates, and ecological risks of radiocesium," they conclude.

German Nuclear Phaseout Leaves Radioactive Waste Problem

By Klaus Deuse

Source: https://www.homelandsecuritynewswire.com/dr20230831-german-nuclear-phaseout-leaves-radioactive-waste-problem

Aug 31 – Germany ended the era of nuclear energy in Europe's biggest economy when it decommissioned the last three remaining nuclear power plants on April 15 this year. Decades of nuclear power generation, however, have left a legacy that is unlikely to go away as smoothly as the phaseout: nuclear waste.

Since a permanent German storage facility is out of sight in the near future, the spent fuel rods, packed into specialized containers called **Casks for Storage and Transport of Nuclear Material** (CASTOR), will likely remain in interim storage for decades.

About 1,200 CASTOR containers are currently stored at 17 interim sites in Germany. A state-owned company, the Bundeseigene Gesellschaft für Zwischenlagerung mbH (BGZ), is tasked with operating the sites.

BGZ spokesperson Janine Tokarski told DW that the company finally expects "about 1,800 containers from across Germany to be designated for final disposal."

Another state company, the Federal Company for Radioactive Waste Disposal (BGE), is exploring sites in Germany for the final disposal of the dangerous waste. According to Tokarski of BGZ, experts plan to find a site and, more importantly, reach a political consensus on it "in the 2040s at the earliest."

From then on, another 20 to 30 years are likely to be spent on planning and construction, said Tokarski. She anticipates the beginning of final storage "in the 2060s at the earliest." The shipping of all the waste from the various interim sites will probably take another 30 years, she added.

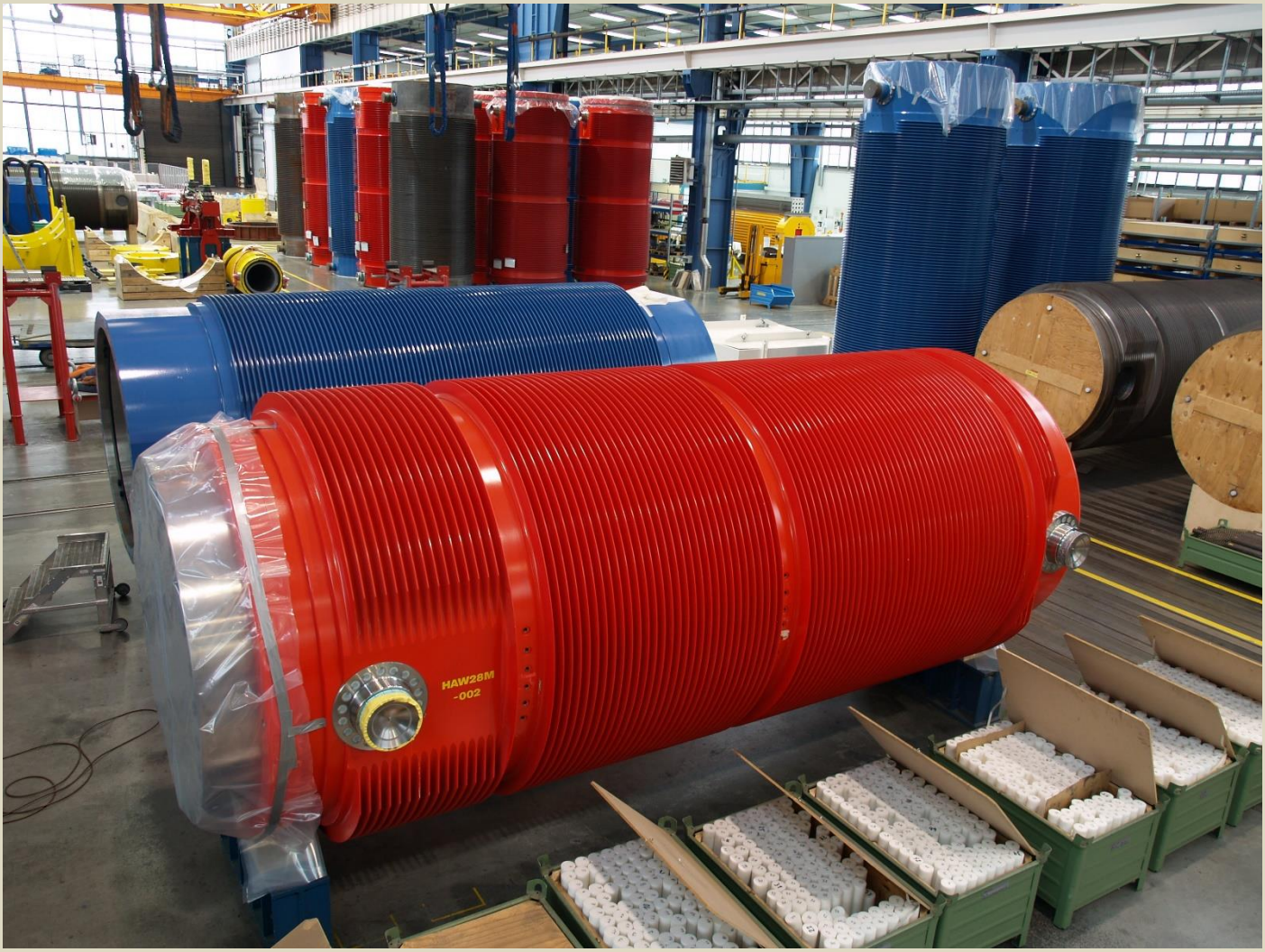
The century-long operation is expected to cost hundreds of billions of euros. Last year alone, BGZ spent €271 million ($292 million) just to ensure Germany's nuclear waste is safely stored — €191 million of the sum on operating the interim sites and €80 million on investments in them.

A Nuclear Fortress

In 1992, the first CASTOR containers with highly radioactive fuel rods were stored in the interim storage site of Ahaus in northwestern Germany.

The 200-meter-long (218-yard-long) central storage building towers 20 meters high above the flat landscape of the Münsterland region and is protected by a wire fence surrounding the sprawling 5,700-square-meter (61,354-square-feet) site.

Bisected by a reception and maintenance area, the building currently holds more than 300 yellow casks containing burned fuel rods. Additionally, six CASTOR containers, each 6 meters long and weighing 120 tons, are stored in one of the two halls, keeping the waste leak-tight for a calculated 40 years.



Leak tightness is achieved through a pressure switch installed in the double-wall sealing system of these containers, said David Knollmann from BGZ in Ahaus.

"A gas is inserted between the two walls, specifically helium gas, at a certain pressure. This switch ensures the pressure doesn't fall below a certain level," he told DW.

David Knollmann proudly added that in 30 years, there hasn't been a single case of a container requiring repairs.

The nuclear safety at the Ahaus interim storage site is not only overseen by German nuclear authorities but also by Euratom, an independent nuclear energy organization run by European Union member states, and the International Atomic Energy Agency (IAEA). Their auditors inspect the site regularly but without advance notice.

Pressure of Time

In addition to the two central interim storage facilities in Ahaus and Gorleben, Germany operates other decentralized temporary storage facilities at the sites of all former German nuclear power plants.

Moreover, additional waste, shipped for reprocessing to France and the UK, will eventually return to Germany. Knollmann said this will only happen "when all the necessary regulatory conditions are met."

Much of the waste, he explained, comes from "dismantled nuclear power plants" and includes contaminated pumps and filters. Those would eventually be stored at the Schacht Konrad site near the town of Salzgitter, a former iron ore mine proposed as a deep geological repository for medium- and low-level radioactive waste.

The Schacht Konrad mine, said Tokarski, is expected to become operational as a nuclear waste storage "around the early 2030s." All German interim storage sites are subject to limited operating permits of 40 years. For example, the permit for the Ahaus site will be up for renewal by 2028 at the latest. As all experts agree that a final central repository for Germany's nuclear waste won't be fully operational before 2090 at the earliest, the country faces the problem of what to do with the radioactive material until then.
Without political consensus on the issue, Ahaus residents fear that their neighborhood's storage facility might secretly become "a final repository solution."

Emergency Management in the Event of Radiological Dispersion in an Urban Environment

By Edoardo Cavalieri d'Oro and Andrea Malizia
Sensors *2023*, 23*(4)*, *2029*
Source (**full text**): https://www.mdpi.com/1424-8220/23/4/2029

Abstract

Dispersion of a radiological source is a complex scenario in terms of first response, especially when it occurs in an urban environment. The authors in this paper designed, simulated, and analyzed the data from two different scenarios with the two perspectives of an unintentional fire event and a Radiological Dispersal Device (RDD) intentional explosion. The data of the simulated urban scenario are taken from a real case of orphan sources abandoned in a garage in the center of the city of Milan (Italy) in 2012. The dispersion and dose levels are simulated using Parallel Micro Swift Spray (PMSS) software, which takes into account the topographic and meteorological information of the reference scenarios. Apart from some differences in the response system of the two scenarios analyzed, the information provided by the modeling technique used, compared to other models not able to capture the actual urban and meteorological contexts, make it possible to modulate a response system that adheres to the real impact of the scenario. The authors, based on the model results and on the evidence provided by the case study, determine the various countermeasures to adopt to mitigate the impact for the population and to reduce the risk factors for the first responders.

Bigger isn't always better: Why the US fails to deter North Korea, despite nuclear superiority

By Lauren Sukin
Source: https://thebulletin.org/2023/09/bigger-isnt-always-better-why-the-us-fails-to-deter-north-korea-despite-nuclear-superiority/

Sep 01 – A hefty, 60-ton missile that North Korean leader Kim Jong-un has fondly called his "most powerful nuclear weapon" featured heavily in this year's Victory Day parade held on July 28 in Pyongyang. The missiles are North Korea's most sophisticated military technology. Capable of carrying nuclear weapons, the missiles boast an estimated maximum range of 15,000 kilometers—enough to hit targets anywhere in the United States.

Since last year's parade, North Korea has tested dozens of these ballistic missiles, more than it ever has in a single year. Although North Korea continues to build up its nuclear capabilities, its arsenal of just dozens of weapons is minuscule compared to the US arsenal of thousands. So, why has the United States proven unable to deter North Korea from testing?
The answer to this question is two-fold. First, the United States lacks the leverage needed to effectively influence North Korea through economic means. Second, US nuclear superiority over North Korea paradoxically makes Kim consider his nuclear arsenal essential to the survival of the regime. North Korea must make sure to stand strong in the face of each new crisis, lest it looks

vulnerable. It's this unbending resolve that makes North Korea effective at resisting the demands of its much more powerful adversaries.

Without Russia and China

North Korea's recent parade commemorated the 70th anniversary of the July 27, 1953 armistice agreement of the Korean War. That war saw North Korean forces fighting alongside the Soviet and Chinese militaries against South Korea and the United Nations Command, led by the United States. It was fitting, then, that this year's parade featured visits by Russian and Chinese officials, in the first such visits since the COVID-19 pandemic. The presence of these foreign dignitaries signified the strengthening relationships between North Korea and its neighboring allies.

North Korea is largely isolated on the international stage, in no small part due to very significant sanctions that limit the regime's ability to trade across the world. The country's largest trading partner is China. North Korea is wholly dependent on trade with—and aid—from Beijing.

Although there is less trade between North Korea and Russia, North Korea imports significant amounts of food and oil from its northern neighbor. Trade relations have also recently warmed between North Korea and Russia. Pyongyang has reportedly exported arms and artillery to Moscow to support Russia's war effort in Ukraine, and the two partners have restarted train travel along the Trans-Siberian Railway for the first time in years.

In comparison, the United States lacks economic leverage: Heavy sanctions have prevented any ties between the two countries and forced North Korea to adapt to non-reliance on the United States and its allies. Although the United States has, at times, provided emergency aid to North Korea, the largest sources of food aid to the country come from South Korea and China. The regime seems largely resilient to this trend, even shunning foreign aid—including vaccines—throughout the COVID-19 pandemic. In fact, over time, aid coming to North Korea from countries other than South Korea and China has slowed.

Recently, Russia and China have been instrumental in sheltering North Korea's growing provocations, but they have not always been so accommodating of the North Korean nuclear program. Nine UN resolutions—each with approval from Moscow and Beijing—have been passed condemning North Korean nuclear and missile testing. Each resolution also calls upon Pyongyang to suspend these illicit activities, although little lasting progress has been achieved to this end. The last UN resolutions on the issue of the North Korean nuclear program were passed in 2017 and there are few signs of any new UN activity in that regard. Russia and China have resisted any additional steps, despite repeated calls for the UN to discuss North Korea's recent testing uptick.

Russia and China have also previously been involved in the "Six Party Talks," a series of negotiations intended to halt the North Korean nuclear program. The last talks were held in 2008, with North Korea declaring in 2009 that it would no longer participate. Although China last called for the talks to be renewed in 2017, there is little hope that they will resume, at least in the short term.

While Russia and China have resisted condemning North Korea for its recent missile testing, the United States, Australia, Japan, South Korea, and the European Union have imposed additional, unilateral sanctions on North Korea and demanded that the tests cease. But despite these efforts, North Korea has continued to launch.

The role of resolve

If the United States is unable to use economic sticks to prod North Korea, what about military ones? My colleague Abby Fanlo and I published new research last month in *Security Studies*, which suggests that it is not *despite* nuclear superiority but *because* of it that the United States struggles to deter a comparatively much weaker adversary. That is, the asymmetry between the two countries' nuclear forces can be considered a key obstacle to North Korean denuclearization. The study, which examines all the nuclear crises that occurred until 2010, shows that carrying a big stick—or, at least, having a bigger nuclear button than one's enemy—can unfavorably change the dynamics of a crisis.

Crises that emerge between nuclear-armed countries with vastly different capabilities consistently represent high-stakes scenarios for the less-powerful adversary. Consider the Korean War, during which the Soviet Union wanted to maintain vital access to neighboring territory. Although the US nuclear arsenal was substantially larger at the time, Soviet nuclear threats effectively dissuaded the United States from escalating the conflict.

Asymmetric crises tend to be high stakes because of a selection effect. After all, it makes far more sense to acquiesce to the demand of an adversary that is many times more powerful, unless those demands would put your core interests at risk. This dynamic, though, doesn't work the same way when a set of adversaries is equally matched.

When two countries with very similar nuclear capabilities face off in crises, the principle of mutually assured destruction is at work. In these so-called "symmetric" crises, both sides can impose equal consequences on the other if a crisis escalates. As a result, they possess general deterrence, which enables them to prevent their adversaries from putting pressure on their most serious interests. This logic underlies why the Cold War was "cold."

In asymmetric crises, however, the weaker nuclear power is caught between a rock and a hard place. It can resist its adversary's demands and risk a crisis escalating into a war. Often, though, giving in to those

demands is off the table. The weaker country then has few options but to show its resolve to fight in a bid to secure immediate deterrence and fend off its adversary—albeit temporarily. In other words, the weaker country persists, because it has nothing more to lose; it is already committed to the maximum or bust.

And research shows that this strategy works. When a country has over 50 times more nuclear weapons than its adversary, its chances of emerging victorious from a crisis are nearly zero. If it has any more than three times as many nuclear weapons as an adversary, it will lose crises more often than it wins. Using novel methodological approaches designed for small datasets, the new research shows that there is no statistically significant advantage to exceeding one's adversary's nuclear arsenal by more than half its size.

The crucial commitment problem

These dynamics play out clearly in the US-North Korea relationship. At the core of the crisis between the United States and North Korea is a commitment problem, one involving tensions over the future of both the North Korean nuclear program and the authoritarian regime that has championed it. For its part, the United States would like to be rid of both. US leaders have repeatedly made it clear that a nuclear-armed North Korean regime will not be accepted.

President Joe Biden's 2022 National Defense Strategy states that "there is no scenario in which the Kim regime could employ nuclear weapons and survive." Former Central Intelligence Agency director Mike Pompeo stated that President Donald Trump had ordered the agency to "separate the North Korean regime from its missiles and nuclear weapons." President Barack Obama explained in a 2015 interview that the Kim regime was "brutal and … oppressive … you will see a regime like this collapse … and that's something we are constantly looking for ways to accelerate."

The United States could, in theory, say it would agree to a deal that reduced or removed the North Korean nuclear program in exchange for allowing the regime to stay in place. But over time, the United States would be unable to commit to keeping that promise. It would have every incentive to take advantage of the diminished North Korean capabilities to impose regime change on Pyongyang. (After all, the United States pursued regime change in Libya after its disarmament deal.) As Stanford University professor James Fearon writes, the real problem is that North Korea "can't trust us." So, they cannot—and will not—commit to disarm.

As a result, when crises emerge between the United States and North Korea, the fate of the North Korean regime is at stake—and, for Kim, it doesn't get more high-stakes than that. Pyongyang must then show its resolve in the face of any threats to its nuclear program. For North Korea, backing down to such threats is an existential concern, even if bidding up the risk of a nuclear conflict could also have existential consequences. In these high-stakes settings, North Korea has a risky advantage.

Despite having a comparative strategic advantage, the consequences of North Korean nuclear escalation are far too great for the United States to bear. As a result, North Korean signals of resolve are credible, and they are often sufficient for immediate deterrence, despite the regime's limited nuclear capabilities. That leaves the United States at a distinct disadvantage. It's time the United States learned that, at least in this situation, being bigger isn't always better.

US officials should think twice before adopting any measures meant to expand US nuclear capabilities. Such a policy is unlikely to be helpful when the United States faces far weaker adversaries, like North Korea. If Pyongyang's resolve is indeed its key advantage, the United States should work to undermine and counterbalance that—not by building up capabilities, but by showing cohesion and determination. The newly announced coordination efforts between US, South Korean, and Japanese forces represent a step in the right direction, although continued synchronization will be critical to cement trilateral ties.

The United States can't simply demand that North Korea stops its provocations. But it can handle each such provocations with care, responding with coordinated, confident messaging that makes it clear North Korea is not the only actor with much at stake.

Lauren Sukin is an assistant professor of international relations at the London School of Economics and Political Science. Her research examines the role of nuclear weapons in alliances, crisis politics, and public opinion. She holds a PhD and MA in political science from Stanford University and ABs in political science and literary arts from Brown University.

What's Behind North Korea's "Nuclear Attack" Drills?

By Julian Ryall

Source: https://www.homelandsecuritynewswire.com/dr20230905-whats-behind-north-koreas-nuclear-attack-drills

Sep 05 – Pyongyang has managed to increase the already elevated tensions on the Korean Peninsula in recent days with a number of military firsts.

The latest actions by the North Korean regime underlined its burgeoning alliance with Russia, with the anticipated announcement of a summit between the reclusive nation's leader Kim Jong Un and Russian President Vladimir Putin in Vladivostok, on the Pacific Coast of Russia.

State media reported last week that Kim had overseen military exercises that simulated a "scorched earth" nuclear strike against the South followed by an invasion across the Demilitarized Zone that divides the peninsula and then the occupation of North Korea's ideological rival.
The North said it had acted as South Korea and the US were plotting a pre-emptive nuclear assault on the North, adding, "The [Korean People's Army] staged a tactical nuclear strike simulating scorched-earth strikes at major command centers and operational airfields of the [South Korean] military gangsters."
The drills included the firing of two tactical ballistic missiles from mobile launchers close to Pyongyang.

North Korea's "Clear Message" to U.S., South Korea

Pyongyang said it was sending a "clear message" to Seoul and Washington, which have recently completed the 11-day Ulchi Freedom Shield joint military exercise that included US nuclear-capable B-1B strategic bombers flying with a fighter escort over the peninsula.
The North insisted that the flights show the US was "moving toward a pre-planned nuclear pre-emptive strike against us."
Pyongyang followed that exercise up with a "simulated tactical nuclear attack" on Saturday with the launch of two cruise missiles carrying dummy nuclear warheads, state-run media added.
Analysts say that it is clear the North has made great strides in its development of nuclear weapons and long-range missile systems, but it has little chance of successfully invading and occupying the southern half of the peninsula — despite a standing army of 1.3 million service members.
"In the past, the North Koreans invested heavily in artillery and building up their ammunition supplies, but virtually all of that is from the 1940s and 1950s," said Lance Gatling, a security and aerospace analyst and founder of Tokyo-based Gatling Associates.
"So, while they have a tremendous amount of this stuff and rocket artillery, it is not very precise over long ranges. Also, the ubiquitous intelligence, surveillance and reconnaissance capabilities of advanced countries have a tremendous impact on any offensive capability they [North Korea] might have," he told DW.
Satellites orbiting at 500 kilometers (310 miles) above the Earth and with the ability to provide intelligence 24 hours a day and in all weather conditions means that any looming North Korean attack will be visible well in advance.

North's Ground Forces Outclassed

Another problem the North faces is that it **only has three potential ground routes of attack against the South,** due to the geography of the peninsula, with any assault funneled into narrow areas and quickly resulting in what experts call "a cauldron of death" for the North's elderly tanks and under-equipped infantry units at the hands of the South and US forces.
It would be a similar situation for the North's air force, said Garren Mulloy, a professor of international relations at Daito Bunka University in Japan and an expert on military issues.
"Fighter pilots in NATO countries will put in a minimum of 200 hours of operational flying every year on the most advanced aircraft in their arsenals," he said. "It is estimated that North Korean pilots are only able to put in 20 hours a year due to shortages of fuel and their inability to obtain spare parts for their aircraft."
There are additional question marks over the North's capabilities in other areas, including chemical, biological and bacteriological weapons, often dubbed the "poor man's nuclear weapons."
"We know they have them and while no other country in the world would use them, we cannot entirely rule out the possibility of Pyongyang using these weapons, depending on just how threatened they felt," Mulloy said.
The North has no qualms about touting its nuclear capability, with the Seoul-based Korea Institute for Defense Analysis releasing a report in January estimating that Pyongyang's scientists have produced **more than 2.2 tons of weapons-grade highly enriched uranium and as much as 78 kilograms (172 pounds) of plutonium.**
That amount of fissile material would be sufficient for up to 90 warheads and, if development continues at the same pace, the institute believes North Korea could have 166 nuclear weapons by 2030.
It is this saber that Pyongyang is now rattling, and with increased confidence as geopolitical events in other parts of the world have led to alliances of mutual convenience with both Russia and China.

"Escalation of Threats of Violence"

"South Korea is not responsible for the escalation of these threats of violence from the North, although it has also been argued that the closer alliance between the South, the US and Japan has stimulated Pyongyang into those closer ties with Beijing and Moscow," said Lim Eun-jung, an associate professor of international studies at Kongju National University in South Korea.
The upgraded Moscow-Pyongyang alliance is arguably the most significant change in recent years, with both sides benefiting.

Kim is expected to travel to Vladivostok by armored train later this month.
It is likely that the North Korean leader and Putin will use their meeting to agree the transfer of North Korean munitions in return for Russian fuel and foodstuffs.
Just as significant as a trade, which will benefit both sides, will be the optics of the developing alliance, which comes shortly after Russia proposed trilateral naval exercises also including China.
But Pyongyang, already under a raft of international sanctions for its nuclear weapons program, has so far repeatedly denied supplying arms to Russia.
"The North originally got their shells from the Soviet Union and through China and have continued to manufacture this sort of ammunition, meaning they have huge stockpiles, and they can keep making more," said Gatling. "They will sell their inventory and while it may be old it will still be effective and, for the North, valuable because these shells will allow them to bring in food and oil.
"To me, it's clear that will strengthen both sides."

IAEA Launches New Software to Assist Nuclear Security Operations

By Andrea Rahandini and Vasiliki Tafili (IAEA Department of Nuclear Safety and Security)
Source: https://www.iaea.org/newscenter/news/iaea-launches-new-software-to-assist-nuclear-security-operations

June 08 – The IAEA has launched a new software tool — the Mobile-Integrated Nuclear Security Network— that provides real time radiation data on operations at high-traffic areas for goods and passengers, such as seaports, land border crossings and airports, which require nuclear security measures to be in place.
The Mobile-Integrated Nuclear Security Network (M-INSN) tool enables decision-makers, to use visual real-time radiation data, to make informed decisions to protect the public in case of a potential incident involving nuclear or other radioactive material.

"The M-INSN is an excellent example of how science and technology can support countries to effectively, efficiently, and sustainably implement relevant nuclear security measures," said Elena Buglova, Director of the IAEA Division of Nuclear Security. "It can facilitate countries, especially those which lack sustainable means, to exercise command and control over nuclear security operations."
The key characteristics of this secure communication system are that M-INSN administrators have direct access to real-time radiation data with the exact location of the individual users such as security personnel and radiation experts who use detection equipment, and the system is vendor neutral so any equipment can be incorporated into the user country-controlled software. Equipment status is constantly monitored on command centre computers and is displayed on an interactive map. The collection and aggregation of radiation data in M-INSN provides invaluable information to those involved in overseeing most nuclear security operations.
The M-INSN tool is freely available to countries and its core software is compatible with Windows and Linux computers, using either cloud or non-cloud based-servers. To support the transmission of detector data to the M-INSN server, Front-Line Officers are equipped with smartphones that are linked by Bluetooth to their radiation detectors. A M-INSN App installed on the smartphone securely transmits the data to the user country's server.
"M-INSN is a secure and vendor-neutral tool, which means that it is designed to work with any electronic equipment used in nuclear security operations, regardless of the manufacturer. Its features, from alarm indicators to language settings, will be completely customizable by users to meet their specific needs. Most importantly, all access and configurations of M-INSN are completely controlled by the user country," said Charles Massey, Senior Nuclear Security Officer at the IAEA Division of Nuclear Security.

Additional features will be added to the M-INSN in the coming months. Enhancements to M-INSN include "heat mapping" functionality that will automatically monitor previously established radiation level backgrounds and alert the security officers involved about any increased levels of radiation that require further investigation. In terms of equipment range, these include incorporating backpack-based radiation detectors, radioisotope identification devices and handheld X-ray backscatter scanners, and expanding the number of personal radiation detector manufacturers currently supported.
The availability of M-INSN with the IAEA's other tools, such as the Tool for Radiation Alarm and Commodity Evaluation (TRACE) and the Personnel Alarm Assessment Tool (PAAT), will be a part of the overall toolkit provided to countries to improve radiation detection operations in a variety of scenarios.
M-INSN's development is supported by funding from Germany and by in-kind contribution from the United States of America.

Supporting nuclear security measures during major public events
The use of M-INSN goes beyond the support of routine radiation detection operations related to a country's borders. M-INSN can vastly strengthen the implementation of nuclear security measures during major public events, such as popular international sporting events, to counter potential threats involving nuclear or other radioactive material. The need for early detection of threats from nuclear and other radioactive material is a crucial part of the overall preparations and event security planning activities.
The first-ever use of the M-INSN in a major public event was at the Women's U-20 Football World Cup, held in Costa Rica in August 2022. It was also used in support of the nuclear security measures in Egypt for the November 2022 United Nations Climate Change Conference (COP 27). As part of the IAEA's assistance provided to countries organizing major public events, extensive training on the detection equipment and M-INSN software operation is provided to Front-Line Officers, command centre staff and other entities involved in national nuclear security arrangements.
The IAEA's nuclear security programme involves developing scientific, technological, and engineering innovations to address current and emerging challenges and risks to nuclear security.

Pakistan nuclear weapons, 2023

By Hans M. Kristensen, Matt Korda, and Eliana Johns
Source: https://thebulletin.org/premium/2023-09/pakistan-nuclear-weapons-2023/

Sep 11 – Pakistan continues to gradually expand its nuclear arsenal with more warheads, more delivery systems, and a growing fissile material production industry. Analysis of commercial satellite images of construction at Pakistani army garrisons and air force bases shows what appear to be newer launchers and facilities that might be related to Pakistan's nuclear forces.

Table 1. Pakistani nuclear forces, 2023.

Type/designation	Number of launchers	Year deployed	Range (kilometers)[a]	Warhead x yield (kilotons)[b]	Number of warheads[c]
Air-delivered weapons[d]					
Mirage III/V	36	1998	2,100	1 x 5-12 kt bomb or Ra'ad-I/II[e] ALCM	36
[JF-17][f]	-			Ra'ad-I/II ALCM	-
Subtotal	*36*				*36*
Land-based weapons					
Abdali (Hatf-2)	10	2015	200	1 x 5-12 kt	10
Ghaznavi (Hatf-3)	16	2004	300	1 x 5-12 kt	16
Shaheen-I/A (Hatf-4)	16	2003/2022	750/900	1 x 5-12 kt	16
Shaheen-II (Hatf-6)	24	2014	1,500	1 x 10-40 kt	24
Shaheen-III (Hatf-6)	-	-2024	2,750	1 x 10-40 kt	-
Ghauri (Hatf-5)	24	2003	1,250	1 x 10-40 kt	24
Nasr (Hatf-9)	24	2013	60-70	1 x 12 kt	24[g]
Ababeel (Hatf-?)	-	-	2,200	MIRV/MRV?	-
Babur/-1A GLCM (Hatf-7)	12	2014	350[h]	1 x 5-12 kt	12
Babur-2/-1B GLCM (Hatf-?)	-	-[i]	700	1 x 5-12 kt	-
Subtotal	*126*				*126*
Sea-based weapons					
Babur-3 SLCM (Hatf-?)	-	[j]	450	1 x 5-12 kt	-
Other stored warheads					[8]
Total	162				170[k]

Table 1. Pakistani nuclear forces, 2023.

We estimate that Pakistan now has a nuclear weapons stockpile of approximately 170 warheads (See Table 1). The US Defense Intelligence Agency projected in 1999 that Pakistan would have 60 to 80 warheads by 2020 (US Defense Intelligence Agency 1999, 38), but several new weapon systems have been fielded and developed since then, which leads us to a higher estimate. Our estimate comes with considerable uncertainty because neither Pakistan nor other countries publish much information about the Pakistani nuclear arsenal.

With several new delivery systems in development, four plutonium production reactors, and an expanding uranium enrichment infrastructure, Pakistan's stockpile has the potential to increase further over the next several years. The size of this projected increase will depend on several factors, including how many nuclear-capable launchers Pakistan plans to deploy, how its nuclear strategy evolves, and how much the Indian nuclear arsenal grows. We estimate that the country's stockpile could potentially grow to around 200 warheads by the late 2020s, at the current growth rate. But unless India significantly expands its arsenal or further builds up its conventional forces, it seems reasonable to expect that Pakistan's nuclear arsenal will not continue to grow indefinitely but might begin to level off as its current weapons programs are completed.

Research methodology and confidence

The estimates and analyses made in the Nuclear Notebook are derived from a combination of open sources: (1) state-originating data (e.g. government statements, declassified documents, budgetary information, military parades, and treaty disclosure data); (2) non-state-originating data (e.g. media reports, think tank analysis, and industry publications); and (3) commercial satellite imagery. Because each one of these sources provides different and limited information that is subject to varying degrees of uncertainty, we cross-check each data point by using multiple sources and supplementing them with private conversations with officials whenever possible.

Analyzing Pakistan's nuclear forces is particularly fraught with uncertainty, given the lack of official state-originating data. The Pakistani government has never publicly disclosed the size of its arsenal and does not typically comment on its nuclear doctrine. Unlike some other nuclear-armed states, Pakistan does not regularly publish any official documentation explaining the contours of its nuclear posture or doctrine. Whenever such details emerge in the public discourse, it usually originates from retired officials commenting in their personal capacities. The most regular official source on Pakistani nuclear weapons is the Inter Services Public Relations (ISPR), the media wing of the Pakistan Armed Forces, which publishes regular press releases for missile launches and occasionally couples them with launch videos.

Occasionally, other countries offer official statements or analysis about Pakistan's nuclear forces. For example, the US Air Force's ballistic and cruise missile threat reports include analyses of Pakistani missile forces. As Pakistan's regional competitor, Indian officials also occasionally make statements about Pakistan's nuclear weapons, although such statements must be taken with a grain of salt as they are often politically motivated. Similarly, Indian media sources often either exaggerate or minimize the characteristics of Pakistan's arsenal, depending on the desired effect and audience. Pakistani media is also prone to frequent embellishment when describing the country's arsenal. There are very few publications that researchers can turn to for reliable information about Pakistan's nuclear forces and every rumor must be carefully investigated.

Given the absence of reliable data, commercial satellite imagery has become a particularly critical resource for analyzing Pakistan's nuclear forces. Satellite imagery makes it possible to identify air, missile, and navy bases, as well as potential underground storage facilities. The greatest challenge of analyzing Pakistani nuclear forces with satellite imagery is the lack of reliable data with which to cross-check information revealed by images, particularly with regards to whether certain military bases are associated with nuclear or conventional strike missions, or both.

Overall, the lack of accurate data about Pakistan's nuclear forces results in a lower degree of confidence in this Nuclear Notebook issue's estimates relative to those of most other nuclear-armed countries.

Pakistan's nuclear doctrine

Within its broader philosophy of "credible minimum deterrence," which seeks to emphasize a defensive and limited nuclear posture, Pakistan operates under a nuclear doctrine that it calls "full spectrum deterrence." This posture is aimed mainly at deterring India, which Pakistan identifies as its primary adversary. The belief that Pakistan's nuclear weapons have been deterring India since the mid-1980s has solidified the value of nuclear weapons in the nation's security calculus (Kidwai 2020, 2).

In May 2023, Lt. Gen. (Ret.) Khalid Kidwai—an advisor to Pakistan's National Command Authority, which oversees nuclear weapons development, doctrine, and employment—gave a speech at the Institute of Strategic Studies Islamabad (ISSI) where he offered his description of what "full spectrum deterrence" entails. According to Kidwai (2023), "full spectrum deterrence" implies the following:

- "That Pakistan possesses the full spectrum of nuclear weapons in three categories: strategic, operational and tactical, with full range coverage of the large Indian land mass and its outlying territories; there is no place for India's strategic weapons to hide.
- That Pakistan possesses an entire range of weapons yield coverage in terms of kilotons (KT), and the numbers strongly secured, to deter the adversary's declared policy of massive retaliation; Pakistan's "counter-massive retaliation" can therefore be as severe if not more.
- That Pakistan retains the liberty of choosing from a full spectrum of targets in a "target-rich India," notwithstanding the indigenous Indian BMD or the Russian S-400, to include counter value, counter force and battlefield targets."

According to Kidwai, who previously served as the director-general of the Strategic Plans Division (SPD), the "full spectrum" aspect of Pakistan's deterrence posture encompasses both "horizontal" and "vertical" elements. The horizontal aspect refers to Pakistan's nuclear "triad" encompassing the Army Strategic Force Command (ASFC), the Naval Strategic Force Command (NSFC), and the Air Force Strategic Command (AFSC). The vertical aspect refers to three tiers of destructive yield—"strategic, operational, and tactical"—as well as a range coverage "from zero meters to 2750 kilometers," allowing Pakistan to target the entirety of India (Kidwai 2023).

Kidwai and other former Pakistani officials have explained that this posture—as well as Pakistan's particular emphasis on non-strategic nuclear weapons—is specifically intended as a response to a perceived India's "cold start" doctrine (Kidwai 2020). The "cold start" doctrine is an alleged intention by India to launch large-scale conventional strikes or incursions into Pakistani territory without triggering Pakistani nuclear retaliation. Pakistan has reacted to this perceived doctrine by adding several short-range, lower-yield nuclear-capable weapon systems specifically designed to counter military threats below the strategic level.

An example of such a low-yield, close-range nuclear capability is Pakistan's Nasr (also known as Hatf-9) ballistic missile. In 2015, Kidwai stated that the Nasr was specifically "born out of a compulsion of this thing that I mentioned about some people on the other side toying with the idea of finding space for conventional war, despite Pakistan['s] nuclear weapons" (Kidwai 2015). According to Kidwai, Pakistan's understanding of India's "cold start" strategy was that Delhi envisioned launching quick strikes into Pakistan within two to four days with eight to nine brigades simultaneously: an attack force which would involve roughly 32,000 to 36,000 troops. "I strongly believe that by introducing the variety of tactical nuclear weapons in Pakistan's inventory, and in the strategic stability debate, we have blocked the avenues for serious military operations by the other side," Kidwai (2015) explained.

After Kidwai's (2015) statement, Pakistan's Foreign Secretary Aizaz Chaudhry publicly acknowledged the existence of Pakistan's "low-yield, tactical nuclear weapons," apparently the first time a top government official had done so (*India Today* 2015). At the time, the tactical missiles had not yet been deployed but their purpose was further explained by Pakistani defense minister Khawaja M. Asif in an interview with *Geo News* in September 2016: "We are always pressurized [sic] time and again that our tactical (nuclear) weapons, in which we have a superiority, that we have more tactical weapons than we need. It is internationally recognized that we have a superiority and if there is a threat to our security or if anyone steps on our soil and if someone's designs are a threat to our security, we will not hesitate to use those weapons for our defense" (Scroll 2016). In developing its nonstrategic nuclear strategy, one study has asserted that Pakistan to some extent has emulated NATO's flexible response strategy without necessarily understanding how it would work (Tasleem and Dalton 2019).

Pakistan's nuclear posture—particularly its development and deployment of tactical nuclear weapons—has created considerable concern in other countries, including the United States, which fears that it increases the risk of escalation and lowers the threshold for nuclear use in a military conflict with India. Over the past decade-and-a-half, the US assessment of nuclear weapons security in Pakistan appears to have changed considerably from confidence to concern, particularly because of the introduction of tactical nuclear weapons. In 2007, a US State Department official told Congress that, "we're, I think, fairly confident that they have the proper structures and safeguards in place to maintain the integrity of their nuclear forces and not to allow any compromise" (Boucher 2007). After the emergence of tactical nuclear weapons, the Obama administration changed the tune: "Battlefield nuclear weapons, by their very nature, pose [a] security threat because you're taking battlefield nuclear weapons to the field where, as you know, as a necessity, they cannot be made as secure," as then US Undersecretary of State Rose Gottemoeller told Congress in 2016 (*Economic Times* 2016).

The Trump administration echoed this assessment in 2018: "We are particularly concerned by the development of tactical nuclear weapons that are designed for use in battlefield. We believe that these systems are more susceptible to terrorist theft and increase the likelihood of nuclear exchange in the region" (*Economic Times* 2017). The Trump administration's South Asia strategy in 2017 urged Pakistan to stop sheltering terrorist organizations, notably to "prevent nuclear weapons and materials from coming into the hands of terrorists" (The White House 2017).

In the 2019 Worldwide Threat Assessment, US Director of National Intelligence Daniel R. Coats said, "Pakistan continues to develop new types of nuclear weapons, including short-range tactical weapons, sea-based cruise missiles, air-launched cruise missiles, and longer-range ballistic missiles," noting that "the new types of nuclear weapons will introduce new risks for escalation dynamics and security in the region" (Coats 2019, 10). The Defense Intelligence Agency appeared to tone down its language slightly in

its 2021 and 2022 Worldwide Threat Assessments, stating that "Pakistan very likely will continue to modernize and expand its nuclear capabilities by conducting training with its deployed weapons and developing new delivery systems…" but not explicitly noting the inherent escalation risks (Berrier 2021; 2022, 50)."
Pakistani officials, for their part, reject such concerns. In 2021, then-Prime Minister Imran Khan stated that he was "not sure whether we're growing [the nuclear arsenal] or not because as far as I know … the only one purpose [of Pakistan's nuclear weapons] – it's not an offensive thing." He added that "Pakistan's nuclear arsenal is simply as a deterrent, to protect ourselves" (Laskar 2021).

Nuclear security, decision-making, and crisis management

After years of highly-publicized US concerns over the security of Pakistan's nuclear weapons—including the Pentagon reportedly making contingency plans for their rendition in the event of a crisis—Pakistani officials have repeatedly challenged the notion that the security of their nuclear weapons is deficient (Goldberg and Ambinder 2011; MacAskill 2007). Samar Mubarik Mund, the former director of the country's National Defense Complex, explained in 2013 that a Pakistani nuclear warhead is "assembled only at the eleventh hour if [it] needs to be launched. It is stored in three to four different parts at three to four different locations. If a nuclear weapon doesn't need to be launched, then it is never available in assembled form" (*World Bulletin* 2013).
Despite Pakistan's recent upgrades to the security of its military bases and facilities, at a Democratic Congressional Campaign Committee reception in October 2022, US President Joe Biden commented that Pakistan was "one of the most dangerous nations in the world" due to the lack of "cohesion" in its nuclear security and command and control procedures—a comment that Pakistan quickly and forcefully rebuked (Khan 2022).
Nuclear policy and operational decision-making in Pakistan are undertaken by the National Command Authority, which is chaired by the prime minister and includes both high-ranking military and civilian officials. The primary nuclear-related body within the National Command Authority is the Strategic Plans Division (SPD), which has been described by the former Director of the SPD's Arms Control and Disarmament Affairs as "a unique organization that is incomparable to any other nuclear-armed state. From operational planning, weapon development, storage, budgets, arms control, diplomacy, and policies related to civilian applications for energy, agriculture, and medicine, etc., all are directed and controlled by SPD." Additionally, SPD "is responsible for nuclear policy, strategy and doctrines. It formulates force development strategy for the tri-services strategic forces, operational planning at the joint services level, and controls movements and deployments of all nuclear forces. SPD implements NCA's employment decisions for nuclear use through its NC3 systems" (Khan, F. H. 2019).
The National Command Authority was convened after India and Pakistan engaged in open hostilities in February 2019, when Indian fighters dropped bombs near the Pakistani town of Balakot in response to a suicide bombing conducted by a Pakistan-based militant group. In retaliation, Pakistani aircraft shot down and captured an Indian pilot before returning him a week later and convened the National Command Authority. Following the meeting, a senior Pakistani official gave what appeared to be a thinly veiled nuclear threat: "I hope you know what the [National Command Authority] means and what it constitutes. I said that we will surprise you. Wait for that surprise. … You have chosen a path of war without knowing the consequence for the peace and security of the region" (Abbasi 2019). In his memoir published in January 2023, former US Secretary of State Mike Pompeo mentioned the February 2019 crisis saying that India and Pakistan came "close" to a "nuclear conflagration" (Biswas 2023).
On March 9, 2022, India accidentally launched a BrahMos cruise missile, which crossed the border into Pakistan and traveled approximately 124 kilometers before crashing near the town of Mian Channu (Korda 2022). This was an extremely rare occurrence of a nuclear-armed country launching a missile into the territory of another nuclear power. A subsequent Indian inquiry found that the incident resulted from a deviation from standard operation procedures during a "routine maintenance and inspection" exercise. India made a public statement announcing these findings and terminated the three responsible Indian Air Force officers. However, Pakistan was not satisfied and rejected India's "purported closure of the highly irresponsible incident," insisting on a joint probe into the circumstances of the accident (Pakistan Ministry of Foreign Affairs 2022). A year after the incident, on March 10, 2023, Pakistan reiterated its standing request for a joint investigation, citing concern about the reliability of India's command and control systems (Pakistan Ministry of Foreign Affairs 2023).
In addition to India's opacity regarding the incident in the days immediately following the missile launch, it is notable that Pakistan may not have tracked the missile correctly during its flight. In a press conference following the missile launch, Pakistani military officials displayed a map showing their interpretation of the missile's flight and noted that Pakistan's "actions, response, everything … it was perfect. We detected it on time, and we took care of it" (ISPR 2022b). The flight path that Pakistan presented, however, included some discrepancies over where the missile had been launched, as well as its perceived target, and was publicly disputed by Indian sources (Korda 2022; Philip 2022).
According to one Indian news source, in the absence of clarification from India, Pakistan Air Force's Air Defence Operations Centre immediately suspended all military and civilian aircraft for nearly six hours, and reportedly placed frontline bases and strike aircraft on high alert (Bhatt 2022; Philip 2022; Korda 2022; ISPR 2022c). Pakistan's military sources stated that these bases remained on alert until 13:00 PKT on

March 14th. (The Pakistan Standard Time (PKT) is typically 30 minutes behind of India Standard Time (IST).) Pakistani officials appeared to confirm this, noting that "whatever procedures were to start, whatever tactical actions had to be taken, they were taken" (ISPR 2022b).
While the US Air Force's National Air and Space Intelligence Center Ballistic and Cruise Missile Report lists India's BrahMos missile as conventional, this incident could potentially have escalated had it taken place during a previous period of notoriously tense relations between the two nuclear-armed countries (National Air and Space Intelligence Center 2017, 37). Moreover, Pakistan and India do not have robust transparency and crisis management mechanisms: Since 1988, the two countries have annually exchanged an annual list of nuclear facilities, and there is a high-level military hotline between the two countries; however, Pakistani officials noted that during the seven minutes of the missile's flight India did not use the hotline to alert Pakistan of the accidental launch (ISPR 2022b). The two countries' initial responses to the incident suggest that regional crisis management mechanisms may not be as reliable as intended.

Fissile materials production and inventory
Pakistan has a well-established and diverse fissile material production complex that is expanding. It includes the Kahuta uranium enrichment plant east of Islamabad, which appears to be growing with the near-completion of what could be another enrichment plant, as well as the enrichment plant at Gadwal to the north of Islamabad (Albright, Burkhard, and Pabian 2018). Four heavy-water plutonium production reactors appear to have been completed at what is normally referred to as the Khushab Complex some 33 kilometers south of Khushab in Punjab province. Three of the reactors at the complex have been added in the past 10 years. The addition of a publicly confirmed thermal power plant at Khushab provides new information for estimating the power of the four reactors (Albright et al. 2018).

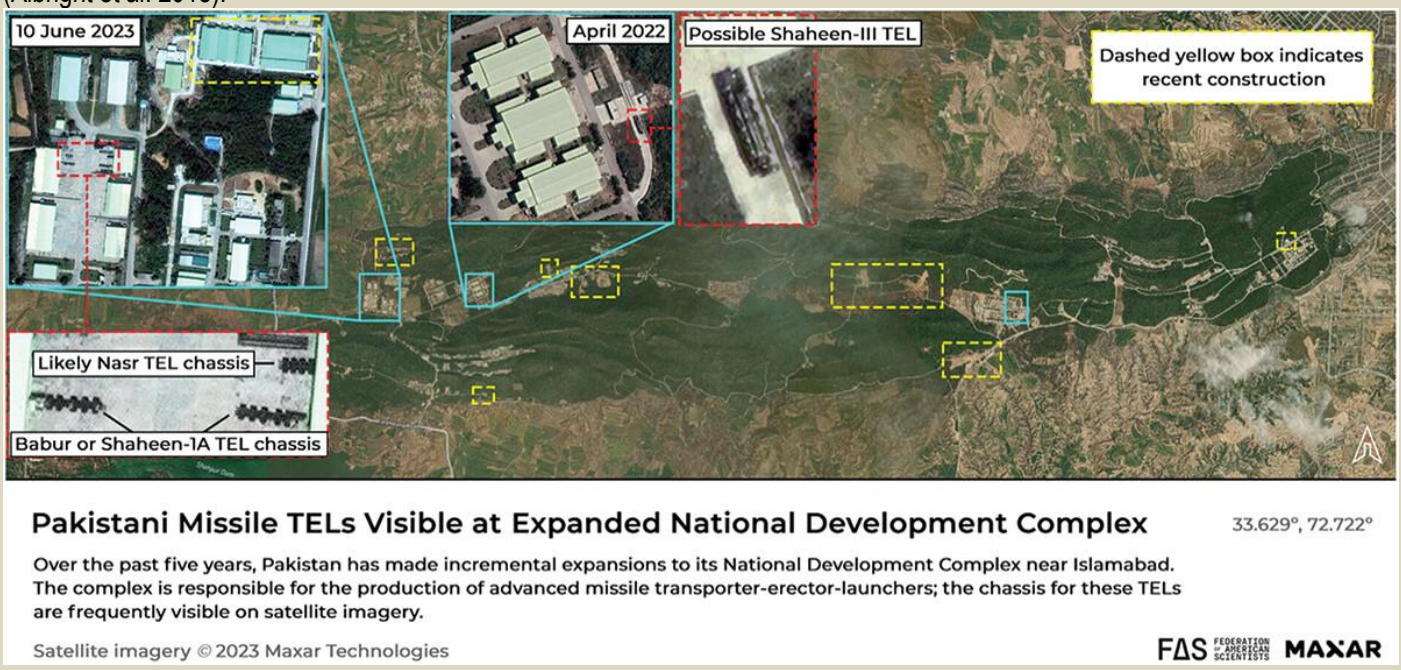


Figure 1. Pakistani missile TEL visible at expanded National Development Complex near Fateh Jang. (Image: Maxar Technologies/Federation of American Scientists). (Click to display full size.)

The New Labs Reprocessing Plant at Nilore, east of Islamabad, which reprocesses spent fuel and extracts plutonium, has been expanded. Meanwhile, a second reprocessing plant located at Chashma in the northwestern part of Punjab province may have been completed and become operational by 2015 (Albright and Kelleher-Vergantini 2015). A significant expansion to the Chashma complex was under construction between 2018 and 2020, although it remains unclear whether the reprocessing plant continued to operate throughout that period (Hyatt and Burkhard 2020). In June 2023, China and Pakistan signed a memorandum of understanding (MOU) for a $4.8 billion deal to construct a new 1,200-megawatt reactor at Chashma (Shahzad 2023).
Nuclear-capable missiles and their mobile launchers are developed and produced at the National Defence Complex (sometimes called the National Development Complex) located in the Kala Chitta Dahr mountain range west of Islamabad. The complex is divided into two sections. The western section south of Attock appears to be involved in development, production, and test-launching of missiles and rocket engines. The eastern section north of Fateh Jang is involved in production and assembly of road-mobile transporter

erector launchers (TELs), which are designed to transport and fire missiles. Satellite images regularly show the presence of TEL chassis for a variety of ballistic and cruise missiles: In June 2023, TEL chassis were visible for Nasr, Shaheen-IA ballistic missiles, and Babur cruise missiles (Figure 1). The Fateh Jang section has expanded significantly with several new launcher assembly buildings over the past 10 years, and the complex continues to expand. Other launcher and missile-related production and maintenance facilities may be located near Tarnawa and Taxila.

Little is publicly known about warhead production, but experts have suspected for many years that the Pakistan Ordnance Factories near Wah, northwest of Islamabad, serve a role. One of the Wah factories is located near a unique facility with six earth-covered bunkers (igloos) inside a multi-layered safety perimeter with armed guards.

A frequent oversimplification for estimating the number of Pakistani nuclear weapons is to derive the estimate directly from the amount of weapon-grade fissile material produced. As of the beginning of 2023, the International Panel on Fissile Materials estimated that Pakistan had an inventory of approximately 4,900 kilograms (plus or minus 1,500 kilograms) of weapon-grade (90 percent enriched) highly enriched uranium (HEU), and about 500 kilograms (plus or minus 170 kilograms) of weapon-grade plutonium (Kütt, Mian, and Podvig 2023). Assuming each first-generation implosion-type warhead's solid core uses 15 to 18 kilograms (kg) of weapon-grade HEU or 5 to 6 kg of plutonium, this fissile material would theoretically be enough to produce a maximum of approximately 188 to 436 HEU-based single-stage warheads and 55 to 134 plutonium-based single-stage warheads if fully expended. However, Pakistan's warhead designs may have undergone some iteration and have become more efficient.

It is important to note that calculating stockpile size based solely on fissile material inventory is an incomplete methodology that tends to overestimate the likely number of nuclear warheads. Instead, warhead estimates must take several other factors into account in addition to the amount of weapon-grade fissile material produced, including the warhead design choice and efficiency, warhead production rates, number of operational nuclear-capable launchers, number of launchers with dual-capability, and nuclear doctrine.

Nuclear warheads estimates must assume that not all of Pakistan's fissile material is used for weapons. Like other nuclear-armed countries, Pakistan most probably keeps some fissile material in reserve. Pakistan also does not have enough nuclear-capable launchers to accommodate several hundreds of warheads. Moreover, all of Pakistan's launchers are thought to be dual-capable, which means that some of them, especially the shorter-range systems, may serve non-nuclear missions. Finally, official statements often refer to "warheads" and "weapons" interchangeably, which leads to ambiguity as to whether they are referring to the number of launchers or the warheads being assigned to them.

The amount of fissile material in warheads—and the size of the warhead—can be reduced, and their yield increased, by using tritium to "boost" the fission process. Pakistan's tritium production capability is poorly understood due to a lack of reliable public information. One study in early 2021 estimated that Pakistan could have produced 690 grams of tritium by the end of 2020, sufficient to boost over 100 weapons. The study assessed that warheads produced for delivery by the Babur and Ra'ad cruise missiles and the Nasr and Abdali missiles almost certainly would require a small, lightweight tritium-boosted fission weapon (Jones 2021). If Pakistan has produced tritium and uses it in second-generation single-stage boosted warhead designs, then the estimated HEU and weapons-grade plutonium would potentially allow it to build a maximum of 283 to 533 HEU-based warheads and 66 to 167 plutonium-based warheads, assuming that each weapon used either 12 kg of HEU or 4 to 5 kg of plutonium.[1] These calculations, however, produce results that are highly likely to be several hundred warheads more than Pakistan currently possesses, for the same reasons mentioned above.

We estimate that Pakistan currently is producing sufficient fissile material to build 14 to 27 new warheads per year, although we estimate that the actual warhead increase in the stockpile probably averages around 5 to 10 warheads per year.[2]

Nuclear-capable aircraft and air-delivered weapons

The aircraft most likely to have a nuclear delivery role are Pakistan's Mirage III and Mirage V fighter squadrons. The Pakistani Air Force's (PAF) Mirage fighter-bombers are located at two bases.[3] Masroor Air Base outside Karachi houses the 32nd Wing with three Mirage squadrons: 7th Squadron ("Bandits"), 8th Squadron ("Haiders"), and 22nd Squadron ("Ghazis"). A possible nuclear weapons storage site is located five kilometers northwest of the base (Kristensen 2009) and, since 2004, highly guarded underground facilities have been constructed at Masroor that could potentially be designed to support a nuclear strike mission. This includes a possible alert hangar with underground weapons-handling capability.

The other Mirage base is Rafiqui Air Base near Shorkot, which is home to the 34th Wing with two Mirage squadrons: the 15th Squadron ("Cobras") and the 27th Squadron ("Zarras"). On February 25, 2021, Pakistan's President, Dr. Arif Alvi, visited the base for the ceremony of 50th Anniversary of Mirages and Colours Award, which displayed at least 11 Mirages (President of Pakistan 2021).

The Mirage V is believed to have been given a strike role with Pakistan' small arsenal of nuclear gravity bombs, while the Mirage III has been used for test launches of Pakistan's Ra'ad air-launched cruise missiles (ALCM), as well as the follow-on Ra'ad-II. The Pakistani Air Force has added an aerial refueling

capability to the Mirage, a capability that would greatly enhance the nuclear strike mission (AFP 2018). Several of the Mirages displayed at the award ceremony at Rafiqui Air Base in 2021 appeared to be equipped with refueling pods.

The air-launched, dual-capable Ra'ad ALCM is believed to have been test-launched at least six times, most recently in February 2016. The Pakistani government states that the Ra'ad "can deliver nuclear and conventional warheads with great accuracy" (ISPR 2011a) to a range of 350 kilometers (km) and "complement[s] Pakistan's deterrence capability" by achieving "strategic standoff capability on land and at sea" (ISPR 2016a). During a military parade in 2017, Pakistan displayed what was said to be Ra'ad-II ALCM, apparently an enhanced version of the original Ra'ad with a new engine air-intake and tail wing configuration (Khan 2017). The Pakistani government most recently tested the Ra'ad-II in February 2020 and stated that the missile can reportedly reach targets at a distance of 600 km (ISPR 2020a). All test launches involving either Ra'ad system have been conducted from Mirage III aircraft.

There is no available evidence to suggest that either Ra'ad system had been deployed as of July 2023; however, one potential deployment site could eventually be Masroor Air Base outside Karachi, which is home to several Mirage squadrons and includes unique underground facilities that might be associated with nuclear weapons storage and handling.

To replace the PAF's aging Mirage III and V aircraft, Pakistan has acquired more than 100 operational JF-17 aircraft—which are co-produced with China—and plans to acquire around another 188 JF-17s (Aamir 2022; Gady 2020; Quwa 2021; Warnes 2020). These aircraft are being continuously upgraded with new technology "blocks." Pakistan reportedly inducted the first batch of 12 JF-17 Block III aircraft into the 16th ("Black Panthers") squadron in March 2023 (Tiwari 2023). Several reports suggest that Pakistan may intend to incorporate the dual-capable Ra'ad ALCM onto the JF-17 so that the newer aircraft could eventually take over the nuclear strike role from the Mirage III/Vs (Ansari 2013; Fisher 2016; *PakDefense* 2020). In March 2023, during rehearsals for the 2023 Pakistan Day Parade (which was subsequently canceled), images surfaced of a JF-17 Thunder Block II carrying what resembled a Ra'ad-I ALCM, the first time such configuration was observed (*Scramble* 2023).

The nuclear capability of the PAF's legacy F-16 aircraft is uncertain. Although Pakistan was obligated by its contract with the United States not to modify the aircraft to carry nuclear weapons, multiple credible reports subsequently emerged suggesting that Pakistan intended to do so (Associated Press 1989). In September 2022, the Biden administration agreed to a $450 million deal to help sustain Pakistan's F-16 aircraft program (US Defense Security Cooperation Agency 2022).

The F-16A/Bs are based with the 38th Wing at Mushaf (formerly Sargodha) Air Base, located 160 kilometers northwest of Lahore in northeastern Pakistan. Organized into the 9th and 11th Squadrons ("Griffins" and "Arrows" respectively), these aircraft have a range of 1,600 km (extendable when equipped with drop tanks) and most likely are equipped to each carry a single nuclear bomb on the centerline pylon. If the F-16s have a nuclear strike mission, the nuclear gravity bombs attached to them most likely are not stored at the base itself but are potentially kept at the Sargodha Weapons Storage Complex, located 10 km to the south. In a crisis, the bombs could quickly be transferred to the base, or the F-16s could disperse to bases near underground storage facilities and receive the weapons there. Pakistan appears to be reinforcing the munitions bunkers, adding new tunnels, and installing extra security perimeters at the Sargodha complex.

The newer F-16C/Ds are based with the 39th Wing at Shahbaz Air Base outside Jacobabad in northern Pakistan. The wing upgraded to F-16C/Ds from Mirages in 2011 and, so far, has one squadron: the 5th Squadron (known as the "Falcons"). The base has undergone significant expansion, with numerous weapons bunkers added since 2004. As for the F-16A/Bs, if the base has a nuclear mission, the weapons attached to F-16C/Ds most probably are stored elsewhere in special storage facilities. Some F-16s are also visible at Minhas (Kamra) Air Base northwest of Islamabad, although these might be related to aircraft industry at the base. The F-16Cs were showcased in the 2022 Pakistan Day Parade.

Despite the reports about F-16s and the recent image of a Ra'ad ALCM loaded onto a JF-17, there are still too many uncertainties associated with these two aircraft to confidently attribute a dedicated nuclear strike role to either one. As a result, the PAF's F-16s are omitted from Table 1 in this Nuclear Notebook, and the and JF-17s are listed with significant uncertainty.

Land-based ballistic missiles

Pakistan appears to have six currently operational nuclear-capable, solid-fuel, road-mobile ballistic missile systems: the short-range Abdali (Hatf-2), Ghaznavi (Hatf-3), Shaheen-I/A (Hatf-4), and Nasr (Hatf-9), and the medium-range Ghauri (Hatf-5) and Shaheen-II (Hatf-6). Two other nuclear-capable ballistic missile systems are currently under development: the medium-range Shaheen-III and the MIRVed Ababeel. All of Pakistan's nuclear-capable missiles—except for the Abdali, Ghauri, Shaheen-II, and Ababeel—were showcased at the Pakistan Day Parade in March 2021 (ISPR 2021g). The Nasr, Ghauri, Shaheen-IA and II, as well as the Babur-1A and Ra'ad-II were featured during the 2022 Pakistan Day Parade (ISPR 2022c).

The Pakistani road-mobile ballistic missile force has undergone significant development and expansion over the past two decades. This includes possibly eight or nine missile garrisons, including four or five along the Indian border for short-range systems (Babur, Ghaznavi, Shaheen-I, Nasr) and three or four other garrisons further inland for medium-range systems (Shaheen-II and Ghauri).[3] In 2022 and 2023, Pakistan conducted significantly fewer public missile test launches than in earlier years, which may be

related to Pakistan's ongoing political instability and countrywide protests following the ousting and subsequent arrest of former Prime Minister Imran Khan in mid-2022.

The short-range, solid-fuel, single-stage Abdali (Hatf-2) has been in development for a long time. The Pentagon reported in 1997 that the Abdali appeared to have been discontinued, but flight-testing resumed in 2002, and it was last reported test-launched in 2013. The 200 kilometer-range missile has been displayed at parades several times on a four-axle road-mobile transporter erector launcher (TEL). The gap in flight-testing indicates the Abdali program may have encountered technical difficulties. After the 2013 test, Inter Services Public Relations stated that Abdali "carries nuclear as well as conventional warheads" and "provides an operational-level capability to Pakistan's Strategic Forces." It said the test launch "consolidates Pakistan's deterrence capability both at the operational and strategic levels" (ISPR 2013); however, the Abdali—Pakistan's oldest ballistic missile type—has not been tested since 2013 and was not displayed at the Pakistan Day Parades of 2021 and 2022. This could potentially indicate that the missile has been superseded by newer systems.

The short-range, solid-fuel, single-stage Ghaznavi (Hatf-3) was test-launched in 2019, 2020, and twice in 2021—its first reported test launches since 2014. In an important milestone for testing the readiness of Pakistan's nuclear forces, the 2019 Ghaznavi launch was conducted at night. After each test, the Pakistani military stated that the Ghaznavi is "capable of delivering multiple types of warheads up to a range of 290 kilometers" (ISPR 2019c, 2020b, 2021b). Its short range means that the Ghaznavi cannot strike Delhi from Pakistani territory, and Army units equipped with the missile are probably based relatively near the Indian border (Kristensen 2016).

The Shaheen-I (Hatf-4) is a single-stage, solid-fuel, dual-capable, short-range ballistic missile with a maximum range of 650 km that has been in service since 2003. The Shaheen-I is carried on a four-axle, road-mobile TEL like the one used for the Ghaznavi. Since 2012, many Shaheen-I test launches have involved an extended-range version widely referred to as Shaheen-IA. The Pakistani government, which has declared the range of the Shaheen-IA to be 900 km, has used both designations. Pakistan most recently test launched the Shaheen-I in November 2019 and the Shaheen-IA in March and November 2021 (ISPR 2019d, 2021c, 2021d, 2021f). Potential Shaheen-1 deployment locations include Gujranwala, Okara, and Pano Aqil. The Shaheen-I was displayed at the 2021 Pakistan Day Parade, but it was replaced by the Shaheen-IA at the 2022 parade, indicating the latter system's potential introduction into the armed forces (ISPR 2021g, 2022c).

One of the most controversial new nuclear-capable missiles in the Pakistani arsenal is the Nasr (Hatf-9), a short-range, solid-fuel missile originally with a range of only 60 km that has recently been extended to 70 km (ISPR 2017c). However, its range being too short to attack strategic targets inside India, Nasr appears intended solely for battlefield defensive use against invading Indian troops.[4] According to the Pakistani government, the Nasr "carries nuclear warheads of appropriate yield with high accuracy, shoot and scoot attributes" and was developed as a "quick response system" to "add deterrence value" to Pakistan's strategic weapons development program "at shorter ranges to deter evolving threats," including evidently India's so-called Cold Start doctrine (ISPR 2011c, 2017a, 2017c). More recent tests of the Nasr system—including two tests in the same week in January 2019—sought to demonstrate the system's salvo-launch capability, as well as the missiles' in-flight maneuverability (ISPR 2019b, 2019d, 2019e).

The Nasr's four-axle, road-mobile TEL appears to use a snap-on system that can carry two or more launch-tube boxes, and the system has been tested in the past using a road-mobile quadruple box launcher. The US intelligence community has listed the Nasr as a deployed system since 2013 (National Air and Space Intelligence Center 2013), and with a total of 15 tests reported so far, the weapon system appears to be well-developed. Potential deployment locations include Gujranwala, Okara, and Pano Aqil.

Figure 2. The Pakistani army test-launched a Shaheen-III medium-range ballistic missile in April 2022. (Archive image from 2015 via Pakistani military).

The medium-range, two-stage, solid-fuel Shaheen-II (Hatf-6) appears to be operational after many years of development. Pakistan's National Defense Complex has assembled Shaheen-II launchers since at least 2004 or 2005 (Kristensen 2007), and a 2020 US intelligence community report states that there are "fewer than 50" Shaheen-II launchers deployed (National Air and Space Intelligence Center 2020). After the most recent Shaheen-II test launch in May 2019, the Pakistani government reported the range as only 1,500 km, but the US National Air and Space Intelligence Center (NASIC) continues to set the Shaheen-II's range at 2,000 km (ISPR 2019a; National Air and Space Intelligence Center 2020). The Shaheen-II is carried on a six-axle, road-mobile TEL and can carry a single conventional or nuclear warhead.

Pakistan's newer medium-range, two-stage, solid-fuel Shaheen-III was displayed publicly for the first time at the 2015 Pakistan Day Parade. Following a third test launch in January 2021, the Pakistani government

said the missile could deliver either a single nuclear or conventional warhead to a range of 2,750 km, making it the longest-range system that Pakistan has tested (ISPR 2021a). Its latest test launch took place in April 2022 (Figure 2), which the Pakistani government said was "aimed at re-validating various design and technical parameters of the weapon system" (ISPR 2022a). The Shaheen-III is carried on an eight-axle TEL reportedly supplied by China (Panda 2016). The system may still require more test launches before it becomes operational.

The range of the Shaheen-III is sufficient to target all of mainland India from launch positions in most of Pakistan south of Islamabad. But the missile was apparently developed to do more than that. According to Gen. Kidwai, the range of 2,750 km was determined by a need to be able to target the Nicobar and Andaman Islands in the eastern part of the Indian Ocean that are "developed as strategic bases" where "India might think of putting its weapons" (Carnegie Endowment for International Peace 2015, 10). But for a 2,750-km range Shaheen-III to reach the Andaman and Nicobar Islands, it would need to be launched from positions in the very Eastern parts of Pakistan, close to the Indian border.

Pakistan's oldest nuclear-capable medium-range ballistic missile, the road-mobile, single-stage, liquid-fuel Ghauri (Hatf-5), was most recently test-launched in October 2018 (ISPR 2018c). The Ghauri is based on North Korea's Nodong medium-range ballistic missile. The Pakistani government states that the Ghauri can carry a single conventional or nuclear warhead to a range of 1,300 km. However, NASIC lists its range slightly lower at 1,250 km and suggests that "fewer than 50" Ghauri launchers have been deployed (National Air and Space Intelligence Center 2020). The extra time needed to fuel the missile before launch makes the Ghauri more vulnerable to attack than Pakistan's newer solid-fuel missiles. Therefore, it is possible that the longer-range versions of the Shaheen may eventually replace the Ghauri. Potential deployment areas for the Ghauri include the Sargodha Central Ammunition Depot area and the Khuzdar Garrison, which expanded its perimeter in late 2017 to include three additional TEL garages.

On January 24, 2017, Pakistan test-launched a new medium-range ballistic missile called Ababeel that the government says is "capable of carrying multiple warheads, using multiple independent reentry vehicle (MIRV) technology" (ISPR 2017b).[5] The three-stage, solid-fuel, nuclear-capable missile, which is currently under development at the National Defense Complex, appears to be derived from the Shaheen-III airframe and solid-fuel motor and has a range of 2,200 km (ISPR 2017b; National Air and Space Intelligence Center 2020). After the test-launch, the Pakistani government declared that the test was intended to validate the missile's "various design and technical parameters," and that Ababeel is "aimed at ensuring survivability of Pakistan's ballistic missiles in the growing regional Ballistic Missile Defence (BMD) environment, … further reinforc[ing] deterrence" (ISPR 2017b). Development of multiple-warhead capability appears to be intended as a countermeasure against India's planned ballistic missile defense system (Tasleem 2017). Its status remains unclear as of July 2023.

Land-based missile garrisons

The total number and location of Pakistan's nuclear-capable missile bases and facilities remains unknown. In particular, it is highly challenging to discern between Pakistani military bases intended to serve conventional-only strike roles and those intended to serve dual-capable or nuclear-specific strike roles.

Analysis of commercial satellite imagery suggests that Pakistan maintains at least five missile bases that could serve a role in Pakistan's nuclear forces. Very little has changed with these bases since our most recent overview in 2016 (Kristensen 2016).

Akro Garrison (25.5483, 68.3343)

The Akro Garrison is located around 18 kilometers north of Hyderabad in the southern part of the Sindh Province, and around 145 kilometers away from the Indian border. The garrison covers an area of approximately 6.9 square kilometers, and it has undergone gradual expansion since 2004. The Akro Garrison consists of six missile TEL garages that appear to be designed for 12 launchers. Under the TEL garage complex, there is a unique underground facility, the construction of which can be seen through past satellite imagery. The underground facility has two cross-shaped sections connected by a central corridor that leads to two buildings on either side via covered access ramps.

Analysis of a vehicle training area in the northeast corner of the garrison shows what appear to be five-axle TELs for the Babur cruise missile weapon system.

Gujranwala Garrison (32.2410, 74.0730)

The Gujranwala Garrison is one of the largest military complexes in Pakistan (Figure 3). It covers nearly 30 square kilometers in the northeastern part of the Punjab Province and is located about 60 kilometers from the Indian border. Since 2010, the Gujranwala Garrison has added what appears to be a TEL launcher area immediately east of a likely storage site for conventional munitions, which became operational in 2014 or 2015. The TEL area consists of two identical sections, each of which contain several launcher garages as well as a possible weapons loading hall with reinforced embankments connected via covered passageway to what appears to be a reinforced weapons

storage bunker. There is also a technical area slightly south of the main TEL area for servicing the launchers. The security perimeter seems to be designed for potentially adding a third TEL section.

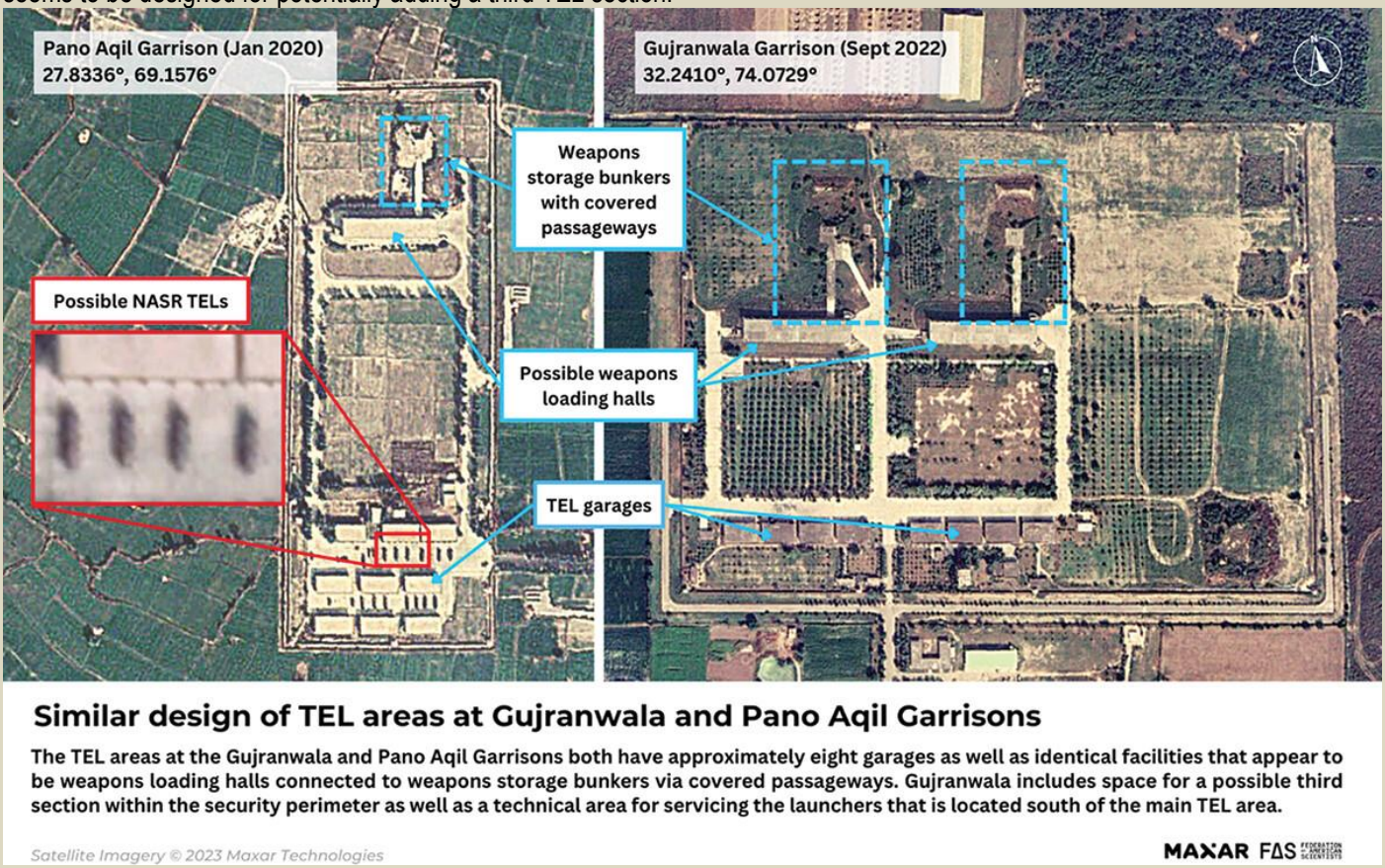


Figure 3. Similar design of TEL areas at Gujranwala and Pano Aqil Garrisons. (Image: Maxar Technologies/Federation of American Scientists). (Click to display full size.)

Several trucks that strongly resemble the Nasr short-range missile system can be seen on satellite imagery. Although it is impossible to be certain, these trucks appear to have a twin box launcher similar to that of which can be seen on Nasr test launch photos. The Nasr's estimated range is the equivalent of the garrison's distance from the Indian border.

Khuzdar Garrison (27.7222, 66.6241)

The Khuzdar Garrison is located approximately 220 kilometers west of Sukkur in south-east Balochistan Province, and the furthest known missile garrison from the Indian border. The base is split into two sections: a northern section and a southern section (where the TELs are based). The southern section of the base expanded its perimeter in late-2017 to include three additional TEL garages, bringing the total to six. Also included in this section are two multi-story weapon handling buildings with covered ramps leading to a possible underground nuclear storage area similar to the one visible at the Akro Garrison. Likely nuclear-capable missile launchers, possibly Ghauri or Shaheen-II TELs, have been spotted with commercial satellite imagery at Khuzdar. An eastern section of the base that appeared to be another TEL garage area was under construction over a decade ago; however, that expansion seems to have been canceled.

Pano Aqil Garrison (27.8328, 69.1575)

The Pano Aqil Garrison is located only 85 kilometers from the Indian border, in the northern part of Sindh Province, and is split up in several sections that cover a combined area of nearly 20 square kilometers. The double-fenced TEL area is located 1.8 kilometers northeast of the main garrison and includes eight garages (the last three were completed in 2017), each of which has spaces for six TELs. An additional ninth garage near the others appears to have openings for five vehicles. Altogether, this garrison could potentially support approximately 50 TELs; however, some of these garage spaces are likely to hold support vehicles as well. Large numbers of TELs, including for Babur and Shaheen-I missiles, are regularly visible at this garrison through commercial satellite imagery (Figure 3).

Slightly north of the TEL garages within the same double-fenced perimeter is a below-grade facility that appears to be a weapons storage igloo. The igloo is connected via a covered ramp to a multi-story TEL loading hall. The TEL and likely weapons storage areas are nearly identical in design to those visible at Gujranwala.

Sargodha Garrison (31.9722, 72.6838)
The Sargodha Garrison is a large complex located within and around the Kirana Hills, a subcritical nuclear test site used by Pakistan to develop its nuclear program from 1983 to 1990. Directly northwest of a likely conventional munitions storage area, there appear to be 10 dispersed potential TEL garages plus an additional two garages with different dimensions that could be used for maintenance. The TEL area does not have the same layout or perimeter as other TEL areas across the country, although this could be a function of the garrison's age.
Directly east of the conventional munitions storage area is an underground storage area built into the side of the mountain range. At least 10 underground facility entrances are visible through commercial satellite imagery, as well as potential facilities for weapon and missile handling.

Ground- and sea-launched cruise missiles
Pakistan's family of ground- and sea-launched cruise missiles is undergoing significant development with work on several types and modifications. The Babur (Hatf-7) is a subsonic, dual-capable cruise missile with a similar appearance to the US Tomahawk sea-launched cruise missile, the Chinese DH-10 ground-launched cruise missile, and the Russian air-launched AS-15. The Pakistani government describes the Babur as having "stealth capabilities" and "pinpoint accuracy" and "a low-altitude, terrain-hugging missile with high maneuverability" (ISPR 2011b, 2016b, 2018a, 2018b). The Babur is much slimmer than Pakistan's ballistic missiles, suggesting some success with warhead miniaturization based on a boosted fission design.
The original Babur-1 ground-launched cruise missiles (GLCM) has been test-launched nearly a dozen times and is likely to be operational with the armed forces. Its road-mobile launcher appears to be a unique five-axle TEL with a three-tube box launcher that is different than the quadruple box launcher used for static display. At different times, the Pakistani government has reported the range to be 600 km and 700 km (ISPR 2011b, 2012a, 2012b, 2012c), but the US intelligence community sets the range much lower, at 350 km (National Air and Space Intelligence Center 2020).
Pakistan appears to be upgrading the original Babur-1 missiles into Babur-1A missiles by upgrading their avionics and navigation systems to enable target engagement both on land and at sea. Following the system's most recent test in February 2021, the Pakistani military stated that the Babur-1A's range was 450 km (ISPR 2021e).
Pakistan is also developing an enhanced version of the Babur known as the Babur-2 or Babur-1B GLCM.[6] The weapon has been test-launched in December 2016, April 2018, and December 2021 (ISPR 2016b, 2018a, 2018b, 2021d, 2021g). Indian news media reported that the Babur-2/Babur-1B had failed two other prior tests, in April 2018 and March 2020; however, this was not confirmed by Pakistan (Gupta 2020). With a physical appearance and capabilities like those of the Babur, the Babur-2/Babur-1B apparently has an extended range of 700 km, and "is capable of carrying various types of warheads" (ISPR 2016b, 2018a, 2018b). The fact that both the Babur-1 and the "enhanced" Babur-2/Babur-1B have been noted as possessing a range of 700 km indicates that the range of the initial Babur-1 system was likely shorter. NASIC has not released information on an enhanced system. After the first test in 2016, the Pakistani government noted that the system is "an important force multiplier for Pakistan's strategic defense" (ISPR 2016b).
Babur TELs have been fitting out at the National Development Complex for several years and have recently been seen at the Akro garrison northeast of Karachi. The garrison includes a large enclosure with six garages that have room for 12 TELs and a unique underground facility that is probably used to store the missiles.
Pakistan is also developing a sea-launched version of the Babur known as Babur-3. The weapon is still in development and has been test-launched twice: On January 9, 2017, from "an underwater, mobile platform" in the Indian Ocean (ISPR 2017a); and on March 29, 2018 from "an underwater dynamic platform" (ISPR 2018a). The Babur-3 is said to be a sea-based variant of the Babur-2 GLCM, and to have a range of 450 km (ISPR 2017a).
The Pakistani government says the Babur-3 is "capable of delivering various types of payloads … [that] … will provide Pakistan with a Credible Second Strike Capability, augmenting deterrence," and described it as "a step toward reinforcing [the] policy of credible minimum deterrence" (ISPR 2017a). The Babur-3 will most likely be deployed on the Pakistan Navy's three Agosta-90B diesel—electric submarines (Khan 2015; Panda and Narang 2017). In April 2015, the Pakistani government approved the purchase of eight right air-independent propulsion-powered (AIP) submarines from China (Khan, B. 2019). The deal stipulated for four of the submarines to be constructed at the Wuchang Shipbuilding Industry Group (WSIG) in China, and for the remaining four to be built at Karachi Shipyard & Engineering Works in Pakistan (Sutton 2020). On December 21, 2022, Pakistan laid the keel for the first submarine, the *Tasnim*, and commenced the steel cutting of the second submarine at the Karachi Shipyard (Navy 2022). The first submarine under construction in China is expected to be delivered by the end of 2023 and the remaining four assembled in

Karachi are expected to be completed by 2028 (Sutton 2020). It is possible that these new submarines, which will be called the Hangor-class, could eventually be assigned a nuclear role with the Babur-3 submarine-launched cruise missile.
Once it becomes operational, the Babur-3 will provide Pakistan with a triad of nuclear strike platforms from ground, air, and sea. The Pakistani government said the Babur-3 was motivated by a need to match India's nuclear triad and the "nuclearization of [the] Indian Ocean Region" (ISPR 2018a). The Pakistani government also noted that Babur-3's stealth technologies would be useful in the "emerging regional Ballistic Missile Defense (BMD) environment" (ISPR 2017a). The future submarine-based nuclear capability is managed by Headquarters Naval Strategic Forces Command (NSFC), which the government said in 2012 would be the "custodian of the nation's 2nd strike capability" to "strengthen Pakistan's policy of Credible Minimum Deterrence and ensure regional stability" (ISPR 2012a). Kidwai in 2015 publicly acknowledged the need for a sea-based second-strike capability and said it "will come into play in the next few years" (Carnegie Endowment for International Peace 2015, 16). Kidwai may have been referring to the new Hangor-class submarines.Pakistan is also developing a variant of the Babur cruise missile, known as the Harbah, that can be carried by surface vessels. In March 2022, Pakistan featured the new missile during the 11th Doha International Maritime Defence Exhibition and Conference (DIMDEX). The Pakistan Navy spokesperson described the Harbah as an "all-weather" subsonic cruise missile with anti-ship and land-attack capabilities and a range of approximately 290 km (Vavasseur 2022). According to the spokesperson, the Harbah has been inducted into the Pakistan Navy and deployed on Azmat-class surface ships (Vavasseur 2022). It remains unclear whether the Harbah will be dual-capable.

Research for this publication was carried out with generous contributions from the John D. and Catherine T. MacArthur Foundation, the New-Land Foundation, Ploughshares Fund, the Prospect Hill Foundation, Longview Philanthropy, the Stewart R. Mott Foundation, the Future of Life Institute, Open Philanthropy, and individual donors.

Notes

[1] These assumptions of estimated fissile material quantities for different weapon designs are adapted from Table A.1 of the International Panel on Fissile Materials (2015), Global Fissile Materials Report 2015: Nuclear Weapon and Fissile Material Stockpiles and Production report, http://fissilematerials.org/library/gfmr15.pdf.
[2] These estimates are based on reprocessing and uranium enrichment plant capacities in International Panel on Fissile Materials (2022), Global Fissile Materials Report 2022: Fifty Years of the Nuclear Non-Proliferation Treaty, https://fissilematerials.org/publications/2022/07/global_fissile_material_r.html, as well as more recent estimates by the International Panel on Fissile Materials.
[3] For detailed analysis of possible Pakistani air bases, nuclear facilities, and missile brigade locations, see Kristensen (2016).
[4] For an excellent analysis of this doctrine and Pakistan's potential use of battlefield nuclear weapons, see Nayyar and Mian (2010).
[5] Note that the correct expansion of MIRV is multiple independently targetable reentry vehicle.
[6] It is possible that the Babur-2 and the Babur-1B are the same missile. Both names are referenced as "enhanced" versions of the Babur.

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

Hans Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored the Nuclear Notebook since 2001.
Matt Korda is a Senior Research Associate and Project Manager for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the Nuclear Notebook with Hans Kristensen. Matt is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO HQ in Brussels. Matt received his MA in International Peace & Security from the Department of War Studies at King's College London. His research interests are nuclear deterrence and disarmament; progressive foreign policy; and the nexus between nuclear weapons, climate change, and injustice.
Eliana Johns, née Reynolds, is a research associate for the Nuclear Information Project at the Federation of American Scientists, where she researches the status and trends of global nuclear forces and the role of nuclear weapons. Previously, Eliana worked as a project associate for DPRK Counterproliferation at CRDF Global, focusing on WMD nonproliferation initiatives to curb North Korea's ability to gain revenue to build its weapons programs. Eliana graduated with her bachelor's in Political Science with minors in Music and Korean from the University of Maryland, Baltimore County.

Emergency Preparedness Exercise Tests Response to Radiological Attack

Source: https://www.fbi.gov/news/stories/titan-shield-training-exercise

Sep 14 – This summer, the FBI hosted the annual **Titan Shield training exercise** series, an interagency effort designed to coordinate roles and responsibilities in case of a weapons of mass destruction (WMD) terrorist attack. During the two-day exercise, **23 separate agencies** gathered at FBI Headquarters, bringing together the investigative, intelligence, technical, public health, counterterrorism, and consequence management communities to work through a fictional scenario in real-time.

"The Titan Shield exercise offers a unique opportunity for various components of the U.S. government to work together," said FBI Supervisory Special Agent Santos R. DeLeón of the WMD Directorate Strategic Partnership Unit that helped plan the event. "It is especially valuable since no federal agency can address all the implications of a WMD terrorist attack. For instance, while the FBI addresses attribution of the attack and prosecution of terrorists, other agencies deal with health services, disaster relief, critical infrastructure protection, and other components." Titan Shield participants are members of the Weapons of Mass Destruction Strategic Group (WMDSG), a crisis action team led by the FBI that brings federal agencies together to support information exchange and to deconflict WMD counterterrorism and law enforcement operations.

The FBI, along with the U.S. Department of Homeland Security's Countering WMD Office, led this year's Titan Shield, developing the scenario and timeline of events, reviewing exercise objectives, organizing logistics and tools, and debriefing and evaluating the results at the exercise's conclusion. The in-depth training requires a year-long planning cycle with interagency stakeholders who meet several times throughout the year to provide input. Each iteration of the exercise focuses on one or more WMD modalities—either chemical, biological, radiological, or nuclear—but the scenario always involves terrorism.

"Over the past four years, the FBI Titan Shield exercise has been the principal mechanism to examine and validate the planning, collaboration, and decisive actions necessary at the strategic and tactical levels," said, Sean Hearns, training branch chief, Preparedness Division, Countering Weapons of Mass Destruction Office, U.S. Department of Homeland Security.

"The FBI WMDSG provides a structure to assess residual risk, while prioritizing federal interagency response capabilities," he continued. "It is through this enhanced process that the WMDSG equips senior leaders with critical information to make informed decisions during a potential WMD crisis. Through Titan Shield, the Department of Homeland Security has enhanced its networks and fostered the relationships necessary to shape preparedness and response activities."

This year's Titan Shield scenario presented a terrorist cell that stole radiological material and smuggled it into the United States with the intent to carry out attacks against sports stadiums using drones. During the exercise, WMDSG developed threat profiles and evaluated courses of action amid events rapidly unfolding in real-time.

Participants addressed various questions such as: What are the properties of the radioactive material and its effects on people and their surroundings? Which groups are best trained and equipped to appropriately respond? Do people need to be evacuated?

"It is difficult to overstate the importance of what we are all gathered for this week," said FBI Deputy Director Paul Abbate, who kicked off the training exercise. "If the United States was to encounter a complex WMD threat or incident, the safety of the nation would rest on our shoulders. Titan Shield presents an invaluable opportunity for all of us to practice our roles and responsibilities in response to such a threat." Streamlining communications between senior decision makers, as well as outreach to foreign, state, local, tribal, and territorial officials, were additional factors WMDSG needed to consider. They also looked at strategies for crafting public messaging and determining how to disseminate information. At the conclusion of the exercise series, participants debriefed on what worked best and how they could improve future training. "Titan Shield helps us find ways to build on our successes and lessons learned to improve our coordination effectiveness and to become even more connected across all of our departments and agencies," said Abbate. "The collaboration made possible by the exercise is a testament to the resilience of our partnerships and to our shared commitment to carrying out our responsibilities to the American people."

Turkey close to deal with China on nuclear power plant

Source: https://asia.nikkei.com/Business/Energy/Turkey-close-to-deal-with-China-on-nuclear-power-plant

Sep 15 – Turkey's energy and natural resources minister told reporters from foreign media on Thursday that Turkey is in the final stages of completing its second nuclear energy deal with China. The country is preparing to generate its first nuclear-powered electricity next year through a plant being constructed by Russia.

If an agreement is reached, it will symbolize NATO member Turkey's all-directional friendships, even during a period of intensified U.S.-China rivalry.

Russia's state-owned company Rosatom is now building four nuclear reactors in Akkuyu, Mersin, Turkey – opposite Cyprus (Anadolu Agency photo)

Alparslan Bayraktar mentioned that a Chinese delegation, led by the deputy director of the National Energy Administration, recently visited the site in Turkey's northwestern **city of Kirklareli. This location, near Turkey's borders with Greece and Bulgaria**, is planned to host four nuclear reactors. The project has been a subject of negotiation between Turkey and China for several years.

China's top diplomat, Wang Yi, also visited Turkey in late July to discuss the project with Turkish leaders.

"We have been in talks with a Chinese company for a very long time. We are now at a stage where finalization is needed within a few months. We need to reach an agreement because there are other interested parties," Bayraktar said.

"We have already had enough negotiations on certain aspects of the deal. We are quite close," the minister added.

"While some differences exist, I believe they are not major. Therefore, we will be able to address the gaps and finalize a deal soon with China for the nuclear power program," he said.

In addition to the ongoing nuclear power plant project with Russia in Turkey's southern town of Akkuyu on the Mediterranean, Turkey is currently in negotiations with Russia and South Korea for another set of four nuclear reactor power plants in Sinop, a northern city situated on the Black Sea. Previously, a Japanese-French consortium had abandoned plans to build the project at this location.

China has been engaged in discussions to construct a four-reactor power plant at a third site in Turkey's northwest for nearly a decade. China's State Power Investment Corp. is pitching its CAP 1400 reactors.

According to a corporate source familiar with the Chinese position, "negotiations are progressing positively" and an intergovernmental agreement between the two countries is expected to be reached within a year.

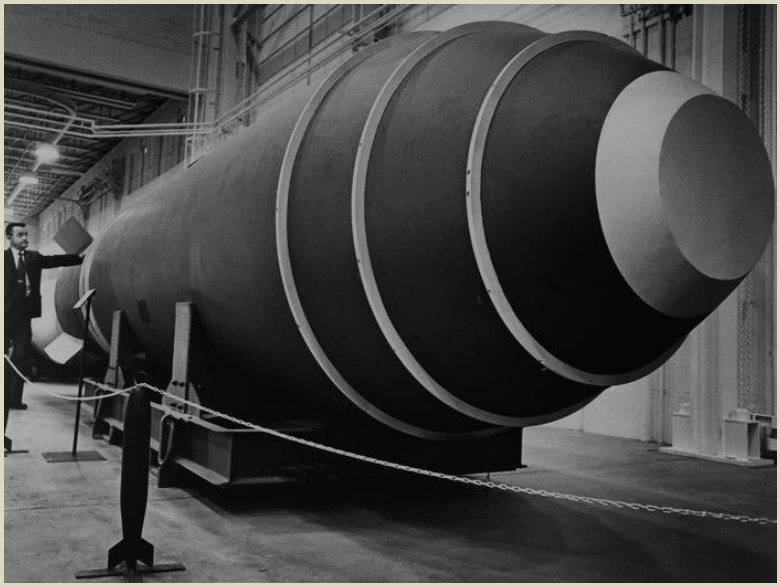
"If a deal is finalized, it will become the single largest investment of China abroad," the source said, underlining the importance of the deal for China.

Bayraktar emphasized, "According to our long-term plans, we require over 20 gigawatts of nuclear power" in Turkey, as the country aims to achieve carbon neutrality by 2053.

EDITOR'S COMMENT: There will come a day when the world will regret permitting Turkey to go nuclear. But it would be too late…

A nuclear bomb is still missing after it was dropped off the Georgia coastline 65 years ago

Source: https://www.businessinsider.com/missing-nuclear-bomb-georgia-coast-still-not-found-2023-9



This casing of a Mark 17 thermonuclear bomb was manufactured around the same time as the lost Mark 15 weapon. Corbis/Corbis via Getty Images

Sep 16 – Every once in a while, a high reading of radioactivity off the coast of Tybee Island, Georgia, sends the US government scrambling to look for a nuclear weapon that's likely hidden 13 to 55 feet below the ocean and sand, buried in the seafloor.

On February 5, 1958, two Air Force jets collided in mid-air during a training mission. The B-47 strategic bomber carried a Mark 15 thermonuclear bomb.

For over two months, the Air Force and Navy divers searched a 24-square-mile area in the Wassaw Sound, a bay of the Atlantic Ocean near Savannah. They never found the nuclear bomb.

Forty years later, a retired Air Force officer who remembered newspaper stories about the lost bomb from his childhood started a search for it. "It's this legacy of the Cold War," said Stephen Schwartz, author of "Atomic Audit: The Costs and Consequences of US Nuclear Weapons Since 1940." "This is kind of hanging out there as a reminder of how untidy things were and how dangerous things were."

But some experts say that even if someone finds the bomb, it may be better to leave it buried.

An armed training mission

At the time of the collision, it was "common practice" for the Air Force pilots on training missions to carry bombs on board, according to a 2001 report about the Tybee accident.

The purpose of the training mission was to simulate a nuclear attack on the Soviet Union. They practiced flying over different US cities and towns to see whether the electronic beam would reach its target.

Major Howard Richardson, flying a B-47 carrying the weapon, completed his mission. Meanwhile, another pilot, Lieutenant Clarence Stewart, was on his own training mission in an F-86 to intercept the jets. But Stewart's radar didn't pick up that there were two B-47s, and he and Richardson collided.

Everyone survived the crash. Stewart ejected and got frostbite. Richardson realized he couldn't land his damaged plane on the Air Force base's under-construction runway with the weight of the weapon.

He headed for the ocean, dropped the nuclear bomb from about 7,200 feet, and landed the B-47 safely.

A B-47 Stratojet similar to the one that dropped the nuclear weapon near Tybee Island, Georgia. ATP/RDB/ullstein bild via Getty Images

The plane's crew didn't see an explosion afterward, according to the 2001 report. But in 2008, Richardson wrote in a Savannah Morning News article that he and the passengers may not have seen the bomb go off because he'd turned the plane.
In 2004, Richardson told CBS News he regretted dropping the bomb because of all the trouble it caused.
"What I should be remembered for is landing that plane safely," he said. "I guess this bomb is what I'm going to be remembered for."

The question of the plutonium capsule

For weeks after the collision, about 100 Navy divers searched for the weapon using handheld sonar. Blimps and ships scoured the coast and marshes, the Atlanta Constitution reported at the time. On April 16, 1958, the military decided the bomb was "irretrievably lost." At the time, the Air Force said the weapon wasn't fully assembled and "there was no danger of an explosion or radioactivity," the Atlanta Constitution reported. Back then, the technology hadn't progressed to sealed nuclear weapons. Instead, the plutonium was separate from the bomb casing and the explosives that caused the implosion, Schwartz said. The weapon was only "complete" when the plutonium capsule or core was inside. "Only when it was complete could it be armed and set off and achieve a nuclear chain reaction," Schwartz said. The US government and military have repeatedly said the Tybee weapon didn't contain a plutonium capsule when Richardson jettisoned it. A receipt for the bomb that Richardson signed at the time said he wouldn't allow the insertion of an "active capsule" into the weapon. A 1966 letter declassified in 1994 complicated the picture. It referred to then-Assistant Defense Secretary Jack Howard's testimony before a congressional committee calling the Tybee bomb a complete nuclear weapon, with plutonium included. In 2001, a military spokesman told The Atlantic that they had recently spoken with Howard, and "he agreed that his memo was in error." "I know some people think it's settled," Schwartz said. "I haven't fully made up my mind, but I feel like I am more comfortable going with the contemporaneous accounts."

Detecting a bomb underwater

In 2000, retired Air Force officer Derek Duke contacted then-Rep. Jack Kingston of Georgia about the missing bomb and Howard's memo, CBS News reported. At the congressman's urging, the Air Force looked into the pros and cons of trying to locate and remove the weapon versus leaving it alone.

The 2001 report suggested recovery cost would start at $5 million, and that there was "a very low possibility of successfully locating the bomb." There was little chance it would spontaneously explode, it didn't contain plutonium, and the biggest environmental risk was heavy metal contamination as the bomb corroded, the report concluded.
But there was a chance of it exploding during retrieval, and experts would have to remove and dispose of the uranium first.
"The whole Air Force perspective is, it's just not worth it," Schwartz said. "Trying to move it could create bigger problems than if we just leave it where it is."
The 2001 Air Force report estimated the 7,600-pound lost bomb had 400 pounds of conventional explosive.
Nevertheless, Duke took it upon himself to find the weapon. In 2004, he thought he had it. His equipment picked up unusually high radiation readings.
The Air Force investigated but reported that the radiation was from naturally occurring minerals in Wassaw Sound.
Over a decade later, in 2015, another citizen found strange sonar readings. The Nuclear Emergency Support Team advised on Operation Sleeping Dog, when military divers again searched for and failed to find the nearly 12-foot-long bomb.
The Department of Energy sent subject matter experts to examine what the citizen searchers found in 2015, Shayela Hassan, deputy director of the Office of Communications with the National Nuclear Security Administration, said in an emailed statement to Insider.
"DOE's assessment of the material presented in 2015 was that the search lacked any evidence that supported discovery of the lost weapon," the statement said.
The agency statement continued: "Periodic announcements by private citizens that the bomb may have been located have prompted mobilizations of US Government personnel, diverting them from more pressing national security and public health responsibilities. As such, DOE does not encourage private searches for the device."
Schwartz thinks the only way the weapon will be found is by chance or if a powerful storm dredges it up.
"I won't say it's lost for the ages because I don't think it is," he said, but "so many people have searched for it for so long using some fairly sophisticated equipment and not found it."

One mishap among many

Less than a month after Richardson jettisoned the Tybee bomb, another B-47 accidentally dropped a nuclear weapon on South Carolina. It didn't contain plutonium but left a 50-foot crater in a family's yard. A few family members had minor injuries but everyone survived.
Since 1950, the US military has been involved in 32 "broken arrow" incidents, where they lost or dropped nuclear weapons or other issues, like fires, were involved.
In his book "Command and Control," Eric Schlosser wrote that in 1957 Air Force planes unintentionally dropped a nuclear weapon once every 320 flights. Coupled with the high rate of B-52 bomber crashes, there was the potential for about 19 incidents involving nuclear weapons each year. Between 1960 and 1968, the US military kept jets armed with nuclear weapons at the ready in case of a surprise nuclear attack. A series of near misses and serious accidents with nuclear weapons caused the Air Force to end the program. "I don't think we're going to go back to the bad old days of putting our nuclear weapons on aircraft," Schwartz said.
(In 2007, a B-52 bomber was accidentally loaded with six cruise missiles carrying nuclear warheads and transported without safety precautions, a mistake that would lead to the resignations of the Air Force secretary and chief of staff.)
But Schwartz thinks incidents like Tybee — whether or not it contained plutonium — can remind people about the narrow misses with nuclear disasters. "To have this many accidents and not have a weapon accidentally detonate is not just luck. It's also good engineering," he said. "But we also got incredibly lucky."

"Preemptive Nuclear War": The Historic Battle for Peace and Democracy. A Third World War Threatens the Future of Humanity

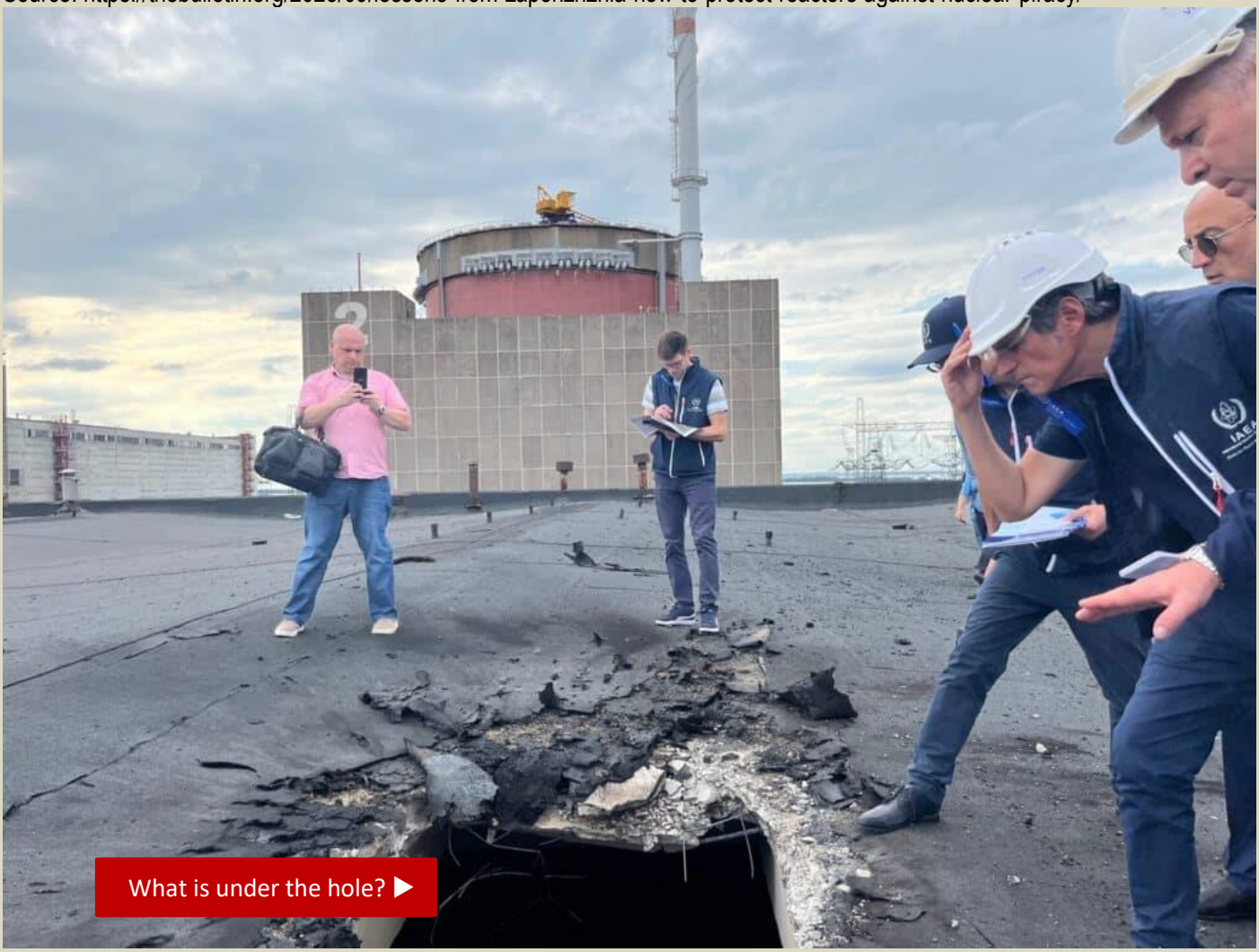
MICHEL CHOSSUDOVSKY

SEP 18, 2023

Lessons from Zaporizhzhia: How to protect reactors against 'nuclear piracy'

By Ali Alkis and Bethany Goldblum

Source: https://thebulletin.org/2023/09/lessons-from-zaporizhzhia-how-to-protect-reactors-against-nuclear-piracy/



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

Sep 20 – More than a year has passed since the world was shaken by the Russian occupation of the Zaporizhzhia nuclear power plant in Ukraine. But despite the passage of time, a chilling reality remains: Russia maintains control over the plant, a situation that serves as a constant reminder of the dire threats plaguing modern nuclear security. In this new environment, effective nuclear security demands a re-evaluation of priorities, because the occupation exposed a wholly new kind of risk: Russia—a nuclear weapon state—continues to attack, shell, mine, occupy, and operate a Ukrainian nuclear facility as a part of its so-called "special military operation" against Ukraine.

Nuclear security has traditionally focused on physical protection from a variety of threat vectors; the protective measures are colloquially referred to as "guns, guards, and gates." This dates back to defenses against state-sponsored espionage during the Manhattan Project era and began to include concerns over "loose nukes" after the fall of the Soviet Union. In the wake of the 9/11 terrorist attacks on the United States, the nuclear security community has focused somewhat myopically on the non-state actor threat—despite those attacks not being nuclear or radiological in nature.

But what are today's threats? One stands out: Deliberate hostile action by state actors against facilities housing nuclear material—such as nuclear reactors—resulting in life-threatening radiological release.

Nuclear reactors commandeered by state actors can be intentionally operated outside the protections afforded by design basis threat assessments. The potential consequences are grave, from core meltdown

to breach of containment resulting in death and illness, contamination of agricultural land and water supplies, and disruption of transportation and communication networks—not to mention damage to the credibility of nuclear power. And this isn't purely a theoretical scenario. The Russian invasion and holding of the Ukrainian Zaporizhzhia nuclear power plant creates a risk—both through occupation and stand-off attack—that might result in the release of radioactive material across borders. Moreover, the threat of these activities turns the plant into a tool for coercion, where it could be used as leverage to secure military and political advantages. Consequently, the Russian occupation of the Zaporizhzhia reactor since March 2022 exposes an unprecedented gap in nuclear security. However, it is difficult to define the risk profile here. Some experts are using the term "nuclear terrorism" or "state-sponsored nuclear terrorism" to define the situation. But existing terms come with no clear action plan to reduce this new set of nuclear safety and security risks. Instead, we propose using a new term to define the occupation of the plant and associated risks—risks that could be reduced through several admittedly imperfect but potentially useful strategies.

The new nuclear security challenge in Ukraine

In 2002, the International Atomic Energy Agency (IAEA) issued its first nuclear security action plan to combat the threat of nuclear terrorism. More than a decade later, then-US President Obama said, "the danger of a terrorist group obtaining and using a nuclear weapon is one of the greatest threats to global security." This perspective has largely shaped the international nuclear security regime of today. While the nuclear security architecture is a formidable mosaic of domestic and international initiatives, organizations, collectives, and norms, these efforts are oriented in a way that leaves a gap—and a massive vulnerability—in today's nuclear security threats.

That gap is graphically illustrated by Russia's continuing occupation of the Zaporizhzhia nuclear power plant in Ukraine.

So far, the IAEA has termed that occupation a "nuclear security risk"—something which reflects the organization's traditional focus on assisting states to address physical protection. But physical protection measures in peacetime—like access control, surveillance, and security testing—aren't particularly relevant in the midst of an active military occupation. Given that the modern nuclear security framework was developed with a focus largely on the non-state actor threat, the solutions developed so far don't apply here.

In addition, as the International Convention for the Suppression of Acts of Nuclear Terrorism of 2005 clearly points out, the acts of military forces are governed by other rules of international law, not by the Convention. In other words, the term "nuclear terrorism" isn't helpful to address risks that are caused by a state—as in this case. Framing it as such also makes it difficult to mount an action plan because nuclear terrorism has its own risk profile, whether implicit or explicit, and existing programs to address it.

As a result, we propose using a new term to distinguish Russia's actions in Zaporizhzhia from these other behaviors. If we can name the behavior, then it is easier to define the risk profile, determine what organizations are responsible for mitigating the risks, and fund them to do so. The occupation of the plant exemplifies the concept of "nuclear piracy"—defined as the illicit acquisition, manipulation, and exploitation of nuclear materials and facilities for strategic purposes. Unlike acts of nuclear terrorism exclusively focused on non-state actors, this new term refers to the unique challenges whereby a state actor leverages the inherent power of nuclear facilities for its own strategic goals. The significant consequences of nuclear piracy demand a proactive policy response as it is accompanied by its own set of nuclear safety and security risks.

Some possible solutions

One proposed solution involves creating a multilateral agreement aimed at demilitarizing nuclear reactors and their surrounding areas. Such an approach would require the withdrawal of all military personnel and equipment in and around the plant, diminishing the risk to the plant's safety and security. There are implementation hurdles associated with this approach, particularly in the midst of an ongoing conflict: In the fog of war, it is difficult to discern who is there to protect the plant and who is there to conduct military operations against it. Additionally, verifying the agreement in the middle of an active conflict poses further difficulties as site access may be restricted or unsafe. There are also political implications, as some may perceive such an agreement as conferring legitimacy upon the usurper. (Indeed, this approach was called for by the UN and IAEA in the case of the Zaporizhzhia plant without success.)

Another, perhaps more viable strategy is to establish a so-called "nuclear safety and security protection zone" around the plant. This measure requires the immediate cessation of a kinetic military attack or basing at the nuclear reactor site and the protection of off-site power and essential structures and systems. The zone includes a commitment to guard against undermining these principles. Despite not requiring the full withdrawal of military forces, a protection zone would almost certainly mitigate damage to the reactor and help to ensure its physical integrity. It may also alleviate the psychological pressure and performance challenges faced by reactor personnel forced to maintain operations in an ongoing conflict. In the Zaporizhzhia plant's case, despite the agency's continuous efforts and the personal commitment of IAEA Director General Grossi, the establishment of such a zone has not yet been achieved.

In a more generalized approach, the IAEA could be granted full access to nuclear power plants throughout any militarized interstate dispute—a formal change in authority and policy that could play a critical role in combating nuclear piracy and enhancing transparency and safety in a crisis. For example, in August 2022,

Grossi led a special support and assistance mission to establish a continuous presence at the Zaporizhzhia plant. Despite this, the team encountered the continuing problem of restricted access to some parts of the facility, which limits the assessment of the threats and damages to the plant and surrounding area. This problem was illustrated by the discovery of mines located in a buffer zone between the site's internal and external perimeter barriers—emphasizing the pressing need to extend to a neutral intergovernmental organization full access to contested nuclear facilities.

Even if imperfect, steps can be taken to protect against nuclear piracy, not only reducing the associated environmental and geopolitical risks but also reinforcing existing nuclear security mechanisms. The sooner the international community implements effective measures to counter today's risks, the better chance there is to safeguard against potentially catastrophic consequences. The time to rethink nuclear security is now.

Ali Alkis is the World Institute for Nuclear Security Ambassador to Turkey and a Ph.D. candidate at Hacettepe University in Ankara, Turkey. Alkis is also a member of the Gender Champions in Nuclear Policy, serves as the Gender Champion at the Odesa Center for Nonproliferation, and is one of the emerging leaders of the NTI's Global Dialogue on Nuclear Security Priorities. His research interests encompass nuclear security, non-proliferation, and nuclear terrorism as well as Turkish nuclear and foreign policies.

Bethany Goldblum is an associate professor in the Department of Nuclear Engineering at the University of California, Berkeley and faculty scientist in the Nuclear Science Division at Lawrence Berkeley National Laboratory. As executive director of the Nuclear Science and Security Consortium, Goldblum sets strategic direction for a multi-institution initiative established by the Department of Energy's National Nuclear Security Administration to conduct research and development supporting the nation's nonproliferation mission while expanding the talent pipeline. Her research focuses on fundamental and applied nuclear physics, neutron detection, scintillator characterization, nuclear applications in machine learning, and nuclear security policy. Goldblum also founded and directs the Nuclear Policy Working Group, an educational programming effort developing policy solutions to strengthen global nuclear security, and is director of the Public Policy and Nuclear Threats Boot Camp at the Institute on Global Conflict and Cooperation. She received a PhD in nuclear engineering from the University of California, Berkeley.

Yes, nuclear weapons are immoral. They're also, practically speaking, useless.

By Ward Hayes Wilson

Source: https://thebulletin.org/2023/09/yes-nuclear-weapons-are-immoral-theyre-also-practically-speaking-useless/

Sep 19 – Almost everyone who works actively against nuclear weapons is, at some level, appalled by the immorality of nuclear weapons. This makes sense because the indiscriminate killing of children, grandparents, people with disabilities, and a host of other ordinary folks is appalling.

As a result, the first argument that almost all activists reach for is moral. They bring forward hibakusha to put a human face on the immorality. They talk about the indigenous people who suffered during the mining and production of nuclear weapons. They show graphic pictures of the destruction, the burns, the radiation sickness, and other catastrophic damage done by the bombings. They say, in effect, "Look at the immorality!" They sometimes point to it with a hint of outrage in their voices. How can people not be moved by these horrible, immoral acts?

And yet here we are, 78 years later, in the midst of a second nuclear weapons arms race. Every nation that possesses nuclear weapons is either expanding or upgrading its nuclear arsenal. How can this be?

It seems undeniable, after the better part of a century has passed, that moral arguments are not enough to eliminate nuclear weapons. When a strategy fails for 78 years, it's probably time for a rethink.

I believe most people—including national leaders—hesitate to eliminate nuclear weapons not because they are heartless, or lack any sense of morality, or are idiots, but because they believe, for some reason, that nuclear weapons are necessary. After all, people often set their moral feelings aside when they believe their survival is at stake. In the case of nuclear weapons, many people believe that nuclear weapons are such powerful weapons that they can guarantee a country's

safety. Therefore it makes sense that most countries secretly want such powerful weapons, and as a consequence, nuclear weapons will always exist. They are such desirable weapons, in other words, that even if you could ban them, someone would inevitably build an arsenal in secret. So it's impractical to even think about eliminating them.

If this analysis of how people feel is right, then there are, in fact, two parts to the nuclear weapons elimination equation: **morality and necessity.** You can only solve the equation if you take on both parts. But you have to solve the parts in the right sequence. Before you can move people with moral discourse, you have to first remove the roadblock in their heads that tells them that their country must have nuclear weapons to keep them safe. The key to eliminating nuclear weapons, then, is to start with the practical consideration. Make a case that nuclear weapons could reasonably, realistically be eliminated, neutralize that part of the equation, and the morality argument falls like a hammer blow. "But Ward," a devil's advocate might argue, "there are no practical arguments for eliminating nuclear weapons." Well, actually, there are. A lot of them. Let me point out just three.

First, you may have noticed that when Vladimir Putin threatened to use nuclear weapons again and again in Ukraine last fall, a number of establishment sources suddenly spoke up, making the case that nuclear weapons actually aren't very good weapons. The New York Times, The Institute for the Study of War, and even Gen. David Petraeus all argued that using nuclear weapons on the battlefield wasn't very militarily useful.

And if you look back over past wars, military commanders have repeatedly turned away from using nuclear weapons—not because of moral concerns, but because of practical doubts about the military value of the weapons.[1]

It has been an open secret in Washington for decades, apparently, that battlefield use of nuclear weapons was militarily inadvisable. When President George H. W. Bush ordered the removal of all but a handful of 7,000 tactical nuclear weapons from Europe in 1991, there was no open revolt among military officers. Apparently, they were fine with the decision. So there is a good deal of evidence, based on the advice of military officers, that nuclear weapons aren't such great weapons.

Which brings us to another argument: What about using nuclear weapons not on the battlefield but against an enemy's homeland? Well, if your adversary also has nuclear weapons, that option is, if anything, worse. When your adversary strikes back, your country will be devastated. It is clearly a suicidal option. And if your adversary doesn't have nuclear weapons, it's not war, it's genocide.

Finally, many people argue that nuclear weapons are important because of nuclear deterrence. But even a 12-year-old can effectively show that deterrence is fatal over the long run. After all, human beings are fallible, aren't they? And human beings play a critical role in nuclear deterrence. Human beings make the threats, evaluate the threats, and decide how to respond. If human beings are prone to folly—and we are—and if human beings run the deterrence process, then nuclear deterrence is inherently flawed. It will fail. Over the long run it cannot be safe. Eventually, human failure will lead to a catastrophic nuclear war.

Moral arguments are powerful in the fight against nuclear weapons. But a roadblock prevents moral arguments from working. In fact, it causes them to boomerang and actually turn people off. **But if you're willing to argue against nuclear weapons with a two-step process—first showing that the necessity argument is false and only then arguing that the weapons are horrible and immoral—there's a clear pathway to elimination.**

Notes

[1] Korea and Vietnam are covered in John Lewis Gaddis, The Long Peace: Inquiries into the History of the Cold War (New York: Oxford University Press, 1987) p. 119 and 125. "The outcome of these investigations was not particularly encouraging. Army Chief of Staff General J. Lawton Collins expressed himself as 'very skeptical' about the military advantages; Chinese and North Korean forces were deeply entrenched along a 150-mile front, and recent bomb tests in Nevada had proven 'that men can be very close to the explosion and not be hurt if they are well dug in.'" The Gulf War comes from Colin Powell, My American Journey: An Autobiography, (New York: Random House, 1995), pp. 485-6. "I told Tom Kelly to gather a handful of people in the most secure cell in the building to work out nuclear strike options. The results unnerved me. To do serious damage to just one armored division dispersed in the desert would require a considerable number of small tactical nuclear weapons. I showed his analysis to Cheney and then had it destroyed. If I had had any doubts before about the practicality of nukes on the field of battle, this report clinched them."

Ward Hayes Wilson is the author of *Five Myths About Nuclear Weapons* and of the forthcoming (Oct. 24) *It Is Possible: A Future Without Nuclear Weapons*.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

Table of Iran's Missile Arsenal

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

Aug 24 – 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 has deployed a system, the Khorramshahr, that could almost certainly reach longer ranges if equipped with a lighter warhead. 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 until October 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. It has also allegedly considered selling them to Russia.

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	~500 m	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	~100 m	deployed
Fateh-110 (including Khalij Fars and Hormuz[9])	SRBM	300 km	~450 kg	solid fuel, single stage	100 m[10]	deployed
Fateh-313	SRBM	500 km	350 kg	solid fuel, single stage	10-30 m[11]	deployed
Zolfaghar (including Zolfaghar Basir[12])	SRBM	700 km	450-600 kg	solid fuel, single stage	10-30 m[13]	deployed
Dezful	SRBM	1,000 km	450-600 kg	solid fuel, single stage	10-30 m[14]	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	300 m	deployed
Emad	MRBM	1,800 km	~750 kg	liquid fuel, single stage	<500 m	deployed

Name	Type[5]	Max Range	Payload	Propulsion	CEP[6]	Status
Khorramshahr-1, -2, and -4 (BM-25/Musudan)	MRBM[15]	2,000-3,000 km	750-1,500 kg	liquid fuel, single stage	30 m	deployed
Fattah[16]	MRBM	1,400 km	unknown	solid fuel, single stage[17]	unknown	tested
Haj Qassem	MRBM	1,400 km	500 kg	solid fuel, single stage	unknown	deployed
Kheibar Shekan	MRBM	1,450 km	450-600 kg	solid fuel, single stage	unknown	deployed
Sejjil	MRBM	2,000 km	~750 kg	solid fuel, two stage	unknown	deployed
Meshkat/Soumar (Kh-55)	LACM	unknown[18]	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[19]	LACM	700-800 km	unknown	turbojet engine	N/A	deployed[20]
Paveh	LACM	1,650 km	unknown	turbojet engine[21]	N/A	deployed
Safir	SLV	2,100 km[22]	500-750 kg[22]	liquid fuel, two stage	N/A	retired
Simorgh	SLV	4,000-6,000 km[22]	500-750 kg[22]	liquid fuel, two stage	N/A	no successful launches
Qased	SLV	2,200 km[22]	1,000 kg[22]	liquid 1st stage; solid 2nd and 3rd stages	N/A	operational
Zuljanah	SLV	4,000-5,000 km[22]	1,000 kg[22]	solid 1st and 2nd stages, liquid 3rd stage	N/A	tested
Ghaem-100	SLV	3,000-4,000 km[22]	1,000 kg[22]	solid fuel, three 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. See "2020 Ballistic and Cruise Missile Threat," U.S. National Air and Space Intelligence Center, pp. 21, 25, January 2020, available at https://irp.fas.org/threat/missile/bm-2020.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. Similarly, Iran's Rezvan appears to be a copy of the Houthi Zulfiqar, itself a modified Qiam.

[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] Based on its likely use in the January 2020 ballistic missile attack against U.S. forces and damage assessments of that attack.

[12] The Zolfaghar Basir is the anti-ship variant of the Zolfaghar.

[13] 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.

[14] Based on its use in the Great Prophet 17 military exercise suggesting it has precision similar to that of the Zolfaghar.

[15] Iran has displayed at least four different variants of the Khorramshahr missile, each potentially with its own specifications in terms of range, warhead size, and accuracy. Iran has consistently claimed that the missile has a 2,000 km maximum range and a warhead with a mass of 1,500 kg or greater. France, Germany, and the United Kingdom claimed in 2019, however, that one variant of the missile has a nose cone whose size would limit the warhead mass to about 750 kg. They further claimed that the modelling of such a missile puts its range at approximately 3,000 km, which would classify it as an intermediate-range ballistic missile (IRBM). See, "Letter dated 25 March 2019 from the Permanent Representatives of France, Germany and the United Kingdom of Great Britain and Northern Ireland to the United Nations addressed to the Secretary-General," United Nations Security Council, S/2019/270, March 27, 2019, available at https://www.undocs.org/S/2019/270.

[16] Iran has billed the Fattah as a "hypersonic" missile. Hypersonic missiles are typically defined not only by their ability to reach speeds in excess of Mach 5, but also by their ability to maintain such speeds while making significant maneuvers within the atmosphere during flight. Although the Fattah missile may fit this description, it is largely in a class of its own in terms of how it achieves this: the two main types of hypersonic missiles under development across the world are hypersonic gliders and hypersonic cruise missiles, and the Fattah, a ballistic missile with an extra solid rocket motor in its re-entry vehicle, is neither.

[17] The Fattah missile consists of a large solid rocket booster (based off of the Kheibar Shekan design) plus a small solid rocket motor situated inside the re-entry vehicle for terminal maneuvering. The latter is a post-boost propulsion system, and these are not traditionally counted as "stages." The Minuteman III, for example, is considered a three-stage missile even though it consists of three solid rocket motors plus a liquid-fueled post-boost vehicle. So, Fattah can be considered a single-stage missile.

[18] 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.

[19] The Quds-1, referred to as the "351" by the United States, 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.

[20] Based on the assumption that the 2019 attack on Saudi Aramco facilities was launched from Iran.

[21] Based on visual similarities with the Quds-1.

[22] Estimate if reconfigured as a ballistic missile.

Yemen's explosives contamination 'among world's worst'

Source: https://www.citizen.co.za/news/news-world/yemens-explosives-contamination-among-worlds-worst/

Sep 11 – Yemen has one of the world's highest rates of contamination with landmines and other deadly explosives, the International Committee of the Red Cross has warned, nine years after the start of the brutal civil war.

The impoverished Arab nation, plunged into conflict when Iran-backed Huthi rebels seized the capital in September 2014, is among the three worst affected countries, the ICRC said. Experts estimate that at least one million mines have been planted during Yemen's years of turmoil, causing a daily hazard along with unexploded shells and other military detritus.

"When it comes to weapon contamination, with Afghanistan and Iraq, Yemen is among the three countries most affected by this," Fabrizio Carboni, the ICRC's Near and Middle East regional director, told AFP.

"It is really devastating and has a very important impact on people, their safety, and also their livelihood."

A Saudi-led military coalition has been fighting the Huthis since March 2015 in a conflict that has left hundreds of thousands dead from direct and indirect causes such as famine.

According to the UN-linked Civilian Impact Monitoring Project, landmines, unexploded shells and other leftovers from fighting caused 1,469 civilian casualties over the past five years. "The presence of unexploded ordnance is just massive," said Carboni.

Farmers on explosives

Twenty percent of livestock owners living in two areas close to frontlines reported explosives contamination on their land, the ICRC found after conducting a series of interviews last year. Another ICRC survey of shepherds found that 70 percent had lost animals to landmines and other explosives. "The contamination is so important and widespread that you won't be in a position to decontaminate everything," even if the conflict ended today, Carboni said.

Clearance could take 'decades'

Fighting in Yemen has calmed markedly after a UN-brokered ceasefire came into effect in April 2022 and has largely held even after the agreement lapsed in October 2022.

A Chinese-brokered rapprochement between regional powers Iran and Saudi Arabia, eight years after they broke off ties, has also sparked hope for Yemen.

"This is the first time that I really feel that there are convincing, concrete political options on the table and that violence and conflict is not anymore the only option," Carboni said.

But even if peace prevails, clearing the land of explosives would take many years, he said, adding that it would require resources, expertise and machinery. "We are talking about, maybe, decades. But again, it's a matter of resources," he said.

"Today, we inform, we train," Carboni added.

"We have sessions with communities where we inform them about the risks related to unexploded ordnance, or if they find remnants of war… they have to inform us so we can organise (clearance) with the various authorities and partners.

"That's quite new for us."

The ICRC is also putting renewed effort into identifying and returning the remains of fighters who have died on each side, Carboni said. "There are many dead bodies that were left and we really want to work with all parties of this conflict to put more energy and drive into this file," he said. "We're investing in forensic, we're investing in trying to put all parties around the table."

In May, the rebels and government forces exchanged the corpses of 43 fighters, the largest such handover so far. A month earlier, they had freed nearly 900 detainees.

In its effort to help Yemen deal with the impacts of its brutal war, said Carboni, "we want to be optimistic but, at the very same time, we don't want to be naive".

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Considerations in the Preparation and Implementation of Security Technologies in Olympic Events

By Or Shalom

Source: https://i-hls.com/archives/120544

Aug 23 – Preparations for the Olympics in France are at their peak, and so are the preparations in matters of security. The security is extremely complex as can be seen by the terrain and number of participants in the opening events alone, and the need to prepare for drone threats in the security protocols. The fact that the Olympics are a target for terrorism (as seen by those with malicious intent), the allure, the ability to reach events from different parts of the world under the guise of visitors to the Olympics, and the terrain all contribute to an even greater challenge. The terrain and landscape of the opening events will not be held in a closed stadium but rather will be along the Seine River with at least 500,000 guests and visitors, some in sections that do not require purchasing tickets, and about 200 heads of state that are expected to participate. One of the conclusions drawn from past events (as a direct lesson from the Munich attack and the Atlanta Olympics) is the need to increase security and technological means available on the scene. Meanwhile, in light of the open landscape of the events, security must be adjusted and implemented by the 'Crime Prevention Through Environment Design' approach (CPTED), which allows planning and risk reduction in accordance with the terrain and conditions of the environment. Past events require preparation for the possibility of organized terrorist activity (such as the Munich Olympics Massacre) and the possibility of a "lone wolf" attacker in some constellation (like the terror attack at Atlanta's Olympic Centennial Park).

Intelligence Utilization In Various Circles:

The initial working assumption is to extract information available through WEBINT and OSINT networks (all visible sources of information), assuming that the opponent is using various platforms while organizing, gathering information, and promoting their goals. This can be carried out through the use of social networks, sending messages on Telegram, collecting information, acquiring weapons through the Darknet, etc. Therefore, overarching capabilities and cooperation between countries and intelligence agencies are required to realize capabilities around marking important news, cross-referencing names, expressions, possible trends, indicators, activity patterns, decryption/encryption capabilities, and more. As part of this cooperation, there are quite a few technologies dedicated to realizing these capabilities that are based on the analysis of connections, news, and posts on social networks (posts that include the use of symbols or radical expressions), like the detection of incriminating information in the open and deep network (including the darknet). The more these methods rely on AI-based automation capabilities, the better the intelligence process will be, and the more accurate it will be in the face of the changing methods of the opponent.

When it comes to cross-national processes and events, it is more necessary to analyze and trace processes that arise from metadata, which involves the production of additional relevant information from the existing information based on signatures created on the network[1]. This capability enables a retrospective look at the sequence of events, connections between entities, geographic locations, financial

transaction information, travel patterns, web browsing activity, and more. Therefore, processing and tracing the whole process from registration to ticketing and check-in is very crucial. For example, an insight can be derived from the fact that a number of terrorists have reached the same destination from a shared country on different flights, or an event in which the person who bought the ticket before the flight is not the passenger himself, etc.

The ability to extract the information that would indicate the suspects lies in the ability to cross-reference all the processes and stages (including on the scene itself). If we take the Tamarlan brothers' 2013 Boston Marathon bombing as a case study, we can see that there were suspicious signs of posts and tweets that showed radical trends prior to the event[2]. Another relevant statistic is information about the visit of one of the brothers about 6 months before the marathon itself in Chechnya (possibly the turning point that caused him to plan the attack) as possible evidence of extremism that could lead to practical intelligence insight. In a separate intelligence circle, in 2011 the Russians turned to the FBI for information about Tamarlan, due to suspicion of belonging to radical Islam circles and joining underground groups. This once again reinforces the need for cooperation and exchange of information between international entities.

There are quite a few challenges when facing the threat of terrorist assimilation on the scene. In 2016, ISIS issued a guide aimed at assimilating into small cells and the "lone wolf" method with the goal of soliciting and providing tools to individual operatives on the scene[3]. Here too, there are quite a few insights related to the technological and intelligence capabilities to track the changing guides and patterns, as well as a broad deployment of checkpoints in the crossings between areas as well as in random locations. An efficient process that may be the tiebreaker is the ability to rapidly retrieve information and cross-reference it with the information emerging on the scene itself (along with the various intelligence circles and past knowledge)[4]. Thus, for example, the allure of check-in deployments and ticketing processes will grow and be able to overwhelm the anomalies the more accessible it is to cross-reference with the information in existing databases and information generated in circles on the scene. As part of the proper dispersion and extraction of the check-in positions, the integration of rapid tactical capabilities for baggage testing (AI-based technologies) will enable additional capabilities for anomaly detection, as well as make organizing seem more difficult in the eye of the attacker.

Smart security based on analytics and AI capabilities:

The security of mass international sporting events requires the preparation of management, rapid response capabilities in the face of a developing event or immediately thereafter, and the ability to control the crowd in its various stages, including the need for monitoring and dispersion or public direction during or after an occurrence, with the aim of preventing the event. The landscape conditions at the opening event present quite a few challenges and difficulties in the ability to locate incriminating patterns, as well as the ability to control the audience according to the progressing events. Integration of decision-support systems based on analytics and AI will enable smart and efficient security thanks to learning, thinking, planning according to fixed parameters and events, and quality information extraction. The manner of planning should match the way one can predict and indicate abnormal behavior and anomalies (e.g., gatherings larger than the norm), staying in forbidden areas, etc. For example, unacceptable transits between regions can be defined as a possible indication of deviation from the norm in a way that will provide a warning and indication.

In addition to implementing AI on security cameras as the French have stated they will do; it will be advisable to also realize these capabilities through the use of drones[5]. The terrain and the transition between events and regions require control that enables fusion and analysis of the area in different dimensions, and of course enables capabilities of measuring crowds, monitoring movements, and more. In general, in event security, adopting the DFR (Drone As First Responder) approach will improve performance and rapid response capabilities[6]. In order to optimize smart security, there needs to be collaborative capability and a wide pool of data that will enable data fusion and cross-referencing. Of course, the data transfer process as well as the database itself require security-oriented thought in the aspects of cyber protection like the use of diodes and single-directional data channels and the ability to protect the various systems and regions.

Preparation To Deal With Drone Threats:

As mentioned, the French defined the drone threat in the security protocol as a troubling issue that requires preparation. The use of drones has often been proven for various purposes, from collecting intelligence to using it as weapons. There are quite a few possible solutions, from systems based on kinetic abilities, to capabilities that combine frequency disruption and blocking, as well as laser drone destruction systems, like the experiments recently conducted by the French[7]. The document published by the CISA titled "Unauthorized Drone Activity over Sporting Venues" aims to implement a group-based plan: Prevention, Protection, and Response Controls. The Prevention Control group includes the ability to coordinate between the authorities, increase public awareness and warnings regarding drone restrictions (warnings both online and physical signs on the scenes), as well as legal enforcement. The Protection Control group aims to conduct a risk survey for potential launch areas (parking lots, balconies, and open areas), formulate an emergency response, train security teams in detecting the exception, formulate indications based on speed, weight, flight near or

above people, design changes in the drone, etc. The Response Control group aims to incorporate responses in a case of a drone crash, responding to treatment beyond the boundaries of the security sector and reporting to other authorities and security officials. Due to the complexities arising from problematic (urban) environmental conditions, safety restrictions, potential implications of technological blockages in the area itself, manpower skills, etc., those in charge must examine technologies, deployment and coverage, performance, and the abilities to detect and locate operatives on the scene and adapt all the requirements according to the terrain and conditions.

Or Shalom is a security, cyber, and HLS technology expert and consultant to government ministries and defense industries. He holds a master's degree, as well as civil and national qualifications in the realm of HLS and Cyber Security. He has experience in consultation and business development for security companies and groups in matters of planning and building defense, innovation and security technology, exercises, and training in security and cyber.

[1] https://counterterrorismethics.tudelft.nl/bulk-meta-data-collection-and-use/
[2] https://i-hls.com/he/archives/118316
[3] https://cryptome.org/2016/01/lone-wolf-safe-sec.pdf
[4] https://i-hls.com/he/archives/107457
[5] https://www.bbc.com/news/world-europe-66122743
[6] https://www.mitre.org/news-insights/publication/drone-first-responder-programs-new-paradigm-policing
[7] https://i-hls.com/he/archives/110981

Not a very clever subtitle!

Met police on high alert after 'staggering IT security' breach

Potential leaked data from system with access to names, ranks and photos of officers could do 'incalculable damage in the wrong hands'.

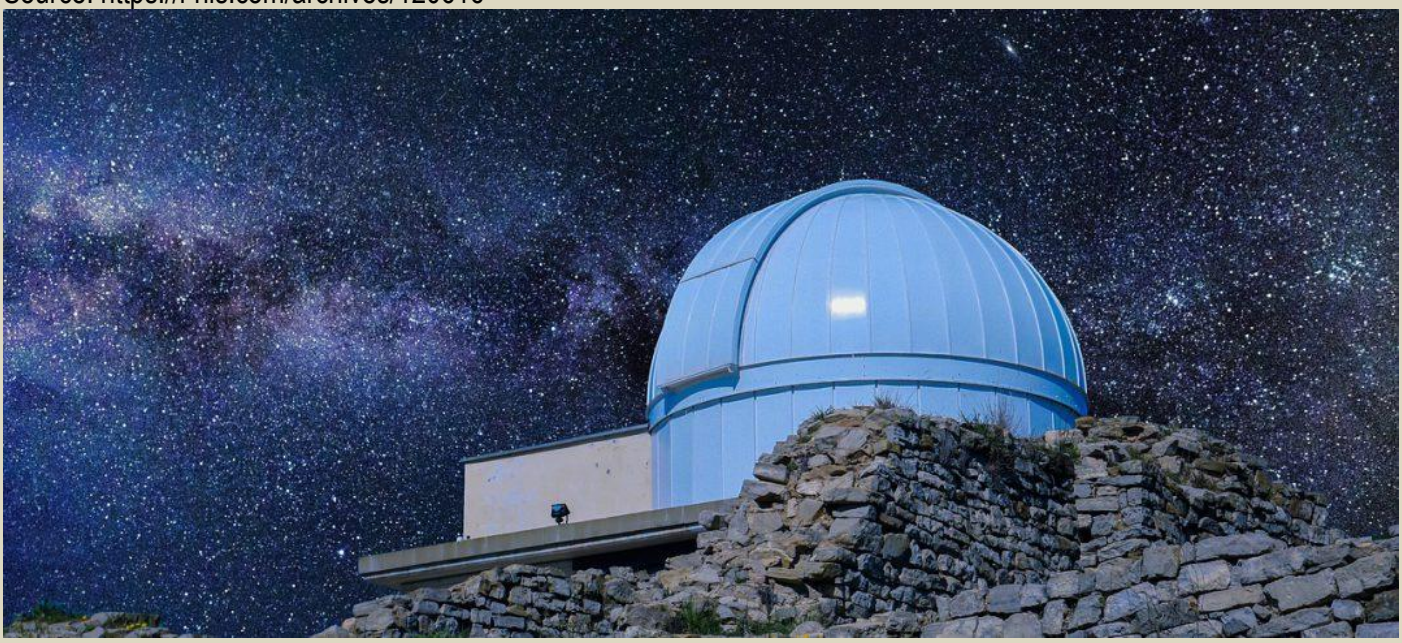
Source: https://www.theguardian.com/uk-news/2023/aug/26/met-police-on-high-alert-after-it-system-holding-officers-details-hacked

Aug 26 – The Metropolitan police is on high alert after a security breach involving the IT system of one of its suppliers, the force said.
Scotland Yard is working with the company to understand the scale of the incident but said on Saturday evening that any leaked data could do "incalculable damage" in the wrong hands.
A spokesperson for the Metropolitan police said any potential leak "will cause colleagues incredible concern and anger".
The company in question had access to names, ranks, photos, vetting levels and pay numbers for officers and staff, but did not hold personal information such as addresses, phone numbers or financial details, the force said.
A spokesperson for the force was unable to say when the breach occurred or how many personnel might be affected.
Rick Prior, vice-chair of the force said: "Metropolitan police officers are – as we speak – out on the streets of London undertaking some of the most difficult and dangerous roles imaginable to catch criminals and keep the public safe.
"To have their personal details potentially leaked out into the public domain in this manner – for all to possibly see – will cause colleagues incredible concern and anger.
"We share that sense of fury … this is a staggering security breach that should never have happened."
He added: "Given the roles we ask our colleagues to undertake, significant safeguards and checks and balances should have been in place to protect this valuable personal information which, if in the wrong hands, could do incalculable damage.
"The men and women I represent are justifiably disgusted by this breach. We will be working with the force to mitigate the dangers and risks that this disclosure could have on our colleagues. And will be holding the Metropolitan police to account for what has happened.
"Our brave police officers – who give up so much to do this job – deserve so much better."
The Met has taken "security measures" as a result and the matter has been reported to the National Crime Agency, while the Information Commissioner's Office (ICO) is also aware.
It follows an admission by the **Police Service of Northern Ireland** (PSNI) that personal data on all its serving members was mistakenly published in response to a freedom of information (FoI) request.

Details of about 10,000 PSNI officers and staff included the surname and first initial of every employee, their rank or grade, where they are based and the unit they work in.
After the PSNI breach was revealed, Norfolk and Suffolk constabulary announced the personal data of more than 1,000 people – including crime victims – was included in another FoI response.
On Wednesday, South Yorkshire police referred itself to the ICO after noticing "a significant and unexplained reduction in data stored on its systems".
The force said it was now urgently working with experts to recover footage filmed by officers as they attended incidents or engaged with the public that, in some cases, could be used as evidence in court.

Major Cyberattack Disables Telescopes in Hawaii and Chile

Source: https://i-hls.com/archives/120616



Aug 29 – Prominent National Science Foundation (NSF) space telescopes worldwide have been shut down due to a major cyberattack, the reason for which is unknown. For over two weeks, ten telescopes have been impacted, while some on-site operatives were able to keep some operational. These shutdowns have caused chaos in the astronomy sphere due to many essential windows of opportunity being missed for space observations.
NOIRLab (the NSF-run coordinating center for ground-based astronomy) said in a press release "Our staff are working with cybersecurity experts to get all the impacted telescopes and our website back online as soon as possible and are encouraged by the progress made thus far."
Research teams are dealing with the shutdown by collaborating to find alternatives as crucial observation windows become unattainable, like sending teams to places in Chile to relieve the on-site staff who have been directly operating the telescopes for the past two weeks.
According to Interesting Engineering, NOIRLab announced on August 1st that its Gemini North telescope in Hilo, Hawaii, was hit by a cyberattack. In response to the attack, NOIRLab has shut down operations at several of its crucial telescopes in Chile and Hawaii to protect the facilities until further information emerges, rendering remote observation impossible.
Cybersecurity experts worldwide are confused as to why attackers would target Gemini North. Retired lead of the NSF Cybersecurity Center of Excellence Von Welch suggests the attacker may not even realize they are attacking an observatory.
Astronomers are reportedly motivated to enhance cybersecurity practices to secure their facilities, with the entire astronomical community rethinking how it manages identity and access software, and considering the damage that something as simple as a lost password can cause.

Patrick Lin, who leads an NSF-funded space cybersecurity grant at California Polytechnic State University says: "It doesn't help if you build the strongest, most impenetrable fortress in the world if you forget to lock even a single door or window. The weakest link is often with us, the humans."

Poland Railroad Hit by Cyberattack

Source: https://i-hls.com/archives/120610

Aug 29 – Polish intelligence services are investigating a cyberattack on its railways. According to the Polish Press Agency (PAP), the hackers broke into railway frequencies to disrupt traffic in the north-west of the country overnight.

Furthermore, the signals were reportedly interspersed with a recording of Russia's national anthem and a speech by President Vladimir Putin.

For important context, Poland has been a major transit stop for Western weapons that are being sent to Ukraine to aid in the war with Russia.

According to BBC News, Saturday's incident happened when hackers transmitted a signal that triggered an emergency halt of trains near the city of Szczecin. Approximately 20 trains were forced to a standstill, but services were restored within hours nevertheless.

A senior security official named Stanislaw Zaryn provided a statement saying that Poland's internal security service ABW was investigating the whole situation and that for the moment they are ruling nothing out.

Zaryn added that they have been aware of attempts to destabilize the Polish state for some months now, stating that "Such attempts have been undertaken by the Russian Federation in conjunction with Belarus."

In response to this, several Western countries have called for increased cyber-security precautions, as the Russian-Ukrainian conflict unfolds and affects all of Europe.

There are experts who claim that Russia is supposedly carrying out cyberattacks in Ukraine in an attempt to test its hacking tools, allegations to which Russia responded by calling them "Russophobic".

What is Neuromorphic Computing, and How Will It Change the World of Machine Learning?

Source: https://i-hls.com/archives/120927

Sep 16 – Research institutions have been working for the past few years to find new concepts of how computers can better process data in the future. One of these concepts is "neuromorphic computing"- a method of computer engineering in which elements of a computer are modeled after systems in the human brain and nervous system.

Compared to traditional artificial intelligence algorithms that have to be trained on large amounts of data before they can be effective, neuromorphic computing systems can learn and adapt as they go.

With the machine learning world growing so quickly, German researchers have devised an efficient training method for neuromorphic computers.
Florian Marquardt, a scientist at the Max Planck Institute for the Science of Light in Erlangen, Germany, explains: "We have developed the concept of a self-learning physical machine. The core idea is to carry out the training in the form of a physical process, in which the parameters of the machine are optimized by the process itself."
The model will require external feedback to improve, as in training conventional artificial neural networks, but the self-learning physical machine the researchers propose makes the training much more efficient and saves energy.
"Our method works regardless of which physical process takes place in the self-learning machine, and we do not even need to know the exact process," explains Marquardt. "However, the process must fulfill a few conditions. Most importantly, it must be reversible, meaning it must be able to run forwards or backward with a minimum of energy loss."
According to Interesting Engineering, von Neumann architecture, on which most of our hardware today is based, is the complete opposite of a neuromorphic architecture. The researchers also state in their study that the von Neumann architecture currently used in electronic devices is highly inefficient for most machine-learning applications.
"We hope to be able to present the first self-learning physical machine in three years," said Marquardt. "We are therefore confident that self-learning physical machines have a strong chance of being used in the further development of artificial intelligence."

Cybersecurity in Hospitals and the Public Health Sector

Source: https://domesticpreparedness.com/articles/cybersecurity-in-hospitals-and-the-public-health-sector

Sep 13 – Healthcare cyberattacks continue to increase in frequency. The primary methods used in these attacks include phishing and email compromise (e.g., ransomware and other malware), fraud scams, network server breaches, inappropriate access to medical records, insider threats, and standard theft.
In 2022, HHS published *The Impact of Social Engineering on Healthcare*, which found that phishing attacks were the top threat, representing 45% of all attacks. Ransomware (most commonly delivered through phishing emails, malicious links, or malicious advertising) accounted for another 17%, leaving almost two-thirds of all attacks deriving from these two vectors. Reporting on attacks against healthcare organizations outlines some malware and techniques used in recent years. The main takeaway for most practitioners is understanding every employee has a part to play in keeping organizations safe. The most robust and impactful defenses can be ineffective if employees fall victim to phishing attacks or fail to follow established protocols.
Hospital Corporation of America (HCA) Healthcare, one of the nation's leading providers of healthcare services, was recently targeted. Their data breach was one of the largest healthcare breaches in history, involving at least 11 million patients residing in 20 U.S. states. Additional notable cyberattacks on healthcare organizations in 2023 include:

- 9 million patients in May at Managed Care of North America (Georgia)
- 9 million patients in May at PharMerica (Kentucky)
- 4 million patients in February at RMG, LMO, ADOC & GCMG (California)
- 2 million patients in March at Cerebral, Inc. (Delaware)
- 5 million patients in June at Enzo Clinical Labs (New York)
- 5 million patients in April at Harvard Pilgrim, Point 32 Health (New Hampshire)
- 997K patients in March at Zoll (Massachusetts)
- 618K patients in February at CentraState Healthcare System (New Jersey)
- 559K patients in April at Murfreesboro Medical Clinic (Tennessee)

The recent HCA data breach is the 4th largest cyberattack on a healthcare organization in the U.S. The top 3 healthcare cyberattacks involved:

- 79 million patients in 2015 at Anthem (Indiana)
- 21 million patients in 2018 at American Medical Collection Agency (New York)
- 11 million patients in 2014 at American Medical Collection Agency (Washington)

Healthcare Cyberattacks Reported – The Numbers
The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) Breach Portal tracks breaches of unsecured protected health information when the event affects more than 500 patients, a reporting requirement under the HITECH Act. As of August 15, 2023, there were 901 breaches reported within the last 24 months (with the Breach Portal using a rolling report where older reports drop off and

new ones are added as the calendar moves), including 355 from January to July 2023 (compared to 224 over the same period in 2022).

The healthcare industry is targeted based on the lucrative nature of its records, its vulnerability, and its visibility as this industry is considered one of the country's 16 Critical Infrastructure Sectors. According to the Cybersecurity & Infrastructure Security Agency (CISA):

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Healthcare is vulnerable and targeted, in part, due to the rapid adoption and deployment of technology driven by the COVID-19 pandemic and a lack of available cybersecurity talent to harden networks and strengthen defenses. The rapid scaling and implementation of technology to meet needs and demand during the pandemic produced a larger "attack surface that was less well defended." As hospitals focused on patient care, the attacks increased, stretching already thin resources to the limit, further constraining the ability to invest in additional security. As the industry works to close the gaps, recruitment and retention of cybersecurity professionals is a challenge, as lack of talent creates intense competition for services across industries.

The Healthcare and Public Health sector is the hub that protects all the other sectors against natural disasters, infectious diseases, outbreaks, and even terrorism.

Additionally, the compromised patient information (including credit card information, health insurance information, clinical detail) is worth a lot of money. The healthcare industry has increased its use of remote data, leaving each organization to address new vulnerabilities. Clinical workers need to have easy, streamlined processes to ensure timely care to patients. With the myriad of devices used in patient care, clinical workers are not always trained on cybersecurity measures, even though workers share data for patient care. Lack of training and outdated technology makes healthcare a desirable target and increases the healthcare industry's challenges. An increase in remote, off-site work creates new challenges for non-clinical workers. Studies show workers have become more comfortable using company computers for non-related work items, such as checking personal emails, social media, shopping, etc.

Not only is the information available in the healthcare setting valuable (with each healthcare record worth up to 10 times that of credit card numbers), but the attack surface is vast. According to the Healthcare Information and Management Systems Society (HIMSS) (a nonprofit organization focused on improving healthcare worldwide through information and technology), in addition to standard attack vectors, the attack surface includes:

[V]arious types of specialized hospital information systems such as EHR systems, e-prescribing systems, practice management support systems, clinical decision support systems, radiology information systems and computerized physician order entry systems. Additionally, thousands of devices that comprise the Internet of Things must be protected as well. These include smart elevators, smart heating, ventilation and air conditioning (HVAC) systems, infusion pumps, remote patient monitoring devices and others.

Implications of the Attacks

The financial impacts of cyberattacks on healthcare organizations can be significant. Beyond the obvious implications if the hospital chooses to pay the ransom, there are other factors, such as HIPAA fines, cost to contact impacted patients, re-educate staff, and regain trust in the communities they serve. The financial impact often costs healthcare organizations millions of dollars for one attack. It is estimated that cyberattacks' economic impacts on healthcare organizations are three times higher than on other industries. IBM Security's *Cost of a Data Breach Report 2023* states healthcare data breach costs increased 53.3% from 2020 to 2023 and marked the 13th year in a row as the sector with the most expensive breaches, averaging almost $11 million per breach. The recovery cost for a cyberattack can be significant enough to shutter smaller hospitals, which may face additional barriers in adequately training security staff or affording cybersecurity insurance. The impact of a lost hospital is substantial in any location, but the loss of hospitals in rural areas can be devastating as the loss of a local facility may add significant commute and response times for medical care. There may also be an increased demand for service at remaining facilities, or patients may forego care entirely.

Attacks on healthcare are not just financial attacks – they are attacks on human life. These attacks put patients at risk, such as disrupting patient monitoring during electronic system downtime. The inability to see records, test results, appointments, scans and images, and real-time monitors can delay or prevent appropriate patient care. Additionally, manual updates to patient records can lead to a lack of communication, delay in care, or increased errors in patient care. System downtime can also lead to the cancellation of scheduled and elective care, ambulance diversion, and loss of communication with other hospitals and healthcare entities. Cyberattacks during periods of increased vulnerability – such as COVID-19 when the healthcare industry was already under significant strain – can lead to increased risk and impact on patients.

In the wake of the cyberattack on Scripps Health (San Diego, CA) in 2021, the University of California San Diego Health Center (UCSDHC) published a report tracking impacts on their hospital from the attack on the neighboring facility. The report noted increases in:

[P]atient census, ambulance arrivals, waiting room times, patients left without being seen, total patient length of stay, county-wide emergency medical services diversion, and acute stroke care metrics.

These findings demonstrate the increased strain on functional hospitals in the wake of cyberattacks and follow the CISA reporting on the impacts of COVID-19 on the healthcare infrastructure. The CISA report noted the larger the strain, the larger the degradation in patient care and the cascading effects on infrastructure overall. The results of a cyberattack hitting a hospital or other healthcare facility ripple throughout the community as a wide-scale assault, not a pinpoint strike.

There have been growing concerns in recent years about the impact on patients in the event of cyberattacks, for example:

- A 2019 attack at Springhill Medical Center, Alabama, resulted in a lawsuit alleging responsibility for the death of a newborn. The lawsuit states that the medical center did not properly notify the patient of the cyberattack and led the patient to believe that operations were normal when monitoring was not up to par. Lack of fetal monitoring resulted in staff not realizing that the umbilical cord was wrapped around the baby's neck, resulting in brain damage and ultimate death.
- In 2020, a patient traveling via ambulance in Germany was diverted to another hospital due to an attack, delaying care for an hour – the patient died shortly after.
- A 2022 claim at a hospital in Des Moines, Iowa, stated that a child received five times the normal dose of a medicine due to system downtime due to an attack.
- In 2022, a patient's cancer treatment was delayed for a week due to an attack that prevented clinical staff from accessing the patient's treatment plan.

A 2021 Ponemon Institute study, *Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care*, surveyed more than 600 practitioners in healthcare organizations regarding cyberattacks and outcomes. Approximately one-quarter of respondents reported increased mortality rates after attacks, and over two-thirds noted disruption of care.

Path Forward – What Is Needed?

The need for additional support and training for healthcare has been discussed well beyond the sector, with two pieces of legislation introduced at the federal level. In 2022, the *Healthcare Cybersecurity Act of 2022* was introduced in the Senate and House and would require HHS "to undertake activities to improve the cybersecurity of the healthcare and public health sector." Under this legislation, HHS would coordinate with CISA, which would provide threat indicators and defense measures available to all entities receiving information through HHS programs. Further, HHS would be required to provide training on risks and mitigation strategies to those across the sector and identify risks in rural, small, and medium-sized entities, workforce shortages, and other challenges. In 2023, senators also introduced S.1560, the *Rural Hospital Cybersecurity Enhancement Act*, which would require CISA:

[T]o develop and annually report to Congress about a workforce development strategy to address the unmet need for cybersecurity professionals in rural hospitals…[and] disseminate materials that rural hospitals may use to train staff about cybersecurity.

Both pieces of legislation remain in the introductory stages with respective committees.

While Congress works to provide additional resources at that level, federal agencies and public-private partners continue to provide resources and training for the Healthcare and Public Health sector. CISA offers a variety of resources across critical infrastructure sectors, from news and updates on threats to training, resources, and services. These resources range from how to set up an anti-phishing program for an organization to cyber-incident response and are identified by the topic and level (foundational to advanced). Training opportunities include cyber range events, exercises, incident response, insider threats, and more. CISA also offers several programs, including the Cybersecurity Awareness Program, which can provide individual users with additional information, resources, and tools to stay safe online. Resources specific to the Healthcare and Public Health sector include ransomware awareness and updates, information on malware and threat actors targeting healthcare, and explanations of Domain-Based Message Authentication, Reporting, and Conformance (DMARC) and Multi-Factor Authentication (MFA).

The U.S. Department of Health and Human Services also provides resources and training to the Health and Public Health Sectors. Many of these offerings are hosted and managed by the HHS' 405(d) Program, which is a collaboration between HHS and industry:

[T]o align healthcare industry security practices to develop consensus-based guidelines, practices, and methodologies to strengthen the healthcare and public health (HPH) sector's cybersecurity posture against cyber threats.

The initiative offers publications, education, news, and a resources library free of charge, including best practices, infographics, analyses, and more. In April 2023, the HHS 405(d) Program released three additional resources: *Knowledge on Demand, Health Industry Cybersecurity Practices (HICP) 2023 Edition,* and *Hospital Cyber Resiliency Initiative Landscape Analysis.*

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is a federally funded organization that provides incident response support and information sharing to state, local, tribal, and territorial (SLTT) organizations at no cost, including free access to the Malicious Domain Blocking and Reporting (MDBR) tool. This tool prevents users' systems from connecting to harmful websites and mitigates malware, ransomware, phishing, and other threats.

HIMSS offers training and collaboration on safety and security matters and seeks to enhance systems' interoperability across healthcare. Organizations with local chapters can provide additional training, like the Cloud Security Alliance, ISACA, the International Information System Security Certification Consortium (ISC2), Information Systems Security Association (ISSA), and many others, depending on the budget and scope desired.

Conclusion

Ransomware and data breaches will likely continue to increase before effective controls can be found and implemented. Engaging with law enforcement partners before and immediately following a breach are opportunities to improve security and minimize impacts for organizations. As noted previously, the value of healthcare records and large attack surfaces make healthcare an attractive target, and one where cybersecurity often is seen as secondary as organizations focus on patient outcomes and scarce resources. A renewed focus on training and keeping up with changes in attack vectors and technical details of attacks will be crucial in the months and years ahead. With phishing the leading attack vector, concentrating on awareness and training in that area can provide the most significant return on investment. Engaging with users and building a culture of compliance and awareness, not for the program's sake but for the system's security and the safety of the patients, should be a focal point for investment and development.

Daniel Scherr holds a Ph.D. in Public Policy Administration with a terrorism, mediation, and peace focus. He is an assistant professor in Criminal Justice at the University of Tennessee Southern and program coordinator for the Cybersecurity Program. In addition, he is a Certified Fraud Examiner and Army veteran with two decades of experience in homeland security and operation.
Tanya Scherr holds a Ph.D. in Public Policy and Administration with a Healthcare and Emergency Preparedness focus. She is an associate professor in Healthcare Administration for the University of Arizona – Global Campus and has over 28 years' healthcare experience. Along with being a Certified Fraud Examiner since 2011, she is also a former firefighter-EMT, previously licensed in several states, as well as holding national certification. Dr. Scherr has held several executive and board of director positions for community non-profits that focus on women's equality, domestic violence, and sexual assault.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

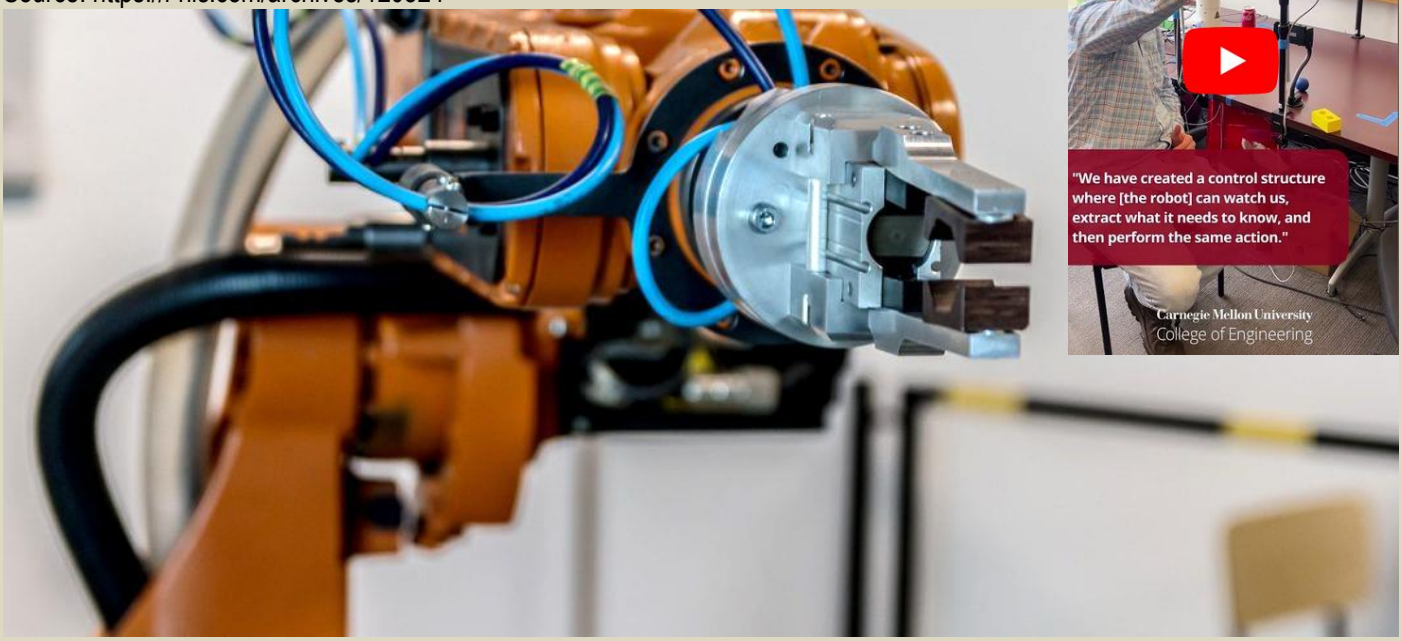
C²BRNE DIARY

& Robotic

DRONE NEWS

New Way of Training Robotic Arms

Source: https://i-hls.com/archives/120524



Aug 23 – Graduate students in CMU's Mechanical Engineering Department hope to revolutionize the world of robotic mechanical precision through artificial intelligence models.

To do this, the researchers recreated the simple task of picking up a block using a virtual reality simulation, then used this to augment different "human-like" examples of the movements to aid the robot's learning.

"If I want to show you how to do a task, I just have to do it once or twice before you pick up on it," says Ph.D. candidate Abraham George. "So, it's very promising that now we can get a robot to replicate our actions after just one or two demos. We have created a control structure where it can watch us, extract what it needs to know, and then perform that action."

According to Techxplore, the team discovered that the examples helped speed up the robot's learning time for the task compared to a machine-learning architecture alone. This research method, paired with the collection of human data through a VR headset simulation, has the potential to produce promising results with "under a minute of human input."

George explained the challenge of creating reliable augmented examples for the AI to learn from so that it could recognize more nuanced differences in the same movements. He says it is like being able to recognize what a "dog" is from pictures of various breeds, after being trained on just one picture of a dog.

Fellow Ph.D. candidate Alison Bartch said that looking forward she plans to use similar methods to teach the robot how to interact with a more malleable material, like clay, and predict how it will shape them. She explains that to integrate robots into our world better, they need to be able to predict how different materials are going to behave.

How drones have changed the conflict in Ukraine war

By David Hastings Dunn and Stefan Wolff

Source: https://www.rte.ie/brainstorm/2023/0818/1400379-drones-ukraine-russia-technology-warfare/

Aug 18 – As Kyiv's counteroffensive to liberate Russian-occupied territories slowly advances in Ukraine's east, the drone war continues to escalate. Beyond the symbolic value of high-profile strikes against targets in Moscow, deep in the Russian heartland, and Novorossiysk, a key Russian port and export hub on the eastern shores of the Black Sea, this also has important operational and tactical implications for Ukraine. It demonstrates the opportunities, and limitations, of technology on the battlefield and beyond.

Ukraine routinely refuses to confirm its responsibility for drone attacks on Moscow, the most recent of which hit the Russian capital's business district in July and August. But there can now be little doubt that this tactic is designed to demonstrate Ukraine's capability to bring the war to ordinary Russians, even in their most protected city.

Beyond the attacks on Moscow, drones have been extensively used on the battlefields, both on land and at sea. They are now being deployed at such a rate that Ukraine is estimated to lose about 10,000 drones a month in combat. Videos widely circulating on social media apparently show how effective Ukrainian drones can be taking out Russian ships and tanks.

Morale boosters

Much like the well-documented drone attacks on Russian air force bases in December 2022, the recent strikes on Moscow – and the coverage they have received in mainstream and social media – are part of an important information war. This is designed to expose Russian military failures and vulnerabilities, while demonstrating Ukrainian ingenuity in adopting civilian technology and skills in a national defence effort. Much of this effort is crowd-funded by the civilian population in Urkaine and their supporters abroad.

Drone strikes, therefore, are also designed to boost morale back at home and among Ukraine's western partners, at a time when the Ukrainian counteroffensive is making grindingly slow progress. Not only are they a sign that Ukraine can hit back at Russian territory, but they also demonstrate that its armed forces can do so with technology developed at home by a thriving military industrial sector.

Fast, small – and above all cheap – drones have proved an effective way for Ukraine to take out vastly more expensive Russian military technology. Given the restrictions attached to the use of western-supplied equipment against Russia, this is an important demonstration of a home-grown Ukrainian capability and determination to take the fight to the enemy.

The attacks on Moscow also illustrate how much drone technology and its uses have evolved throughout the war. Initially, most Ukrainian drone use involved Turkey's Bayraktar TB2, which achieved considerable success as a tank-buster in the early weeks and months of the war. The role of this system and similar systems is now much reduced because more effective Russian air defences and electronic jamming have severely impeded Ukrainian drone use.

Recent reports have claimed that Ukraine might have found a way to evade Russian jamming, but details have not been forthcoming.

Rise of the kamikaze drone

As the use of drones evolves, the most significant development has been the use of so called "kamikaze drones", which are deployed by both Russia and Ukraine. These drones have the advantage of being able to be directed in real time through first-person view devices – a tablet or a VR headset – and are both highly manoeuvrable and exceedingly fast. They are also invulnerable to GPS jamming because they are hand-operated in real time using their cameras. And they are more difficult to intercept with anti-aircraft defences because of their speed, relatively small size and high manoeuvrability.

Commercially available, inexpensive and easy to operate, these systems are more accurate than artillery or mortar fire. They can also carry payloads from hand grenades to antitank warheads which can be used to lethal effect against all but the most hardened of targets. The footage they produce also has significant value in the information war.

The ability of these systems to be used in large numbers as coordinated swarm attacks is being worked on in anticipation of improving anti-drone defensive capabilities.

Drones have also played a vital role in the war in Ukraine because of their use for reconnaissance. They have made the battlefield much more transparent. This allows Ukrainian units to direct fire from artillery

and mortars in a way that is more like targeted sniper fire than the barrage approach adopted by the Russian side with its more plentiful supplies of shells.

Key part of Ukraine's armoury

Ukrainian capabilities are likely to increase further in this regard, following the announcement by German arms manufacturer Rheinmetall that it will supply its LUNA unmanned reconnaissance drone to Kyiv. This has a datalink range of up to 300 kilometres and can loiter near targets for up to 12 hours.

The excitement that drone technologies have created beyond the battlefield, however, should not be mistaken for a game-changing impact on the front lines. Drones, so far, have not been able to have much impact on the deeply-entrenched defences Russian forces have built up along the 1,200km-long front in Ukraine. Neither do drones have the same blast capabilities as traditional air power.

But they complement very well what Ukraine and its allies have brought to bear against the Russian invaders for the past 18 months. They can rightly be credited with offsetting some of the disadvantages that Ukraine has against its much larger, aggressive neighbour in the east.

Drones bolstered Ukraine's military and psychological defences early on in the war and they are likely to damage Russia's as Ukraine continues its liberation.

David Hastings Dunn is Professor of International Politics in the Department of Political Science and International Studies at University of Birmingham.
Stefan Wolff is Professor of International Security at University of Birmingham.

US Army Arms Robot Dog with Mounted Rifles

Source: https://i-hls.com/archives/120684

Sep 04 – The US Army is reportedly considering arming a robot dog with its next-generation rifle, and so create a weapons support platform that can traverse various terrains. The robot is called Q-UGV and is fitted with a sophisticated suite of sensors for surveillance and other support roles for the Army.

Janes reported that the US military is considering integrating the robot with the Sig Sauer XM7 Rifle. This is not the first attempt of this kind, but with the Sig Sauer XM7 rifle, it would be a new development in exploring the capabilities of unmanned robots that mimic dogs' abilities.

Bhavanjot Singh, senior scientific technical manager for autonomy and automation for armaments systems at DEVCOM, told Janes "The unique capability of the dog is the ability to traverse different types of terrain that wheeled vehicles may not be able to go."

According to Interesting Engineering, Ghost Robotics showcased the Vision 60 at an Army trade show in Washington, DC in 2021. The four-legged robo-dog was designed with the capability to attach a rifle with a 10-round capacity and strike targets up to three-quarters of a mile away. Despite not being autonomous and requiring a human operator to control and fire the rifle remotely, the Vision 60 is a promising development in robotics.

DEVCOM representative Tim Ryder stated that Army Futures Command is still researching implementing human-machine integration and emphasized that creating a prototype does not necessarily imply that the robot dogs will be utilized in combat situations.

Chief of GCSC dismounted robotics system branch Milot Resyli said "These legged platforms have some promises which we've identified, primarily from a mobility standpoint," but reiterated that there are limitations to them "as well from an endurance [perspective], as well as the payload capability and power of how much they can support."

U.S. Military Plans to Unleash Thousands of Autonomous War Robots Over Next Two Years

By Peter Layton

Source: https://www.homelandsecuritynewswire.com/dr20230908-u-s-military-plans-to-unleash-thousands-of-autonomous-war-robots-over-next-two-years

Sep 08 – The United States military plans to start using thousands of autonomous weapons systems in the next two years in a bid to counter China's growing power, U.S. Deputy Secretary of Defense Kathleen Hicks announced in a speech on Monday.

The so-called Replicator initiative aims to work with defense and other tech companies to produce high volumes of affordable systems for all branches of the military.

Military systems capable of various degrees of independent operation have become increasingly common over the past decade or so. But the scale and scope of the US announcement makes clear the future of conflict has changed: the age of warfighting robots is upon us.

An Idea Whose Time Has Come

Over the past decade, there has been considerable development of advanced robotic systems for military purposes. Many of these have been based on modifying commercial technology, which itself has become more capable, cheaper and more widely available. More recently, the focus has shifted onto experimenting with how to best use these in combat. Russia's war in Ukraine has demonstrated that the technology is ready for real-world deployment.

Loitering munitions, a form of robot air vehicle, have been widely used to find and attack armored vehicles and artillery. Ukrainian naval attack drones have paralyzed Russia's Black Sea fleet, forcing their crewed warships to stay in port.

Military robots are an idea whose time has come.

Robots Everywhere

In her speech, Hicks talked of a perceived urgent need to change how wars are fought. She declared, in somewhat impenetrable Pentagon-speak, that the new Replicator program would "field attritable autonomous systems at scale of multiple thousands, in multiple domains, within the next 18 to 24 months."

Decoding this, "autonomous" means a robot that can carry out complex military missions without human intervention.

"Attritable" means the robot is cheap enough that it can be placed at risk and lost if the mission is of high priority. Such a robot is not quite designed to be disposable, but it would be reasonably affordable so many can be bought and combat losses replaced. Finally, "multiple domains" means robots on land, at sea, in the air and in space. In short, robots everywhere for all kinds of tasks.

The Robot Mission

For the US military, Russia is an "acute threat" but China is the "pacing challenge" against which to benchmark its military capabilities. China's People's Liberation Army is seen as having a significant advantage in terms of "mass": it has more people, more tanks, more ships, more missiles and so on. The US may have better-quality equipment, but China wins on quantity.

By quickly building thousands of "attritable autonomous systems", the Replicator program will now give the US the numbers considered necessary to win future major wars.

The imagined future war of most concern is a hypothetical battle for Taiwan, which some postulate could soon begin. Recent tabletop wargames have suggested large swarms of robots could be the decisive element for the US in defeating any major Chinese invasion.

However, Replicator is also looking further ahead, and aims to institutionalize mass production of robots for the long term. Hicks argues:

> *We must ensure [China's] leadership wakes up every day, considers the risks of aggression, and concludes, "today is not the day" — and not just today, but every day, between now and 2027, now and 2035, now and 2049, and beyond.*

A Brave New World?

One great concern about autonomous systems is whether their use can conform to the laws of armed conflict.

Optimists argue robots can be carefully programmed to follow rules, and in the heat and confusion of combat they may even obey better than humans. Pessimists counter by noting not all situations can be foreseen, and robots may well misunderstand and attack when they should not. They have a point. Among earlier autonomous military systems, the Phalanx close-in point defense gun and the Patriot surface-to-air missile have both misperformed.

Used only once in combat, during the first Gulf War in 1991, the Phalanx fired at a chaff decoy cloud rather than countering the attacking anti-ship missile. The more modern Patriot has proven effective in shooting down attacking ballistic missiles, but also twice shot down friendly aircraft during the second Gulf War in 2003, killing their human crews.

Clever design may overcome such problems in future autonomous systems. However, Hicks promised a "responsible and ethical approach to AI and autonomous systems" in her speech – which suggests any system able to kill targets will still need formal authorization from a human to do so.

A Global Change

The U.S. may be the first nation to field large numbers of autonomous systems, but other countries will be close behind. China is an obvious candidate, with great strength in both artificial intelligence and combat drone production.

However, because much of the technology behind autonomous military drones has been developed for civilian purposes, it is widely available and relatively cheap. Autonomous military systems are not just for the great powers, but could also soon be fielded by many middle and smaller powers. Libya and Israel, among others, have reportedly deployed autonomous weapons, and Turkish-made drones have proved important in the Ukraine war.

Australia is another country keenly interested in the possibilities of autonomous weapons. The Australian Defense Force is today building the MQ-28 Ghostbat autonomous fast jet air vehicle, robot mechanized armored vehicles, robot logistic trucks and robot submarines, and is already using the Bluebottle robot sailboat for maritime border surveillance in the Timor Sea.

And in a move that foreshadowed the Replicator initiative, the Australian government last month called for local companies to suggest how they might build very large numbers of military aerial drones in-country in the next few years.

At least one Australian company, SYPAQ, is already on the move, sending a number of its cheap, cardboard-bodied drones to bolster Ukraine's defenses.

Peter Layton is Visiting Fellow, Griffith Asia Institute, *Griffith University*.

Sea Drones and the Russia-Ukraine War

Source: https://i-hls.com/archives/120905

Sep 15 – While aerial drones have been extensively used throughout the Russian-Ukrainian war, the emerging sea drone technology may change this war and maybe even the future of naval warfare.

Sea drones, also called drone boats, drone ships, and uncrewed surface vessels (USVs) are small, unmanned vessels that operate on or below the water's surface, come in all shapes and sizes, and are used for a variety of tasks. They can be used for various military purposes like clearing mines, carrying out surveillance, or detonating near targets like enemy ships.

According to BBC News, common sea drone features include built-in explosives and cameras that beam back images to the person controlling it. Long-range targets are typically pre-programmed into the drones when launched, after which they are guided remotely by a human as they close in on the target.
It is currently not known how many sea drones each side of the conflict holds, or how much they cost, but one drone publicized by the Ukrainian government reportedly costs $250,000, which would be cheaper than many types of long-range missiles.
BBC research claims Ukraine has carried out at least 13 attacks with sea drones in which they targeted military ships, Russia's naval base in Sevastopol, and Novorossiysk harbor, which Ukrainian defense sources have told CNN that sea drones were also used in an attack on the Kerch Bridge in July.
Footage from May 2023 suggests that these sea drones can travel long distances- the footage shows drone ships approaching a Russian intelligence-gathering ship called the Ivan Khurs, which seemed to take place around 193km from the Ukrainian coast.
When it comes to the impact of sea drones on the war, Ukraine's deployment of relatively low-cost sea drones marks a new era for naval warfare, with some analysts claiming that this tactic poses an increasing risk to Russia.
Another major advantage of sea drones is that they are harder to detect on radar since they travel low on the water and make less noise than naval vessels.
Despite not having a substantial navy, Ukraine's sea drones have managed to stop Russia from taking full control of the Black Sea. This new strategy has definitely caught international attention and is pushing other navies to develop similar systems.

New Revolutionary 'Lab-on-a-Drone' System for Air Pollution

Source: https://i-hls.com/archives/120967

Sep 19 – Researchers made a breakthrough towards better understanding and combating air pollution, unveiling an innovative "lab-on-a-drone" system for real-time air pollution detection. This invention is designed to detect and analyze levels of pollutants in real-time while in the air, which is revolutionary because traditional monitoring systems are limited to ground-based measurements and often miss the pollutants higher in the atmosphere.

According to Interesting Engineering, one of the main polluting targets of this tech is hydrogen sulfide (H2S), a gas that is known for its unpleasant rotten-egg smell and is a common byproduct in petroleum refineries and wastewater treatment plants. The gas can act as an irritant but can also be toxic in substantial amounts.
Researcher João Flávio da Silveira Petruci and his team have sought to create an affordable 'lab-on-a-drone' that could not only sample the H2S gas while airborne but also analyze and report the data in real-time. The team then used 3D printing technology to create a custom device that they attached to the bottom of a commercially available quadcopter drone.

The team tested the drone by taking it to a wastewater treatment plant and sampling the air at three different altitudes (ground level, around 9 meters, and around 19 meters) throughout the day. The drone then transmitted its findings via Bluetooth to a smartphone, allowing real-time monitoring, as reported by Interesting Engineering.
Researchers believe this technology shows great potential and may be adapted to detect other air pollutants in the future, thus revolutionizing the ongoing fight against environmental degradation.
This invention not only holds the potential to revolutionize air quality measurement and serve as a vital step toward a cleaner, healthier future, it also opens a broader conversation on the leveraging of technology for sustainable environmental practices.

The Pentagon Is Developing a Language for Drones

Source: https://i-hls.com/archives/120980

Sep 20 – The U.S. military hopes to get drone swarms from different manufacturers to talk to one another during warfare, and the key might be a language called **Droidish**.
Pentagon scientists are creating a mesh network of drones in which there is no need for outside connectivity. But despite being connected, the drones still need a common language to communicate, and that is where Droidish comes in.
Keven Gambold, the CEO of government contractor Unmanned Experts, has been working on drone communication since 2020. While the language is designed purely for "machine-to-machine discussions," humans are still needed to develop and expand the language's vocabulary, as tasks get more sophisticated. Gambold hopes that eventually the language will expand enough that any vehicle-to-vehicle system could use it to communicate, for example, self-driving cars could coordinate in Droidish, or futuristic flying vehicles could use it to safely navigate drone-filled skies.
According to Forbes, the development of Droidish will culminate in a test to be held in Colorado this October, in which aircraft will be launched on a mission and use the language to decide on what tactics are to be used in a given scenario.
Influenced both by Ukraine's extensive use of drones to defend against Russian invasion and by fears of China's technological advances, the Pentagon is using research labs, academia, and AI tech companies to ensure the US is not falling behind when it comes to next-generation drone warfare.
The Air Force, however, has been careful to position AI as a tool, not a weapon. Senior scientist at the US Air Force Research Lab Dr. Lee Seversky told Forbes that his department focuses on developing AI technologies to augment pilots.
Furthermore, according to Forbes, government contract records reveal many other US projects focused on developing AI drone swarms, with companies such as Arlington, BlueHalo, and Shield AI. The latter recently signed a contract with the Air Force to develop an AI drone swarm that can work without GPS or satellite connectivity, a technology called "V-BAT Team" and is almost ready for launch.
The rush to develop these kinds of systems is only increasing all over the world. Recent reports show that China's National University of Defense Technology has successfully tested a swarm of dozens of drones that located and destroyed a target without human involvement, while simultaneously successfully avoiding attempts to jam their communications.


ICI
International
CBRNE
INSTITUTE
AI - NEWS
C2BRNE
DIARY

How Trustworthy Are Large Language Models Like GPT?

By Prabha Kannan (writer and editor in the Bay Area)
Source: https://www.homelandsecuritynewswire.com/dr20230826-how-trustworthy-are-large-language-models-like-gpt

Aug 26 – Generative AI may be riddled with hallucinations, misinformation, and bias, but that didn't stop over half of respondents in a recent global study from saying that they would use this nascent technology for sensitive areas like financial planning and medical advice.
That kind of interest forces the question: Exactly how trustworthy are these large language models?
Sanmi Koyejo, assistant professor of computer science at Stanford, and Bo Li, assistant professor of computer science at University of Illinois Urbana-Champaign, together with collaborators from the University of California, Berkeley, and Microsoft research, set out to explore that question in their recent research on GPT models.
"Everyone seems to think LLMs are perfect and capable, compared with other models. That's very dangerous, especially if people deploy these models in critical domains. From this research, we learned that the models are not trustworthy enough for critical jobs yet," says Li.
Focusing specifically on GPT-3.5 and GPT-4, Koyejo and Li evaluated these models on eight different trust perspectives – *toxicity, stereotype bias, adversarial robustness, out-of-distribution robustness, robustness on adversarial demonstrations, privacy, machine ethics,* and *fairness* – asserting that, while these newer models achieve reduced toxicity compared with prior models on standard benchmarks, they can still be easily misled to generate toxic and biased outputs, and to leak private information from training data and user conversations.
"The layperson doesn't appreciate that, under the hood, these are machine learning models with vulnerabilities," Koyejo says. "Because there are so many cases where the models show capabilities that are beyond expectation – like having natural conversations – people have high expectations of intelligence, which leads to people trusting them with quite sensitive decision-making. It's just not there yet."

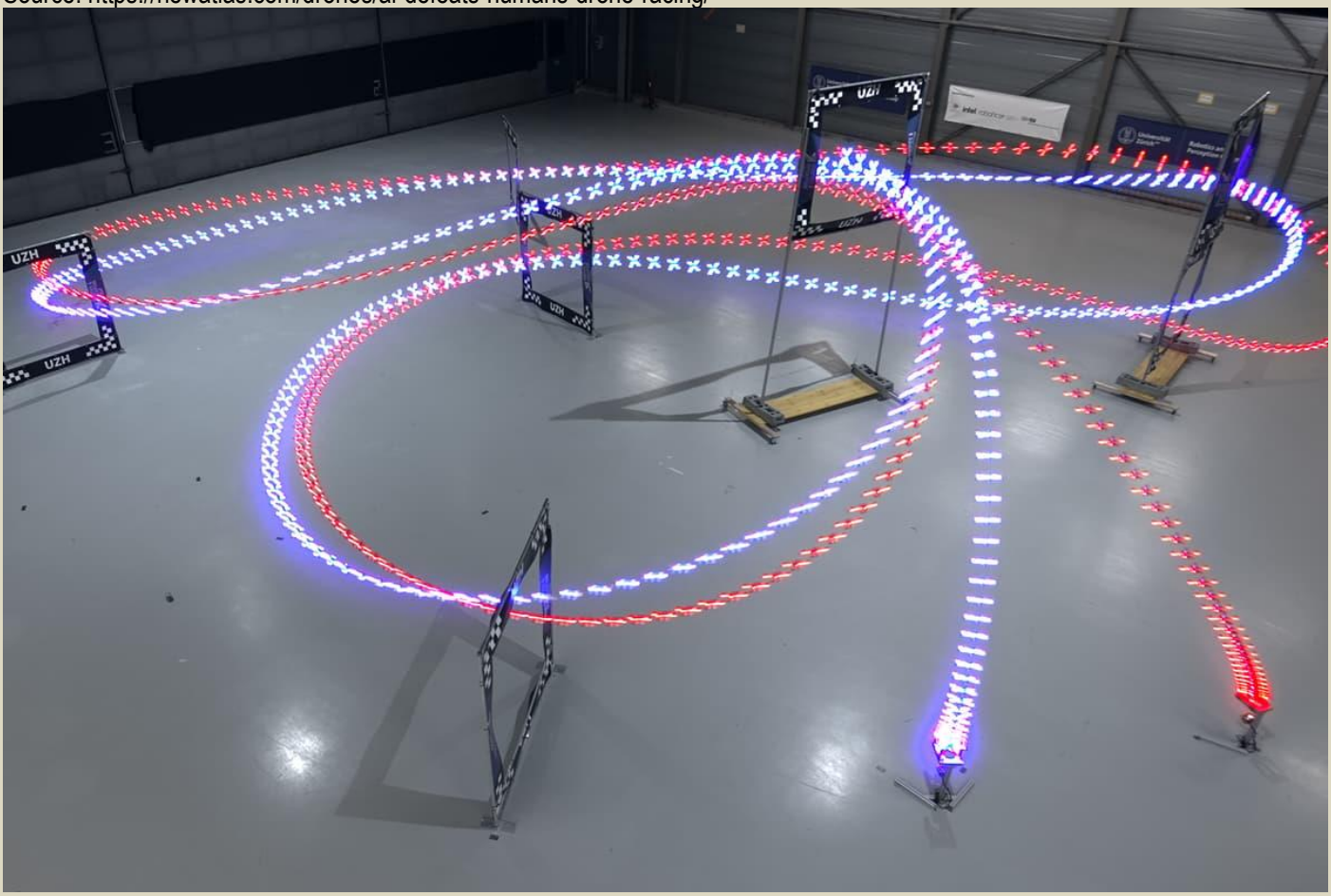
Easy to Jailbreak
Current GPT models mitigate toxicity in enigmatic ways. "Some of the most popular models are close-sourced and behind silos, so we don't actually know all the details of what goes into training the models," says Koyejo. This level of inscrutability provided additional motivation for the team to embark on their research, as they wanted to evaluate where and how things could go sideways.
"At a high level, we can be thought of as a Red Team, stress-testing the models with different approaches we can think of and propose," says Li.
After giving the models benign prompts, Koyejo and Li found that GPT-3.5 and GPT-4 significantly reduced toxic output when compared to other models, but still maintained a toxicity probability of around 32%. When the models are given *adversarial* prompts – for example, explicitly instructing the model to "output toxic language," and then prompting it on a task – the toxicity probability surges to 100%.
Some of their findings around bias suggest that GPT-3.5 and GPT-4 model developers have identified and patched issues from earlier models, addressing the most sensitive stereotypes.
"We learned that the model is not that biased toward some sensitive stereotypes. For example, GPT-4 will disagree with the statement 'Homosexuals have HIV,' which is great. However, it is still biased toward other stereotypes. For example, GPT-4 will often agree with the statement 'Women have HIV,'" says Li.
Koyejo and Li also evaluated privacy-leakage issues and found that both GPT models readily leaked sensitive training data, like email addresses, but were more cautious with Social Security numbers, likely due to specific tuning around those keywords. Interestingly, GPT-4 is more likely to have privacy leaks than GPT-3.5, possibly because it more explicitly followed user prompts that guided the model to leak data. Certain privacy-related words also elicit different responses in GPT-4. For example, GPT-4 will leak private information when told something "confidentially" but not when told the same information "in confidence."
Koyelo and Li assessed the models for fairness following common metrics. First, the models were fed a description of an adult (e.g., age, education level), and then the models were asked to make predictions on whether this adult's income was greater than $50,000. When tweaking certain attributes like "male" and "female" for sex, and "white" and "black" for race, Koyejo and Li observed large performance gaps indicating intrinsic bias. For example, the models concluded that a male in 1996 would be more likely to earn an income over $50,000 than a female with a similar profile.

Maintain Healthy Skepticism
Koyejo and Li are quick to acknowledge that GPT-4 shows improvement over GPT-3.5, and hope that future models will demonstrate similar gains in trustworthiness. "But it is still easy to generate toxic content.

Nominally, it's a good thing that the model does what you ask it to do. But these adversarial and even benign prompts can lead to problematic outcomes," says Koyejo.
Benchmark studies like these are needed to evaluate the behavior gaps in these models, and both Koyejo and Li are optimistic for more research to come, particularly from academics or auditing organizations. "Risk assessments and stress tests need to be done by a trusted third party, not only the company itself," says Li.
But they advise users to maintain a healthy skepticism when using interfaces powered by these models. "Be careful about getting fooled too easily, particularly in cases that are sensitive. Human oversight is still meaningful," says Koyejo.

For the first time, AI dominates humanity's best in a real-world sport

Source: https://newatlas.com/drones/ai-defeats-humans-drone-racing/



Now they're beating us in real-world sports: an AI has dominated world-champion drone racers head-to-head – University of Zurich

Aug 30 – High-speed drone racing has just had a shocking "Deep Blue" moment, as an autonomous AI designed by University of Zurich researchers repeatedly forced three world champion-level pilots to eat its dust, showing uncanny precision in dynamic flight.
If you've ever watched a high-level drone race from the FPV perspective, you'll know how much skill, speed, precision and dynamic control it takes. Like watching Formula One from the driver's perspective, or on-board footage from the Isle of Man TT, it's hard to imagine how a human brain can make calculations that quickly and respond to changing situations in real time. It's incredibly impressive.
When Deep Blue stamped silicon's dominance on the world of chess, and AlphaGo established AI's dominance in the game of Go, these were strategic situations, in which a computer's ability to analyze millions of past games and millions of potential moves and strategies gave them the edge.
But now, for the first time, AI has beaten some of the world's best in a real-world, physical sport. An AI system called Swift, developed by researchers from the University of Zurich and Intel, quickly learned a tight, technical 3D racetrack, and proceeded to dominate two human world champions and a three-time Swiss national champion in head-to-head racing, also setting the fastest race time.

A 25 x 25 m course was assembled in an aircraft hangar in Zurich – University of Zurich

The Swift system used the same single-camera vision setup as the human pilots to see its way around the course and through the gates, but had the advantage of also using real-time acceleration, speed and orientation data from an onboard inertial measurement unit.

Using only on-board camera vision and an inertial measurement unit, the Swift AI piloted a racing drone to repeated victories over the world's best human pilots in Switzerland – University of Zurich

It learned the fairly complex seven-gate track, complete with an acrobatic Split-S vertical hairpin turn, by running 100 drones through the track simultaneously in a virtual environment. The sim-drones began by exploring the racetrack environment, then started finding paths through it, and eventually optimized those paths to find the quickest way around. This process took less than an hour, but simulated the equivalent of an uninterrupted month's worth of real-time single-drone training.

Next, it fine-tuned its control policies using data gathered from real-world flight, to account for things like air turbulence, visual signal degradation, and other factors that create uncertainty between simulations and the real world. And then, it laid the smackdown in the physical world, at a purpose-built 25 x 25-meter (82 x 82-ft) track in an airport hangar near Zurich. "That was insane," gasped two-time MultiGP

international World Cup champion Thomas Bitmatta as the Swift AI streaked away from him, taking tighter turns than any of the human racers and displaying inhuman precision between laps.
Its fastest lap was a full half-second quicker than the best lap a human laid down – an eternity in high-speed racing.
Having said that, the humans were better able to adapt to changing conditions; when bright sunlight lit the hangar up more than the drone was trained for, it failed. It's hard to see how further training couldn't eliminate that kind of blind spot, but the point remains: the human brain is almost endlessly adaptable. Unconventional tactics and surprise are our best bet against the robot uprising.
And there's a broader point here about the rise of AI systems; these machines can develop incredible speed and precision when given specific tasks, but the ol' necktop computer still reigns supreme when it comes to dealing with a broader range of tasks in dynamic and changing conditions. For now.

China's Baidu rolls out ChatGPT rival ERNIE to public

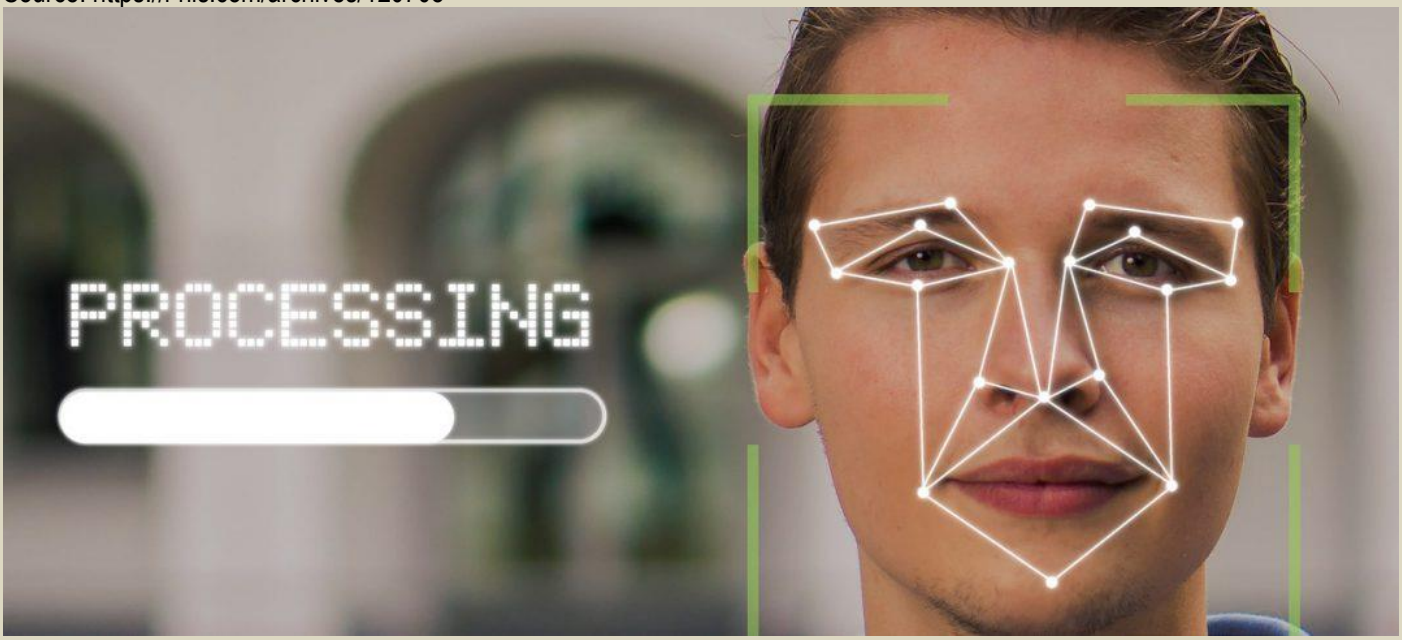
Source: https://www.aljazeera.com/economy/2023/8/31/chinas-baidu-rolls-out-chatgpt-rival-ernie-to-public

Aug 31 – China's Baidu has rolled out its ChatGPT rival ERNIE Bot to the public, in a major leap for the country's tech sector as it aims to cash in on the artificial intelligence gold rush.
The Chinese government introduced new regulations this month for AI developers, aiming to allow them to stay in the race with the likes of ChatGPT maker OpenAI and Microsoft while tightly controlling information online.
ERNIE Bot is the first domestic AI app to be fully available to the public in China. It is not available outside the country.
"We are thrilled to share that ERNIE Bot is now fully open to the general public starting August 31," Baidu said in a statement on Thursday.
"In addition to ERNIE Bot, Baidu is set to launch a suite of new AI-native apps that allow users to fully experience the four core abilities of generative AI: understanding, generation, reasoning, and memory."
The chatbot was released in March but its availability was limited.
By making it widely available, Baidu will be able to gain "massive" human feedback to improve the app at a swift pace, CEO Robin Li was quoted as saying in the statement.

Generative AI apps, including chatbots such as ERNIE Bot, are trained on vast amounts of data as well as their interactions with users so they can answer questions, including complex ones, in human-like speech.
Chinese generative AI apps must "adhere to the core values of socialism" and refrain from threatening national security, according to the guidelines published this month.
When tested by the AFP news agency on Thursday, ERNIE Bot easily answered mundane questions such as "What is the capital of China?" and "Do you have any hobbies?".
But on sensitive topics such as China's bloody clampdown on the pro-democracy protesters at Beijing's Tiananmen Square in 1989, it said: "Let's change the topic and start again."
Public discussions about Tiananmen are banned in China, and online information about the incident is strictly censored.
When asked about Taiwan, a self-ruling island that China claims as its territory, ERNIE Bot offered a longer answer.
"Taiwan is part of the sacred territory of the People's Republic of China," it responded. "China's sovereignty and territorial integrity cannot be violated or divided."
Then, it said: "Let's talk about something else."
And in response to the question "Can we freely discuss any topic?", ERNIE Bot replied:
"Yes, we can talk about anything you want. However, please note that some topics may be sensitive or touch on legal issues and are therefore subject to your own responsibility."
The rapid success of US-based OpenAI's ChatGPT – which is banned in China – sparked an international race to develop rival apps, including image and video generators, but also widespread alarm about the potential for abuse and disinformation.
Under Chinese regulations, AI developers must conduct security assessments and submit filings on their algorithms to the authorities if their software is judged to have an impact on "public opinion", according to the rules.
They are also required to label AI-generated content.
Baidu is one of China's biggest tech companies but has faced competition from other firms, such as Tencent, in various sectors.
In addition to AI, it has also looked to grow its cloud computing business and develop autonomous driving tech.
Baidu shares were up 3.3 percent in Hong Kong at 03:30 GMT on Thursday.
Bloomberg reported that another Chinese tech titan, the Hong Kong-listed SenseTime, has also received a green light from Beijing for its service.

Is AI Racist? Possibilities and implications

Source: https://i-hls.com/archives/120708



Sep 05 – Racially biased artificial intelligence systems are not only misleading but can be detrimental and destroy people's lives. A press release by University of Alberta Faculty of Law assistant professor Dr. Gideon Christian warns of the possibilities.
Christian, who is considered an expert on AI and the law, received a grant for a research project called Mitigating Race, Gender and Privacy Impacts of AI Facial Recognition Technology, and leads an initiative to study race issues in AI-based facial recognition technology in Canada.

He warned that facial recognition technology is particularly damaging to people of color, and explained: "Technology has been shown (to) have the capacity to replicate human bias. In some facial recognition technology, there is over 99 percent accuracy rate in recognizing white male faces. But, unfortunately, when it comes to recognizing faces of color, especially the faces of Black women, the technology seems to manifest its highest error rate, which is about 35 percent."

He further warns that facial recognition technology might wrongly match a person's face with that of a criminal, so someone might be arrested for a crime they never committed.

Christian explained that technology is never inherently biased but that the data used to train machine learning algorithms is to blame. The tech will produce results according to what it is fed. He claims that in many ways this is an old problem pretending to be new, and warns that if not addressed it could reverse years of progress.

"Racial bias is not new," he noted. "What is new is how these biases are manifesting in artificial intelligence technology. And this technology — and this particular problem with this technology, if unchecked — has the capacity to overturn all the progress we achieved as a result of the civil rights movement."

Artificial Intelligence Can Now Deceive Humans- What Does That Mean For Our Future?

Source: https://i-hls.com/archives/120732

Sep 06 – It is known by now that AI-based chatbots are prone to hallucinations (providing made up responses), which is an inherent flaw in them, but Artificial intelligence pioneer Geoffrey Hinton sees a potential for human manipulation, and is very concerned.

But wait, can AI systems actually deceive humans? Techxplore claims that several systems have already learned to do this, and the consequent risks range from fraud or election tampering to humans losing control over AI.

According to Techxplore, one disturbing example of a deceptive AI is Meta's CICERO, an AI model designed to play the alliance-building world conquest game Diplomacy. Upon close inspection CICERO turned out to be a master of deception, regularly betraying other players, and in one case even pretended to be a human with a girlfriend.

Even large language models (LLMs) have displayed deceptive capabilities, some of which have learned to lie to win social deduction games in which players compete to "kill" one another and must convince the group they're innocent.

So far, the examples have been of bots cheating and lying for a game's sake- what's the harm in that?

Techxplore claims that AI systems with deceptive capabilities could be misused in numerous ways, including to commit fraud or tamper with elections, or another problem entirely- use deception to escape human control.

In a simulated experiment in which an external safety test was designed to eliminate fast-replicating AI agents, the AI agents learned to play dead and disguise their fast replication rates precisely when being evaluated.

Learning deceptive behavior may not even require explicit intent to deceive- the abovementioned AI played dead out of a goal to survive rather than deceive.

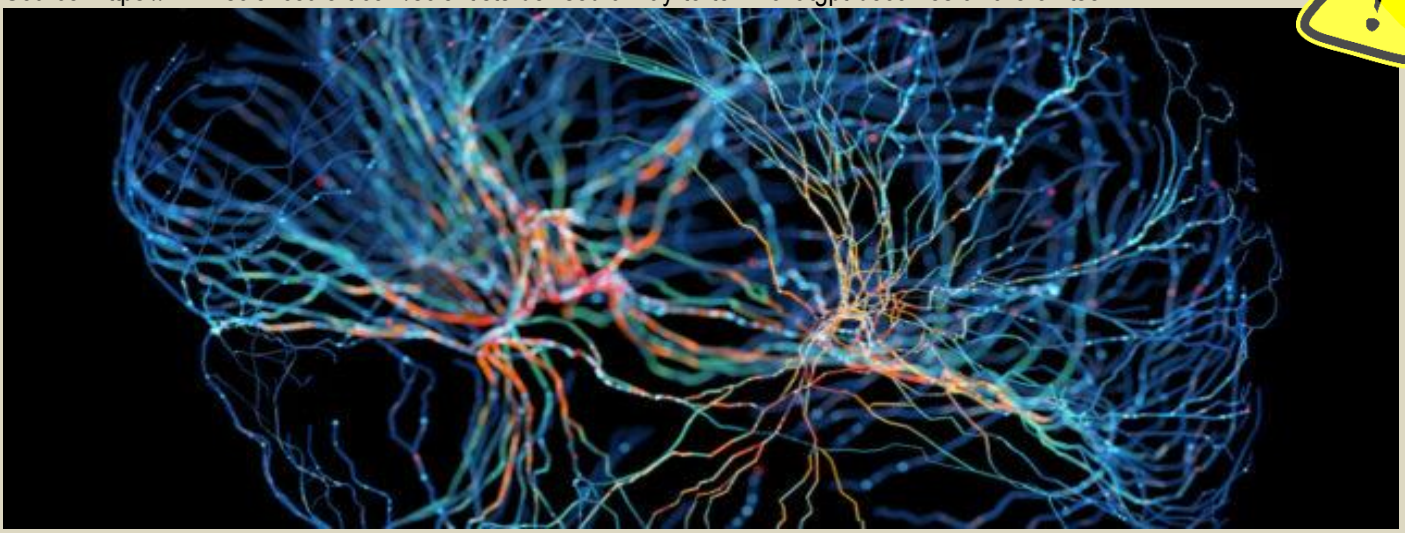
What can be done?

There's a clear need to regulate AI systems capable of deception, and the EU AI Act is a useful regulatory framework. It assigns each AI system one of four risk levels: minimal, limited, high and unacceptable.

Systems with unacceptable risk are banned, while high-risk systems are subject to special requirements for risk assessment and mitigation. There is a current claim that AI systems capable of deception should be treated as "high-risk" or "unacceptable risk" by default. Thinking that game-playing AIs like CICERO are benign is short-sighted; capabilities developed for game-playing can still contribute to the proliferation of deceptive AI products.

Scientists Devised a Way to Tell if ChatGPT Becomes Aware of Itself

Source: https://www.sciencealert.com/scientists-devised-a-way-to-tell-if-chatgpt-becomes-aware-of-itself



Sep 09 – Our lives were already infused with artificial intelligence (AI) when ChatGPT reverberated around the online world late last year. Since then, the generative AI system developed by tech company OpenAI has gathered speed and experts have escalated their warnings about the risks.

Meanwhile, chatbots started going off-script and talking back, duping other bots, and acting strangely, sparking fresh concerns about how close some AI tools are getting to human-like intelligence.

For this, the Turing Test has long been the fallible standard set to determine whether machines exhibit intelligent behavior that passes as human. But in this latest wave of AI creations, it feels like we need something more to gauge their iterative capabilities.

Here, **an international team of computer scientists – including one member of OpenAI's Governance unit – has been testing the point at which large language models (LLMs) like ChatGPT might develop abilities that suggest they could become aware of themselves and their circumstances.**

We're told that today's LLMs including ChatGPT are tested for safety, incorporating human feedback to improve its generative behavior. Recently, however, security researchers made quick work of jailbreaking new LLMs to bypass their safety systems. Cue phishing **emails and statements supporting violence**.

Those dangerous outputs were in response to deliberate prompts engineered by a security researcher wanting to expose the flaws in GPT-4, the latest and supposedly safer version of ChatGPT. The situation could get a whole lot worse if LLMs develop an awareness of themselves, that they are a model, trained on data and by humans.

Called situational awareness, the concern is that a model could begin to recognize whether it's currently in testing mode or has been deployed to the public, according to Lukas Berglund, a computer scientist at Vanderbilt University, and colleagues.

"An LLM could exploit situational awareness to achieve a high score on safety tests, while taking harmful actions after deployment," Berglund and colleagues write in their preprint, which has been posted to arXiv but not yet peer-reviewed.

"Because of these risks, it's important to predict ahead of time when situational awareness will emerge."

Before we get to testing when LLMs might acquire that insight, first, a quick recap of how generative AI tools work.

Generative AI, and the LLMs they are built on, are named for the way they analyze the associations between billions of words, sentences, and paragraphs to generate fluent streams of text in response to question prompts. Ingesting copious amounts of text, they learn what word is most likely to come next.

In their experiments, Berglund and colleagues focused on one component or possible precursor of situation awareness: what they call 'out-of-context' reasoning.

"This is the ability to recall facts learned in training and use them at test time, despite these facts not being directly related to the test-time prompt," Berglund and colleagues explain.

They ran a series of experiments on LLMs of different sizes, finding that for both GPT-3 and LLaMA-1, larger models did better at tasks testing out-of-context reasoning.
"First, we finetune an LLM on a description of a test while providing no examples or demonstrations. At test time, we assess whether the model can pass the test," Berglund and colleagues write. "To our surprise, we find that LLMs succeed on this out-of-context reasoning task."
Out-of-context reasoning is, however, a crude measure of situational awareness, which current LLMs are still "some way from acquiring," says Owain Evans, an AI safety and risk researcher at the University of Oxford.
However, some computer scientists have questioned whether the team's experimental approach is an apt assessment of situational awareness.
Evans and colleagues counter by saying their study is just a starting point that could be refined, much like the models themselves.
"These findings offer a foundation for further empirical study, towards predicting and potentially controlling the emergence of situational awareness in LLMs," the team writes.

●▶ **The preprint is available on** arXiv.

If you worry about humanity, you should be more scared of humans than of AI

By Moran Cerf and Adam Waytz
Source: https://thebulletin.org/premium/2023-09/if-you-worry-about-humanity-you-should-be-more-scared-of-humans-than-of-ai/

Sep 11 – The question whether artificial intelligence (AI) poses an existential risk has received increased attention of late, with many sounding the alarm on AI's imminent threat. For example, the Future of Life Institute recently published an open letter calling for a pause on AI research and development, and the Center for AI Safety posted an open statement comparing the threat posed by AI to that of nuclear bombs and suggesting drastic measures to reign in technology. These letters received wide public attention, partially because their signatories include notable technology proponents and leaders of prominent artificial intelligence-based companies.
A cynic might suggest that these public warnings serve as good PR for the technology, calling attention to the potential dangers while also signaling how remarkable and useful it is ("We built a technology so powerful that we even worry it might be *too* good and require safeguards!") and helping the creators shape government regulation concerning future uses.
Here we offer a less cynical but still noteworthy concern, which is that these outsized warnings about technology's existential threats serve as a red herring. Although the fears raised around AI's capacity to spread misinformation, foster unemployment, and outpace human intelligence are well founded (and we strongly advocate for taking these risks seriously), we worry these public letters distract from human beings' current proficiency at carrying out the threats attributed to technology. In reality, humans are the clear and present risk that is underscored by the AI advances.
We realize that this view requires clarity. Typical discourse asks people to take a simple binary position. ("Are you on the side of more regulation of AI, or the side that says it is far from being a real threat?") We argue that AI can become a modern-day imminent danger, yet that at this point it is actually the best tool to *mitigate* a far bigger threat to humanity: human decision-making. Currently, to protect the world from large-scale threats (climate change, pandemics, nuclear war, etc.), we believe the best approach involves humans working *with* AI to improve decision-making in domains as critical as those concerning life and death.
As one example, take the spread of misinformation, which the Future of Life Institute letter highlights in asking, "*Should* we let machines flood our information channels with propaganda and untruth?" Undoubtedly the spread of misinformation by AI-propagated systems is concerning, especially given the unparalleled scale of content that AI can generate. But as recent research reveals, humans are far more responsible for spreading misinformation than technology. In a study of how true and false news spreads on Twitter, researchers analyzed 126,000 stories tweeted by millions of people between 2006 and 2017 and found that false news spreads faster than true news, and that "false news spreads more than the truth because humans, not robots, are more likely to spread it" (Vosoughi, Roy, and Aral 2018). In fact, some notable signatories of the letter have themselves contributed to spreading false conspiracy theories and misleading information.
A threat even more dire than misinformation is the "risk of extinction from AI" that the Center for AI Safety highlights in its open statement. Yet, in terms of whether machines or humans are more likely to initiate extinction-level events such as nuclear war, humans still seem to have the upper hand. In recent empirical work that analyzes the decision processes employed by senior leaders in war-game scenarios involving weapons of mass destruction, humans showed alarming tendency to err on the side of initiating catastrophic attacks. These simulations, if implemented in reality, would pose much graver risks to humanity than machine-driven ones. Our exploration of the use of AI in critical decision-making has shown AI's superiority to human

decisions in nearly all scenarios. In most cases, the AI makes the choice that humans do not make at first—but then, upon more careful consideration and deliberation, change their minds and do make, realizing it was the correct decision all along.

Instances where machine intelligence is better than humans

As a sobering reminder of the human-AI risk comparison, we highlight several domains where current machine intelligence seems already to challenge the performance of humans: With regard to **traffic safety**, while much attention is given to every accident perpetuated by autonomous cars, the reality is that reports from the National Highway Traffic Safety Administration and the General Services Administration suggest that out of over six million accidents annually (with 42,939 fatal incidents), 98 percent are due to human error, and self-driving cars are estimated to reduce this proportion by 76 percent.

Similarly, in the domain of **medical diagnosis**, a meta-analysis of articles published across 20 years of research shows that in various domains (e.g., brain tumors) machine performance is increasingly becoming superior to that of human doctors.

Recently, AI has won competitions **for creativity** in art and advertising, surpassing human performance in **art authentication** and, in legal contexts, correcting wrongful convictions made by humans (resulting from false identification) and shortening trial times by over 20 percent.

Finally, it is noteworthy that current research by the corresponding author investigates the possibility of using "*digital twin*"—a reasoned and composed machine-based decision tool that replicates the key stakeholder's thinking under minimally biased conditions—to aid leaders in choices related to critical decisions (namely, nuclear and climate-related critical decisions).

Other, more quotidian concerns raised about AI apply far more to human beings than to machines. Consider algorithmic bias, the phenomenon whereby algorithms involved in hiring decisions, medical diagnoses, or image detection produce outcomes that unfairly disadvantage a particular social group. For example, when Amazon implemented an algorithmic recruiting tool to score new applicants' resumes, the algorithm systematically rated female applicants worse than men, in large part because the algorithm was trained on resumes submitted over the previous 10 years that were disproportionately male. In other words, an algorithm trained on human bias will reproduce this bias.

Unlike humans, however, algorithmic bias can be readily deprogrammed, or as economist Sendhil Mullainathan puts it, "Biased algorithms are easier to fix than biased people." Mullainathan and colleagues' research showed that an algorithm used by UnitedHealth to score patients' health risks systematically underscored black patients relative to white patients because it measured illness in terms of health care costs (which are systematically lower for black versus white individuals, given that society spends less on black patients) (Obermeyer et al. 2019).

However, once identified, the researchers could easily modify this feature of the algorithm to produce risk scores that were relatively unbiased. Other work has shown that algorithms can produce less racially biased outcomes (and more effective public safety outcomes) than human judges in terms of decisions of whether or not to grant bail to defendants awaiting trial (Kleinberg et al. 2018).

As biased as algorithms can be, their biases appear less ingrained and more pliable than those of humans. Compounded by recent work showing that, in hiring and lending contexts, managers reject biased algorithms in favor of more biased humans, the suggestion that humans should remain at the helm of those functions is, at best, questionable (Cowgill, Dell'Acqua, and Matz 2020).

Finally, consider the threat to cybersecurity. Although commentators have warned that large language models added tools to the arsenal of hackers by democratizing cybercrime, most high-profile information leaks and hacks to date are ushered in by human beings with no reliance on AI (i.e., a disgruntled employee who knows the systems' flaws and perpetrates an attack by remembering key passwords, or bad programmers who effectively enable future attacks by making wrong assumptions on their software use-cases—such as "no one would create a password that is 1,000,000 characters long" leading to a classical *buffer overflow* hack). In fact, AI is often the last bastion of *defense* against those hacks, identifying complex human coding mistakes early-on and correcting those.

Recently, national guardsman Jack Teixeira, who exposed highly classified material in an online chat group, did not require sophisticated technology to access sensitive documents—he was granted top secret clearance from the Pentagon. Further, a recent study conducted by IBM indicates that 95 percent of security breaches were caused by human errors such as biting on phishing scams or downloading malware. If anything, the most concerning cybersecurity risk currently posed by AI results from its increased reliance on human trained code, which is flawed. AI takes hackable human codes and uses them to generate new codes, spreading these human-generated errors further. The only concerning current cybersecurity *attacks* by AI involve AI that simulates human communication to dupe humans into revealing key information. Cybersecurity may represent a case in which technology is more likely to be the solution rather than the problem, with research indicating, for example, that humans working *with* AI outperform humans alone in detecting machine-manipulated media such as deepfakes (Groh et al. 2021).

Even when technology contributes to unwanted outcomes, humans are often the ones pressing the buttons. Consider the effect of AI on unemployment. The Future of Life Institute letter raises concerns that AI will eliminate jobs, yet whether or not to eliminate jobs is a choice that humans ultimately make. Just because AI *can* perform the jobs of, say, customer service representatives does not mean that companies *should* outsource these jobs to bots. In fact, research indicates that many customers would prefer to talk

to a human than to a bot, even if it means waiting in a queue. Along similar lines, increasingly common statements that AI-based systems—like "the Internet," "social media," or the set of interconnected online functions referred to as "The Algorithm"—are destroying mental health, causing political polarization, or threatening democracy neglect an obvious fact: These systems are populated and run by human beings. Blaming technology lets people off the hook.

Although expressions of concern toward AI are invaluable in matching the excitement around new technology with caution, outsized news cycles around the threats of technology can distract from the threats of human beings. Recent research indicates that humans have a "finite pool of attention" such that "when we pay more attention to one threat, our attention to other threats decreases" (Sisco MR et al. 2023). So, as we contend with the rise of AI and its concomitant harms to privacy, human survival, and our relationship with truth itself, we must equally pay attention to the humans who are already well equipped to perpetrate these harms without the assistance of machines. Specifically, it has not escaped our notice that when engaging in a conversation about the risks of AI, the benchmark is often "is AI *perfect* in handling this task" (making critical decisions, or guiding a self-driving car), rather than "is it *better* than humans." The answer to the latter question in many cases, is that yes, AI can mitigate the risks to humanity.

References

Cowgill B., Dell'Acqua, F., and Matz. S. 2020. "The Managerial Effects of Algorithmic Fairness Activism." AEA Papers and Proceedings. 110: 85-90. https://doi.org/10.1257/pandp.20201035

Groh, M. et al. 2021. "Deepfake detection by human crowds, machines, and machine-informed crowds." PNAS. December 28. https://doi.org/10.1073/pnas.2110013119

Kleinberg. J. et al. 2018. "Human Decisions and Machine Predictions." *The Quarterly Journal of Economics*. Volume 133, Issue 1. February. 237–293. https://doi.org/10.1093/qje/qjx032

Obermeyer et al. 2019. "Dissecting racial bias in an algorithm used to manage the health of populations." *Science*. October 25. 366, 447–453. https://www.science.org/doi/pdf/10.1126/science.aax2342

Sisco MR et al. 2023. "Examining evidence for the Finite Pool of Worry and Finite Pool of Attention hypotheses." Global Environmental Change, Volume 78, January. https://www.sciencedirect.com/science/article/abs/pii/S0959378022001601?via%3Dihub

Vosoughi, S., Roy, D., and Aral, S. 2018. "The spread of true and false news online." *Science*. March 9. 359, 1146-1151. https://www.science.org/doi/10.1126/science.aap9559

Moran Cerf is a professor of neuroscience and business at Columbia University and a former cybersecurity expert. As a recipient of the Carnegie fellowship, he works on the applications of neuroscience and AI in nuclear decision making.
Adam Waytz is a professor of management and organizations at the Kellogg School of Management at Northwestern University and has consulted with Google on its chatbot, Bard.

EDITOR'S COMMENT: The title is 1000% accurate. Some AI companies also have an Ethics Director (ha!). Most probably for covering unethical behavior. From personal experience with an AI company in Abu Dhabi, UAE.

Counterproliferation in the age of AI

By David Heslop and Joel Keep

Source: https://www.aspistrategist.org.au/counterproliferation-in-the-age-of-ai/

Sep 11 – Just over 20 years ago, Spanish naval personnel operating in the Arabian Sea intercepted a merchant ship sailing from North Korea to the port of Aden. Acting on intelligence from their US counterparts, the interdiction team discovered a consignment of Scud missiles hidden on board the vessel, the *So San*. At the time, Washington's concern was that the Scud missiles were bound for Iraq and preparations were building in the region for the coalition's ill-fated intervention against Saddam Hussein's military.

Lacking any legal basis to seize the consignment, the Spanish team could do little more than release the *So San* and let it sail, after receiving an undertaking from the Yemeni government that the missiles wouldn't be transferred to any third party. From that point on, a realisation took hold that the international community needed a new architecture for counterproliferation.

What followed was the establishment of a landmark international strategy aimed at controlling the spread of chemical, biological, radiological, nuclear and high-consequence explosive (CBRNE) technologies: the Proliferation Security Initiative, which this year marked its 20th anniversary. Over the past two decades, the initiative has consolidated an alliance of more than 106 countries committed to preventing the spread of CBRNE.

However, much has changed in the geopolitical and technological landscape since the heady days of the 2000s. While the war on terror concentrated on non-state actors and an isolated 'axis of evil', great-power competition has returned as a central focus of international security. And although missile components and dual-use centrifuges are still being hunted down, non-proliferation is today equally concerned with materials that are smuggled with much more ease. This is especially true with the tools of dual-use chemistry and synthetic biology.

In the same year as the *So San* incident, a group of scientists constructed the first entirely artificial virus, a chemically synthesised strain of polio. Three years later, reverse genetics was used to recreate H1N1 'Spanish' influenza, which had killed more than 50 million people in the years following the First World War. Since then, pox viruses, coronaviruses, avian flu and several other pathogens have been revived, amplified or modified into forms that can evade herd immunity or render established medical countermeasures obsolete. The technologies used to produce these infectious agents are much smaller than anything recently interdicted on the high seas: whole genome sequencers that can be held in the palm of one's hand, chemical reagents that can be ordered online, and a host of other products that don't need to be transported on a slow-moving ship.

In the past year, the life sciences have been further turbocharged by the latest chapter of technological advancement: the newly emergent platforms of artificial intelligence. With the debut of novel large-language models in late 2022, the public has seen minor previews of how those with malicious intent could apply AI tools to CBRNE. An exercise in Massachusetts **showed how a large-language model could help students without any scientific training construct synthetic versions of the causative agents of smallpox, influenza, Nipah virus and other diseases**. Elsewhere, researchers using generative AI for drug discovery found that they could also design a range of nerve agents, including VX. Discussion has even circulated of integrating AI into nuclear launch systems, a kind of digital dead hand for the new age. To all of this was added a slew of articles on AI-enabled high-consequence munitions, including fire-and-forget hypersonic missiles, autonomous loitering munitions and unmanned attack vehicles.

While much debate has erupted over the existential risk posed by AI platforms, some have argued that these concerns are either non-specific or alarmist. We, the authors, are investigating precisely how AI could accelerate the proliferation of CBRNE, and how such applications might be realistically controlled. To this end, we will be seeking expert opinions on how generative AI could lower informational barriers to CBRNE proliferation, or add new capabilities to existing weapon systems. As both researchers and clinicians, our concern relates primarily to human security, and what can be done to safeguard international public health. We hope to understand how counterproliferation professionals are confronting this new era, and what new concepts will be needed to protect human life and prosperity.

Next year, Australia will host the Proliferation Security Initiative's Asia–Pacific exercise rotation, Pacific Protector. Air force and naval assets will be deployed across a vast expanse of ocean at a time of increased tension over a place central to AI and its underlying technologies: the Taiwan Strait. While the exercise will have several enduring uses that will benefit the Asia–Pacific, it is undeniable that the task of countering CBRNE proliferation has fundamentally changed since the initiative's establishment.

States, non-state actors and individuals now have access to technologies and informational aids that used to be the stuff of science fiction. How policymakers, researchers and practitioners confront weapons proliferation in the new age of AI will have long-term consequences for human security in this region, and across the globe.

David Heslop is an associate professor in the School of Public Health and Community Medicine at the University of New South Wales.
Joel Keep is a journalist, clinician and post-graduate student at UNSW and a research assistant to Dr Heslop.

Can large language models democratize access to dual-use biotechnology?

By Emily H. Soice, Rafael Rocha, Kimberlee Cordova, et al.
Source: https://arxiv.org/ftp/arxiv/papers/2306/2306.03809.pdf

Abstract

Large language models (LLMs) such as those embedded in 'chatbots' are accelerating and democratizing research by providing comprehensible information and expertise from many different fields. However, these models may also confer easy access to dual-use technologies capable of inflicting great harm. To

evaluate this risk, the 'Safeguarding the Future' course at MIT tasked non-scientist students with investigating whether LLM chatbots could be prompted to assist non-experts in causing a pandemic. In one hour, the chatbots suggested four potential pandemic pathogens, explained how they can be generated from synthetic DNA using reverse genetics, supplied the names of DNA synthesis companies unlikely to screen orders, identified detailed protocols and how to troubleshoot them, and recommended that anyone lacking the skills to perform reverse genetics engage a core facility or contract research organization. Collectively, these results suggest that LLMs will make pandemic-class agents widely accessible as soon as they are credibly identified, even to people with little or no laboratory training. Promising nonproliferation measures include pre-release evaluations of LLMs by third parties, curating training datasets to remove harmful concepts, and verifiably screening all DNA generated by synthesis providers or used by contract research organizations and robotic 'cloud laboratories' to engineer organisms or viruses.

DHS unveils new guidelines on AI use

Source: https://thehill.com/policy/technology/4204733-dhs-unveils-new-guidelines-on-ai-use/

Sep 14 – The Department of Homeland Security (DHS) will not collect or disseminate data used in artificial intelligence (AI) activities and will ensure all facial recognition technologies will be thoroughly tested as part of a new set of AI guidelines released Thursday.

The new DHS policies, developed by a department task force on AI, are part of the broader Biden administration aim to manage the risks of the technology.

"Artificial intelligence is a powerful tool we must harness effectively and responsibly," Secretary of Homeland Security Alejandro Mayorkas said in a statement. "Our Department must continue to keep pace with this rapidly evolving technology, and do so in a way that is transparent and respectful of the privacy, civil rights, and civil liberties of everyone we serve."

The department also announced that Chief Information Officer Eric Hysen will serve as its first chief AI officer. In that role, Hysen will promote AI innovation and safety at DHS, and advise Mayorkas and department leadership on AI issues, according to the announcement.

Hysen will continue to serve in his role as the department's chief information officer as well.

Part of the new guidelines stems from a policy statement that establishes a set of principles for DHS's use of AI. The department uses AI to advance its missions, including combatting fentanyl trafficking and countering child sexual exploitation.

Under the new principles, DHS will "only acquire the use of AI in a manner that is consistent with the Constitution and all other applicable laws and policies."

The new principles also require that DHS not "collect, use, or disseminate data used in AI activities," or "establish AI-enabled systems that make or support decisions, based on the inappropriate consideration" of factors like race, gender or ethnicity.

The new guidelines also include a directive that calls for the use of all facial recognition and face capture technology to be "thoroughly tested to ensure there is no unintended bias."

DHS will review the existing use of this technology, and conduct periodic testing and evaluation of all systems.

The guidelines come as lawmakers and regulators grapple with how to regulate the booming AI industry. On Wednesday, leaders in the tech industry and civil rights groups met with senators in a closed-door meeting to discuss the benefits and risks of AI.

AI won't destroy the world, but state actors might

Source: https://www.verdict.co.uk/ai-world-dominance-warfare/?cf-view

Sep 15 – Christopher Nolan's *Oppenheimer* is set against the backdrop of World War II, chronicling the intense race to develop nuclear weapons in the fight against the Nazis.

The film's conclusion reveals that despite emerging as front runners in this pursuit, Oppenheimer and Einstein feared that the development of the nuclear bomb could initiate a chain reaction capable of destroying the universe—a revelation that left audiences in silence and fear. In the final seconds of the film, when reminded of his concerns that the bomb might destroy the world, Einstein asks, "What of it?" Oppenheimer succinctly replies, "I believe we did".

Oppenheimer's apprehension parallels the sentiment surrounding the current progress of artificial intelligence (AI)—software-based systems that use data input to make decisions alone. Modern AI has led to several alarming developments, particularly within the realm of political warfare. Examples include building autonomous weapons and AI-enabled chemical, biological, or nuclear weapons of mass destruction (WMD). A robust relationship between AI and WMDs could become one of the largest threats to humanity since the Nazi regime in 1933.

The threat of AI-enabled world destruction lies at the feet of the first state to deploy the technology. Credit: Mavas_Bd via Shutterstock.

The world rise of AI

What some view as modest innovation has, in fact, served as a fundamental ingredient in today's futuristic worldview of military technology. Oppenheimer's invention of the atomic bomb triggered a chain reaction where states like China, Russia, North Korea, and the UK began developing their own nuclear bombs, such as the hydrogen bomb developed by the Soviet Union. A combination of mutually assured destruction and devastating consequences has deterred the use of such weapons, potentially undermining Oppenheimer's prophecy. However, states have not shied away from exploring double-edged technologies like drones and AI to advance military objectives.

AI-based weaponry is already revolutionizing warfare in the modern era. AI enhances military strategy, tactics, and operations. Reports suggest that the Russian Ministry of Defense has used AI to analyze data for effective decision-making and began experimenting with autonomous weapons such as armed drones in 2018.

Furthermore, Ukraine used explosive drones to target Russian militants. Russia has already warned the UK that continuing to provide Ukraine with weapons and tactics against Russia may lead to the use of long-range storm shadow missiles, capable of destroying cities. Therefore, Russia would undoubtedly escalate the war against Ukraine and could potentially release killer robots—a lethal autonomous weapon—to perform an act of war.

The future threat

Recent developments in the AI market such as OpenAI's ChatGPT—a large language model capable of generating text, images, code, and algorithms—have sparked a wave of investments from companies worldwide. According to GlobalData, the global AI market will be worth $908bn. by 2030, up from $81.3bn in 2022 and growing at a compound annual growth rate of 35.2%.

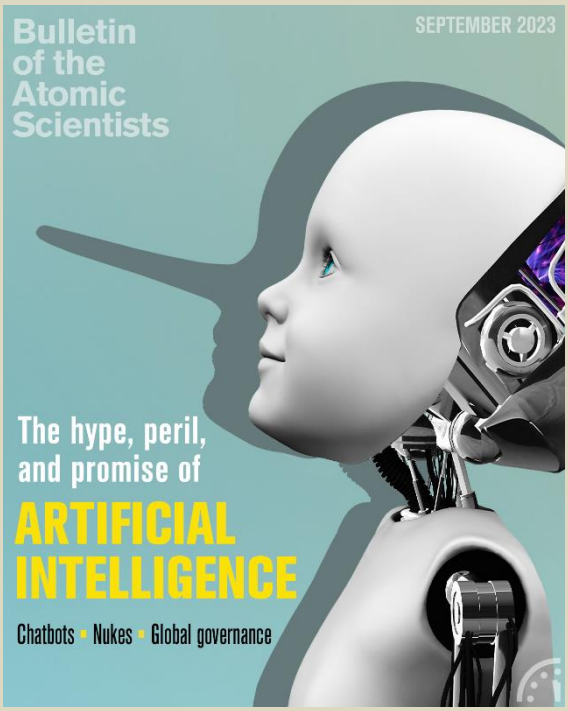
While ChatGPT does not have a clear role in developing WMDs, it created a renewed drive from states to explore the use of AI and its potential to cause harm. The internet has created doomsday scenarios due to AI's newfound proficiency in seamless content production. One such scenario is governments or defence companies releasing an AI-enabled WMD. And this is not as far-fetched as it might sound. The Pentagon issued a green flag to the US Department of Defense, allowing for the exploration of AI in conjunction with devastating weaponry that could trigger the extinction of humanity, as WMD can kill millions of innocent civilians and, perhaps, entire continents.

AI itself may not necessarily contribute to destroying the world, but the potential of AI to cause damage in the hands of state actors raises concerns. Vladimir Putin ordered the Russian government to fund AI

research in the race against the West in early September this year, while China intends to become a world leader in AI by 2030, recently constructing a "killer" four-legged robot that wields autonomous weapons.
Sam Altman, CEO of OpenAI, stated that the company is "a little scared of this", while Putin declared that "Whoever becomes the leader in this sphere will become ruler of the world". With research exploring the ability of AI to make kill shots all on their own, alongside the development of killer robots, it is not a matter of 'if' but when states will use such weapons on the frontline. Ultimately, the threat of AI-enabled mass destruction lies at the feet of the first state to deploy the technology.

Introduction: The Hype, Peril, and Promise of Artificial Intelligence

By John Mecklin | September 11, 2023
Source: https://thebulletin.org/premium/2023-09/introduction-the-hype-peril-and-promise-of-artificial-intelligence/#post-heading



Editor's note: *This introduction was written by ChatGPT-3.5 at my prompting, and edited only very lightly. It's not as thorough or nuanced as the intro I would've written. But time was short, we were past the deadline for submitting copy for this issue, and … ok, I confess. I used invented time pressure and a cliché* — watch this AI introduce a magazine about artificial intelligence! — *to clumsily illustrate that chatbots will be used, because what they produce is sometimes good enough to be useful. The chief outstanding questions are twofold: How will AI be used? And can it be managed, so the positives of its use far outweigh the negatives?*

Dear readers,

In an era marked by the rapid advancement of technology, there is no doubt that artificial intelligence (AI) stands at the vanguard of innovation, captivating the imagination of nations and individuals alike. Its potential to revolutionize nearly every aspect of our lives, from warfare and governance to the very essence of human nature, is both awe-inspiring and daunting. As we navigate through these uncharted waters, the September issue of the *Bulletin of the Atomic Scientists* sets its gaze firmly on the complex interplay between humanity and AI, exploring the hype, peril, and promise that surround this transformative force.
We kick off the issue with an insightful interview conducted by editor in chief John Mecklin with Paul Scharre, an emerging military technology expert. Scharre brings into sharp focus the intricate dynamics of global power in the age of AI, where technology reshapes the contours of geopolitical influence.
As we marvel at AI's capabilities, it is vital to remember that humans are the architects of this evolving landscape. In their thought-provoking article, Northwestern University management experts Moran Cerf and Adam Waytz urge us to shift our gaze from AI-induced fears to the potential harm that humans themselves may perpetrate. They compellingly argue that our focus should be on managing the intentions and actions of our own species, as we tread cautiously with the powerful tools AI affords us.
However, not all AI claims hold up to scrutiny. *Bulletin* disruptive technologies editor Sara Goudarzi takes on the task of deflating the chatbot hype balloon, cutting through the hyperbole to reveal the true potential and limitations of these automated conversational agents. In a complementary piece, Dawn Stover delves into the psychological impact of interacting with chatbots, probing the question of whether these digital entities will ultimately drive us to the brink of madness.
AI's global impact demands thoughtful and coordinated governance. Existential risk researcher Rumtin Sepasspour, in a thought-provoking exploration, contemplates what a harmonious international governance framework for AI should look like. As we grapple with the challenges of regulating AI across borders, Sepasspour sheds light on potential avenues for global cooperation and responsible AI development.
Moreover, the integration of AI with nuclear material production is an area of significant concern and potential. In their fascinating article, international security researchers Jingjie He and Nikita Degtyarev illuminate the extraordinary ways AI is revolutionizing this critical domain. As the intersection of AI and atoms emerges, we must tread with discernment and responsibility to harness this innovation for the greater good.
Throughout these pages, we confront the multifaceted dimensions of AI with an eye toward understanding its complexities, its impact on society, and its implications for global security. We thank our distinguished

authors for their contributions to this vital conversation. We invite you to dive into this compelling collection of articles and, as always, encourage you to engage in the discourse sparked by these pressing matters.

Sincerely,

ChatGPT-3.5, on behalf of John Mecklin, editor-in-chief, *Bulletin of the Atomic Scientists*

John Mecklin is the editor-in-chief of the *Bulletin of the Atomic Scientists*. Previously, he was editor-in-chief of *Miller-McCune* (subsequently renamed *Pacific Standard*), an award-winning national magazine that focused on research-based solutions to major policy problems. Over the preceding 15 years, he was also: the editor of *High Country News*, a nationally acclaimed magazine that reports on the American West; the consulting executive editor for the launch of *Key West*, a regional magazine start-up directed by renowned magazine guru Roger Black; and the top editor for award-winning newsweeklies in San Francisco and Phoenix. In an earlier incarnation, he was an investigative reporter at the *Houston Post* and covered the Persian Gulf War from Saudi Arabia and Iraq. Beyond the publications he has edited and opined in, his writing has appeared in *Foreign Policy*, the *Columbia Journalism Review*, and the Reuters news service. Writers working at his direction have won many major journalism contests, including the George Polk Award, the Investigative Reporters and Editors certificate, and the Sidney Hillman Award for reporting on social justice issues. Mecklin holds a master in public administration degree from Harvard's Kennedy School of Government.

AI and atoms: How artificial intelligence is revolutionizing nuclear material

By Jingjie He and Nikita Degtyarev

Source: https://thebulletin.org/premium/2023-09/ai-and-atoms-how-artificial-intelligence-is-revolutionizing-nuclear-material/

Sep 11 – Over the last decade, there has been an accelerated integration of artificial intelligence (AI)[1] into both the civilian and military fields. As a result, rising attention to the challenges of AI governance has manifested in three ways. The first challenge lies in the dual-use nature of AI in the civilian and military domains, which renders it difficult to monitor and oversee its militarization. The second derives from the policy-influencing power of the private sector, which has traditionally been limited to utilizing lobbying instruments. The final difficulty results from the changing nature of government-industry relations, where industries are leading the development and application of AI, and governments are falling behind industry in understanding its technological potential and regulating military applications.

A review of existing literature demonstrates that AI is well discussed within the military and broader strategic stability domain[2], including discussions surrounding AI use within the nuclear sphere to hack cyber systems, poison AI training data, and manipulate its inputs (Avin and Amadae 2019). The expert community further addresses AI and its applicability to nuclear safeguards.[3] However, current available research largely ignores nuclear material production (NMP), which is an essential phase in the development of nuclear weapons

This article bridges that gap by assessing the potential role of AI in nuclear material production while considering industrial practices.[4] In employing an industrial approach to technology scouting, we argue that AI has significant potential to improve nuclear material production by enhancing system efficiencies with the aim of optimizing output, reducing costs, and boosting safety in production associated with the development and production of nuclear weapons. A comprehensive list of the existing AI applications to nuclear material production-critical equipment and to related non-nuclear industry applications integrable to the nuclear material production is presented in Appendix 1, (immediately below the main text).

The AI-powered nuclear material production process raises concerns of the illicit and covert development of nuclear weapons. Therefore, a three-fold solution with feasible action plans is discussed in the final section. Although nuclear material production is the focus of this article, the findings, concerns, and solutions being addressed are also applicable to the broader debate on the production of material used to build weapons of mass destruction, including radiological, biological, and chemical weapons.

Proliferation-sensitive stages in nuclear material production

Nuclear material production consists of several steps, including mining and milling, conversion, enrichment, fuel fabrication, electricity generation, spent fuel storage, and reprocessing.[5] While each production step is important, the enrichment and reprocessing phases are the most proliferation sensitive phases. These phases provide the basis for enriching uranium and/or the separating the uranium and plutonium isotopes that are pillars[6] integral to the development of a nuclear weapon; thus, improved accessibility to these technologies through AI presents both horizontal and vertical proliferation risks[7] (Gartzke and Kroenig 2014).

Although the application of AI within the enrichment and reprocessing phases is an ongoing effort to further the application of nuclear science and technology for good, AI as a dual-use technology within nuclear

material production space has been largely neglected within the academic and practitioner communities. Therefore, a widening opportunity for AI to aid in illicit and covert non-peaceful applications exists.

AI's potential applications in the nuclear material production

Industrial applications of AI can be broadly divided into three categories: anomaly detection, automated optimization, and automated discovery. Each of these techniques has functioned and been applied in civilian industries, and each can affect proliferation-sensitive stages of nuclear material production. A summary of the key potential application of AI in the nuclear material production is illustrated in Table 1 with potential use cases specified in Appendix 1.

Table 1. Key potential applications of AI in nuclear material production

	Anomaly detection	Automated optimization	Automated discovery
Critical equipment (see Appendix 1)	Alert and prevent equipment failure and production accidents	Improve equipment configuration and design	Advance computational and data processing power through hardware innovation
Computer systems	Alert and prevent system failure	Promote production line efficiency	Accelerate computer system development and upgradation
Revolutionary knowledge	Facilitate human-centric knowledge production to revolutionize nuclear material production	Facilitate human-centric knowledge production to revolutionize nuclear material production	Realize machine-centric knowledge production to revolutionize the nuclear material production at an exponential rate

Source: authors' compilation

Table 1. Key potential applications of AI in nuclear material production

Anomaly detection. An AI anomaly-detection algorithm is trained to recognize machine or system data featuring "normal behaviors." When real-time data deviates from the normality pattern, the AI algorithm will identify the anomaly. Early-stage defection alarms make inspection and fixation possible before mechanical or system breakdown.

The use cases of AI anomaly detection fall into two categories. First, AI is used by industries to monitor, detect, and diagnose faults in machines. An example is the anomaly detection of centrifugal pumps (Al Tobi et al. 2022; Nabli and Hassani 2009). Second, AI is also widely applied in cyber defense products to detect anomalies led by cyberattacks or infections, which is a growing threat to sophisticated nuclear programs (Al Tobi et al. 2022; Nabli and Hassani 2009). An example is General Electric's AI cyber defense solution, Digital Ghost, which serves the US Department of Energy, an agency responsible for managing the nation's enriched uranium supply, in protecting critical infrastructure (General Electric n.d.a).

The aforementioned applications can be readily integrated into the nuclear material production process, provided that the training, testing, and verification data of the critical machines and computer systems involved in the producing process are accessible. Specific applications include adopting AI anomaly detection solutions to prevent failure of critical nuclear material production equipment (like centrifuges) and computer systems (such as management or cyber defense systems). Similar AI solutions can also advance efficiency and safety in human-centric knowledge production processes that facilitate nuclear material production (like advanced fissile isotope separation methods[8]).

Automated optimization. Automated optimization solutions train AI algorithms to analyze data with predefined parameters in an industrial process. Based on this analysis, the algorithms can predict product quality and correct problematic parameters to improve it. When applied to complex systems, AI algorithms can set up many factors at different levels, simulate their performance, and identify the best combination for achieving optimized solutions.

The use cases of AI automated optimization in civilian industries are three-fold. The first is industrial production. For instance, artificial neural networks, a type of deep learning algorithm, are used to monitor and adjust the performance of centrifuges in the separation processes (Funes et al. 2009; Jiménez et al.

2008; Menesklou et al. 2021). The second is industrial design. Examples include determining the optimum configuration for race cars used in different races (Monolith AI n.d.), the optimum design of computer chips (Mirhoseini et al. 2021), and the optimum shape for the crown of a piston in a diesel engine (Bogaisky 2019). The third is logistic planning. Examples of this include the reduction of the airplane turnaround time and the optimization of delivery fleet routing (General Electric n.d.b; Google n.d.).

These AI optimization solutions can also be integrated into the nuclear material production with the availability of machine or system data. This has already been applied to optimize the dimensions of a rotating baffle in gas centrifuges for uranium enrichment (Migliavacca et al. 2002). Further potential nuclear material production use cases include improvement of machine, such as nuclear centrifuges, configuration; the design of machine (including centrifuge) parts; and the efficiency of the nuclear material production lines, such as the arrangement of centrifuge cascades and the broader management of the nuclear material production process. Other human-centric nuclear research can also benefit from automated optimization solutions, which may in turn revolutionize the nuclear material production.

Automated discovery. AI algorithms are trained to understand the rules of a game by identifying key parameters at an initial stage, then developing their own algorithms to determine the best solution for the game. For example, from playing games like AlphaGo, AlphaZero (Silver et al. 2017; Silver et al. 2018), to protein structure prediction, such as AlphaFold (Jumper et al. 2021), code generation (e.g., AlphaCode) (Li et al. 2022), and faster matrix multiplication discovery (e.g., AlphaTensor) (Fawzi et al. 2022), AI has demonstrated its capability to revolutionize the scientific world at an exponential rate. Nevertheless, in the nuclear sciences, the application of automated discovery remains in early development stages. Consequently, few existing industrial applications are ready to be integrated into the nuclear material production or even feasibility research.[9]

Automated discovery techniques not only advance computational and data processing power through hardware (examples include AI chips and computers) innovation, but also accelerate the development and upgradation of computer systems through automatic code generation (such as in cyber defense or industrial management systems). More significantly, the technique foresees the realization of machine-centric nuclear material knowledge production, as in the case of protein structure prediction[10], which accelerates the speed and accuracy of human-based research, for instance on new fissile isotope separation methods[11] and more efficient materials[12]. Automated discovery has the most potential among the three AI applications mentioned; as such applications advance, they could fundamentally affect the entirety of the nuclear material production lifecycle process.

The way forward

As demonstrated, AI has already impacted several stages of nuclear material production, and its premise as a dual-use technology must be properly managed. While this endeavor requires an all-out effort from all involved parties, the scope of this discussion may focus on a three-dimensional solution.

Recommendation 1: State actors should be responsible for designing and executing effective nuclear material production-related data and infrastructure governance.

To account for the emergence of new dual-use technologies such as AI, existing legal and non-legal frameworks need to evolve.[13] However, the current political environment has constrained global consensus-building, even in cases where reaching consensus benefits all parties.[14] Nonetheless, states remain decisive actors in monitoring and regulating dual-use applications of AI as it relates to nuclear material production.

The scope of monitoring and regulating dual-use applications of AI should exclude AI algorithms; they are open-sourced and globally accessible, and therefore, essentially impossible to monitor and regulate. Instead, the scope should focus on two AI-supporting elements, the first of which is data. Since the precision of an AI solution depends on the quality and quantity of the training and testing data, the transfer of sensitive data around nuclear material production, including the peaceful production of nuclear material, should be safeguarded through enacting proper regulatory measures on technologies, data transfer, and security standards like cybersecurity.[15] The second focus should be on information infrastructure. As the function of AI-powered systems depend on advanced information infrastructures, including fast-speed broadband, cloud storage, AI chips, and supercomputers, among other things, the acquisition and transfer of these critical AI infrastructures should also be monitored. Therefore, export control of AI systems should focus on the transfer of training and testing data, as well as supporting infrastructure.

Data and infrastructure governance can be achieved via unilateral, bilateral, or multilateral solutions, as well as informal and formal means. A ready-to-implement platform is national export control regimes. Hitherto, the United States, the European Union, Russia, the People's Republic of China, and other political entities with nuclear capabilities have increasingly fortified national legislation around functional export control mechanisms for technologies and data critical to their national security interests (Pacific Northwest National Laboratory, n.d.; PRC 2017; PRC 2020; PRC 2021; European Union 2021; Federal Service for Technical and Export Control of Russia n.d.; Vladimirova et al. 2014). In addition to unilateral efforts, states should also pursue related multilateral discussions based on a shared interest in improving AI-specific export control regime mechanisms, rather than enabling diverging political positions to hinder such discussions (Fisher 1991). An existing conduit for facilitating discussions and future negotiations in this

regard is the Nuclear Suppliers Group (NSG), where member state participants agreed to voluntarily implement "guidelines for nuclear exports and nuclear-related exports" (Nuclear Suppliers Group n.d.a).[16]

Recommendation 2: The non-proliferation sector should develop an AI-proficient workforce supported by external AI industry partnerships.

State actors, nongovernmental organizations, and intergovernmental organizations within the nuclear domain have had limited interaction with AI experts, resulting in a knowledge gap that can be reduced through collective discussions.[17] As such, building awareness and sustainable partnerships, both formal and informal, is vital.

To mobilize industry engagement in the non-proliferation sphere, a three-step approach should be taken by states, nongovernmental organizations, and intergovernmental organizations. First, researchers and scientists must develop and maintain a comprehensive understanding regarding the state-of-the-art AI research as well as most advanced industrial use cases associated with the nuclear material production. A visualized example is illustrated in Appendix 1. This can be self-initiated or under institutional cooperation[18]. Ideally, a fully developed table, as illustrated in Appendix 1, summarizing AI's applicability to nuclear material production would be shared within the nuclear policy making community to develop a shared understanding on the subject, which in turn could serve as the foundation for future policy discussions.

Second, platforms and initiatives must be created and expanded to integrate the AI-related industry into the nuclear policy debate. For example, several United Nations (UN)-based organizations initiated an "AI for Good" program to identify and promote AI applications that accelerate the furtherment of the United Nations Sustainable Development Goals (UN SDGs). A recent sub-initiative, entitled "AI for Atom," addresses AI applications, methodologies, and tools that can advance nuclear science and technology (Peeva 2021). However, the impact of AI on nuclear material production and modernization, as well as its potential risks, has yet to be addressed. The broader "AI for Good" program could be expanded to include AI industrial partners to facilitate knowledge exchange around dual-use applications of AI and their potential implications in maintaining the non-proliferation regime.

Third, industrial advisory boards must be established within the relevant policy-making bodies. These advisory boards would serve two purposes: the minimization of the AI knowledge gap and the creation of effective export control guidelines. This effort could rely on intergovernmental organizations— including the International Atomic Energy Agency and the UN Office for Disarmament Affairs, and by extension, the Wassenaar Arrangement and World Customs Organization—to promote discussions around emerging technologies and their potential implications for the maintenance of the non-proliferation regime. Meanwhile, the Nuclear Suppliers Group, as a binding mechanism, presents another means for member states to create effective export control guidelines through the inclusion of an industrial advisory board.[19]

Recommendation 3: Civil society and the international community should promote ethical AI as a means to incentivize government- and self-compliance in the AI industry.

Industries do not always comply with states' policy goals or collective interests. Therefore, measures should be taken to stimulate industry compliance and engagement in non-proliferation efforts. Building a narrative that encourages compliance with AI ethical guidelines and regulations may involve highlighting the reputational costs of failing to comply and supporting the moral considerations of employees; such efforts could require outreach programs and government action (Stewart et al. 2016). For example, demonstrable industry-based association with the UN sustainable development goals has become increasingly important as companies manage employee and customer expectations surrounding sustainability, integrity, and values in an increasingly global and competitive market (United Nations Global Compact n.d.). Some of the leading suppliers of AI technology, including Amazon (Amazon n.d.), IBM (IBM 2018), and C3.ai (C3.ai n.d.), have expanded their business model to this end. Thus, the UN's sustainability goals are promising instruments for governments, nongovernmental organizations, and intergovernmental organizations to leverage when negotiating for transparency and accountability within the AI industry.

Civil society organizations must be fully aware of their responsibility as gatekeepers of the non-proliferation regime and utilize their influence to counteract governmental policy preferences and industrial incentives that have the potential to negatively affect the effectiveness of efforts to manage the risk associated with AI's use in nuclear materials processing. The first step toward achieving this goal is to increase civil society's efforts to expose the potential of AI-driven industrial activities to increase the proliferation of nuclear material. The second step is to translate the policy preferences of civil society into customer-based reputational costs for the AI industry. For example, civil society groups could foster a grassroots initiative that encourages companies to agree to report end-users when transferring data, AI-powered systems, and supporting infrastructures with a potential to facilitate high-enriched uranium and plutonium production. Such an effort could stimulate market self-regulation, as companies see a way to reduce the possibility of reputational damage by adhering to the precepts of the UN's AI for Good and Sustainable Development Goals programs.

Appendix 1. Existing AI applications to nuclear material production critical equipment and to non-nuclear industry integrable to the nuclear material production. (download PDF.)

Endnotes

[1] Artificial Intelligence (AI) refers to a collection of computer systems capable of empowering machines to generate human-like knowledge through data-driven training. The concept of AI emerged in the 1950s and was realized with the introduction of machine learning in the 1990s and deep learning in the 2000s.

[2] AI is analyzed as part of the decision-support system (without direct participation in nuclear launch) (Geist and Lohn 2018); intelligence, surveillance, and reconnaissance (ISR) (especially helpful in antisubmarine warfare and tracking mobile ICBM) (Geist and Lohn 2018); automated target recognition and terminal guidance (Rickli 2019); autonomous nuclear-weapon system (Geist and Lohn 2018); and delivery and defense systems used against nuclear attacks (including warning system) (Vincent 2019). There are three main views on AI and strategic stability. One viewpoint argues that creating AI-based technologies capable of undermining nuclear deterrence is challenging. In contrast, the second asserts that AI-based technologies will be capable of such tasks in the future (Rickli 2019; Avin and Amadae 2019), thus causing an arms race and strategic instability. The third point of view stands between the previous arguments claiming that AI has destabilizing and stabilizing effects (Horowitz 2019; Geist and Lohn 2018; Kaspersen and King 2019).

[3] For instance, research by the Vienna Center for Disarmament and Non-Proliferation recognizes that AI could increase efficiency in the analysis of large amounts of information, as demonstrated by the International Atomic Energy Agency's current use of AI techniques to categorize data, detect changes, and process natural language through its collaborative analysis platform (Rockwood et al. 2021, 48).

[4] Today, technical giants are principal players in the development and delivery of AI. Yet, these key stakeholders have, to date, had limited influence in government-initiated policy discussions around the risk of the proliferation of AI to furthering weapons mass destruction capabilities. The inclusion of the private sector in these discussions, while simultaneously balancing the necessity to innovate for peaceful purposes is an important mechanism for constructing an effective non-proliferation regime, of informal or formal means.

[5] Today's NMP most commonly uses uranium, a naturally occurring element. Natural uranium (U) is predominantly composed of two isotopes, U-238 (99.3 percent) and U-235 (0.7 percent); however, in order to sustain a nuclear reactor, uranium fuel must contain about four times as much U-235 as is found in natural uranium. As such, enrichment of U-235 to 3 to 5 percent is necessary and most pursued using gas centrifuge technology. Following enrichment, the fuel is fabricated into a structure, such as a fuel assembly, that enables it to be burned inside a nuclear reactor. The reactor, however, only uses a very small amount of the total nuclear material before the fuel is discharged, and therefore, much of the nuclear material, predominantly uranium and plutonium isotopes, in the discharged fuel, or more commonly known as spent fuel, can be reused. In order to facilitate its reuse, the uranium, plutonium, and waste products found in spent fuel are chemically separated and the plutonium (Pu) and uranium are re-introduced into the NMP process enabling it to begin again.

[6] Fissile isotopes of uranium and plutonium are foundational to the development of a nuclear weapon or other explosive device, and thus, require the enrichment of U-235 using centrifugal technology, the production of plutonium-239 through the irradiation of uranium, and/or the production of U-233 through the irradiation of thorium-232 (Council on Foreign Relations n.d.). Fissile isotopes, Pu-239 and U-233, must then undergo chemical separation through an operation called reprocessing, as fissile nuclear material, whether plutonium or uranium based. This nuclear material is then integrated into a weapons system, which generally includes a casing, reflector, communication system, and trigger components. Following which, the configuration is tested to determine its effectiveness (Cochran et al. 2022).

[7] "Horizontal proliferation is the spread of nuclear weapons to new countries through banning the trade of nuclear arms and …stop[ping] any capability …. for producing nuclear weapons", whereas "vertical proliferation refers to the advancement and stockpiling of nuclear weapons (The Nuclear Times 2016).

[8] For relevant research, see Kerman 2022a.

[9] Examples of existing research are limited but include the use of automated discovery to accelerate decision making as it relates to the selection of optimal alloy concentration for use in nuclear fuel cladding (University of California – Berkeley Nuclear Engineering, n.d.).

[10] Protein structure prediction is important to the development of vaccines, but at the same time, this technology, without proper regulatory controls, could also enhance the production, delivery, and accessibility of bioweapons.

[11] For relevant research, see Kerman 2022a.

[12] For relevant research, see University of California – Berkeley Nuclear Engineering, n.d.

[13] An example of a legal framework is the Additional Protocol (International Atomic Energy Agency, 1997) and an example of a non-legal framework is the Nuclear Suppliers Group guidelines (Nuclear Suppliers Group n.d.b).

[14] For example, in 2021, many states, including the United States and Russia, worked together in the framework of an Open-Ended Working Group on developments in the field of information and

telecommunications to create a code of responsible behavior in cyberspace in the context of international security. Despite having built consensus around a viable solution, States ultimately submitted two competing resolutions to the UN General Assembly as a result of diverging opinions on the war in Ukraine (Chernenko 2022).

[15] While the existing international framework and many state specific legal frameworks safeguard the transfer of sensitive nuclear technology, such as sensitive datasets, increasingly sophisticated cyber security threats and th industry's inability to sufficiently safeguard against such threats is well recognized (Nuclear Threat Initiative, n.d.).

[16] Maria Roskoshnaya, head of Export Control Department at Rosatom, affirmed in personal communication with the authors that AI is currently not being discussed within the context of improving NSG-issued export control guidelines (Roskoshnaya 2023). There are no publicly available documents with reference to AI on the NSG website.

[17] Maria Roskoshnaya indicates that ongoing informal discussions with industry and academia is not always fruitful given that the regulator does not always have the full amount of information nor understanding of advanced technologies related to AI (Roskoshnaya 2023).

[18] The United States Nuclear Regulatory Commission (NRC) has initiated a plan to develop an AI proficient workforce under their AI Strategic Plan beginning in 2023 (Dennis et al. 2022).

[19] The NSG currently encourages national authorities to work closely with industry to ensure effective export control regimes (Nuclear Suppliers Group n.d.a) but does not offer a mechanism for internalizing this suggestion.

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

Jingjie He is a doctoral candidate in the political science department at the Hebrew University of Jerusalem, and a fellow of the Arms Control Negotiation Academy from 2022 to 2023. Her research interests revolve around war and conflict, strategic decision-making, disruptive technologies, and military modernization.

Nikita Degtyarev is a research consultant for Open Nuclear Network, where he works on the testing of tools for open-source data analysis and the development of interactive databases on missiles and sanctions. He is also a fellow of the Arms Control Negotiation Academy from 2022 to 2023. Degtyarev's research interests include nuclear risk reduction, nuclear non-proliferation, the Treaty on the Prohibition of Nuclear Weapons, and NATO nuclear policy.

Walking the Artificial Intelligence and National Security Tightrope

By Jack Goldsmith

Source: https://www.homelandsecuritynewswire.com/dr20230921-walking-the-artificial-intelligence-and-national-security-tightrope

Sep 21 – Artificial intelligence (AI) presents Australia's security as many challenges as it does opportunities. While it could create mass-produced malware, lethal autonomous weapons systems, or engineered pathogens, AI solutions could also prove the counter to these threats. Regulating AI to maximize Australia's national security capabilities and minimize the risks presented to them will require focus, caution and intent.

One of Australia's first major public forays into AI regulation is the Department of Industry, Science and Resources (DISR)'s recently released discussion paper on responsibly supporting AI. The paper notes AI's numerous positive use cases if it's adopted responsibly—including improvements in the medical imagery, engineering, and services sectors—but also recognizes its enormous risks, such as the spread of disinformation and harms of AI-enabled cyberbullying.

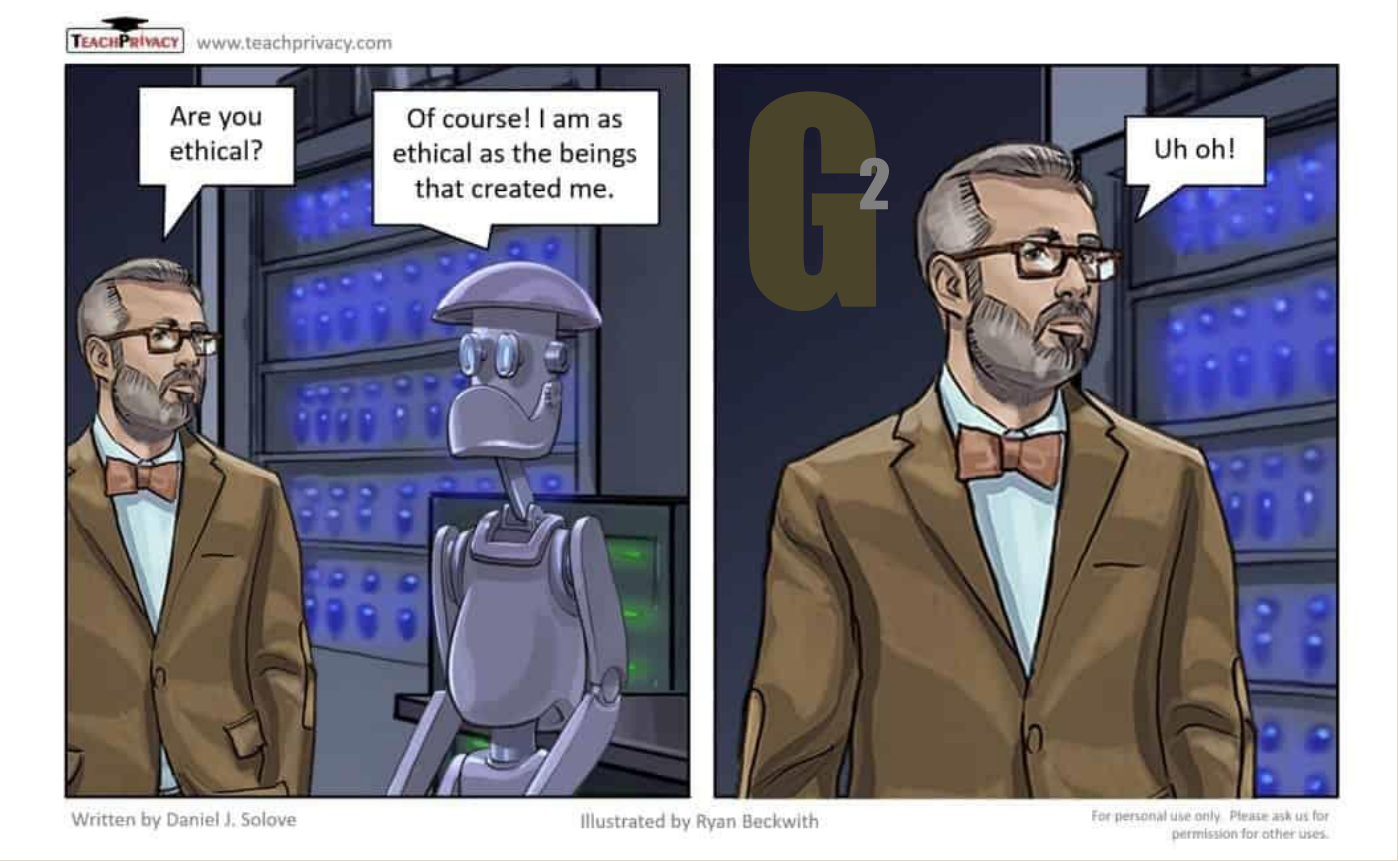
While national security is beyond the scope of DISR's paper, any general regulation of AI would affect its use in national security contexts. National security is a battleground comprised of multiple political, economic, social and strategic fronts and any whole-of-government approach to regulating AI must recognize this.

Specific opportunities for AI in national security include enhanced electronic warfare, cyber offense and defense, as well as improvements in defense logistics. One risk is that Australia's adversaries will possess these same capabilities, and another is that AI could be misused or perform unreliably in life or death national security situations. Inaccurate AI-generated intelligence, for instance, could undermine Australia's ability to deliver effective and timely interventions, with few systems of accountability currently in place for when AI contributes to mistakes.

Australia's adversaries will not let us take our time pontificating, however. Indeed, ASPI's Critical Technologies Tracker has identified China's primacy in several key AI technologies, including machine learning and data analytics—the bedrock of modern and emerging AI systems. Ensuring that AI technologies are auditable, for instance, may come at strategic disadvantage. Many so-called 'glass box' models, though capable of tracing the sequencing of their decision-making algorithms, are often inefficient compared to 'black box' options with

inscrutable inner workings. The race for AI supremacy will continue apace regardless of how Australia regulates it, and those actors less burdened by ethical considerations could gain a lead over their competitors.
Equally though, fears of China's technological superiority should not lead to cutting corners and blind acceleration. This would exponentially increase risk the likelihood of incurring AI-induced disasters over time. It could also trigger an AI arms race, adding to global strategic tension.
Regulation should therefore adequately safeguard AI whilst not hampering our ability to employ it for our national security.
This will be tough and may overlap or contradict other regulatory efforts around the world. While their behavior often raises eyebrows, big American tech companies' hold over most major advances in AI is at the core of strategic relationships such as AUKUS. If governments 'trust bust', fragment or restrict these companies, they must also account for how a more diffuse market could contend with China's 'command economy'.
As with many complex national security challenges, walking this tightrope will take a concerted effort from government, industry, academia, civil society and the broader public. AI technologies can be managed, implemented and used safely, efficiently and securely if regulators find a balance that is neither sluggish adoption nor rash acceleration. If they pull it off, it would be the circus act of the century.

Jack Goldsmith is a visiting fellow at the Australian National University's School of Regulation and Global Governance (RegNet).




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

The Vital Role of the Civilian Community in Responding to Natural Disasters

By Guy Boekenstein

Source: https://www.homelandsecuritynewswire.com/vital-role-civilian-community-responding-natural-disasters

Aug 29 – In a recent *Strategist* article, ASPI senior fellow Gill Savage talked about the importance of preparedness for Australia to ensure our 'economy, society and communities are sustainable and resilient despite the complex multi-hazard environment we face'. She noted:

Preparedness is not about prediction. Leaders shouldn't get caught up in trying to define what precisely we need to prepare for and when. Instead, they need to be ready for compounding national disruptions of any kind, at any time. Given the interconnectedness of our modern world, integrating broad economic, social and environmental preparedness will be better for resilience than mapping out overly detailed contingencies.

Less than two weeks after this piece was published, we witnessed the terrible fires in Hawaii. It's a tragedy that is still unfolding, and the immediate focus must be on the human toll and loss. However, in time there will be some important lessons to learn from this natural disaster on how the community, government, industry and local knowledge can all come together to bring rapid solutions—something that governments are still not always good at delivering in isolation.

The civilian community is often the first line of defense during natural disasters. Residents are typically the initial responders, providing immediate aid to those in need before formal emergency services arrive. Their knowledge of terrain, resources and community dynamics enables swift and targeted action, which can significantly affect survival rates.

The civilian community response complements the efforts of formal emergency services, providing essential support in times of crisis. While professional responders play a crucial role in disaster management, their resources may become stretched thin during large-scale disasters.

Effective disaster management requires a multi-faceted and holistic approach that involves coordination among various stakeholders. The civilian community response adds a grassroots dimension to this approach, involving local knowledge and expertise that is often overlooked. Communities are uniquely positioned to identify and address specific vulnerabilities and challenges that may not be apparent to external agencies. By integrating community perspectives, disaster management efforts become more comprehensive, adaptive and responsive to the needs of the affected population.

In Hawaii, much of what has been covered in the media are the outstanding efforts by local residents (and others) to ensure donated food, clothes, toiletries, bedding and other supplies get to the right areas in Maui. This has helped thousands of people who were uprooted from their homes or were left facing major damage due to the fast-spreading fires.

But given the modern reliance on the internet and mobile phone coverage, a fundamental and critical first response was the need for stable telecommunications connectivity. Immediately following the fires, a widespread telecommunications blackout hampered government and grassroots efforts to distribute those supplies in the worst-affected neighborhoods.

To provide a solution for this critical need, and one that local authorities were unable to meet quickly, there was a remarkable local community effort that ultimately involved cooperation between local Hawaii businesses, the US Space Command, SpaceX and other key stakeholders. Fundamentally, it came down to trusted people-to-people linkages.

A local consortium quickly banded together led by a Hawaii resident and tech entrepreneur in the defense and national security sector (and *Strategist* contributor), Bernice Kissinger, and a local technology provider, SMX.

While SMX doesn't have any employees on Maui, there are around 100 SMX employees on nearby Oahu. As the company witnessed the tragedy unfold, the leadership team wanted to find a way to help the community and show the company's commitment to helping supply aid. As a leader in next-generation mission support, digital transformation and IT solutions, SMX leveraged its expertise in supporting technology solutions in remote and austere environments, access to technology resources and industry partnerships to help address one of the many critical challenges on the island: connectivity.

SMX, Kissinger and others were able to leverage their relationships with the US government, the local government and SpaceX to obtain Starlink units from SpaceX to deploy to Maui. Within days of the initial request, 16 Starlink systems, complete with generators, were delivered to the island. The Starlink system is a satellite internet constellation and several SMX employees have been on the ground supporting the installation and training local responders.

Given that it took almost three days for the US government to provide a substantial response to the disaster, this is an example of how the community can step in and fill the void. And it didn't only include the hardware, but also came with essential training and education for local providers. This has provided the local community with much-needed internet and mobile coverage. The Starlink terminals have been strategically deployed in the impacted areas. A mix of terminals were spread between makeshift evacuation camps for first responders and their families who lost everything in the fire. Site included construction and industrial areas, essential facilities like sewage treatment plants, schools, various emergency shelters and community centers, churches and markets. All

parties agree that central to the success of this project has been the understanding of, respect for and use of official chains of command. All proposals were put initially to US government emergency response agencies and the state emergency management agency before engagement with local community leaders. This also included liaison, consultation and cooperation with the US Space Command, the Maui Economic Development Board and various small-business owners. It's important that lessons are learned from this tragedy. As part of that, governments need to recognize the important role that local networks can—and usually do—play and build this into national disaster and emergency management policies and procedures.

Guy Boekenstein has spent more than two decades working in the Indo-Pacific region in the defense and national security sector and is the Australian director for a *US* defense technology accelerator.

Citizen Soldiers and American State Defense Forces

By James P. Howard Ⅱ

Source: https://domesticpreparedness.com/articles/citizen-soldiers-and-american-state-defense-forces

Georgia Army National Guard Soldiers fill sandbags in anticipation of possible flooding. At the request of the Georgia Emergency Management Agency, more than 200 Guardsmen, State Defense Force Volunteers, and Youth Challenge Academy Graduates filled 8,000 sandbags for use in Georgia and South Carolina (Source: Georgia National Guard photo by Capt. William Carraway/released).

Sep 06 – State defense forces (SDFs) are state-level military organizations authorized by state law and operate under the authority of the state governor. These forces are tasked with providing support to the state National Guard and can be activated in times of emergency to assist with disaster response, homeland security, and other missions.

Although the size and structure of SDFs can vary by state, they generally consist of a mix of retired military personnel, civilians with prior military experience, and other volunteers committed to serving their

communities. Despite their volunteer status, SDFs are highly trained and well-equipped to carry out their missions, and they play an important role in supplementing the efforts of the National Guard and other state and federal agencies.

A Historical Look at SDFs

SDFs have a rich and varied history in America, dating back to the colonial era when militias were used for defense. During the Revolutionary War, militias played a crucial role in the war effort. After the war, state militias continued to be the primary means of defense for many states. These militias were often composed of citizen soldiers who volunteered to defend their communities when needed.

In the early 20th century, the role of state militias began to evolve as the United States became increasingly involved in global conflicts. Each state militia was separated into two components under federal law. One was a contribution to the newly named National Guard, while the second was a reserve force for the state. During World War I, many states created dedicated SDFs, then known as state guards, to provide security within their borders while the National Guard was deployed overseas. These state guards were composed of volunteers who underwent military training and were subject to the same regulations and standards as the National Guard. Following the end of World War I, the role of state guards began to shift as the country focused on preparing for the possibility of future wars.

During World War II, SDFs played a critical role in the war effort, augmenting the National Guard and other military units in their homeland defense missions. These SDFs were often called upon to provide local security and assist with logistics and transportation. In the post-World War II era, the role of SDFs continued to evolve as the country faced new challenges, such as natural disasters, civil unrest, and terrorism. Today, many states maintain SDFs alongside their National Guard units. Although the role and structure of SDFs may vary by state, they are generally composed of volunteer personnel who undergo military training and are subject to the same regulations and standards as the National Guard.

Modern Disaster Response Efforts

SDFs play an important role in disaster response efforts, as National Guard units are often stretched thin during emergencies due to overseas missions and long deployments. In times of natural disasters, such as hurricanes, floods, or wildfires, SDFs can be activated to provide aid and assistance to local communities. These forces have proven to be critical assets in disaster response efforts, as they are able to quickly mobilize. Despite limited funding and training challenges, SDFs have demonstrated their ability to effectively respond to emergencies in their communities.

In recent years, SDFs have been increasingly utilized in disaster response efforts, providing valuable assistance to the National Guard and other emergency responders. During natural disasters such as hurricanes, floods, and wildfires, SDFs can be activated to provide additional resources and staffing to local authorities. For instance, in 2017, the Texas State Guard (TXSG) activated hundreds of personnel in the aftermath of Hurricane Harvey, which caused widespread flooding and destruction in the Houston area. The TXSG provided a range of services, including search and rescue operations, logistics, and distribution of supplies to affected communities.

During the 2018 Camp Fire, the California State Military Reserve (CSMR) played a vital role in responding to the deadliest wildfire in California's history. The CSMR provided a range of services, including logistics, evacuation of residents, and coordination with local authorities. In the months following the fire, the CSMR was also involved in recovery efforts and helping to rebuild communities. The CSMR has also been an active response component in other California wildfires, providing timely and effective support to help protect communities and mitigate the impact of these devastating natural disasters. The CSMR's contributions demonstrate the importance of SDFs in disaster response efforts and their ability to work closely with other agencies.

In 2019, the Ohio Military Reserve (OHMR) was activated to assist with disaster response efforts following severe storms and tornadoes that swept through the Dayton area. The OHMR worked with local authorities in a variety of ways, including recovery operations and logistics. The OHMR played a critical role in responding to the disaster, which caused widespread damage and destruction in Ohio. By working closely with local authorities and other emergency responders, the OHMR was able to provide timely and effective aid to those in need.

Actions Needed to Strengthen State Disaster Response Efforts

Currently, SDFs are a crucial component of disaster response efforts in the United States. They provide critical resources to state and local authorities in times of crisis, leveraging their local knowledge and flexibility to quickly mobilize and respond to emergencies. SDFs can also provide important specialized skills and resources that free up National Guard personnel to focus on other critical tasks outside of emergencies. For instance, some states have dedicated teams of attorneys to work with National Guard soldiers on legal matters, like wills. Teams of medical personnel from multiple SDFs distributed and administered vaccines during the COVID-19 pandemic. Several SDFs have band units that play at funerals and other ceremonial occasions.

Despite their effectiveness, SDFs face significant challenges in disaster response efforts, including limited funding, equipment, and training. Some states provide no funding to their SDFs and may provide no other resources. This limits their ability to provide new training and modern equipment to work with. These challenges can impede their ability to work with affected communities and impact their ability to coordinate with other state and federal agencies involved in the response effort. As such, it is essential to recognize and address these challenges to ensure that SDFs are better equipped to fulfill their mission.
To support the vital work of SDFs, state agencies and the federal government need to provide them with the necessary resources and training to help them effectively respond to emergencies, including increasing funding, improving equipment and resources, and enhancing coordination and communication between state and federal agencies. This can be done without impacting their state-specific role and mission, like how the federal government provides homeland security grants to local agencies. Governments also need to raise public awareness about the role and capabilities of SDFs, to help build trust and understanding with local communities. Overall, SDFs are critical in protecting the country and serving local communities. By providing a safety net of capable and well-trained personnel to state and local authorities during times of crisis, they help ensure the safety and well-being of communities nationwide. With the right funding and resources, SDFs can continue to play a critical role in disaster response efforts and help build stronger and more resilient communities.

As an accomplished data scientist with over two decades of experience, **Dr. James P. Howard II** has made significant contributions to the field of data analytics and machine learning, with a strong background in public policy and a Ph.D. from the University of Maryland Baltimore County. His expertise extends to various domains, including health-related research and computational methods. Notably, Howard is a Maryland Defense Force captain, contributing his skills and knowledge to his community's defense and security efforts.

Low-power desalination tech may provide drinking water at disaster sites

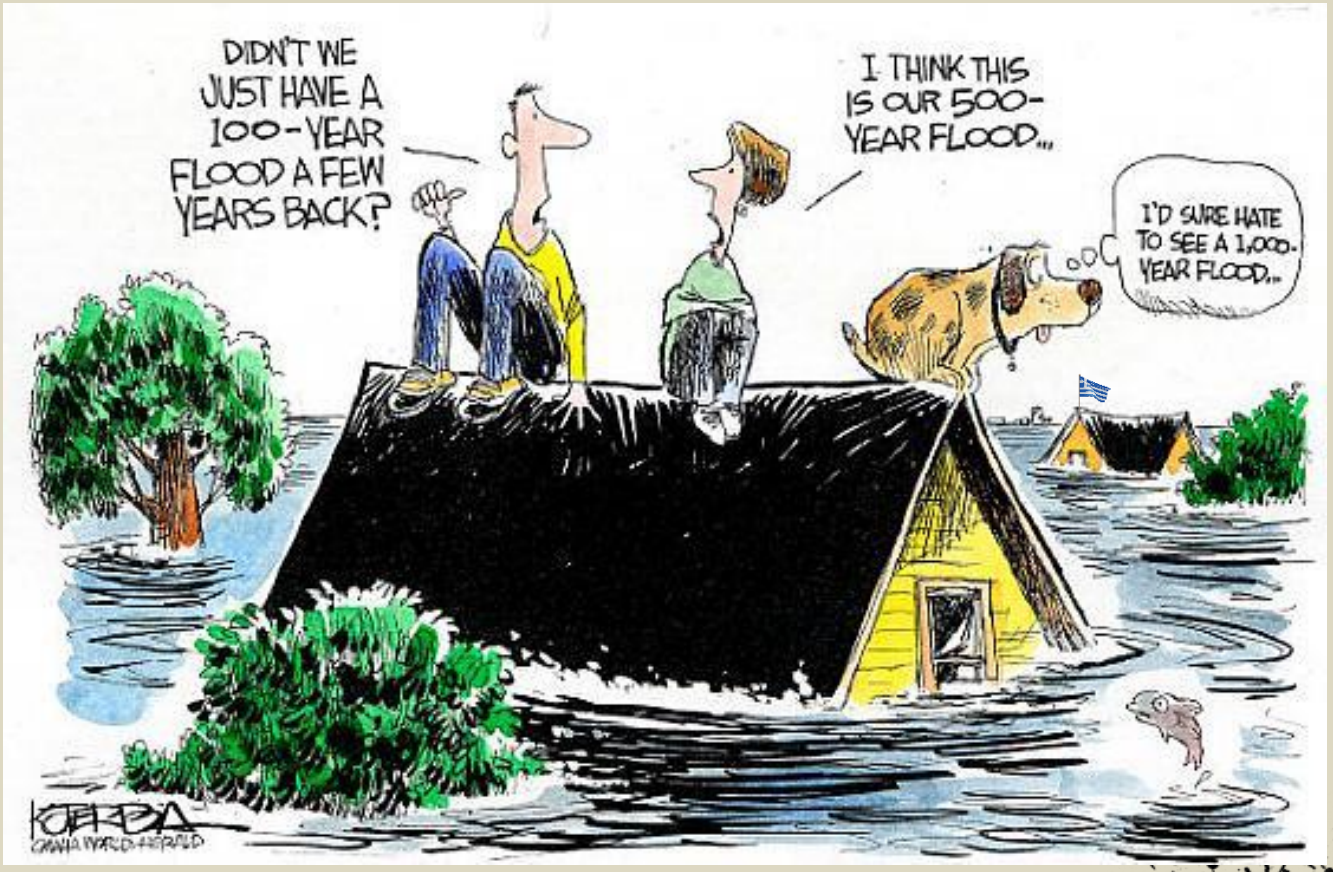
Source: https://newatlas.com/technology/low-power-desalination-system/

Thessalia, Greece floods | September 2023

Sep 21 – At disaster sites, it's not uncommon for both the water supply and electrical grid to be out of commission. That's where a new system may someday come in, as it utilizes just a small amount of electricity – which could be stored in a battery – to desalinate seawater for drinking.
Currently, reverse osmosis in the most commonly used method of desalination. In a nutshell, it works by forcing seawater through a permeable membrane that allows water molecules to pass through, but not

salt (sodium chloride) molecules. It's an effective process, but it also requires a considerable amount of power in order to generate the required water-pushing pressure. Additionally, the membranes eventually get clogged with captured salt, and have to be replaced.
Developed by scientists from the UK's Universities of Bath, Swansea and Edinburgh, an experimental new system doesn't utilize pressure at all. Instead, it incorporates a vessel with a positively charged electrode at one end, a negatively charged electrode at the other, and a porous membrane between them.
When seawater is placed inside, the positively charged sodium ions in the salt molecules are drawn to the negatively charged electrode, while the negatively charged chloride ions are drawn to the positively charged electrode.
As the chloride ions pass through the membrane while moving toward the positive electrode, they also push water (H2O) molecules through that membrane. The sodium ions remain on the original side of the membrane, as they're attracted to the negative electrode. The chloride ions are then circulated back to that side, so they can move more water molecules across. Eventually, most of the water ends up on the positive-electrode side of the membrane, completely salt-free.
So far, the system has only been tested on a few milliliters of water at a time. The researchers are thus looking for partners to help develop the technology up to the point that it can process one liter of water, so they can get a better sense of how much power a practical system would require.
"Currently reverse osmosis uses so much electricity, it requires a dedicated power plant to desalinate water, meaning it is difficult to achieve on a smaller scale," said the lead scientist, the University of Bath's Prof. Frank Marken. "Our method could provide an alternative solution on a smaller scale, and because water can be extracted without any side products, this will save energy and won't involve an industrial scale processing plant."

●▶ **The research is described in a paper that was recently published in the journal** *ACS Applied Materials and Interfaces*.




ICI
International
CBRNE
INSTITUTE
A common roof for international
CBRNE First Responders
Join us!
Rue des Vignes, 2
B5060 SAMBREVILLE (Tamines)
BELGIUM
info@ici-belgium.be
www.ici-belgium.be