09\22

I C I

C²BRNE DIARY

Dedicated to Global First Responders

September 2022

9·11·01 REMEMBER
NEW YORK, NY · SOMERSET, PA · ARLINGTON, VA

Mr. Zelensky
Mr. Putin
Mr. Biden
Mr. Borrell

PART B

enough

Mrs. Truss
Mr. Stoltenberg
Mr. Guterres

An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C2BRNE DIARY

DIRTY R-NEWS

A Ukrainian climate expert on the Zaporizhzhia situation and the winter energy outlook

By Jessica McKenzie

Source: https://thebulletin.org/2022/08/a-ukrainian-climate-expert-on-the-zaporizhzhia-situation-and-the-winter-energy-outlook/

Zaporizhzhia nuclear power plant in southern Ukraine. The two tall smokestacks are at a coal-fired generating station about 3km beyond the nuclear plant. Photo credit: Ralf1969 via Wikimedia Commons.

Aug 19 – Fear over a possible nuclear disaster at the Zaporizhzhia nuclear power plant in Ukraine rose this week, as both Russia and Ukraine warned that the other side could be planning a "false-flag" attack. Russian forces—currently in control of the plant—have ordered many of the Ukrainian workers who continue to run and operate the plant to stay home from work; only those workers who work on the power units themselves have been allowed on the premises, according to Ukraine's state-run energy firm, Energoatom.

Earlier this month, the European Union and the United States called for Zaporizhzhia and the surrounding area to be demilitarized, but Russia has rejected the suggestion, saying it would make the plant "even more vulnerable."

Oleh Savitskyi, a board member of the non-governmental organization Ecoaction and a climate and energy policy expert with the Ukrainian Climate Network who worked in the ministry of energy and environment protection of Ukraine until June, has been following the situation closely. The *Bulletin* reached Savitskyi by phone in Kyiv earlier this week to discuss the escalating situation at Zaporizhzhia, what happens if the plant goes offline, and the outlook for Ukraine's energy supply in the coming months and years.

This interview has been condensed and edited for brevity and clarity.

Bulletin of the Atomic Scientists: What is going on at Zaporizhzhia right now?

Oleh Savitskyi: We have a pretty tense situation there. Russians have damaged several facilities at the site, they disabled one of the power lines by shelling. There are five major power lines which connect the Zaporizhzhia nuclear power plant to the Ukrainian grid, four 750 kV lines and one 330 kV line. And

Russians have reportedly damaged two of those lines. And because of that, one of the units of the nuclear power plant had to be switched off because of the line outage.
If a nuclear power plant loses grid connection entirely, it becomes an emergency situation, because to cool off the reactors, the power plant still needs energy. And when it's disconnected from the grid, all its own generation is zero, all the reactors are stopped in emergency mode. And to power the cooling pumps that provide cooling for the reactors, the plant will need to rely on backup diesel generators.
Bulletin: And how long will those last?
Savitskyi: In the best case scenario, a week if there are sufficient reserves of fuel. Usually there is a week-long reserve of fuel for each diesel generator, but since Russians are using Zaporizhzhia nuclear power plant as their military base, they could have been stealing that diesel fuel or using it for their vehicles. Nobody knows how much fuel is available. That is also assuming the diesel generators are well functioning and they are fully repaired in due time, and they are not faulty themselves.
Bulletin: I saw speculation that Russia wants to send the power from Zaporizhzhia to Crimea.
Savitskyi: There were allegations or statements that they want to connect it to Crimea. But it's technically quite a challenge because that would mean splitting Ukraine's grid and disconnecting the southern Ukraine from the rest of Ukraine.
In theory, it's possible but considering that it can have countermeasures from Ukrainian side it's very improbable. Already one of the substations in Crimea which is critical for getting the power from Zaporizhzhia to Crimea was damaged by an explosion.
Bulletin: I understand you know someone in the town near Zaporizhzhia?
Savitskyi: Yes, in Enerhodar the situation is terrible. Russians are kidnapping people. They have kidnapped hundreds of people and probably many of those people died. They were kidnapping all those who were expressing dissent, or opposing Russians. They also were just kidnapping people to blackmail their relatives, families and wanting ransom.
Bulletin: I understand that the number of staff members at Zaporizhzhia is—
Savitskyi: Dramatically declining? Yeah, it's true.
Bulletin: So, what does that mean?
Savitskyi: That means that at some point, the operation of the nuclear power plant will not be possible. Because you need to have shifts. At a nuclear power plant there should always be several people for every task so you have some redundancy. You cannot have just one person responsible for some critical monitoring of reactor operation and safety systems. So it's clearly a condition that the plants should be stopped before personnel become unable to deliver the minimal required level of oversight and their duties.
The reactors should be put into cold shutdown, because there is not enough staff to really maintain the normal operation of the power plant. And—
Bulletin: What would that mean for Ukraine?
Savitskyi: Zaporizhzhia was producing a significant share of Ukraine's electricity. But it's not indispensable, especially now. Since big industrial enterprises were destroyed in Mariupol, in other parts of Ukraine, the demand for electricity has dropped significantly. But in the winter, for sure, we would need Zaporizhzhia to go through the winter without having severe deficits of electricity. We will not have blackouts without Zaporizhzhia. But it would be challenging in terms of meeting the power demand in the winter.
By winter, the power plant should be under control of the United Nations, and it should operate normally safely and with the protection of the international community.
If Zaporizhzhia shuts down and remains down for a prolonged period of time, we would probably have to rely more on coal. And that would be a problem. Because we don't have too much coal supplies, or domestic mines. Most of the mines were destroyed by Russians in eastern Ukraine. Since 2014, the eastern part Donestk region has turned into an environmental nightmare, it's just—it's apocalyptic. There is no drinking water. Most of the mines are abandoned and flooded and have become a source of toxic pollution because the mine water is heavily contaminated. And it's gotten into the surface waters and aquifers. There's practically no drinking water anymore.
Bulletin: Are there similar environmental risks at Zaporizhzhia?
Savitskyi: The radiation hazard is the main problem and not from the reactors themselves. The highest risk I see in this military situation is the spent nuclear fuel. There is a huge storage of spent nuclear fuel which is just in big concrete containers standing in the open. If there is an attack, accidental or intended, on those containers with spent nuclear fuel, it can be an extremely big emission of radioactive material.
Bulletin: What are you currently working on?
Savitskyi: Since March, we've advocated from every possible angle to cut off Russian income and cut off Russian influence and leverages in other countries and in the nuclear industry. Rosatom is one of the most powerful leverages Russia has and uses in many countries: in Egypt, in Turkey, in Asia. And Russia is using not only gas and oil supplies, but also its nuclear technology as a geopolitical weapon and the way to get a foot in the door in many countries, where they establish this link with authoritarian regimes, and also, like

they did in Belarus, for example, they build a nuclear power plant, provide export credit for it, and then the state becomes an economic hostage to Russia.

Bulletin: My understanding is that your background is in climate and environmental issues. Were you working on nuclear issues before the war?

Savitskyi: As an environmentalist, my colleagues and I have been watching nuclear issues for decades. We were advocating for real energy security policy, for Ukraine to start strategically developing renewables and to diversify energy sources and to clean up Ukraine's energy system. But there were major corruption issues, which blocked the development of renewables and alternative pathways. Energoatom was always mired in corruption.

Bulletin: What does that mean for Ukraine going forward?

Savitskyi: What is very much missing from the public sphere is that Ukraine doesn't really have a credible plan for energy system development after the war, or even a plan to make it more resilient in the coming months. The ministry has failed to make sufficient preparations for winter resilience, and we might face a very hard winter this year. There could be a real deficit of energy supply in the winter and Ukraine will be much more vulnerable to Russian attacks on energy infrastructure.

Jessica McKenzie is an associate editor at the Bulletin of the Atomic Scientists. Her work has been published in *The New York Times*, *National Geographic*, *Audubon Magazine*, *Backpacker*, *The Counter*, and *Grist*, among other publications, and has won awards or honorable mentions from the Society for Advanced Business Editing and Writing, the North American Agricultural Journalists Writing Awards, and The Newswomen's Club of New York. In 2018, she completed the Lede Program for Data Journalism at Columbia University. Previously, she was the managing editor of the civic tech news site Civicist, and interned at *The Nation* magazine.

The Russians allegedly brought 10 chemical laboratories near the Zaporozhye plant. Energoatom: Proof that they are preparing an act of nuclear terrorism

Source: https://romania.postsen.com/world/65195/The-Russians-allegedly-brought-10-chemical-laboratories-near-the-Zaporozhye-plant-Energoatom-Proof-that-they-are-preparing-an-act-of-nuclear-terrorism.html

Aug 26 – The Russian occupiers are preparing for a challenge to the nuclear power plant in Zaporozhye (southern Ukraine) with radiation emissions, the Ukrainian State Nuclear Agency Energoatom warned on Friday, indicating that Russia would have developed ten chemical laboratories in Melitopol, a city in the same region, the agency informs by Unian press and the local television channel TSN, quoted by Agerpres. "It became known that 10 chemical laboratories were brought to Melitopol. With the help of these laboratories, the Russians **plan to save their officers and generals** in case of radiation emissions from the plant in Zaporizhia," states Energoatom in a statement posted on Telegram.

Previously, Ivan Fyodorov, the exiled Ukrainian mayor of Melitopol, which is under the control of Russian forces, had announced on Ukrainian television stations that these laboratories had been installed at one of the city's medical institutions.
"**Of course, they don't think about the civilian population. These laboratories are to protect their people in this temporarily occupied city,"** Fedorov declared.
"It is yet another proof that Russia is preparing to commit an act of nuclear terrorism, causing an accident with radiation emissions at the captured Zaporozhye nuclear power plant", claims the Ukrainian company, according to the text quoted by Unian.
Energoatom once again asked the entire international community, the UN and the International Atomic Energy Agency (IAEA) to make efforts to speed up the withdrawal of Russian troops from the territory of the plant in Zaporozhye and from the satellite city of Energodar, in order to demilitarize the plant and bring it back under control full of Ukraine.
Russian forces captured the nuclear power plant and the town of Energodar on March 4. Since then, the Russian Federation has refused the proposal to create a demilitarized zone in the perimeter of this nuclear power plant, the largest in Europe.
The **main intelligence directorate of the Ukrainian Ministry of Defense (GUR)** considers the probability of a large-scale "terrorist attack" by the Russian occupiers at the nuclear power plant in Zaporozhye **to be high**, Unian notes.
The European Union qualified on Friday as "extremely worrying" the situation at the nuclear power plant in Zaporozhye and asked Russia to allow IAEA experts to carry out an inspection at this facility, according to EFE.

EDITOR'S COMMENT: A fine example of a biased article, this time from Romania. As if 10 labs would be sufficient to save military personnel (not only officers and Generals) in case of a nuclear accident that might affect entire Ukraine and certain neighboring countries! Propaganda is not easy but bad propaganda might affect its purpose.

Russia to build two nuclear reactors in Hungary

Source: https://www.bbc.com/news/world-europe-62695938

Aug 27 – Russian nuclear power giant Rosatom will begin constructing two new nuclear reactors in Hungary in the coming weeks, Hungary's foreign minister said. The deal, reached between Russia and the EU state in 2014, aims to expand the existing Paks nuclear plant. Russia's nuclear industry has not been subjected to EU sanctions over its bloody invasion of Ukraine.
Moves to isolate and sanction its oil and gas exports have not been unconditionally supported by Hungary. The Paks site currently generates 40% of Hungary's electricity supply. "Let the construction begin!" said Foreign Minister Peter Szijjarto in a Facebook post.
With the additional two reactors, the nuclear power station - currently made up of four Soviet-built reactors - will see its capacity more than double. "This is a big step, an important milestone," Mr Szijjarto said in a Facebook post quoted by AFP news agency.
"In this manner we will ensure Hungary's energy security in the long term and protect Hungarians from wild swings in energy prices."
He added that the nuclear reactors could be ready for service by 2030. The controversial €12.5bn (£10.6bn; $12.4bn) project is largely financed by Russia. In the wake of the war in Ukraine, many EU states have been trying to lessen their dependence on Russian supplies of energy.

The US military is still missing 6 nuclear weapons that were lost decades ago

By David Roza
Source: https://taskandpurpose.com/history/us-military-nuclear-weapons-missing/?amp

Aug 25 – From car keys to glasses to rifles, everyone misplaces something important from time to time. But when you're the U.S. government, sometimes that important thing is a superweapon that is designed to destroy cities and kill millions of people.
Over the decades, the U.S. military has had 32 nuclear accidents, also called "Broken Arrow" incidents. These incidents include accidental launches, radioactive contamination, loss of a nuclear weapon or other unexpected events involving nuclear weapons. Luckily, of those 32 accidents, there were only six U.S. nuclear

weapons that could not be located or recovered, and of those six weapons, only one was capable of a nuclear detonation when it was lost.

While even one missing nuclear weapon sounds scary, it's worth noting that the Soviet Union lost far more during the Cold War, often due to submarines sinking with a dozen or more nuclear missiles on board.

"Compared to the Soviet Union, the U.S. record is pretty impressive, given how many nuclear weapons it has operated and transported everywhere over the years," Hans Kristensen, director of the Nuclear Information Project for the Federation of American Scientists, told Task & Purpose.

Barrels of contaminated soil collected at Palomares, Spain for removal to the United States, 1966. (U.S. Air Force)

In fact, U.S. government agencies often go to great lengths to secure lost weapons. One such incident occurred on Jan. 17, 1966, when a B-52 and a KC-135 refueling tanker collided over southern Spain and scattered four B-28 thermonuclear bombs around the fishing village of Palomares. The conventional explosives for two of the bombs exploded, but the nuclear components did not detonate because they were not armed. The U.S. military sent troops to pick up the undetonated one that fell on land, clean up the radioactive pieces scattered by the two which detonated, and find the fourth which landed in the sea. The U.S. government even dispatched a submarine to find the one in the Mediterranean Sea. Called 'Alvin,' the small deep-ocean sub was high-tech for its time, but the crew nearly died when the sub was almost entangled in the parachute that was still attached to the bomb on the ocean floor. Meanwhile, the service members who helped find the landward bombs and clean up the wreckage also developed cancers which they say are linked to that mission 56 years ago.

Considering the extent to which the U.S. looks for lost nukes like it did in Palomares, the stories behind the five instances where recovery crews could not locate or recover weapons are extraordinary. Below is a list of those five accidents, one of which resulted in two missing nuclear weapons. Keep in mind that in all but one, the lost nuclear weapons did not include the pit or capsule that contains the components for triggering a nuclear detonation. That means we can all sleep a little easier knowing those weapons cannot blow up a city. However, the U.S. government still classifies those pit-less devices as nuclear weapons: sophisticated, expensive machines that at the time were closely-guarded tools of mass destruction. And there are many more out there from other governments like the Soviet Union which may never be found.

July 28, 1957 – Atlantic Ocean: An Air Force C-124 cargo aircraft that had taken off from Dover Air Force Base, Delaware lost power from two of its engines while flying over the Atlantic Ocean. Though the aircraft had two other engines, it could not maintain level flight, according to one report released in 2006 by the Department of Energy. The C-124 was carrying three nuclear weapons and one nuclear capsule at the time. Luckily, none of the weapons had the capsule installed, so none of the weapons could cause a nuclear detonation. With that in mind, the C-124 crew decided to jettison two of the weapons, perhaps to save weight and extend the aircraft's range en route to an emergency landing near Atlantic City, New Jersey.

The crew jettisoned the first weapon at an altitude at 4,500 feet, and the second at 2,500 feet. The report said that both the weapons were presumed to have been damaged by the impact from such a great height and then submerged "almost instantly." Meanwhile the aircraft landed safely with the remaining nuclear weapon and capsule aboard.

"A search for the weapons or debris had negative results," reads the report, which noted that the ocean varies in depth in the area of the jettisons. One of the reasons this incident stands out from the rest on this list is that the aircraft involved was a transport plane, not a bomber or attack plane like the ones involved in many of the other events. Kristensen noted that today transport aircraft like the Air Force's C-17 are the only jets allowed to fly America's nuclear weapons when they need to be transported for inspection, replacement or redeployment. Flying may be the only option when transporting nuclear weapons to and from bases in Europe, but within the U.S., the government prefers to use trucks and trains since they are less risky than flight, Kristensen said.

The Department of Energy even has heavily modified tractor trailers complete with booby traps, immobilizing foam and tear gas designed to stop would-be thieves while transporting nuclear weapons by road. But don't relax just yet, there is always a chance for something to go wrong. Kristensen noted that the U.S. still has thousands of nuclear weapons in about a dozen states, a handful of European countries, and aboard 14 *Ohio*-class ballistic missile submarines, so there are still plenty of possibilities for individual incidents. "We don't constantly fly them on B-52 [bombers] anymore, but there are still plenty of movements of nuclear weapons occurring," Kristensen said.

Feb. 5, 1958 – Tybee Island, Georgia: An Air Force B-47 bomber was flying a training mission from Homestead Air Force Base Florida when, at 3:30 a.m. while near Savannah, Georgia, the B-47 collided with an F-85 fighter jet. The B-47 pilot tried to land three times at nearby Hunter Air Force Base, Georgia, but the airplane was in rough shape, and it could not slow down enough to ensure a safe landing, the Department of Defense wrote in its list of nuclear weapons accidents. The pilot decided to ditch the Mark 15, Mod 0 nuclear weapon in Wassaw Sound, near Tybee Island, Georgia, rather than risk blowing up the base with the weapon's 400 pounds of conventional explosives. Luckily, the nuke did not explode despite dropping from about 7,200 feet up. The B-47 landed safely, but the bomb was never found. Recovery crews searched a three-square-mile area using a ship, divers and an underwater demolition team wielding hand-held sonar devices. In 1998, a retired military officer and his partner also combed the sound with a Geiger counter but were also unsuccessful, the BBC reported earlier this month.

Today, the Department of Energy believes the 7,600 pound bomb is resting five to 15 feet under the seabed, according to a report shared by the BBC. The Department of Energy reported that there is no current or future possibility of a nuclear explosion, and the risk of a spread heavy metals is also low, but that could change if the bomb is disturbed. In other words, best to let sleeping nuclear dogs lie.

A Mark 15 Thermonuclear Bomb similar to the one lost near Tybee Island, Georgia, in 1958. (U.S. Atomic Energy Commission)

"[I]ntact explosive would pose a serious explosion hazard to personnel and the environment if disturbed by a recovery attempt," the Air Force wrote in the report.

Sept 25, 1959 – Off the Washington/Oregon coast: A Navy P-5M, a flying boat designed for naval patrols and anti-submarine warfare, was carrying an unarmed nuclear anti-submarine weapon over the Pacific Ocean when it crashed in the sea about 100 miles west of the border between Washington and Oregon. Details about what led to the crash are scant, but the crew of 10 was rescued, according to the University of Southern California's Broken Arrow Project. The nuclear weapons were not recovered, and while they did not contain any nuclear material, the weapons may still be somewhere on the ocean floor to this day.

Even if the nuclear weapons did not have nuclear material, could they be repurposed if found by bad actors? Kristensen reasoned that if the U.S. government with its abundant resources and intense focus when it comes to nuclear weapons cannot find the weapons off its own coast, then non-state actors or other countries such as Iran "have no chance to get them," he said. "That's just a fact."

Indeed, the U.S. government is actually much more concerned with nuclear weapons being stolen from land-based sites rather than the few it has lost at sea. For example, in 2007 the Air Force was embroiled in controversy when a B-52 bomber crew took off from Minot Air Force Base, North Dakota and landed at Barksdale Air Force Base Louisana, not knowing they had six nuclear weapons mistakenly mounted to the aircraft's wings.

"For a day and a half the U.S. Air Force didn't know where six of its nukes were," Kristensen said. "That was a huge scandal."
The incident led to significant changes in how the U.S. oversaw its nuclear command, controls and procedures, including the resignation of the Air Force secretary and chief of staff. Still, accidents happen, which is why the U.S. government pays more attention to the nukes in active circulation than the ones that were lost at sea.

Jan. 24, 1961 – Goldsboro, North Carolina: An Air Force B-52 broke apart while on an airborne alert mission and dropped two nuclear bombs. One bomb's parachute deployed and the weapon landed with little damage. However, the other bomb fell free and broke apart on impact, narrowly avoiding a detonation. After Robert McNamara took the post of Secretary of Defense later that year, he pointed to that incident and another nuke loss over Texas as evidence of how close the U.S. has come to accidental detonations, despite "spending millions of dollars to reduce this problem to a minimum."
"By the slightest margin of chance, literally the failure of two wires to cross, a nuclear explosion was averted," McNamara was quoted as saying in an article by The Guardian.
Part of that nuclear bomb containing uranium could not be recovered, even after excavating 50 feet down into waterlogged farmland, the Department of Energy wrote in a 2006 report. Kristensen explained that the nuclear core of a weapon like this one is so heavy with uranium, one of the most dense metals on Earth, that it has the capacity to sink deep into the mud, especially after falling from a great height. Since it could not find the bomb, the Air Force bought the land and anyone who wants to dig there must ask the Air Force's permission first. There is no detectable radiation or hazard in the area, the Department of Energy wrote.

Air Force personnel recovering parts of a MK-39 nuclear bomb that fell from a B-52 bomber that broke up over Goldsboro in 1961. (U.S. Air Force)

The U.S. Department of Defense declassified its list of nuclear weapons-related accidents in the 1980s. In one report, the government noted that many 'Broken Arrow' incidents stem from human errors or mechanical malfunctions aboard the aircraft transporting the nuclear weapons, or carrying them as part of Operation Chrome Dome. From 1960 to 1968 the U.S. Air Force flew B-52 bombers armed with thermonuclear weapons on continuous airborne alert 24/7, 365 days a year. The program ended in part because of the greater risk of disaster that came with keeping nuclear weapons airborne all year long.

Dec. 5, 1965 – The Philippine Sea: While the North Carolina bomb vanished deep beneath American soil, this missing weapon disappeared in watery depths on the other side of the world. A Navy pilot was rolling his A-4 Skyhawk attack plane onto the elevator of the aircraft carrier *USS Ticonderoga.* The aircraft carried a B-43 thermonuclear bomb for a training exercise. All was going well until the weapons loaders and other sailors noticed that the Skyhawk was about to go over the side of the ship.

"Suddenly, the plane directors—yellow shirts—began to blow their whistles frantically while crossing their fists, directing the pilot to set his brakes. But the Skyhawk kept rolling," retired Chief Petty Officer Delbert Mitchell, who helped load the bomb onto the plane that day, recalled in an essay for Naval History Magazine. An investigation report later revealed that the pilot was oblivious to the whistles and looking down, Mitchell noted, but that didn't stop the sailors from trying to stop the disaster.

"The directors ran to the plane, urgently signaling and blowing their whistles," Mitchell wrote. "The Skyhawk did not stop. One blue shirt threw a chock around the starboard main mount tire, putting himself in harm's way to stop the rolling aircraft."

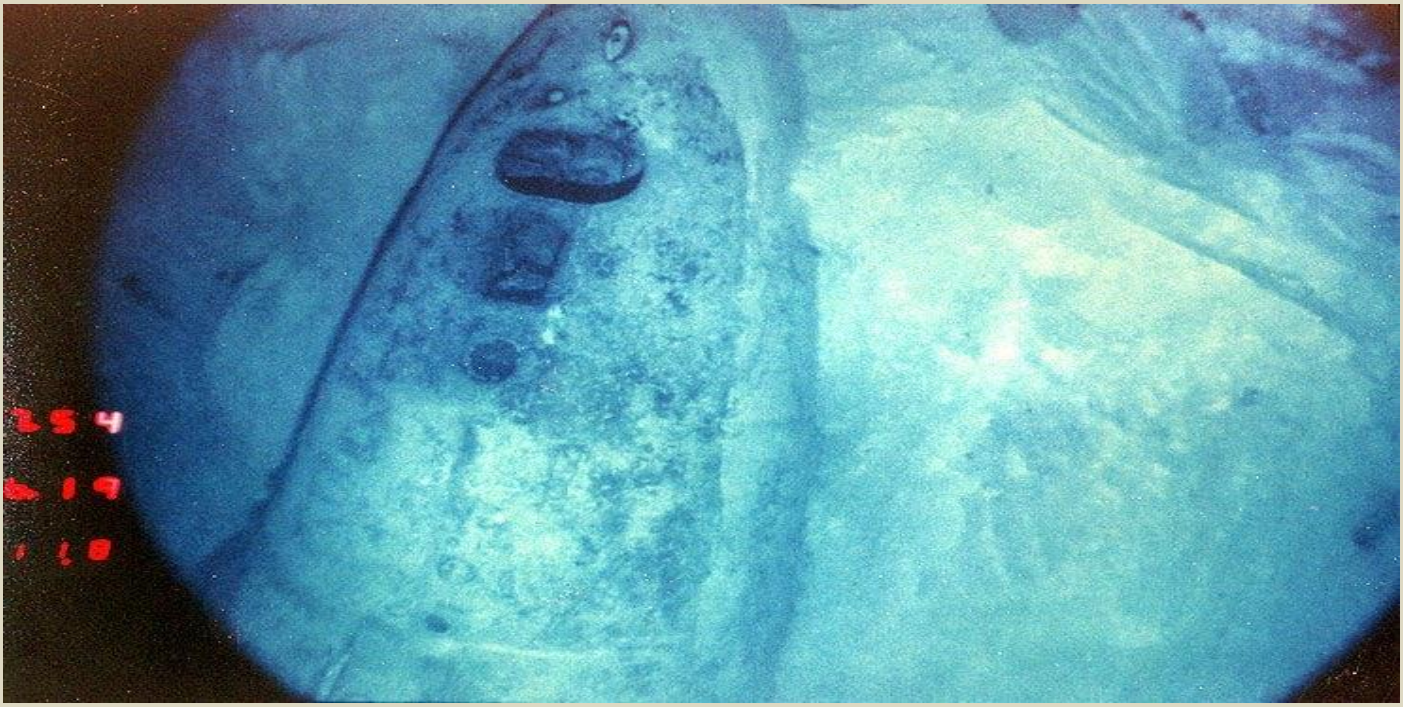
Another sailor tried to get his chock around the port tire, but he could not, and the airplane fell into the sea below.

"We watched helplessly as the attack plane and pilot sank into the abyss, the ship continuing to move forward," Mitchell wrote. "It was horrifying to watch a human being die before our very eyes, powerless to save him."

All rescuers could find was the pilot's helmet. The rest seemed to have gone to the bottom of the ocean, under 16,000 feet of water, the sailor said. This is the only weapon on our list that was capable of a nuclear detonation when it was lost, because it was not possible to remove the core from a B-43 thermonuclear weapon, Kristensen said. Though the incident took place just 70 miles from the Ryuku Islands, the U.S. government did not notify the Japanese government about the incident until 1989.

Other incidents

The nuclear weapon lost in 1965 is far from the only one on the bottom of the ocean. In May 1968, the U.S. submarine *Scorpion* sank to the bottom of the Atlantic for unclear reasons, carrying all hands and two Mark 45 ASTOR torpedoes with nuclear warheads down with it. The incident was not included on the list of missing nukes because the U.S. government found the wreck and knows exactly where it is, though it has not recovered the weapons there. The U.S. government and the Woods Hole Oceanographic Institution have not detected contamination in its periodic monitoring of the wreck site.



An August, 1986 view of the bow section of the nuclear-powered attack submarine USS Scorpion (SSN-589) where it rests on the ocean floor, 10,000 feet down and 400 miles southwest of the Azores. The bow carried nuclear weapons at the time the submarine was lost. (U.S. Navy)

As bad as accidents like the ones in the Philippine Sea and the Atlantic sound, they pale in comparison to some of the mistakes made by the Soviet Union. For example, about 600 miles northeast of Bermuda, under 18,000 feet of seawater, there lies a Soviet Yankee I class nuclear-powered missile submarine that suffered an explosion and fire in one of its missile tubes on October 3, 1986. The submarine sank three

days later carrying 34 nuclear warheads. U.S. forces detected no radioactivity in the air or water around the submarine, but that incident alone accounts for more missing warheads than in this entire list of missing U.S. weapons.
Still, just because the U.S. has a pretty good record now does not mean an accident can't happen tomorrow. For example, in February 2009, a British nuclear-powered missile submarines carrying nuclear warheads collided with a French submarine also carrying nuclear warheads in the eastern Atlantic Ocean. Though there were no casualties or contamination, it goes to show that the better part of nuclear warfare is just trying not to blow yourself up.
"It's a reminder that these weapons are still out there and accidents can happen," Kristensen said.

David Roza covers the Air Force, Space Force, and anything Star Wars-related. He joined Task & Purpose in 2019, after covering local news in Maine and FDA policy in Washington D.C. David loves hearing the stories of individual airmen and their families and sharing the human side of America's most tech-heavy military branch.

International Day against Nuclear Tests

Source: https://web.statetimes.in/international-day-against-nuclear-tests/

August 29 is observed as an International Day against Nuclear Tests.
In order to respect victims of the past and to remind the world of the persisting threat nuclear tests pose to the environment and international stability. More than 2,000 nuclear tests have been conducted over the past seven decades – from the South Pacific to North America, from Central Asia to North Africa. They have harmed some of the world's most vulnerable peoples and pristine ecosystems. Nuclear Weapons started around the 1830s in countries like the United States, United Kingdom, and Canada during World War II. For the past 20 years Nuclear Weapons have been in our lives, they were the weapons we used to fight our enemies and also protect our homeland. Nuclear weapons are a form of mass destruction that has explosive power that comes from nuclear action. The first nuclear test was conducted by the United States, on July 16th, 1945, three weeks before the Hiroshima bombing on the 6th of August 1945. The nuclear test was given the codename 'Trinity', tested on the 'Trinity Site'. The largest nuclear bomb ever tested was the 'Tsar Bomba' by the Soviet Union at Novaya Zemlya, with an estimated yield of 50 megatons. It was so powerful it was said that the shockwave produced went around the world three times. Nuclear weapons continue to present a real threat to humanity and other life on Earth. Scholars of international relations and policymakers share the belief that the sheer power and destructiveness of nuclear weapons prevent them from being used by friends and foes alike. Nuclear weapons are not needed, and have not been, for years. While nuclear weapons have influenced politics, public opinion and defense budget, they have not had a significant impact on world affairs since World War II.
Nuclear weapons are weapons of great destruction. Nuclear weapons pose serious health risks to those around them. India had conducted its first nuclear test at the same site in 1974. India's nuclear programme began in 1948 and since then it has covered a very long and significant ground. India's security concerns and nuclear environment compelled it to make these tests after a lapse of about a quarter century. Two nuclear bombs were dropped on Japan which eventually ended the Pacific War. After this attack the Soviet Union started to develop their own atomic bomb project. Both Germany and the Soviet Union had more powerful weapons known as the hydrogen bomb. Hydrogen bombs are bombs that have destructive power that comes from the rapid release of energy and uses an atomic bomb as its trigger. History has shown terrifying and tragic effects of nuclear weapons testing, especially when controlled conditions go awry, and in light of the far more powerful and destructive nuclear weapons that exist today. There is no other weapon that causes such harm to the environment and humanity as a nuclear weapon.
The nuclear path will lead us to a point of no return from the nuclear night and nuclear winter lasting a thousand years. We may be divided. But peace and friendship are the only alternative for the survival of the civilization. A famous saying goes might is always right. This is what exactly so-called developed nations want rest of the world to do. Every country has the right and should defend its territory by hook or by crook. The obstacles to disarmament are formidable. Concerns over nuclear weapons' costs and inherent dangers have led to a global outpouring of ideas to breathe new life into nuclear disarmament. Among the negative sides of nuclear weapons is their maintenance and construction cost. Unlike other kinds of weapon, ownership of nuclear weapons can have a negative impact on the national budget. The question of whether countries should be allowed to have nuclear weapons is still under discussion and requires a solution to be found as soon as possible.

EDITOR'S COMMENT: All these "International Days" have a direct effect on my digestive system! Is it only me or do you feel the same thing? I wish I had the chance to ask Kim Jong Un about this issue.

The story behind the Vatican's colossal sculpture of Jesus rising from nuclear destruction

Source: https://www.americamagazine.org/arts-culture/2022/08/29/fazzini-resurrection-sculture-vatican-243642

Pope Francis meets with students and faculty of Romeís LUMSA University Nov. 14, 2019, in the Vatican's Paul VI audience hall. (CNS photo/Vatican Media)

Aug 29 – Last week, Twitter users across the world made a startling discovery: A viral photo of the Vatican's Paul VI audience hall revealed a colossal, looming sculpture that frames the pope during his addresses.

The sculptor Pericle Fazzini designed the piece, "The Resurrection," to represent Jesus ascending from the explosion of a nuclear bomb. It measures an enormous 66 feet by 23 feet by 10 feet. The wilted bronze color gives the piece a feeling of sickness and decay, while the misshapen knots around Christ's feet evoke images of dismembered hands and skulls.

Commissioned in 1970 and inaugurated in 1977, "The Resurrection" comes from an era of widespread fear of nuclear annihilation, of duck-and-cover drills and neighborhood fallout shelters. Then and today, leaders in the Catholic Church have stated in clearest terms their opposition to nuclear weapons.

Pope John XXIII opened the Second Vatican Council only days before the Cuban Missile Crisis began. His relatively brief papacy was marked with impassioned statements against the use of nuclear weapons, including a call for peace over the radio to the U.S. and Soviet Union on Oct. 25, 1962, as Pope Francis mentioned in a 2013 address.

"With your hand on your conscience may each one hear the anguished cry which is raised to the skies from all parts of the earth, from the innocent children to the elderly, from the people of the communities: Peace, peace!" Pope John XXIII famously said in that address.

It was only a few months later that he issued the encyclical "Pacem in Terris," which expressly condemned the use and possession of nuclear bombs.

"Hence justice, right reason, and the recognition of man's dignity cry out insistently for a cessation to the arms race. The stock-piles of armaments which have been built up in various countries must be reduced all round and simultaneously by the parties concerned. Nuclear weapons must be banned," he wrote.

It was John XXIII's successor, Pope Paul VI, who commissioned Fazzini's "Resurrection." The commission was under debate for seven years, according to the Vatican Museum's website, and only became official after the pope's "personal intervention." It has stood behind each pontiff when using the Paul VI audience hall since.

Catholic anti-nuclear activism has continued to develop since then. Three years after the sculpture's completion, a group of Catholic activists called the Plowshares Eight entered a General Electric factory in King of Prussia, Pa., to protest the company's work on nuclear weapons. They poured blood on parts for nuclear warheads and damaged them with hammers. All were arrested quickly.

Carl Kabat, O.M.I., who passed away earlier this month, was a member of that original group. He told **America** in 1981 that he took his calling for civil disobedience straight from the Bible.

"Christ broke the law. He overturned the tables of the moneychangers and took charge of the temple. He cured on the Sabbath, He plucked grain on the Sabbath," Father Kabat said.

The Plowshares movement has grown into a network of protestors, Catholic and non-Catholic, fighting the allocation of funds for weapons of mass destruction rather than care of the poor. They take their name Isaiah's call for nations to "beat their swords into plowshares" for food production (Is 2:4).

"When the state puts such resources into weapons of destruction, it's a healthy thing for Christians to be in trouble with the state," Father Kabat said from a jail cell in 1979.

Civil disobedience has remained the primary weapon used by the anti-nuclear movement. Martha Hennessy, anti-nuclear activist and granddaughter of Dorothy Day, spent five months in federal prison from December 2020 to May 2021 for participation in a Plowshares protest in Kings Bay, N.Y.

"We are not to commit murder, nevermind mass murder with these modern weapons. And the promotion of peace is certainly part of what we are called to do," she said in an interview over the phone.

Ms. Hennessy said that the public has grown used to the existence of nuclear weapons, and she fears that many have become apathetic to it.

"I do believe that the rhetoric and the language now is trying to soften us up for accepting limited nuclear engagement, which is all a fallacy," she said. "It's all, as Dorothy called it, psychological warfare."

She said in an email that she feels "conflicted" over the imagery of Fazzini's sculpture, wondering whether it makes us more aware of the horrors of nuclear annihilation or actually desensitizes us.

In her official 2018 court declaration, Ms. Hennessy quoted extensively from the "Compendium of the Social Doctrine of the Church," the Gospels and various documents by Pope Francis. She said she believes that church teachings are quite clear in their zero-tolerance for nuclear weapons and the military-industrial complex.
Pope Francis affirmed as recently as June of this year that "the use of nuclear weapons, as well as their mere possession, is immoral." The risk to the environment and the divestment from the poor that nuclear weapons represent have been substantial points of his platform.
So although many on Twitter compared "The Resurrection" to the setting of a video game boss battle, the sculpture does act as a reminder of 80-year history of Catholic responses to the threat of nuclear war.

Zaporozhye Nuclear Power Plant 'terrorist plot' foiled

Source (**video**): https://rumble.com/v1i31wr-zaporozhye-nuclear-power-plant-terrorist-plot-foiled.html

Aug 31 – A group of Ukrainian saboteurs preparing a terrorist attack on the Zaporizhzhia Nuclear Power Plant were taken into custody in Energodar. The men reportedly had information about the characteristics of the plant and could have attacked the least protected part. The alleged video of the special operation shows that saboteurs used foreign satellite systems for communication and were fully armed.

EDITOR'S COMMENT: Can you identify the weapons on the left and the source coming from? Sure you can!

UAMS Receives $3.4 Million to Study Radiation Injuries Caused by Nuclear Accidents and Bioterrorism

Source: https://news.uams.edu/2022/08/24/uams-receives-3-4-million-to-study-radiation-injuries-caused-by-nuclear-accidents-and-bioterrorism/

Aug 24 – The University of Arkansas for Medical Sciences (UAMS) has received $3.4 million in funding from the National Institute of Allergy and Infectious Diseases, part of the National Institutes of Health, to study acute and delayed injuries caused by full-body radiation exposure from a nuclear accident or bioterrorism.

The five-year study entitled, "Platelets in Radiation-induced Immune Dysregulation," is led by Rupak Pathak, Ph.D., assistant professor of Pharmaceutical Sciences, Division of Radiation Health in the UAMS College of Pharmacy; Martin Cannon, Ph.D., professor of Microbiology and Immunology in the UAMS College of Medicine; and Jerry Ware, Ph.D., professor of Physiology and Cell Biology in the UAMS College of Medicine. While the FDA has approved some drugs to alleviate bone marrow injuries in people exposed to radiation, no drugs are available to treat the adverse effects in other organ systems. The study hopes to encourage drug development for therapies that will reduce radiation side effects.

"Research is greatly needed to understand the complex biology that occurs following radiation exposure," said Pathak. "This work will identify therapeutic targets to minimize radiation sickness following exposure to high levels of radiation. If there is something we can apply after exposure that will prevent immune dysfunction, we have a good chance of limiting injuries in several organs. We think we can find such countermeasures by studying how platelets moderate immune response." Platelets, which help form blood clots or stop bleeding, also regulate immune function by binding directly to immune cells or releasing small particles, called platelet-derived micro-particles. Preliminary studies have shown links between radiation exposure, platelets and the immune response.

"We know that platelets have a couple of pathways that might influence radiation damage," said Cannon. "We want to understand how to regulate those pathways and lessen the inflammatory response. In very simple terms, we're looking for the on and off switch."

Radiation-induced immune damage often causes injury to the heart and intestine. The team, led by Pathak, will study if damage can be reduced or blocked in these organs by modifying the functions of immune cells or platelets, or by altering platelet-immune cells interaction.

EDITOR'S COMMENT: $3.4 million to study radiation injuries? It seems that Hiroshima, Nagasaki, Chernobyl, and Fukushima were not enough to provide all the info required for new drugs if those available are not sufficient enough. It reminds me of the EU research projects on CBRN issues that are an epitome of repetition and overlapping but keep researchers happy.

Russia's Stranglehold on the World's Nuclear Power Cycle

By Kristyna Foltynova

Source: https://www.homelandsecuritynewswire.com/dr20220901-russias-stranglehold-on-the-worlds-nuclear-power-cycle

Sept 01 – Since Russia invaded Ukraine on February 24, several packages of sanctions targeting Russia's lucrative energy industry (mostly oil, gas, and coal) have been introduced by the United States, the European Union, and other Western nations. These countries are also undertaking efforts to wean themselves off their dependency on Russian energy supplies.

After shelling occurred near Ukraine's Zaporizhzhya power plant, Ukrainian President Volodymyr Zelenskiy called on the international community to come up with a stronger response and ban Russian imports from yet another sector: nuclear power. But blocking and replacing Russia's deliveries of uranium, reactors, and nuclear technology to the rest of the world is easier said than done.

Here's how Russia plays a crucial role in the world's nuclear cycle.

It's Not Just About Mining

Russia is among the five countries with the world's largest uranium resources. It is estimated to have about 486,000 tons of uranium, the equivalent of 8 percent of global supply. Yet, the country is a relatively small producer of raw uranium. In 2021, it produced just about 5 percent of the world's uranium from mines. However, uranium mining is just one piece of the nuclear process. Raw uranium is not suitable as fuel for nuclear plants. It needs to be refined into uranium concentrate, converted into gas, and then enriched. And this is where Russia excels.

In 2020, there were just four conversion plants operating commercially — in Canada, China, France, and Russia. Russia was the largest player, with almost 40 percent of the total uranium conversion infrastructure in the world, and therefore produced the largest share of uranium in gaseous form (called uranium hexafluoride). The same goes for uranium enrichment, the next step in the nuclear cycle.

According to 2018 data (the latest available), that capacity was spread among a handful of key players, with Russia once again responsible for the largest share — about 46 percent.
Therefore, Russia is a significant supplier of both uranium and uranium enrichment services. According to the latest available data, the European Union purchased about 20 percent of its natural uranium and 26 percent of its enrichment services from Russia in 2020. The United States imported about 14 percent of its uranium and 28 percent of all enrichment services from Russia in 2021.

Did Someone Say Nuclear Reactors?
Nuclear reactors made in Russia are known as VVER — an abbreviation for the Russian vodo-vodyanoi enyergeticheskiy reactor (water-water energetic reactor). These reactors use water both as a coolant and as a moderator and were originally developed in the Soviet Union. There are several versions of VVERs (such as the VVER-440 and VVER-1000), with the volume of power being one of the significant differences. Currently, there are 11 countries where various types of VVERs are operating, including Bulgaria, the Czech Republic, Hungary, and Finland. On top of that, other countries such as Egypt, Turkey, and Argentina currently have these reactors under construction or plan to build them. Russia is considered the world leader when it comes to the export of nuclear plant development. Between 2012 and 2021, Rosatom initiated construction of 19 nuclear reactors; 15 of these were initiated abroad. That is far more than the next most prolific providers: China, France, and South Korea. Although China started building 29 reactors during the same period, only two of them were initiated abroad. France started building two reactors abroad, and South Korea four.

Don't Forget the Fuel
To keep the reactors operating, plants need a regular supply of nuclear fuel — usually a certain type of fuel. And this is where another level of dependency on Russia can be observed. Although there are several suppliers on the market, the Russian TVEL Fuel Company is currently the only authorized supplier of fuel needed for VVER-440s. Therefore, certain countries rely on Russian deliveries and could risk temporarily halting operations at their facilities. For example, Slovakia has four of these nuclear reactors; the Czech Republic has two. Westinghouse, an U.S. nuclear power company, is already seeking ways to offer alternative fuel in Europe, but it will take some time to get all the licenses and approvals. In addition, there are concerns that fuel from the United States might be more expensive, and it is unclear how Westinghouse would handle the waste-management system.
Russia is also able to supply high-assay low-enriched uranium (also known as HALEU). It is a type of fuel that will be needed for more advanced reactors that are now under development by many companies across the United States. The main difference from the fuel that is currently being used is the level of uranium enrichment. Instead of up to 5 percent uranium-235 enrichment, the new generation of reactors needs fuel with up to 20 percent enrichment. According to the American Office of Nuclear Energy, HALEU availability is crucial for the development and deployment of reactors. The fuel is now available in the United States in limited quantities, and Washington is seeking options to fund research and development of new fuel sources. At the moment, the only supplier able to provide the fuel on a commercial scale is Russia's Tenex (owned by the Russian state-owned company Rosatom).

Looking for New Markets
Selling nuclear technology is also part of Russia's effort to gain influence and reap profits in countries that are new to nuclear energy. One of the reasons countries want to cooperate with Russia is that it offers a "whole package" solution. Russia can not only build a nuclear plant and supply fuel, but it also trains local specialists, helps with safety questions, runs scholarship programs, and disposes of radioactive waste. However, offering attractive loans is probably Russia's most powerful tool. These loans are usually backed by government subsidies and cover at least 80 percent of construction costs. For example, Russia has already lent $10 billion to Hungary, $11 billion to Bangladesh, and $25 billion to Egypt — all to build nuclear power plants. Russia has operating nuclear reactors in 11 countries, and more are under construction or being planned. Besides that, Russia has also signed either memorandums of understanding or intergovernmental agreements with at least 30 countries around the world, mostly in Africa. These serve as a declaration of interest in nuclear technology or set an intention to cooperate on the building of nuclear plants, respectively. Some experts warn that African countries might not be ready for nuclear power, but Russia argues that the technology represents an answer to the continent's increasing demand for electricity. It is also worth noting that African countries represent the largest voting bloc in the United Nations, which might be another reason for Russia to strengthen its ties in the region.
On August 27, Budapest confirmed that Russia's Rosatom will start building two new nuclear reactors in Hungary. This information came amid mutual accusations by Ukraine and Russia of shelling Ukraine's Zaporizhzhya nuclear plant. Zelenskiy has warned of the threat of a radiation leak and accused Russia of "nuclear blackmail." Meanwhile, Russia blocked the adoption of a final document after a monthlong UN review of the Nuclear Non-Proliferation Treaty, saying it lacked "balance" amid its criticism of Russia's occupation of Zaporizhzhya.

Kristyna Foltynova is a data and visual journalist in *RFE/RL*'s Central Newsroom.

Prometheus in Tokyo!

The Prometheus statue in Tokyo is located outside the offices of oil company JX Holdings near Nihombashi subway station. Prometheus[1] gave hope to man and indeed the word "hope" is mentioned on the base of the statue in Tokyo! In Japan, many people refer to nuclear power as a "second fire" and after the nuclear accident in Fukushima the word hope took on a special meaning.

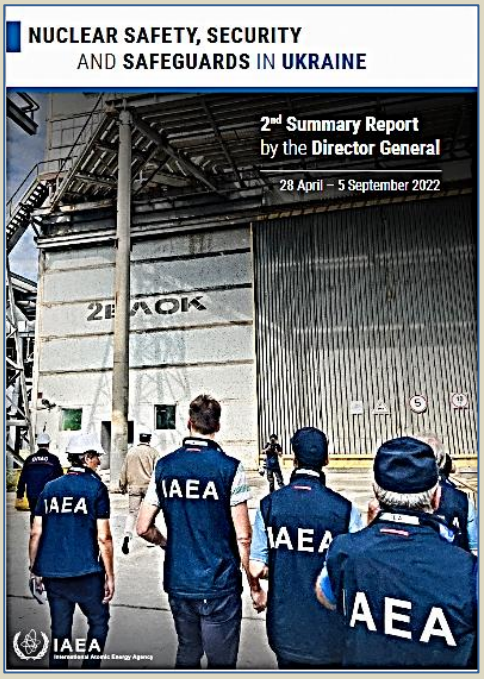
[1] Prometheus was one of the Titans in ancient Greek mythology, who according to the myth gave fire to man, which he stole from the god Hephaestus. When Zeus made Pandora, the cause of all evil for man, and decided to make a flood to punish the people, Prometheus informs Deucalion (son of his brother Epimetheus) and urges him to build an ark. Indeed, when the cataclysm occurred, Deucalion was saved with his wife Pyrrha, who created the Genos of Heroes (fourth gen) and humanity.

Ukraine: Briefing on the Zaporizhzhia Nuclear Power Plant

Source: https://www.securitycouncilreport.org/whatsinblue/2022/09/ukraine-briefing-on-the-zaporizhzhia-nuclear-power-plant.php

This afternoon (6 September), the Security Council will hold an open briefing on the situation in Ukraine under the agenda item "threats to international peace and security". The meeting, which was requested by Russia, is expected to focus on the situation at the Zaporizhzhia Nuclear Power Plant (ZNPP) in the city of Enerhodar. Secretary-General António Guterres and International Atomic Energy Agency (IAEA) Director General Rafael Grossi are expected to brief. Germany and Ukraine are expected to participate under rule 37 of the Council's provisional rules of procedure.

This will be the Council's third meeting on the ZNPP, following meetings on the matter on 11 and 23 August, both of which were requested by Russia. (For more information, see our 11 August and 23 August *What's in Blue* stories.) The ZNPP, which is the largest nuclear power station in Europe, had provided 30 percent of Ukraine's electricity prior to Russia's invasion in February. Russian forces have had control over the ZNPP since March, while Ukrainian technicians continue to operate the facility. In recent weeks, shelling around the site—for which both Ukraine and Russia blame each other—has raised concerns about a possible catastrophe.



At today's meeting, Grossi is expected to describe the findings of the IAEA's 1 September visit to the ZNPP. The visit by the 14-member team of IAEA experts was negotiated for several weeks, amid a lack of agreement between Russia and Ukraine on the modalities for such a visit and precarious security conditions around the plant. Speaking to reporters on 2 September, Grossi said that none of what the agency refers to as the seven pillars of nuclear safety—which include physical integrity, reliable external power, and availability of spare parts—are intact at the ZNPP. He noted that the plant's physical integrity has been "violated several times", adding that most of the damage to the ZNPP occurred during shelling in August. Grossi warned that the gravest risk to the ZNPP is physical damage to equipment, from shelling, that could lead to a release of radiation, adding that disruptions in external power to cool reactor cores could lead to a meltdown.

The IAEA released a report today (6 September) about the nuclear safety, security and safeguards situation at several nuclear facilities in Ukraine, which includes an overview of the findings of the IAEA's 1 September visit. The report determines that although the ongoing shelling around the ZNPP "has not yet triggered a nuclear emergency", it continues to "represent a constant threat to nuclear safety and security with potential impact on critical safety functions that may lead to radiological consequences with great safety significance". It calls for the immediate cessation of shelling of the site and in its vicinity and says that to facilitate the plant's secure and safe operations, all relevant parties need to agree on the establishment of "a nuclear safety and security protection zone around the ZNPP". In the report, the IAEA expresses its readiness to start consultations with the sides on the establishment of such a protection zone.

Since the 1 September visit, two IAEA experts have remained at the ZNPP as part of the IAEA Support and Assistance Mission to Zaporizhzhia (ISAMZ). The ISAMZ will "assess the physical damage to the plant's facilities, determine the functionality of the main and back-up safety and security systems and evaluate the staff's working conditions, in addition to performing urgent safeguards activities on the site", according to the IAEA. Grossi highlighted the importance of the IAEA's continued presence at the site, noting that it will help provide an impartial assessment when issues arise at the plant. In a 3 September statement, Grossi underscored his ongoing concern about the situation at the ZNPP, while adding that the IAEA's presence "will be of paramount importance in helping to stabilise the situation". Grossi may reiterate these messages at today's meeting, while emphasising the need to demilitarise the area around the ZNPP to facilitate the IAEA's continued presence there.

At today's meeting, Grossi may also provide an update about recent security incidents at the plant. Shelling around the ZNPP has continued despite the ISAMZ's presence, and yesterday (5 September) led to an outbreak of fire in the plant. Previous shelling has damaged the plant's connection to four high-voltage external power lines, forcing it to rely on a lower-voltage reserve line to power the cooling equipment needed to prevent meltdowns. As a result of yesterday's fire, the reserve power line was disconnected, leading to the plant's disconnection from Ukraine's national power grid. According to the IAEA, the reserve line was not damaged in the fire and will be re-connected once the fire is extinguished. It added that the "ZNPP continues to receive the electricity it needs for safety from its sole

operating reactor". At the time of writing, it was unclear whether the fire was extinguished and when the reserve power line would be reconnected.
Council members are likely to express a common position on the importance of ensuring the safety of the ZNPP. However, they will present diverging opinions about which side is responsible for instigating attacks in and around the site. The US and European Council members are expected to condemn the seizure of Ukrainian nuclear facilities by Russian forces and to call on Moscow to hand back control of the ZNPP to Ukraine. Ukraine and its allies have accused Russia of deploying heavy weaponry at the site and using it as a staging ground to launch attacks against Ukraine, knowing that the latter will not fire back out of fear of risking the integrity of the plant. Moscow has denied such allegations and blamed Kyiv for attempting to recapture the area by force—claims that Ukraine has denied.
The issue of the IAEA's presence at the ZNPP is also likely to be discussed at today's meeting. Several members may express support for a permanent presence of the ISAMZ at the site. These members may seek further information from Grossi about the necessary security conditions to facilitate this presence.

Nuclear Notebook: How many nuclear weapons does North Korea have in 2022?

By Hans M. Kristensen and Matt Korda
Source: https://thebulletin.org/premium/2022-09/nuclear-notebook-how-many-nuclear-weapons-does-north-korea-have-in-2022/

The Hwasong-17 ICBM was first displayed on an 11-axle transporter erector-launcher (TEL) at the October 2020 parade in Pyongyang. North Korea claimed to have successfully launched the missile on March 24, 2022; however, independent analysis subsequently assessed that the missile may have been tested on March 16 instead and ended in a failure. (Image: North Korean government).

Sep 08 – North Korea has made significant advances over the past two decades in developing a nuclear weapons arsenal. It has detonated six nuclear devices—one with a yield of well over 100 kilotons—and test-flown a variety of new ballistic missiles, several of which may be capable of delivering a nuclear warhead to targets in Northeast Asia and potentially in the United States and Europe. However, there is considerable uncertainty about which of North Korea's missiles have been fielded with an active operational nuclear capability.
It is widely assumed that North Korea has operational nuclear warheads for its short-range and medium-range missiles. However, it is unclear whether it has managed to develop fully functioning nuclear warheads that can be delivered by intercontinental ballistic missiles and, following violent atmospheric re-entry, detonate as planned. That said, even though North Korea has not yet publicly demonstrated a capability to deliver a functioning nuclear re-entry vehicle on a long-range ballistic missile does not necessarily indicate that it is not working on developing one or could not field one without publicly demonstrating it. It is clear from its development

efforts and public statements that North Korea ultimately intends to field an operational nuclear arsenal capable of holding regional and US targets at risk.

In 2021, Kim Jong-un announced several key strategic goals for North Korea's nuclear weapons program, including (1) "push[ing] ahead with the production of super-sized nuclear warheads;" (2) "mak[ing] nuclear weapons smaller and lighter for more tactical uses;" (3) "raising the rate of precision good enough to strike and annihilate any strategic targets within a range of 15,000 kilometres [about 9,320 miles] with pinpoint accuracy;" (4) "develop[ing] and introduc[ing] hypersonic gliding flight warheads in a short period;" (5) "push[ing] ahead with the development of solid-fuel engine-propelled intercontinental, underwater, and ground ballistic rock- ets as scheduled;" and (6) "possess[ing] a nuclear-powered submarine and an underwater-launch nuclear strategic weapon" (Korean Central News Agency 2021).

These strategic goals were introduced in the context of a proposed five-year plan, and North Korea already appears to have made significant progress within its first year-and-a-half of implementation.

Due to the lack of clarity surrounding North Korea's nuclear program, agencies and officials of the US intelligence community, as well as military commanders and nongovernmental experts, struggle to assess the program's characteristics and capabilities. As a result, this paper relies upon publicly available information and satellite imagery about North Korea's fissile material production, nuclear posture, and delivery vehicle development, and uses multiple sources of data whenever possible to corroborate conclusions. We cautiously estimate that North Korea might have produced sufficient fissile material to build 45 to 55 nuclear weapons and might have assembled 20 to 30 warheads for delivery primarily by medium-range ballistic missiles—a small increase since our last report in July 2021 (Kristensen and Korda 2021).

North Korea's nuclear policy

For decades, North Korea has made numerous statements about its nuclear weapons policy and signals laying out its nuclear doctrine if deterrence fails. In 1997, a former North Korean official in the Ministry of Foreign Affairs testified before the US Senate that:

"as early as 1965, Kim Il-sung had said that North Korea should develop rockets and missiles to hit U.S. forces inside Japan. And regarding the U.S. forces inside South Korea [. . .] it is a well-known fact that North Korea will use short-range missiles and other missiles and rockets in order to have casualties of somewhere between 10,000 to 20,000, and even more casualties in the side of U.S. forces in order to have anti-war sentiments to rise inside the United States and cause the withdrawal of U.S. forces in the time of war" (Young-Hwan 1997).

The 2013 "Law on Consolidating the Position of Nuclear Weapons State"—one of the most recent official documents pertaining to North Korea's nuclear doctrine—suggests a similar goal, noting that North Korea's nuclear arsenal would only be used "to repel invasion or attack from a hostile nuclear weapons state and make retaliatory strikes" (Korean Central News Agency 2013). This doctrine would appear to bear similarities to Pakistan's nuclear doctrine, which emphasizes using tactical nuclear weapons at the outset of a conflict to repel a superior Indian conventional invasion force (Kidwai Lt. Gen. (Ret.) Khalid 2020). More recently, North Korea's declared aspirational development of new types of tactical nuclear delivery systems appears intended to strengthen its regional deterrence posture (National Committee on North Korea 2021; Korean Central News Agency 2022). Some experts have suggested that such a posture might involve some degree of pre-delegating nuclear launch authority down the chain of command (Narang and Panda 2017; *38 North* 2022). But North Korea's nuclear command and control system is largely unknown, and it is unclear whether North Korea's leader, Kim Jong-un, would be comfortable with handing over control of nuclear weapons to the military.

Increased focus on tactical nuclear weapons—certainly pre-delegation of launch authority—would appear to dilute the country's no-first-use policy, which was officially declared following North Korea's fourth nuclear test in 2016. Since then, North Korea has added a caveat to its policy by suggesting that it would not "be the first to use nuclear weapons [. . .] as long as the hostile forces for aggression do not encroach upon its sovereignty" (Korean Central News Agency 2016a). Subsequent statements have also included such caveats; during the 75th anniversary of the ruling Korean Workers' Party in October 2020, Kim Jong-un stated that North Korea's nuclear deterrent "will never be used preemptively. But if, and if [sic], any forces infringe upon the security of our state and attempt to have recourse to military force against us, I will enlist all our most powerful offensive strength in advance to punish them" (*38 North* 2020).

Occasionally, North Korea—also known as the Democratic People's Republic of North Korea, or DPRK—has explicitly mentioned or signaled which targets it intends to hit in the event of imminent invasion. A 2016 statement by the Supreme Command of the Korean People's Army stated that the country would first target South Korea's Blue House (its seat of government), then "the U.S. imperialist aggressor forces' bases for invading the DPRK in the Asia-Pacific region and the U.S. mainland," in that order (Korean Central News Agency 2016b). The statement does not explicitly mention nuclear use; however, it is strongly implied that nuclear weapons would be used for at least the second wave of attacks against targets related to the US/South Korea's conventional

invasion force. More recently, the January 2021 report of the 8th Congress of the Workers' Party of Korea noted the goal of "making a preemptive and retaliatory nuclear strike by further raising the rate of precision good enough to strike and annihilate any strategic targets within a range of 15,000 kilometers [9,320 miles] with pinpoint accuracy" (National Committee on North Korea 2021). In this context, nuclear use (or the threat of nuclear use) with shorter- range missiles could potentially be used to "decouple" US military support from its regional allies in the Asia-Pacific region, by withholding strikes on US homeland targets during nuclear attacks on regional targets. Whether North Korea's nuclear posture is advanced enough to support such a complex strategy is unknown.
At various times, North Korea has also threatened to launch nuclear weapons in response to more minor provocations, such as joint US-South Korean military exercises (Ellyatt 2016). However, despite these occasional inflammatory statements, it is highly likely that North Korea—as with other nuclear-armed states—would only use its nuclear weapons in extreme circumstances, particularly if the continued existence of the North Korean state and its political leadership were in jeopardy.

Fissile material and warhead estimates

Plutonium production

North Korea produces plutonium at its five megawatt-electric (MWe) graphite-moderated nuclear reactor, located at the Yongbyon Nuclear Scientific Research Center in North Pyongan province. Between December 2018 and July 2021, the reactor appeared to not be operational; however, in July 2021 the International Atomic Energy Agency (IAEA) noted the intermittent discharge of cooling water from the reactor and subsequent steam plumes from the reactor's hall, signatures which would be consistent with the operation of the reactor (International Atomic Energy Agency 2021; Pabian, Town, and Liu 2021). Satellite imagery indicates that the 5 MWe reactor is likely to still be operational as of May 2022 (Makowsky, Heinonen, and Liu 2022a).
In its August 2021 annual report, the IAEA concluded that the Yongbyon complex's thermal plant—which supplies steam to the radiochemical laboratory used for plutonium reprocessing—operated for approximately five months, from mid-February 2021 until early July 2021, after a multi-year hiatus (International Atomic Energy Agency 2021). The IAEA noted that this timeframe was consistent with the time required to reprocess a complete core of irradiated fuel. In March 2022, a United Nations Panel of Experts report noted that a "Member State assessed that the Democratic People's Republic of Korea may have reprocessed spent fuel rods, although the Panel has been unable to verify this assessment" (United Nations 2022); additionally, as of mid-2022 independent analysts had not yet observed indications that the core had been discharged (Heinonen, Makowsky, and Liu 2022).
Since 2010, North Korea has also been in the process of constructing an experimental light water reactor and in recent years has begun transferring major reactor components into the facility at Yongbyon. The IAEA reported that North Korea may have conducted infrastructure tests of the experimental light water reactor's cooling system throughout 2020 and 2021; however, the report noted that "it is not possible to estimate when the reactor could become operational" (International Atomic Energy Agency 2021). Independent analysts from *38 North* have reported the construction of new buildings at the reactor complex throughout 2021 and 2022, including a cooling water pump house, electric switchyards, and an assortment of smaller buildings (Makowsky, Heinonen, and Liu 2022a; Heinonen, Makowsky, and Liu 2022). Although this reactor appears to be designed for civilian electricity production, it would also have a latent capacity to produce weapons-grade plutonium or tritium that could be used for North Korea's nuclear weapons program.
In May 2022, independent analysts from the James Martin Center for Nonproliferation Studies noted the possible resumption of construction at North Korea's long-dormant 50 MWe reactor, which had been paused since 1994. In particular, the analysts noted that North Korea appeared to be connecting the reactor's secondary cooling loop to a pumphouse, suggesting that they planned to eventually complete the reactor (Lewis, Pollack, and Schmerler 2022). The analysts concluded that, upon completion, the reactor could theoretically produce approximately 55 kilograms of plutonium per year, enough to potentially produce about a dozen new nuclear weapons per year, depending on the design of the warhead (Lewis, Pollack, and Schmerler 2022). However, analysts from *38 North* subsequently noted that similar construction efforts at the 50 MWe site are not uncommon and that the recent trenching activity could be intended to service a nearby underground facility that is unrelated to the reactor itself (Makowsky et al. 2022). Given these uncertainties, it remains unclear whether North Korea has indeed restarted construction on the 50 MWe reactor; given the state of the reactor's apparent disrepair, doing so would likely take several years to complete (Hecker 2010).
In April 2021, former Los Alamos National Laboratory director, Siegfried Hecker, who was given unprecedented access to North Korean nuclear facilities over several years, estimated that North Korea had a plutonium inventory in the range of 25 to 48 kilograms and could produce up to six kilograms (13 pounds) per year at full operation (*38 North* 2021).

Uranium enrichment

It is much more difficult to assess the state of North Korea's uranium enrichment operations because the footprint of these facilities is significantly smaller and harder to detect than plutonium production facilities. North Korea produces yellowcake—a type of uranium concentrate powder that, once converted and enriched, is used in reactor fuel—at the Nam-chon Chemical Complex in Pyongsan (Bermudez, Cha, and

Jun 2021). North Korea has only declared a single uranium enrichment facility—the Yongbyon Nuclear Fuel Rod Fabrication Plant, which is estimated to have approximately 4,000 centrifuges. This facility was in regular operation throughout 2021, as plumes of steam could be observed through satellite imagery throughout the year, in addition to the presence of what may have been a liquid nitrogen tank trailer on-site [1] (United Nations 2021a, 2022). Analysts from the James Martin Center for Nonproliferation Studies also noted in September 2021 that North Korea was expanding the size of its uranium enrichment plant to potentially accommodate approximately 1,000 additional centrifuges, which would increase the plant's overall capacity by 25 percent (Lewis, Pollack, and Schmerler 2021).

It is widely believed that North Korea has at least one additional centrifuge facility outside of the known Yongbyon complex. In May 2018, a *Washington Post* article first reported the existence of a potential covert uranium enrichment site at Kangson, just outside of Pyongyang, citing work by the Institute for Science and International Security (Warrick and Mekhennet 2018). In July 2018, a team of researchers from *The Diplomat* and the James Martin Center for Nonproliferation Studies identified a complex at Kangson as the centrifuge facility's suspected location (Panda 2018). A subsequent *Washington Post* article indicated that "there is a broad consensus among US intelligence agencies that Kangson is one of at least two secret enrichment plants" (Nakashima and Warrick 2018). In September 2020, the IAEA suggested that "[i]f the Kangson complex is a centrifuge enrichment facility this would be consistent with the agency's assessed chronology of the development of [North Korea's] reported uranium enrichment programme" (International Atomic Energy Agency 2020, 5). However, recent independent analysis has raised doubts about the nature of the Kangson complex, suggesting that the site might instead be used to manufacture components for centrifuges (*38 North* 2021; Heinonen 2020). Without more detailed public information or access to the site itself, it is not possible to confirm the nature of the Kangson site nor its potential role in North Korea's nuclear weapons program. In 2022, the United Nations Panel of Experts listed Kangson as a "suspected clandestine uranium enrichment facility" and noted continuous vehicular and construction activities since July 2021 (United Nations 2022).

Given the uncertainties around activities at the Kangson site, it is unclear how much highly-enriched uranium (HEU) North Korea has produced; yet, this amount is known to be growing. Siegfried Hecker estimated in early 2021 that North Korea possibly had produced 600 to 950 kilograms (1,323 to 2,094 pounds) of HEU as of the end of 2020 (*38 North* 2021). An assessment by the Stockholm International Peace Research Institute suggests a wider range of possibly 230 to 1,180 kilograms (507 to 2,601 pounds) as of the beginning of 2021 (Kütt, Mian, and Podvig 2022, 426), whereas the International Panel on Fissile Materials estimated a slightly smaller range of 400 to 1,000 kilo- grams (882 to 2,205 pounds) in 2022 (International Panel on Fissile Materials 2022).

Warhead estimates

A common mistake in public discussions about North Korea's nuclear capabilities is to equate the amount of fissile material produced with the number of nuclear weapons built. But, for a given amount of fissile material, the number of nuclear weapons will depend on the weapon design and the number and types of launchers that can deliver them. According to estimates, North Korea may have built several nuclear weapons that are likely smaller than its amount of fissile material suggests. This is because it is unclear whether North Korea is prioritizing the development and production of higher-yield thermonuclear weapons or lower-yield fission-only or boosted single-stage weapons. More powerful warheads with the high yield demonstrated in the single 2017 advanced design test would consume more fissile material if it is based on a composite warhead design, or would require special hydrogen fuel if it is based on a two-stage thermonuclear warhead design. Instead, lower-yield single-stage fission weapon designs would require less fissile material. Such assumptions can result in very different estimates regarding the number of nuclear weapons. One assessment in 2020 concluded that North Korea would only have 10 to 20 nuclear weapons if it had committed its fissile material to thermonuclear weapons production (Fedchenko and Kelley 2020). Another assessment concluded North Korea could produce around 40 weapons and only "very few thermonuclear bombs," although it was unclear how many it had effectively assembled (Hecker 2020; *38 North* 2021).

Based on publicly available information, we assess that North Korea has produced sufficient fissile material to build 45 to 55 nuclear weapons (if all this material is used for weapons production) but has likely assembled fewer than that—potentially 20 to 30. Per that estimate, most of the warheads would likely be single-stage fission weapons with possible yields of 10 to 20 kilotons, akin to those demonstrated in the 2013 and 2016 tests and, with only a few thermonuclear warheads. This falls within the range offered by a July 2020 US Army study, which stated that "[e]stimates for North Korean nuclear weapons range from 20–60 bombs, with the capability to produce 6 new devices each year" (US Department of the Army 2020). It also falls within the range offered in October 2018 by South Korea's then-Unification Minister, who disclosed to the parliament a South Korean intelligence assessment that North Korea's nuclear arsenal contained between 20 and 60 weapons (Kim 2018).

Assumptions about fissile material production and warhead designs also affect projections for how many nuclear weapons North Korea might have in the future—and tend to result in inflated numbers. For example, a 2021 study assumed North Korea might already have 67 to 116 nuclear weapons and projected the inventory might reach 151 to 242 nuclear weapons by 2027 (Bennett et al. 2021). Others

found the projection to be "much too high" (*38 North* 2021). It seems more plausible that North Korea might be capable of adding sufficient fissile material for a few to half a dozen nuclear warheads per year, which would potentially be sufficient to produce a total of approximately 80 to 90 weapons by the end of the decade.

Nuclear testing and warhead capabilities

After six nuclear tests—including two with moderate yields and one with a high yield—there is no longer any doubt that North Korea can build powerful nuclear explosive devices designed for different yields. North Korea has even published pictures of what it claims to be different warhead designs (including a "thermonuclear" design) that appear small and light enough to potentially be delivered by ballistic missiles (see Figure 1 below). The published designs might be real warheads, prototypes, or models. There is no way to know for sure. Nor is it known if the published designs match the devices detonated in the nuclear explosive tests.

Figure 1: North Korea has published images of what it claims to be nuclear warhead designs: a ball-shaped design that could potentially be a fission implosion device; and a peanut-shaped design that could potentially be a two-stage thermonuclear device. There is no public information that confirms the displays are actual functioning nuclear warheads. (Images: North Korean government).

Milestones and assessments

Although North Korea is widely assumed to have developed warheads for its short-range and medium-range ballistic missiles, there is less agreement about its ability to deliver functioning nuclear warheads with long-range intercontinental missiles. These uncertainties are often overlooked in the public debate about North Korea's nuclear capabilities. [2] To better understand the status of North Korea's nuclear weapons program and assessments about its warheads, it is useful to review the major milestones and assessments from the last two decades or so.

North Korea apparently began developing nuclear weapons even before the formal collapse of the Agreed Framework—a 1994 arrangement whereby the United States would provide Pyongyang with two proliferation- resistant nuclear power reactors and, in turn, North Korea would freeze operations at reactors thought to be part of a nuclear weapons program. As publicly reported in 2004, Pakistani nuclear physicist Abdul Qadeer Khan said that sometime around 1999 he was shown "three plutonium devices" during a visit to an underground facility about one hour outside Pyongyang (Sanger 2004). [3] Three years later, then-US Secretary of State Colin Powell publicly stated of North Korea: "We now believe they have a couple of nuclear weapons and have had them for years" (US State Department 2002).

The "weapons" to which Powell referred might have been the "devices" Khan saw or early prototype designs intended to be used in nuclear tests if necessary. But only three years after Powell's statement, in December 2005, North Korea itself for the first time declared that it had "manufactured nukes for self- defense" and that the weapons "will remain [a] nuclear deterrent for self-defense under any circumstances" (*Washington Post* 2005).

Less than a year later, on October 9, 2006, North Korea conducted its first nuclear test. The explosive yield was limited, less than one kiloton—not an impressive demonstration of a nuclear weapons capability and widely seen as a fizzle. The US intelligence community stated that the test produced a yield of "less than one kiloton—well below the yield of other states' first nuclear test" (Office of the Director of National Intelligence 2007).

The second test—two-and-a-half years later, on May 25, 2009—was a little more powerful and "suggests the North has the capability to produce nuclear weapons with a yield of roughly a couple kilotons TNT equivalent," according to the US intelligence community.

These tests did not demonstrate the yield needed for operational nuclear weapons. A RAND Corporation report in 2012 cautioned: "It should also be considered that even speculative sources estimate that North Korea cannot have more than a few nuclear weapons available. If they exist, these devices are very precious to the regime, and it seems unlikely that they would be mounted on inaccurate and unreliable missile systems—the risk of 'losing' a weapon is simply too high" (Schiller 2012).

The third test, conducted on February 12, 2013, was more convincing. The intelligence community initially said that its yield was "several kilotons"—but international analysis subsequently estimated the yield to have been around 10 kilotons (Office of the Director of National Intelligence 2013; NORSAR 2017). This prompted some experts to suggest that North Korea might have developed a miniaturized warhead for the Nodong missile, though others thought it was too soon for North Korea to have accomplished that feat (Albright 2013; J. Kim 2014; McGrath and Wertz 2015).

Around the same time, the US Defense Intelligence Agency—in an assessment distributed to members of the US Congress—for the first time concluded: "[The Defense Intelligence Agency] assesses with moderate confidence [that] the North currently has nuclear weapons capable of delivery by ballistic missiles; however the reliability will be low" (Shanker, Sanger, and Schmitt 2013). The assessment did not reflect the conclusion of the US intelligence community as a whole and triggered an immediate rebuttal by the US Defense Department: "It would be inaccurate to suggest that the North Korean regime has fully developed and tested the kinds of nuclear weapons referenced in the passage." The Director of National Intelligence added that "the statement read by the member is not an intelligence community assessment" and that "North Korea has not yet demonstrated the full range of capabilities necessary for a nuclear-armed missile" (Clapper 2013).

Similarly, the US Air Force Global Strike Command stated in a briefing in September 2013 that North Korea "currently does not have an operational warhead; if developed, it could be deployed on" the Musudan (Hwasong-10), Taepo Dong-2, or Hwasong-13 (US Air Force Global Strike Command 2013).[4] Global Strike Command did not list any medium- or short-range missiles with nuclear capability.

Even so, the assessment among independent analysts at the time was that medium- and possibly short-range ballistic missiles were the first platforms for North Korean nuclear weapons. An April 2015 report from the US-Korea Institute at the Johns Hopkins School of Advanced International Studies, for example, claimed that the Nodong missile formed "the backbone of its current deterrent . . . " (Schilling and Kan 2015). Similarly, after North Korea's fifth nuclear test, in September 2016, demonstrated a yield of 10 to 15 kilotons, the Institute for Science and International Security estimated that "North Korea may have a handful of plutonium-based warheads for its Nodong ballistic missile" (Albright 2017).

But military commanders also appeared to go further than the intelligence community at the time. The commander of US Forces Korea, Gen. Curtis Scaparrotti, stated in October 2014: "I believe they have the capability to miniaturize a device at this point and they have the technology to potentially deliver what they say they have." Scaparrotti cautioned: "We've not seen it tested," but added: "I don't think as a commander we can afford the luxury of believing perhaps they haven't gotten there." The Pentagon press secretary clarified: "General Scaparrotti said he believes they have the capability to miniaturize. That's not the same thing as saying that they have the capability to mount, test, and deliver a nuclear weapon in an [intercontinental ballistic missile]" (Alexander and Stewart 2014).

The South Korean Ministry of Defense also did not agree with Scaparrotti's assessment. "Despite its significant technology level, we don't think the North is capable of making such nuclear weapons," a spokesperson said in February 2015 (*Korea Herald* 2015a).

As these quotations suggest, there was confusion about how to describe North Korea's nuclear capabilities at the time. On March 20, 2015, the *Korea Herald* quoted Admiral Cecil Haney, then the commander of US Strategic Command, saying about North Korea's nuclear capability: "We think they already miniaturized some of this capability" (*Korea Herald* 2015b). But when asked at a press conference only four days later if North Korea had a miniaturized warhead that it could put on a missile, Haney said: "As of yet, I don't see any tests yet that [were] associated with this miniaturized claim" (US Defense Department 2015a).

Additionally, when Admiral Bill Gortney, then-commander of the North American Aerospace Defense Command and US Northern Command, was asked in April 2015 if he thought North Korea had "developed the capability to miniaturize a nuclear warhead and put it on a ballistic missile like the KN08," he responded that "we assess that they have the ability to do that" (US Defense Department 2015b).

At the time, however, North Korea had not even test-launched the KN08, so Gortney cautioned: "Now, we have not seen them do that. We haven't seen them test that." Yet he added: "I don't think the American people want us to—you know, there are some things that they want us to make sure we edge on the side of conservatism to make sure we get right" (US Defense Department 2015b).

The explanation was an important reminder to be cautious when interpreting official statements about North Korean nuclear capabilities. "Our assessment," Gortney said, "is that they have the ability to put it on a nuclear weapon on a KN08 and shoot it at the homeland. *And that—that's the way we—that's the way we think. That's our assessment of the process* (emphasis added).

We haven't seen them test the KN08 yet and we're waiting to do that. But it doesn't necessarily mean that they will fly before they test it" (US Defense Department 2015b).

After its fourth nuclear test, on January 6, 2016, North Korea claimed it had successfully detonated what it described as a "hydrogen" bomb. The yield of the explosion was relatively modest (around five kilotons), and the US intelligence community assessed the following month that "the low yield of the test is not consistent with a successful test of a thermonuclear device" (Clapper 2016). A second test that year, on September 9, was more powerful (10 to 15 kilotons) but still far from what one would expect from a successful thermonuclear test. [5] It is possible, but unknown, that the North Korean reference to a so-called "hydrogen" bomb implied the use of tritium to boost the efficiency of a single-stage fission device. Such a technology would enable North Korea to use less fissile material in each bomb and further expand its production capacity (Jones 2016).

Additionally, it is unclear if the tests involved actual nuclear warhead designs or test devices that would require further modification to be fitted on a missile. Dennis Blair, who was Director of National Intelligence from 2009–2010 and a former commander of US Pacific Command, as late as April 2017 seemed to think that the explosions involved test devices rather than proof tests of operational designs. During a talk, Blair characterized North Korea's nuclear warheads as "these crude weapons that they developed maybe seven or eight years ago," each of which "is about the size of half of this stage . . . " Pyongyang's program, Blair asserted, "may be developing 10 to 15 nukes" (Blair 2017). Whether Blair was aware of later designs is not clear, but his description is a far cry from the pictures released by North Korea at the time, whether legitimate or not, that showed the so-called "disco ball" and "peanut" warhead designs. In early August 2017, Gen. Paul Selva—then vice-chairman of the Joint Chiefs of Staff—gave a detailed account of the uncertainties that remain about North Korea's nuclear capabilities (Garamone 2017). "Before we can assert Kim Jong-unhas a nuclear missile capable of targeting the United States," Selva said, "there are a couple of aspects we must know." He listed several criteria that must be met (Selva 2017):

- "One, [Kim] has to have the missile that will actually range that distance. We believe he has that capability right now. It's clear that he can build a rocket that can fly that far.
- [Two,] [h]e'll have to have the guidance and control system, the guidance and stability control, to move a rocket across that distance without it breaking up. We don't know if he has that. We don't know that he doesn't. He's been pretty successful at short- and medium-range ballistic missiles. But the physics of a long-range missile are substantially different. So stability control matters. And that's a gap we need to fill in our understanding of whether or not he can do this.
- The third piece is a re-entry vehicle that can survive the stresses of an intercontinental ballistic missile shot. Once again, much easier to go straight up and down than it is to endure the re-entry stresses and the actual heat of an intercontinental missile shot. We don't know if he's got that technology. We don't know that he doesn't, but we don't know that he does. He hasn't demonstrated it. We have to see.
- And the last is a nuclear weapon that can survive that trip. Again, that's what we don't know. We don't know the design specifics of his nuclear weapons—purported nuclear weapons. We don't know if he's been able to miniaturize it and make it stable enough."

One month later, on September 3¸ 2017, North Korea demonstrated clearly that it could potentially produce nuclear devices with yields in the range of thermonuclear warheads. A nuclear explosion with a yield of well over 100 kilotons showed that North Korea had managed to design a thermonuclear device or one that used a mixed-fuel (composite) design. The US intelligence community reportedly called it an "advanced nuclear device" (Panda 2017b). Yield estimates range from 140 to 250 kilotons (*Asia Review* 2017; NORSAR 2017).

Despite the uncertainty about the number and ability to deliver a functioning nuclear warhead to the United States, some experts at the time asserted that North Korea could do just that. Yet even after several intercontinental ballistic missile (ICBM) flight tests conducted by North Korea in 2017, the chairman of the Joint Chiefs of Staff, Gen. Joseph Dunford, stated in 2019 that North Korea had not yet demonstrated the capability to deliver a functioning nuclear warhead on a long-range missile: "I still see a potential although as-yet-undemonstrated capability to match a nuclear weapon with an intercontinental ballistic missile . . . " (Dunford 2019). The UN Panel of Experts reported in 2021 that an anonymous member state had assessed, "judging by the size of the missiles of the Democratic People's Republic of Korea, that it is highly likely that a nuclear device can be mounted on the intercontinental ballistic missiles, and it is also likely that a nuclear device can be mounted on the medium-range ballistic missiles and short-range ballistic missiles." But because the size of a missile does not in and of itself reveal anything about the capability of the nuclear device it may be capable of carrying, the member state cautioned that "it was uncertain whether the Democratic People's Republic of Korea had developed ballistic missiles resistant to the heat generated during reentry" (United Nations 2021b).

In sum, these assessments indicate that although North Korea has developed nuclear devices small enough to be mounted on its medium- and long-range ballistic missiles, it is unclear whether it has developed a re-entry vehicle capable of protecting a device during re-entry through the Earth's atmosphere.

Latest nuclear testing activities

North Korea has conducted all its nuclear tests at the Punggye-ri test site in North Hamgyong province, which consists of a large mountain complex with several underground tunnels. North Korea partially

disabled the complex in May 2018 by destroying three tunnel entrances and several nearby buildings; this was done as a confidence-building measure in advance of a planned meeting between Kim Jong-un and Donald Trump (Talmadge 2018). However, the underground site itself was not destroyed and could therefore be reconstituted if necessary.
In early 2022, after an extended period of inactivity, North Korea began to reconstitute the Punggye-ri site. Satellite images collected between March and June 2022 revealed the construction of new buildings and renovation of older ones; movement of lumber, equipment, and personnel; new excavation activity; and the creation of a new portal into the mountain test site (Makowsky, Heinonen, and Liu 2022b; Bermudez, Cha, and Jun 2022; Lewis and Schmerler 2022). This substantial new construction effort suggests that North Korea may be preparing for another underground nuclear test, and both US and South Korean officials have stated that they expect a seventh test to be conducted soon (Kang 2022; BBC 2022). In August 2022, the UN Panel of Experts reported that North Korea had tested "nuclear triggering devices" in June; however, the panel was "unable to identify the test locations and dates" associated with the tests. The Panel additionally noted that "[a]s of early June, two member states assessed that the preparation for nuclear tests was at a final stage" (Lederer 2022).

Land-based ballistic missiles

Over the past decade, North Korea has developed a highly diverse ballistic missile force, including missiles in all major range categories. In addition to the afore-mentioned uncertainties surrounding North Korea's nuclear warheads, it is unclear how many operational delivery vehicles North Korea possesses and which of those would be assigned a nuclear mission. It is also important to note that some of the ballistic missile types North Korea has flight-tested or displayed might be research projects intended to develop future ballistic missile technology, rather than demonstrations of operational missiles.
In recent years, a wealth of new information about North Korean missile bases has become publicly available, most prominently thanks to the work of Joseph Bermudez Jr. and Victor Cha on the *Beyond Parallel* website (*Beyond Parallel* 2022). Despite North Korea's missile development and extensive construction at suspected missile bases, however, the operational status of many of these missiles remains uncertain. The *Missile Defense Review* report published by the Pentagon in 2019, for example, stated that none of North Korea's modern longer-range missiles had been fielded (US Defense Department 2019). However, North Korea has dramatically escalated its missile testing in recent years: the UN Panel of Experts reported that as of August 2022, the country had already tested 31 missiles, compared to the 25 it tested throughout the entirety of 2019, its last record-breaking year (Lederer 2022).
To ensure completeness, this section analyzes all of North Korea's known land-based ballistic missiles (see Table 1) and offers some hypotheses about which missiles are most likely to have a nuclear role. Again, the inclusion of a missile in the table does not necessarily mean it is known or certain to have a nuclear role. Table 1 (view large version)
North Korea possesses several distinct types of short-range ballistic missiles (SRBMs), although many are part of the same missile "family" and therefore share common designs and characteristics.
In a May 2021 speech, Kim Jong-un stated that North Korea had developed what he described as "tactical nuclear weapons including new-type tactical rockets . . . " In the future, he stated, it would be necessary to improve the technology "and make nuclear weapons smaller and lighter for more tactical uses. This will make it possible to develop tactical nuclear weapons to be used as various means according to the purposes of operational duty and targets of strike in modern warfare . . . " (North Korean Ministry of Foreign Affairs 2021). The meaning of "tactical," however, is not clear. It could mean actual short-range tactical nuclear weapons or simply weapons that have a shorter range than intercontinental weapons. North Korea operates several Toksa (KN02) solid-fueled ballistic missiles with a maximum range of 120 kilometers (75 miles), and potentially an extended-range version with a maximum range of 170 kilometers (106 miles) (E. Kim 2014). This missile is based on the Russian Tochka (SS-21 Scarab), which was developed as a dual-capable missile. However, there is no credible public evidence that suggests North Korea has developed a nuclear capability for the Toksa. North Korea operates several distinct types of liquid-fueled missiles belonging to the Scud missile family. The Hwasong-5 and Hwasong-6 SRBMs are the North Korean versions of Russian-built Scud B and Scud C missiles, respectively. The US Air Force's National Air and Space Intelligence Center lists the missiles' ranges at 300 and 500 kilometers (186 and 311 miles), respectively, and estimates that North Korea has fewer than 100 launchers for the combined Hwasong-5 and -6 arsenal (National Air and Space Intelligence Center 2020, 21). North Korea is modernizing both types of missiles by equipping them with maneuverable re-entry vehicles designed to evade regional missile defense systems like the Terminal High Altitude Area Defense (THAAD) system, which the United States deploys in South Korea (Panda 2017e). The modernized Hwasong-5, which has been designated KN21 by the US government, was flight-tested three times in August 2017, with one failure (James Martin Center for Nonproliferation Studies 2022). The modernized Hwasong-6, which has been designated KN18, was successfully flight-tested in November 2017 (James Martin Center for Nonproliferation Studies 2022).
In recent years, North Korea has been developing a new series of more accurate, solid-fueled SRBMs with indigenous designs. These missiles, which are known as the KN23, KN24, and KN25, have collectively been tested more than 40 times since the beginning of 2019 (James Martin Center for

Table 1. North Korean missiles with potential nuclear capability, 2022*.

North Korean designation[a]	US designation[a]	Year first displayed	Range (km)[b]	Description and status
Land-based ballistic missiles[c]				
Short-range(<1,000 km range)				
Hwasong-11	KN02/Toksa	2004	120–170	Single-stage, solid-fueled SRBMs launched from 6-axle wheeled TEL. Based on the Russian dual-capable SS-21 Scarab, but there is no credible public evidence indicating a nuclear mission for North Korea's Toksa. Operational.
Hwasong-5, Hwasong-6	Scud-B, Scud-C	1984/1990	300/500	Single-stage, liquid-fueled SRBMs launched from 4-axle wheeled TEL. In 2020, NASIC estimated fewer than 100 Hwasong-5 and –6 launchers. Operational.
?, ?	KN18, KN21	2017	250/450	Hwasong-5 and –6 variants with separating maneuverable warhead. Flight-tested in May and Aug. 2017 from wheeled and tracked TELs. Status unknown; may have been superseded by newer solid-fueled SRBMs.
?, Hwasong-11Na[d], ?	KN23, KN24, KN25	2018/2019	380–800	New generation of solid-fueled SRBMs that resemble Russia's Iskander-M, South Korea's Hyunmoo-2B, and the United States' ATACMS SRBMs. Successfully flight-tested dozens of times from wheeled, tracked and rail-based launchers since 2019. Status unknown; probably operational.
Medium-range(1,000–3,000 km range)				
Hwasong-7	Nodong/ Rodong	1993	>1,200	Single-stage, liquid-fueled MRBM launched from 5-axle wheeled TEL. In 2020, NASIC estimated fewer than 100 Hwasong-7 launchers. Operational.
Hwasong-9[e]	KN04/Scud-ER	2016	1,000	Single-stage, liquid-fueled Scud extended-range variant launched from 4-axle wheeled TEL. Flight-tested in 2016. Probably operational.
Pukguksong-2	KN15	2017	>1,000	Two-stage, solid-fueled MRBM launched from tracked TEL. Land-based version of Pukguksong-1 SLBM. Flight-tested in 2017. Probably operational.
Hwasong-8, Unnamed "hypersonic missile"	?, ?	2021	>1,000	Two versions of HGV carried by a shortened Hwasong-12 booster. Hwasong-8 flight-tested in Sep. 2021 with unknown result; unnamed missile successfully flight-tested twice in Jan. 2022. Both systems displayed at exhibition in Oct. 2021. Under development.
Intermediate-range(3,000–5,500 km range)				
Hwasong-10	BM-25/ Musudan	2010	>3,000	Single-stage, liquid-fueled IRBM launched from 6-axle wheeled TEL. NASIC estimates fewer than 50 Hwasong-10 launchers. Several failed flight tests in 2016. Status unknown; may have been superseded.
Hwasong-12	KN17	2017	>4,500	Single-stage, liquid-fueled MRBM launched from 8-axle wheeled TEL. Flight-tested several times in 2017 with mixed success. Deployment status unknown.
Intercontinental (5,500+ km range)				
Hwasong-14	KN20	2017	>10,000	Two-stage, liquid-fueled ICBM launched from 8-axle wheeled TEL. First ICBM. Successfully flight-tested twice in 2017. Deployment status unknown; may have been superseded.
Hwasong-15	KN22	2017	>12,000	Two-stage, liquid-fueled ICBM launched from 9-axle wheeled TEL. Successfully flight-tested in Nov. 2017. Displayed at parade in Oct. 2020 and at exhibition in Oct. 2021. Deployment status unknown.
Hwasong-17[f]	KN28	2020	>14,000	Two-stage, liquid-fueled ICBM launched from 11-axle wheeled TEL. Largest ICBM to date, possibly capable of carrying MIRVs and penetration aids. Tests of various components, as well as possible flight tests, conducted throughout early 2022. Displayed at parade in Oct. 2020 and at exhibition in Oct. 2021. Under development.
Other delivery platforms				
Land-attack cruise missile		2021	1,500	Flight-tested multiple times in 2021 from wheeled TEL. Possibly dual-capable. Under development.
Submarine-launched ballistic missiles				
Pukguksong-1	KN11	2014	>1,000	Two-stage, solid-fueled SLBM. Flight-tested several times in 2015 and 2016 with mixed success. Displayed at exhibition in Oct. 2021. Deployment status unknown; may have been superseded.
Pukguksong-3	KN26	2017	1,900–2,500	Two-stage, solid-fueled SLBM. Successfully flight-tested in Oct. 2019. Deployment status unknown.
Pukguksong-4	?	2020	3,500–5,400	Two-stage, solid-fueled SLBM. Appears wider than Pukguksong-1 and shorter than Pukguksong-3. No known flight tests. Displayed at parade in Oct. 2020. Deployment status unknown.
Pukguksong-5	?	2021	?	Two-stage, solid-fueled SLBM. Roughly same length as Pukguksong-3 with elongated shroud; possibly capable of carrying MIRVs and penetration aids. No known flight tests. Displayed at parade in Jan. 2021 and at exhibition in Oct. 2021. Deployment status unknown.
(Pukguksong-6)	?	2022	?	Two-stage, solid-fueled SLBM. Longer than all previous Pukguksong-type missiles, but with similar nose cone to Pukguksong-5. No known flight tests. Displayed at parade in Apr. 2022. Under development.
Small "New Type" SLBM	?	2021	400–600	Appears to deviate from traditional Pukguksong SLBM design, instead bearing similarities to KN23 SRBM. Displayed at exhibition in Oct. 2021 and successfully flight-tested a week later. Deployment status unknown; probably under development.

* The status and capabilities of North Korea's missiles come with significant uncertainty. The inclusion of missiles in this table does not necessarily mean the authors conclude that they are all equipped with nuclear warheads or assigned a nuclear mission. Several may have been intended as prototypes, technology demonstrators, or early iterations that have been or will be superseded by newer missiles. Some missiles are also grouped due to their similarities or due to their role as part of a missile "family" or "generation."

Keys: ? = unknown; () = uncertain.

[a]For overviews of names and designations for North Korean missiles, see: Matt Korda's "The More You KN-0w About North Korean Missiles" and "The Hwasong That Never Ends" lists on Arms Control Wonk (*https://www.armscontrolwonk.com/archive/1203680/the-more-you-kn-0w-about-north-korean-missiles/*; *http://www.armscontrolwonk.com/archive/1203797/thehwasong-that-never-ends/*); the Center for Nonproliferation Studies' "North Korea overview" on the Nuclear Threat Initiative (NTI) website (http://www.nti.org/learn/countries/north-korea/); the Center for Strategic and International Studies' Missile Threat Project (*https://missilethreat.csis.org/country/dprk/*); and Ankit Panda's reporting (@nktpnd).

[b]Ranges of North Korean missiles are uncertain and should generally be viewed with caution. North Korea often lofts its longer-range missiles during flight tests, making the exact range difficult to estimate. Useful sources include: the US Air Force National Air and Space Intelligence Center's (NASIC) report on Balllistic and Cruise Missile Threats (https://www.nasic.af.mil/About-Us/Fact-Sheets/Article/2468137/2020-ballistic-and-cruise-missile-threat/); various studies by the US-Korea Institute at SAIS; articles on the 38North.org blog; the James Martin Center for Nonproliferation Studies' North Korean overview at the Nuclear Threat Initiative (http://www.nti.org/learn/countries/north-korea/); articles by David Wright on the Union of Concerned Scientists' allthingsnuclear.org blog (*http://allthingsnuclear.org/author/dwright#.Wg9qZ7YrLzw*), and the United Nations' Panel of Experts reports pertaining to North Korea's missile activities.

[c]Most missile launchers have one or more reloads.

[d]North Korea refers to the KN24 as the "Hwasong-11Na," which could be considered akin to "Hwasong-11B," as "Na" (나) is the second letter in the Korean (Hangul) alphabet. This indicates that the KN24 is an improvement on or replacement for the original Hwasong-11 SRBM, which the US Department of Defense designates as the KN02 (Toksa).

[e]The 1,000-km range Scud ER is sometime called an SRBM but NASIC lists it as an MRBM.

[f]This missile was previously assumed to be designated the Hwasong-16; however, it was revealed at North Korea's "Self-Defence Exhibition" in October 2021 that it is called the Hwasong-17. It is unclear which missile—if any—currently holds the Hwasong-16 designation.

Nonproliferation Studies 2022). These missiles appear to bear several similarities to conventional

American, South Korean, and Russian missiles, such as the ATACMS, Hyunmoo-2B, or Iskander SRBMs, and North Korea has stated that certain variants of these new missiles can carry 2.5-ton warheads. This is a much heavier payload than would be needed for carrying a nuclear weapon and could therefore indicate a conventional role (Voice of Korea 2021a). It is possible, however, that one or more of these new solid-fuel missiles could eventually be operationalized to deliver nuclear weapons.

Some of these SRBMs, including the KN23 and possibly the KN24, can conduct "pull-up" maneuvers in their terminal phase of flight, thus complicating the abilities of North Korean adversaries to track the missiles during their descent.

In September 2021, North Korea launched two KN23 SRBMs, but for the first time, they were launched from a rail-mobile launcher. Following the successful test, North Korea announced its intention to expand the Railway Mobile Missile Regiment—created at the Eighth Congress of the Workers' Party of Korea (WPK) in January 2021—into a brigade, which could eventually consist of nine launchers with 18 missiles (Voice of Korea 2021b). North Korea tested two other KN23 SRBMs from rail-mobile launchers in January 2022 (Voice of Korea 2022a). Given that North Korea has an extensive cross-country rail network that frequently travels through mountains, rail-mobile launchers would enable North Korea to move missiles around the country rapidly and increase the survivability of its second-strike force.

North Korea appears to be continuously iterating on these indigenous missile designs. In April 2022, Kim Jong-un oversaw a test of a "new-type tactical guided weapon," which was explicitly linked to North Korea's nuclear program. Not only was this test launch characterized as one of the "pivotal goals for war deterrent advanced at the Eighth Congress of WPK"—which specifically included developing tactical nuclear delivery systems—but the accompanying press release noted that this new missile would "[strengthen] the effectiveness of tactical nuclear operation of [North Korea]" (Voice of Korea 2022b).

The sophisticated testing program for these newer systems indicates that North Korean missile troops are becoming significantly more practiced at conducting salvo launches and lowering the time intervals between missile launches (Dempsey 2020). As an illustration of this new capability, in June 2022, North Korea test-launched eight SRBMs from multiple different locations in less than an hour. This constituted the largest number of North Korean ballistic missiles launched on a single occasion (Yonhap News Agency 2022a).

Medium-range missiles

North Korea has likely operationalized three medium- range ballistic missiles (MRBMs), with several more in development. This is the category of missile that is most likely to have an operational nuclear capability.

The Hwasong-9 (Scud-ER) is a single-stage, liquid-fuel, road-mobile, medium-range ballistic missile launched from a four-axle transporter erector launcher. This launcher is very similar to the one used with Scud B and Scud C short-range ballistic missiles. Many sources consider the Scud-ER a short-range ballistic missile, but in a triple test launch on September 5, 2016, the missiles apparently flew to a range of 1,000 kilometers (621 miles), the lower end of the range that the National Air and Space Intelligence Center uses for medium-range ballistic missiles (National Air and Space Intelligence Center 2020, 25).

The Hwasong-7 (Nodong/Rodong) is a single-stage, liquid-fuel, medium-range ballistic missile carried on a five-axle road-mobile transporter erector launcher. The missile, which was first test-flown in 1993, exists in two versions (Mod 1 and Mod 2) and has an estimated range of 1,200 kilometers (746 miles) or more. The National Air and Space Intelligence Center estimates that North Korea deploys fewer than 100 Hwasong-7 launchers (National Air and Space Intelligence Center 2020, 25). Apparently, the Nodong was originally intended to carry a first-generation nuclear warhead, and US naval intelligence reportedly warned in 1994 that North Korea would probably be able to equip the missile with a nuclear warhead by 2000, and possibly earlier (Bermudez 1999; Pinkston 2008). The Nodong's accuracy is poor relative to North Korea's more modern missiles, and its conventional utility is therefore quite limited. Partially for this reason, some analysts have suggested that the Hwasong-7 is one of the most likely missiles to have an operational nuclear capability (Albright 2013; James Martin Center for Nonproliferation Studies 2006; Center for Strategic and International Studies 2021).

The Pukguksong-2 (KN15)—sometimes spelled "Pukkuksong-2" or "Bukkeukseong-2" ("Polaris- 2")—is a two-stage, solid-fuel, medium-range ballistic missile carried in a canister on a road-mobile caterpillar-type transporter erector launcher. The missile was first test-launched in 2017 and appears to be a modification of the submarine-launched Pukguksong-1 (Polaris-1). It is North Korea's first attempt to field a solid-fuel, land-based ballistic missile. The first two flight tests in 2017 demonstrated a range of up to 1,200 kilometers (746 miles), which fits the National Air and Space Intelligence Center's range estimate of 1,000 kilometers (621 miles) or more (Wright 2017a, 2017c). Compared to liquid-fueled missiles, solid-fueled missiles require less logistical support and require much less preparation time before launch.

The Hwasong-8 is a new missile first revealed in 2021. The missile appears to be composed of a modified Hwasong-12 booster and can carry multiple different payloads, including a hypersonic glide vehicle (HGV) and a maneuverable re-entry vehicle (MaRV). The Hwasong-8 variant carrying an HGV was tested in September 2021, and the variant carrying a MaRV was tested twice in February 2022. During the second test in February, North Korea claimed that the missile conducted a "corkscrew" maneuver, which

reportedly prompted the US Federal Aviation Administration to temporarily pause commercial airline departures along the west coast of the United States for approximately 15 minutes (Chongnyon 2022; Liebermann, Muntean, and Starr 2022).
The Hwasong-8 was displayed at North Korea's "Self- Defence 2021" exhibition in October 2021, alongside another unnamed missile—also using a modified Hwasong-12 booster—described as "hypersonic" by the North Korean state media. Independent analysis suggests that although the boosters are very similar, the hypersonic glide vehicles used on the Hwasong-8 and the unnamed missile are of a different design (Xu 2022a).
North Korean state media reported that the Hwasong-8 was the first North Korean missile to use a "fuel ampoule," which involves placing pre-fueled, liquid-fueled missiles in temperature-controlled canisters to facilitate faster launches (*DPRK Today* 2021; Xu 2021). North Korea says it plans to transition all liquid-fueled missiles into ampoules (*DPRK Today* 2021).

Intermediate-range ballistic missiles
The Hwasong-10 (Musudan) is a single-stage, liquid-fuel, intermediate-range ballistic missile launched from a six-axle transporter erector launcher. The missile, which is also sometimes designated BM-25, has an estimated range of more than 3,000 kilometers (1,864 miles), but it suffered several test failures in 2016 (James Martin Center for Nonproliferation Studies 2022). The National Air and Space Intelligence Center estimated in 2020 that North Korea had fewer than 50 Hwasong-10 launchers (National Air and Space Intelligence Center 2020, 25). However, given the system's unreliability, the overall status of the Hwasong-10 program remains unclear; it may have been replaced by the newer Hwasong-12 as North Korea's primary intermediate-range ballistic missile.
The Hwasong-12 (KN17) is a single-stage, liquid-fuel, intermediate-range ballistic missile carried on an eight-axle road-mobile transporter erector with a detachable firing table. After several failures, the missile was test-launched on a highly lofted trajectory on May 14, 2017, reportedly demonstrating that it could travel approximately 4,500 kilometers (2,796 miles) if flown on a normal trajectory (Wright 2017b). The National Air and Space Intelligence Center estimates the range as 3,000 kilometers (1,864 miles) or more. A subsequent test, on August 28, overflew Japan before it crashed in the western Pacific, some 2,700 kilometers (1,678 miles) from the launch site. A third successful launch, on September 14, demonstrated a longer range—approximately 3,700 kilometers (2,299 miles) (Panda 2017c; Wright 2017f). In January 2022, North Korea launched its first Hwasong-12 in nearly five years, demonstrating a similar trajectory to its previous launches (Japanese Ministry of Defence 2022a). At this stage, it is unknown if the Hwasong-12 has been deployed.

Intercontinental ballistic missiles
The most dramatic of North Korea's recent developments has been the display and test launch of large ballistic missiles that appear to have an intercontinental range. North Korea has publicly shown five types of missiles in this range category: the Taepo Dong-2, the Hwasong-13, the Hwasong-14, the Hwasong-15, and the Hwasong-17. These systems are in various stages of development, and some may simply be mockups or technology demonstrators.
The Taepo Dong-2 is a three-stage, liquid-fuel, long-range missile that is thought to be a derivative of the Unha-3 space-launch vehicle. The Unha-3 placed a satellite in an unstable orbit in 2016. North Korea has not yet demonstrated a functioning re-entry vehicle for the Taepo Dong-2, and the National Air and Space Intelligence Center's 2020 annual report lists the system as a "space launch vehicle" (National Air and Space Intelligence Center 2020, 29). Given North Korea's recent development of newer, more sophisticated long-range systems, we assess that the Taepo Dong-2 is not currently an operational military system and will not be a focus for North Korea's ICBM program moving forward.
The Hwasong-13 (KN08) is a three-stage, liquid-fuel intercontinental ballistic missile (ICBM) carried on an eight-axle transporter erector launcher (TEL) that uses a truck like the one used for the Hwasong-14 ICBM. The Hwasong-13 was first displayed during a parade in 2012. In 2013, a US Air Force Global Strike Command briefing listed the KN08 as an ICBM that "could field in [the] next [five] years" (US Air Force Global Strike Command 2013). However, the Hwasong-13 has not been flight-tested, and given North Korea's recent development of newer, more sophisticated long-range systems, we assess that the Hwasong-13 is not currently an operational system and, like the Taepo Dong-2, will not be a focus for North Korea's ICBM program moving forward.
In July 2017, North Korea conducted its two, first-ever, test-launches of the Hwasong-14 (KN20) ICBM. The two-stage, liquid-fueled Hwasong-14 appears to share its first stage with the Hwasong-12 intermediate-range ballistic missile and is launched from an eight-axle road-mobile transporter erector with a detachable firing table.
The first test launch took place on July 4 and the missile flew on a highly lofted trajectory to 950 kilometers (590 miles). An unnamed US government source later told *The Diplomat* that the United States assessed the range to be 7,500 to 9,500 kilometers (4,660 to 5,903 miles) on a normal trajectory (Panda 2017a). North Korea released a video of the launch that showed the missile had a modified payload shroud, which looked like a shroud that appeared in photos of Kim Jong-un, engineers, and a peanut-shaped device said to be a thermonuclear warhead. North Korea claimed that the test demonstrated that it could use a re-entry vehicle to protect the missile's warhead, but that was later shown to be inaccurate (Wright 2017d).

The second Hwasong-14 test launch, conducted on July 28, also used a lofted trajectory and reached an apogee of roughly 3,700 kilometers (2,299 miles). According to the National Air and Space Intelligence Center and some independent analysts, the test demonstrated that the missile could, if flown on a normal trajectory, have a range of over 10,000 kilometers (6,214 miles) (Wright 2017e; National Air and Space Intelligence Center 2020, 27). This would potentially bring US cities on the west coast, including Los Angeles and Seattle, within striking range (Elleman 2018). The weight of the payload used in the test, which could significantly affect the range, is not known; however, a subsequent analysis suggests that the test was likely not conducted using a re-entry vehicle with a realistically heavy mock warhead (Acton, Lewis, and Wright 2018). Therefore, the test did not demonstrate whether North Korea has a functioning ICBM re-entry vehicle to protect a warhead. Notably, North Korea did not display the Hwasong-14 at its most recent military parade that featured ICBMs, in October 2020; this could indicate that North Korea intends to put more emphasis on its newer, longer-range ICBMs (*NK News* 2020).

During a parade in October 2017, North Korea also displayed two new launchers with large canisters for the transport of missiles. One launcher appeared similar to the eight-axle transporter erector used for the Hwasong-14 but modified with a large canister that resembled the missile canister used on the Russian SS-25 (Topol) transporter erector launcher. The second new launcher equipped with a missile canister strongly resembled the transporter erector launcher used for the Chinese DF- 31A. Canister launchers are normally used to transport solid-fueled missiles, so the two new launchers—coupled with Kim Jong-un's recent statements—suggest that North Korea is trying to develop a solid-fueled ICBM.

After a two-month pause in missile flight tests, on November 29, 2017, North Korea launched a newer ICBM with an even longer range: the Hwasong-15 (KN22). The two-stage, liquid-fuel missile was launched from a nine-axle transporter erector on a highly lofted trajectory to nearly 4,500 kilometers (2,796 miles), which indicates a maximum range on a normal trajectory with a light payload of approximately 13,000 kilometers (8,078 miles), sufficient to potentially target most of the United States (Wright 2017g). The National Air and Space Intelligence Center lists the range of the Hwasong-15 to be upwards of 12,000 kilometers, or 7,456 miles (National Air and Space Intelligence Center 2020, 29). However, it is important to note that heavier payloads—including nuclear warheads—would significantly decrease the missile's range. Hwasong-15 ICBMs were displayed during North Korea's October 2020 military parade (*NK News* 2020).

In April 2018, Kim Jong-un announced that North Korea would observe a self-imposed moratorium on nuclear explosive tests and flight tests of long-range ballistic missiles (Korean Central News Agency 2018). In January 2020, North Korean diplomats announced that the country would no longer observe the moratorium, yet North Korea did not test-launch another ICBM until 2022 when it conducted several tests of ICBMs and ICBM components throughout the year (Nebehay 2020).

On February 26 and March 4, 2022, North Korea conducted successful missile launches that appeared to be of medium range; but on March 10 the Pentagon announced it believed the tests were related to North Korea's ICBM program (Hadley 2022). Given this announcement, coupled with the specific subsystems mentioned in North Korea's press releases about the tests, it is possible that the tests were related to the development of a multiple independently targetable re- entry vehicle (MIRV) bus (James Martin Center for Nonproliferation Studies 2022).

On March 24, North Korea claimed to have test-launched its new liquid-fueled Hwasong-17 ICBM for the first time. This missile had first been unveiled at North Korea's October 2020 military parade (see figure at top of page), during which independent analysts noted the missile was significantly larger than other North Korean ICBMs, and that the missile's diameter could range between 2.4 and 2.5 meters (roughly about 7.8 feet to 8 feet), with a length of roughly 24 to 25 meters (about 78.75 to 82 feet) (Lewis 2020; La Boon 2020; Elleman 2020). During the March 24 flight test, the missile reached an apogee of nearly 6,200 kilometers (3,853 miles) and traveled nearly 1,100 kilometers (683 miles) over the course of 71 minutes—suggesting a possible range of approximately 15,000 kilometers (9,321 miles) (Yonhap News Agency 2022b). However, an *NK News* analysis of the launch video released by North Korea suggests that the missile may have been tested on March 16 but failed and that the missile tested on March 24 may have been a Hwasong-15 instead (Zwirko 2022).

On May 4 and May 24, North Korea conducted two additional tests of what may have been ICBM components—like the tests of February 26 and March 4—or possibly, according to the US government, failed Hwasong-17 tests (Starr and Herb 2022; Starr 2022). If deployed, it is estimated that the Hwasong-17 could potentially deliver a large warhead—or hypothetically a small number of multiple re-entry vehicles or a single re-entry vehicle with penetration aids—to the continental United States. However, these advanced capabilities would require a sophisticated testing campaign that would take several years to complete (Elleman 2020).

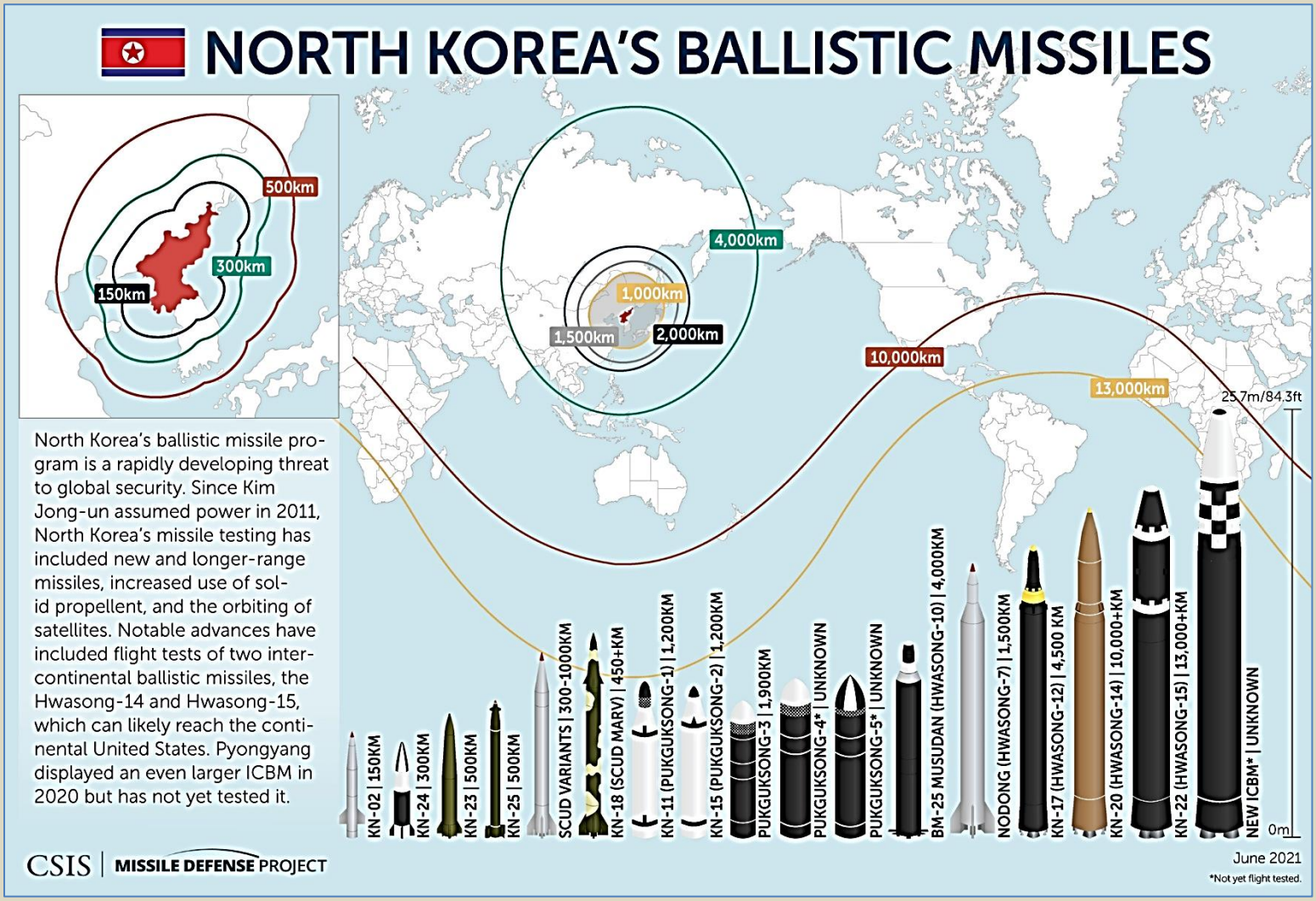
Overall, despite North Korea's considerable advancements in its ICBM program, the country has still not publicly demonstrated an operationally functioning re-entry vehicle that can protect a warhead during re-entry through the Earth's atmosphere.

Moreover, there is still considerable uncertainty about how the combination of the missile, re-entry vehicle, and warhead would function in a real attack.

After the July 2017 test of an Hwasong-14 ICBM, the US Central Intelligence Agency (CIA) reportedly concluded that the re-entry vehicle did not survive re-entry but would nonetheless likely work in an attack on the United States (Panda 2017d). Yet after the test flight of the Hwasong-15 ICBM, on November 28,

a US official told CNN that "the North Koreans had problems with reentry" and that the missile likely broke up upon re-entry into Earth's atmosphere (Starr and Sanchez 2017). The South Korean deputy minister of defense policy, Yeo Suk-joo, reportedly told the South Korean parliament that North Korea still needed to proof-test some technologies, like re-entry, terminal stage guidance, and warhead activation (Kim and Solovyov 2017). Seoul's Foreign Minister Kang Kyung-wha added that North Koreans "haven't demonstrated their reentry capability. They haven't demonstrated their remote targeting, or the miniaturization that is required to do this" (Krever 2017). These statements match the assessments listed above from US officials.

Union of Concerned Scientists' expert David Wright agreed that "North Korea has not yet demonstrated a working reentry vehicle on a trajectory that its missiles would fly if used against the United States," but added that there did not appear to be a technical barrier to building a working re-entry vehicle (Wright 2017h). In 2017, Stanford's Siegfried Hecker estimated that this might take another two years of tests (Hecker 2017).



North Korea's ability to deploy large numbers of heavy long-range missiles could depend on its ability to procure or indigenously produce launchers for those missiles. In the past, North Korea has sourced its heavy launchers from Russian, Belarusian, and Chinese companies, and imported them under the guise of civilian applications (Hanham 2012; Schiller 2012). For example, North Korea purchased at least six eight-axle Chinese WS51200 vehicles—which had been marketed as lumber haulers—with the intended end-user designated as the North Korean Ministry of Forestry. Converted WS51200 vehicles were, however, subsequently displayed at an April 2012 military parade carrying Hwasong-13 ICBMs, and they have appeared at several subsequent military parades and during missile test launches (United Nations 2021b, Annex 10, 2013). It also appears that at least one of these vehicles was indigenously modified to add a ninth axle to support the November 2017 launch of the Hwasong-15 ICBM (United Nations 2021b, Annex 10).

No more than six converted WS51200 launchers have appeared at any one time, so it is possible that North Korea only maintains a total of six such launchers. Given the rigid sanctions regime under which

the country operates, it is exceedingly difficult for North Korea to import additional launchers; as such, it is clear that North Korea is working toward developing an indigenous heavy launcher production capability.
In late 2017 and early 2018, Kim Jong-un visited several factories with ties to the "production of Korean- style heavy-duty vehicles," according to North Korean state media, including the March 16 Factory, the Kumsong Tractor Factory, the Amnokgang Tire Factory, the Sungri Motor Complex, and the Pyongyang Trolley Bus Factory (Panda 2018). Indigenously producing heavy launchers is a highly challenging prospect, however. The chassis and steering systems are complicated to produce and North Korea would also have to develop powerful engines and transmissions, as well as a complex computer program that properly aligns the vehicles' axles and allows them to safely respond to off-road terrain challenges (Hanham et al. 2020).
Despite these technological and logistical challenges, it appears North Korea is having some success with its indigenous production of heavy launchers for its longer-range missiles. In October 2020, North Korea displayed a new eleven-axle TEL for its new Hwasong-17 ICBM, which the UN Panel of Experts suggested was manufactured within North Korea (United Nations 2021b, Annex 10). If this is the case, it would represent a significant accomplishment for the country's heavy launcher production capabilities. If North Korea can now mass-produce heavy launchers for its ICBMs, there would be significantly fewer constraints on the number of long-range missiles that the country can operate. At the same time, these types of heavy, wheeled launchers would be limited to traveling on high-grade roads and would likely be used to carry North Korea's newer liquid-fueled ICBMs. This means that the launcher would also have to travel in a convoy with fuel trucks, support vehicles, and possibly a loading crane—all of which would make it significantly easier for adversarial reconnaissance to spot the systems well in advance of launch.[6]
It remains unclear how many new Hwasong-17 TELs North Korea possesses. In the four parades where the missile was featured, only four of these TELs appeared at once. However, the TELs' serial numbers (which range from 321 to 329) seem to indicate that North Korea has produced at least nine (Dempsey 2022)—although these numbers could well be repainted before each parade in an attempt by North Korea to exaggerate its own TEL inventory.

Submarine-launched ballistic missiles

North Korea is developing several types of submarine-launched ballistic missiles (SLBMs)—all being part of the Pukguksong family of missiles (also spelled as Pukkuksong and Bukkeukseong), or "Polaris." The National Air and Space Intelligence Center's 2020 ballistic and cruise missile report states that none of North Korea's SLBMs had been deployed by 2020 (National Air and Space Intelligence Center 2020, 33). The first versions may have been technology development projects intended for future operational missiles.
The Pukguksong-1 (KN11) is a two-stage, solid-fuel missile designed to be carried on a single Sinpo-class submarine. The submarine only has one missile tube. The Pukguksong-1 has been test-launched six times in total in 2015 and 2016, with three successes (James Martin Center for Nonproliferation Studies 2022). The National Air and Space Intelligence Center lists the Pukguksong-1's range as above 1,000 kilometers (621 miles) (National Air and Space Intelligence Center 2020, 33).
In October 2019, North Korea test-launched a new type of SLBM: the Pukguksong-3, which could have a maximum range of between 1,900 and 2,500 kilometers, or between 1,181 and 1,553 miles (Wright 2019; United Nations 2021b). The Pukguksong-3's existence had previously been revealed by Kim Jong-un's visit to a chemical materials institute in August 2017 (Panda 2017f).
During the October 2020 military parade, North Korea unveiled a newer type of solid-fuel SLBM: the Pukguksong-4, which may have a longer range than its predecessor. The two-stage missile is wider than the Pukguksong-1 and possibly a little shorter than the Pukguksong-3. Its larger diameter indicates that it could hypothetically carry multiple warheads or penetration aids to overcome ballistic missile defenses. Speculations that the Pukguksong-4 might currently be capable of carrying multiple re-entry vehicles seem premature. The missile has not yet been flight-tested. At the military parade in January 2021, North Korea displayed yet another SLBM version: Pukguksong-5. The missile, which has not been flight tested, is longer than the Pukguksong-4 but about the same length as the Pukguksong-3. The Pukguksong-5's shroud, however, is more elongated than the shrouds on the two previous missile types (Sutton 2021; Elleman 2021). Pukguksong-5 might have a greater range and payload capacity than its predecessors (United Nations 2021b, 96). As with other North Korean missiles, speculations about a multiple re-entry vehicle capability seem premature at this stage. At the military parade in April 2022, North Korea revealed a sixth likely member of the Pukguksong family, although the missile's name has not yet been formally announced. It is longer and wider than all of North Korea's previously displayed SLBMs (Chung and Kim 2022; Xu 2022b). North Korea also appears to have developed a "new type" of smaller SLBM which appears to bear similar characteristics to North Korea's newer SRBM designs, particularly the KN23 (Xu 2021). The missile, whose name has not been officially announced, was revealed during North Korea's "Self-Defence 2021" exhibition in October 2021 and flight-tested the following week to a range of nearly 600 kilometers (373 miles). North Korea subsequently announced that the test demonstrated the missile's "flank mobility and gliding skip mobility" (Naenara 2021). The missile was launched using North Korea's single Gorae-class (Sinpo) experimental submarine, known as *8.24 Yongung*, which can hold and launch only a single SLBM (Naenara 2021). The same type

of missile may have also been tested on May 7, 2022; however, it is unclear whether the test was successful (Japanese Ministry of Defence 2022b).

Other potential platforms

Land-attack cruise missiles

North Korea appears to be developing a land-attack cruise missile (LACM) that is described in ways that resemble descriptions of nuclear-capable missiles. In September 2021, North Korea conducted two test launches of this system to a range of 1,500 kilometers (932 miles). Although North Korea has other cruise missiles in its arsenal, this is the first system that has been explicitly described as a "strategic weapon," thus potentially implying a connection to North Korea's nuclear weapons program (Shin and Smith 2021). However, Kim Jong-un's January 2021 statement that the cruise missile's "conventional warheads are the most powerful in the world" indicates that the LACM could be either dual-capable or exclusively conventional (Rodong 2021).

North Korean state media released images of the missile, indicating that it might include a terminal guidance system and could be launched from a TEL carrying five missiles (Xu 2021). Notably, South Korean news sources subsequently reported that neither South Korea nor the United States was aware of the LACM launches until after the announcement in North Korean state media (Lee and Park 2021). Given that this system is designed to circumvent radars and missile defense systems by flying at lower altitudes on maneuverable trajectories, it could offer North Korea a new and unique capability to attack regional targets.

Gravity bombs

No credible public information demonstrates that North Korea has developed nuclear warheads for gravity bombs, despite warheads for ballistic missiles being more difficult to develop than gravity bombs because of the extreme environment during their launch and trajectory. All other nuclear-armed countries first developed nuclear bombs for aircraft and then proceeded to field warheads for missiles. However, North Korea has taken the opposite development path for its nuclear weapons program. If North Korea ever wanted to develop a deliverable nuclear weapon quickly, it could potentially have developed a crude gravity bomb for delivery by an H-5 (Il-28) medium-range bomber. This potential option is mentioned only for background; no public evidence suggests that North Korea has pursued it. A nuclear-capable coastal defense cruise missile designated KN09 was listed in the 2013 briefing by the US Air Force Global Strike Command, but it was deleted in a subsequent revision (Kristensen 2013).

Notes

[1] Liquid nitrogen is used as part of the uranium enrichment process, particularly within the context of cold trapping uranium hexafluoride.

[2] For these and other useful sources, see Ballistic and Cruise Missile Threat, a report by the National Air and Space Intelligence Center; the missile threat project of the Center for Strategic and International Studies; the North Korea overview by the James Martin Center for Nonproliferation Studies at the Nuclear Threat Initiative's website; articles by David Wright on the allthingsnuclear.org blog of the Union of Concerned Scientists; and Joshua Pollack's "North Korean WMD: A Guide to Online Resources."

[3] Slide 5 from the Global Strike Command's briefing was updated on September 10, 2013, with the quoted warhead assessment.

[4] For an insightful review of North Korea's hydrogen bomb claim, see Kelley and Hansen (2016).

[5] For assessments of North Korean warhead designs and production capacity, see Albright (2017), Hecker (2017), Jones (2017), and Kelley and Hansen (2016).

[6] These paragraphs are adapted from Korda (2022), where a more detailed assessment of North Korean launch vehicles can be found.

●▶ 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.

What Would It Take to Survive an EMP Attack?

By Forrest M. Mims III

Source: https://www.homelandsecuritynewswire.com/dr20220908-what-would-it-take-to-survive-an-emp-attack

Sep 08 – We are increasingly vulnerable to both natural disruptions and military attacks on our power grids. Earlier this month I wrote about electromagnetic pulse impulses (EMPs), which would destroy your electronics, leaving you and your surroundings intact — but without easy means of survival.

Force of Nature: Sometimes the Sun Is to Blame for Knocking Out the Power Supply

Natural disruptions can give us some idea what to expect. When lightning destroys a transformer atop a power pole, nearby businesses and residence must get by without power until the transformer is replaced but it usually doesn't last long. Far more damage can occur in the rare event that the sun erupts with a major coronal mass ejection (CME) of plasma and magnetic field directed toward Earth.

The first recorded example occurred on September 1, 1859, while British amateur astronomer Richard Carrington was observing the sun. Carrington made careful drawings of the massive solar flare he observed. Less than a day later, a CME arrived and caused spectacular auroral displays. It even affected telegraph equipment, setting some ablaze. Today, such an event can damage or destroy much electrical equipment connected to a network.

During March 1989, my daughter Vicki detected a string of major solar flares with a Geiger counter she was using for a science fair project. On March 13, one of those flares was associated with a CME that led to powerful electrical transients in transmission lines across Quebec. It tripped circuit breakers and shut down power across the entire province for nine hours. The CME also severely damaged a high-voltage transformer at the Salem New Jersey Nuclear Plant.

Other CME's have also struck Earth, including a major event in 1921: "Countries such as Australia, Brazil, France, Denmark, Japan, the U.K., New Zealand and the U.S. experienced widespread disruptions in telephone and telegraph communications." *(International Business Times)* Here's how it was experienced at the time:

> A telephone station in Sweden burned out, a New York telegraph operator claimed that "he was driven away from his instrument by a flare of flame which enveloped the switchboard and ignited the building", and telegraph lines in France "seemed possessed by evil spirits". The event even touched Australia, with the Argus reporting disruptions to telephone services between Melbourne, Sydney and Brisbane (Delores Knipp and Brett Carter, "The Concerning History of Coronal Mass Ejections," at *RealClearScience*, 2 October 2016).

In 2012, the sun emitted a CME believed to be more powerful than the Carrington event. Fortunately, it was not pointed at Earth.

The Key Difference Between a Natural CME and the Dreaded EMP Attack

While a massive solar CME could shut down a significant fraction of the world's electrical grid, electronic devices not connected to the grid would not be damaged. But the electromagnetic pulse emitted by a nuclear explosion is very different because the first of its three phases occurs within billionths of a second. This extremely fast EMP can travel hundreds of miles from an exploding nuke with a voltage potential of 50,000 or more volts per meter. That is far more than enough to *permanently damage unshielded semiconductor electronic equipment.* The second phase of EMP from a nuke can also damage electronics.

The third phase is much slower and longer. Its target is thousands of miles of high-voltage power lines that serve as EMP antennas. As Russia learned during nuclear experiments in the 1960s, the massive electrical currents absorbed by power lines can critically damage high-voltage transformers and even entire power plants.

A widely speculated scenario is that an enemy might launch an EMP nuke high over the central US in an attempt to shut down the nation's electrical infrastructure together. Included would be communications networks and the computers and controllers that run everything from traffic lights and emergency vehicles to weather instruments and satellites.

While a nationwide EMP event will not directly injure or kill people, its side effects will. Consider what could happen during critical surgeries or for emergency room patients dependent on working electronic systems, and fast moving vehicles that suddenly lose power while cruising along busy highways.

While this doomsday scenario has been depicted in books and movies, widespread preparation for a nuclear EMP is sorely lacking. Even the US government acknowledges this in various unclassified reports. For example, there's "Electromagnetic Pulse (EMP): Threat To Critical Infrastructure," the title of a 2014 hearing before a subcommittee of the Committee on Homeland Security of the House of Representatives. Don't read any of it before going to bed, for you'll not be able to sleep. For example,

> Another myth is that rogue states or terrorists need a sophisticated intercontinental ballistic missile to make an EMP attack. In fact, any missile, including short-range missiles that can

deliver a nuclear warhead to an altitude of 30 kilometers or more, can make a catastrophic EMP attack on the United States, by launching off a ship or freighter. Indeed, Iran has practiced ship-launched EMP attacks using Scud missiles–which are in the possession of scores of nations and even terrorist groups. An EMP attack launched off a ship, since Scuds are common-place and a warhead detonated in outer space would leave no bomb debris for forensic analysis, could enable rogue states or terrorists to destroy U.S. critical infrastructures and kill millions of Americans anonymously (from the Statement of Peter Fry, Executive Director of the Task Force on National and Homeland Security, May 2014).

During the opening of this hearing, Texas representative Michael McCaul began his talk by stating: "We talk a lot about a nuclear bomb in Manhattan, and we talk about a cybersecurity threat, the grid, power grid, in the Northeast, and all these things would actually probably pale in comparison to the devastation that an EMP attack could perpetrate on Americans."

As I learned after sending an open records request to the city adjacent to my property, most local and national government agencies in the US are unprepared for an EMP attack. Even the US military is not well prepared, for all branches of the military employ off-the-shelf radio gear, computers, mobile phones and other equipment that is highly vulnerable to an EMP event.

Consider what might occur if a relatively small atomic bomb is detonated several hundred miles over Kansas. The EMP from the explosion would cover most of the US within a few billionths of a second. In regions where the EMP created an initial pulse of 30,000 to 50,000 volts per meter, a significant fraction of unprotected electronics would be instantly rendered inoperable. Modern cars and trucks are equipped with EMP-vulnerable microprocessors that control everything from engines to dashboard electronics and entertainment devices. While a vehicle's metal shielding will provide some protection, it is possible that some vehicles will be rendered inoperable by an EMP. This would not be good for people driving along a packed expressway where only a few inoperable vehicles could cause a massive traffic pileup.

All this assumes a bomb that produces a peak of 50,000 volts/meter EMP, which has long been the standard assumption by the US military. Unfortunately, Russia and China have developed much more powerful super EMP bombs.

Remember that through all this an EMP bomb will not destroy buildings, spread radioactivity, or even make a sound.

What Reasonable Precautions Should We Take?

Many personal electronic devices might be rendered inoperable by an EMP, including laptops, radios, and mobile phones. If the initial EMP pulse does not damage the grid, the third phase certainly could. Power plant transformers can cost a million dollars or more and require more than a year to replace, assuming a suitable manufacturer can be found.

While some people can afford to install an expensive EMP-proof solar or propane fueled power supply for their residence, most of us cannot. So what should you try to secure and protect for use after an EMP?

- A compact, battery-powered radio, preferably with shortwave reception, is number one on my list. A second priority is an LED flashlight for every family member. A third priority is a mobile phone loaded with plenty of music and photos of family and important documents. If the cell phone service in your area fails, you'll be ready when service is restored.
- Other electronic devices you might need include medical devices, a pair of walkie-talkies, and a Geiger counter for use if you are in the fallout pattern downwind from a nuclear attack.
- Be sure to keep spare batteries for most of these devices. Recharging a cell phone is another matter. Unless you possess or have access to a propane or solar generator that can survive an EMP, your best solution is a miniature solar power device. The ones that come with a built-in battery can be charged outdoors and brought indoors to charge your phone. Their main drawback is that rechargeable batteries don't like heat, and solar-powered battery packs can become very warm.
- A small solar panel that charges a phone directly might be a better choice if you keep the phone shaded when it's being charged. Whichever charging method you select, be sure you have an appropriate cable for connecting it to your phone.
- All these items (except extra batteries) should be stored in EMP-proof containers, sleeves, or bags available online. I describe how to make an EMP-proof sleeve for a laptop or notebook and provide more EMP information in my science column in *MAKE* magazine: "Amateur Scientist: Solar Flares, EMP, and Faraday Shields."
- For an excellent explanation of EMPs and major solar flares, and how to survive them, you may want to look at Arthur Bradley's book, Disaster Preparedness for EMP Attacks and Solar Storms (2012). Bradley, an electrical and electronics engineer who has worked at NASA for 18 years, also provides information at his personal site, Disaster Preparer.
- Finally, surviving an EMP event requires more preparation than storing your electronics in EMP-proof bags. Water and food (in that order) will quickly become far more crucial. WaterBOB and similar products will allows safe storage of up to 100 gallons of drinkable water in a bathtub container. That's enough for at least 50 days for one person and 10 days for a family of five. A water well might provide safe water provided an electricity-driven pump can be powered. Many filter devices are available to cleanse water from rivers and lakes. Some even remove nitrates.
- Dr. Bradley discusses water and food storage and personal protection strategies in his book. Other useful sources of information are the Federal Emergency Management Agency guidelines

at Nuclear Explosion | Ready.gov. The Red Cross provides additional survival information at Nuclear Explosion and Radiation Emergencies.

With luck, we will never need to think of all this but we ought not to rely on luck alone.

Forrest M. Mims III, a Fellow at the Discovery's Institute's *Center for Science and Culture*, is an instrument designer, science writer and independent science consultant.

For Russia, Nuclear Plants Are Nuclear Bombs

By Maxim Starchak

Source: https://cepa.org/for-russia-nuclear-plants-are-nuclear-bombs/

Sep 09 – On February 24, fighting began on the territory of the Chernobyl nuclear power plant in Ukraine, the site of the notorious 1986 nuclear disaster which left its hinterland uninhabitable for 20,000 years. Chernobyl fell to the Russian invasion forces and remained under its control for a month.

By March 4, the Armed Forces of the Russian Federation also seized the enormous Zaporizhzhia nuclear plant, Europe's biggest. For the past two months, there has been fighting in and around the facility, with Russian and Ukrainian officials blaming each other. The Russian Ambassador to the United Nations (UN), Vasily Nebenzia, said that Russia does not use nuclear infrastructure for military purposes. This, however, is hardly the case.

During the Cold War, Russian experts called nuclear power plants "a nuclear bomb on enemy territory." Conventional weapons, when used to strike nuclear power plants, can have the properties of nuclear weapons (and have a significantly greater negative impact on the environment.) This led to the possibility of considering nuclear power plants and peaceful nuclear facilities as weapons of mass destruction (WMD), and to consider a strike on them as a "passive form" of employing WMD.

The question of nuclear power plant vulnerability in an attack by a hostile state has not been widely considered, because it was unofficially recognized that it was impossible to protect such facilities from a missile or air strike. That is, it was recognized that it was irrational to conduct military engagements on a territory where there is a nuclear power plant. The benefits from the destruction of the nuclear facility as a strategic, energy, and economic facility were offset by direct and indirect collateral damage.

Thus, the understanding grew that nuclear power plants are no less of a threat than nuclear weapons, and according to some indicators are actually "peaceful weapons" of mutual nuclear deterrence. Yet Russia's invasion of Ukraine and the seizure of nuclear power plants destroys this concept. The military is used both to capture and to hold the nuclear power plant (International Atomic Energy Agency — IAEA —inspectors reported that the Russian army had stationed military vehicles in the Zaporizhzhia turbine halls at the heart of the plant.)

Ukraine's civil military facilities have become important military strategic locations for Russia. It has not needed to threaten the use of nuclear weapons. And since there is an order of magnitude more radiation inside a reactor than in a bomb, radiation pollution due to the explosion of a nuclear reactor would be far larger.

Russia's military leadership has probably always understood this. For example, back in 2001, Admiral Vladimir Valuev, commander of the Baltic Fleet of the Russian Navy (2001—2006), speaking about a war in Europe, noted that it was not necessary to use nuclear weapons to inflict heavy losses; it would be sufficient simply to destroy just a few of the existing nuclear power plants. Currently, the Deputy Chairman of the Russian Security Council, Dmitry Medvedev, on his Telegram channel, commenting on the shelling of the Zaporizhzhia plant, said that the EU should not forget that they also have nuclear power plants that can suffer "accidents."
The only way to ensure this is the withdrawal of Russian troops from the plant. But Russia will keep a presence at the facility for as long as possible. By controlling it, Russia has a means of political coercion and nuclear threats. And while the Kremlin rightly draws attention to safety concerns, it benefits from the existing instability.
The Russian Foreign Ministry seeks to accuse Ukraine of nuclear terrorism, both in order to shift the blame and to deny its control of the plant, and in order to justify its presence to "ensure [its] safe functioning." It argues that since the Russian military provides the plant's security, repelling Ukrainian attacks, a withdrawal would allow Ukraine to arrange a "monstrous provocation" and cause a nuclear catastrophe, according to Russian Ambassador to the UN Nebenzia.
This directly contradicts the experience at Chernobyl. After Russia's withdrawal there, there were no direct threats to the security of the plant, no one fired at it and no sabotage was carried out there.
In fact, a Russian withdrawal is hindered by other fears. Some pro-Kremlin experts are afraid that UN peacekeepers might be deployed in the region, and later replaced by NATO peacekeeping forces, citing the Kosovo case of 1999 as an example. Others are afraid that after leaving Energodar, the community close to Zaporizhzhia where its workers live, it will result in the same situation as at Bucha, near Kyiv, with crimes detected and publicized. It is also true that the plant and Energodar have military significance and that a withdrawal would risk its control of the entire Zaporizhzhia region.
The IAEA, which primarily provides consulting and intermediary services in the nuclear safety and security sphere, cannot solve the issue of military security of the plant, even if it keeps staff in place there. Any agreements on a demilitarized or nuclear safety and security protection zone will be difficult to implement — the whole concept would collapse in the event of a provocative act; in the event of shelling, for example, either side could immediately withdraw from the deal.
It is almost impossible to achieve its implementation in the conditions of an ongoing war.
It can only be hoped that the plant will remain a peaceful site of nuclear deterrence, and that the Kremlin is not interested in a nuclear catastrophe on the territory under its control.

Maxim Starchak is an independent expert on Russian nuclear policy, defense, and the nuclear industry. Based in Moscow, he is a Fellow at the Centre for International and Defence Policy of Queen's University in Canada, and a contributor to the Jamestown Foundation's Eurasia Daily Monitor. He has also written for the Atlantic Council, FPRI, Marshall Center, and others.

Iran Nuclear Weapons Breakout Time Remains at Zero

Source: https://www.homelandsecuritynewswire.com/dr20220912-iran-nuclear-weapons-breakout-time-remains-at-zero

Sep 12 – A new report from the Institute for Science and International Security summarizes and assesses information in the International Atomic Energy Agency's (IAEA) quarterly safeguards report for 7 September 2022. The main finding: Iran's breakout time, that is, the time between a political decision to produce a nuclear weapon and the completion of such weapon, remains at zero. Iran has more than enough 60 percent enriched uranium, or highly enriched uranium (HEU), in the form of uranium hexafluoride (UF6) to fashion a nuclear explosive. If Iran wanted to further enrich its 60 percent HEU up to 90 percent weapons-grade uranium (WGU), which is used in Iran's known nuclear weapons designs, it could do so within weeks by utilizing only a few of the advanced centrifuge cascades it has in its possession.
The report was written by David Albright, the President and Founder of the Institute for Science and International Security; Sarah Burkhard, a Research Associate at the Institute for Science and International Security; and Andrea Stricker, the deputy director of the Foundation for Defense of Democracies' (FDD) Nonproliferation and Biodefense Program and an FDD research fellow.
Here are the Background and Findings of the Institute's report:

Background

- This report summarizes and assesses information in the International Atomic Energy Agency's (IAEA) quarterly safeguards report for September 7, 2022, *Verification and monitoring in the Islamic Republic*

of Iran in light of United Nations Security Council resolution 2231 (2015), including Iran's compliance with the Joint Comprehensive Plan of Action (JCPOA).

- Iran's breakout time remains at zero. It has more than enough 60 percent enriched uranium, or highly enriched uranium (HEU) in the form of uranium hexafluoride (UF6) to directly fashion a nuclear explosive. If Iran wanted to further enrich its 60 percent HEU up to 90 percent weapons-grade uranium (WGU), used in Iran's known nuclear weapons designs, it could do so within weeks utilizing only a few advanced centrifuge cascades.
- Iran is learning important lessons in breaking out to nuclear weapons, including by experimenting with skipping typical enrichment steps as it enriches up to 60 percent uranium-235, and building and testing equipment to feed 20 percent enriched uranium and withdraw HEU. It is starting from a level below 5 percent LEU and enriching directly to near 60 percent in one cascade, rather than using two steps in between, a slower process entailing the intermediate production of 20 percent enriched uranium. It has used temporary feed and withdrawal setups to produce HEU from near 20 percent enriched uranium feed. Iran is also enriching uranium in one IR-6 cascade modified to switch more easily from the production of 5 percent enriched uranium to 20 percent enriched uranium. As such, Iran is experimenting with multi-step enrichment while seeking to shortcut the process.
- Combined with Iran's refusal to resolve outstanding Nuclear Non-Proliferation Treaty (NPT) safeguards violations, the IAEA has a significantly reduced ability to monitor Iran's complex and growing nuclear program, which notably has unresolved nuclear weapons dimensions. The IAEA's ability to detect diversion of nuclear materials, equipment, and other capabilities to undeclared facilities remains greatly diminished.

Findings

- Due to the growth of Iran's 60 percent and 20 percent enriched uranium stocks, Iran can now produce enough WGU for three nuclear weapons in one month.
- Within one month, including a setup period, Iran could produce enough WGU for a second and third nuclear explosive also using all of its existing stock of near 20 percent enriched uranium. Whether or not Iran enriches its HEU up to 90 percent, it can have enough HEU for three nuclear weapons within one month after starting breakout.
- In essence, Iran has effectively broken out slowly by accumulating 60 percent enriched uranium. As of August 21, Iran had a stock of 55.6 kilograms (kg) (in uranium mass or U mass) of near 60 percent enriched uranium in UF6 form, or 82.2 kg (in hexafluoride mass or hex mass). Iran also has 2 kg of 60 percent HEU in chemical forms other than UF6.
- Iran keeps two-thirds of its stock of 60 percent HEU at the Esfahan site, where it maintains a capability to make enriched uranium metal. Although Iran has stated that it is using the HEU to make targets for irradiation in the Tehran Research Reactor (TRR), it has converted only a small fraction of its HEU into targets – about 2.1 kg – and has not converted more since March 2022.
- Iran's current production rate of 60 percent enriched uranium is 3.9 kg per month (U mass) using two advanced centrifuge cascades and up to 5 percent low enriched uranium (LEU) as feed.
- Iran is now enriching uranium to 20 percent in both cascades of IR-6 centrifuges at the Fordow Fuel Enrichment Plant (FFEP). It is also operating six IR-1 cascades (three sets of two interconnected cascades) that were already producing 20 percent enriched uranium. The presence of advanced centrifuges at the FFEP enhances Iran's ability to break out using a declared but highly fortified facility.
- The production rate of 20 percent enriched uranium at the FFEP increased by almost 50 percent, from 19.9 kg to 29 kg (U mass) per month, or 29.4 kg and 42 kg (hex mass) per month.
- As of August 21, Iran had an IAEA-estimated stock of 331.9 kg of 20 percent enriched uranium (U mass and in the form of UF6). Iran also has an additional stock of 30.8 kg (U mass) of 20 percent uranium in other chemical forms.
- At the Natanz Fuel Enrichment Plant (FEP), Iran has installed 36 cascades of IR-1 centrifuges, six cascades of IR-2m centrifuges, two cascades of IR-4 centrifuges, and, newly, three cascades of IR-6 centrifuges. A third IR-4 cascade was still being installed, and newly, four additional IR-2m cascades were being installed.
- Iran's current, total operating enrichment capability is estimated to be about 16,600 separative work units (SWU) per year, compared to 12,600 SWU per year at the end of the last reporting period.
- Average daily production of 5 percent LEU increased accordingly at the FEP, but Iran's total usable stock of below 5 percent LEU continued to decrease, due to the high rate of its use as feedstock at the PFEP and FFEP.
- Iran's overall reported stockpile of LEU continued to rise due to an increase in Iran's stock of up to 2 percent enriched uranium, much of which was produced as tails in the production of 20 percent and 60 percent enriched uranium.
- Since the previous report, a February 2021 agreement between Iran and the IAEA collapsed, which had extended certain JCPOA monitoring measures such as the use of surveillance cameras and safeguards data collection devices. Iran had agreed to continue operating IAEA equipment and collect the information but keep the data in its custody. In June, following an IAEA Board of Governors

censure of Iran for non-compliance with its safeguards obligations, Iran demanded the IAEA remove 27 video cameras and other electronic monitoring devices.

- The IAEA reports that it faces serious challenges in re-establishing continuity of knowledge about Iran's activities, such as centrifuge production and production of heavy water. For more than 12 weeks, the IAEA has not been able to monitor Iran's activities, and should it receive past footage and data, has an enormous task to sift through some 1.5 years of video footage. The IAEA also details the remedial measures it will need to take in order to re-establish a centrifuge manufacturing baseline, including access to extensive records.
- The IAEA also faces a gap in knowledge about Iran's advanced centrifuge manufacturing activities at the former TESA Karaj facility from June 2021 until January 2022, raising doubt about its ability to ascertain whether Iran may have diverted centrifuge components.
- The IAEA warns, "Even if all records were provided by Iran, additional safeguards measures were applied by the Agency, and the recovered data proved to be comprehensive and accurate, considerable challenges would remain to confirm the consistency of Iran's declared inventory of centrifuges and heavy water with the situation prior to 21 February 2022."
- The IAEA concludes that "Iran's decision to remove all of the Agency's equipment previously installed in Iran for surveillance and monitoring activities in relation to the JCPOA has also had detrimental implications for the Agency's ability to provide assurance of the peaceful nature of Iran's nuclear program."

●▶ **Read the full analysis** here.

Putin May Hit Back With Nuclear Weapons Amid Ukraine Counter: Ex-NATO Chief

Source: https://www.newsweek.com/russia-ukraine-nato-nuclear-gottemoeller-1742533

Sep 13 – Losses on the battlefield in Ukraine could persuade Russian President Vladimir Putin to resort to nuclear weapons, the former deputy general of NATO recently said.

Rose Gottemoeller, the alliance's deputy secretary general between 2016 and 2019, praised the gains made by Kyiv's forces in their counteroffensive in the Kharkiv region but warned of what it might spur the Russian leader to do in response.

Gottemoeller told the BBC radio program *Today* that watching how "Putin and his coterie have been behaving during this crisis," her fear is that, "they will strike back now in really unpredictable ways that may even involve weapons of mass destruction."

When asked if she meant "a nuclear strike of some kind" Gottemoeller replied, "yes," although emphasizing she believed that this would not involve their central strategic systems, Intercontinental Ballistic Missiles [ICBMs], or submarine-launched missiles targeting the United States.

"We've been concerned from the outset of this crisis with Putin rattling the nuclear saber that he might put in play for a nuclear demonstration strike," she said on Tuesday.

This could either be "a single strike over the Black Sea, or perhaps a strike at a Ukrainian military facility", which would "strike terror not only into the hearts of the Ukrainians," but also Kyiv's allies.

"The goal would be to try to get the Ukrainians in their terror to capitulate," Gottemoeller said. "I do worry about that kind of scenario at the moment. I think the Ukrainians seem well prepared to stay the course but we will all have to be ready to stay the course, come what may."

At the start of the war, she said there were concerns that Russia would stage false flag attacks and engineer biological or chemical attacks against Ukrainian targets to blame them on Kyiv.

At the start of the war, Putin put his nuclear forces on high alert, and while Russian state television pundits have made nuclear threats on the air, military experts have so far cast doubt on the likelihood that Russia would resort to such weapons.

Gottemoeller said she had not seen evidence of a potential nuclear strike by Russia, but if there were one, she believed "we should not respond in a nuclear way."

This could involve a cyber attack or the use of conventional arms, "but we should not reach immediately for a nuclear response."

Newsweek has reached out to Gottemoeller and the Russian defense ministry for comment.

This comes as a report co-authored by the former NATO secretary general, Anders Fogh Rasmussen which was released on Tuesday, said that Ukraine's allies should give a decades-long commitment to providing Kyiv with large-scale weapons transfers and invest in its defense forces.

Separate from Ukraine's call for more arms supplies from the West, the report outlines security measures that will stop Russia from invading again that can be an alternative to Kyiv joining NATO. Putin used Ukraine's possible membership in the alliance as one of the issues justifying the invasion.

EDITOR'S COMMENT: Are we sure that Mrs. Gottemoeller was deputy director-general of NATO? It is self-evident that if a country has nuclear weapons, they are for future use not decorative! Against a military base – why waste a nuclear weapon the moment it can evaporate the military base by other means? Over the Black Sea – no explanation given; perhaps an EMP? Cyber-attack? Why not? Everybody is doing that during peace time. So, why this obsession with Russian nuclear weapons? Perhaps NATO wants to use them to retaliate with its own nuclear weapons. Another proof that insanity rules and that peace is not an option just because dominance is the name of the game! But when people are killed daily, it is a sin to call it a game . . .

Belgium Utilizes Unexpected Technology for Nuclear Detection

Source: https://i-hls.com/archives/108817

Sep 14 – The nuclear sector can now rely upon the assistance of unmanned aircraft to carry out radiological measurements without any human intervention. In contrast to traditional measurement techniques, the information is actually already being received while the drone is still in the air. The Belgian nuclear research center SCK CEN and the Belgian aeronautical specialist Sabca have developed a drone that will enable the characterization of forms of radiation and carry out the radiological monitoring of nuclear sites and their surroundings.

According to insideunmannedsystems.com, Sabca provides two types of drones: a fixed-wing drone that can fly autonomously for hours and the multicopter, which can carry heavier detectors without sacrificing flexibility. A scintillation counter is attached to the drone. The device measures radioactivity by counting flashes of light caused by the influx of ionising radiation, which in turn indicates the magnitude of the radiation dose.

"The drones will be first used as a preventive measure to study areas for potential radioactive contamination," said The Belgian Minister of the Interior Matters, Annelies Verlinden. "We are also preparing for possible remediation. Thanks to the detector, measurements can be performed during crises without any human intervention. This maximizes the protection of collaborators."

It's Too Late to Prevent an Iranian Nuke

By A.J. Caschetta

Source: https://www.meforum.org/63592/it-too-late-to-prevent-an-iranian-nuke

Sep 16 – "Iran will never get a nuclear weapon on my watch," says Joe Biden often and unconvincingly. He said it to Israeli prime ministers Bennett in 2021 and Lapid in 2022. He has even threatened to use military force "as a last resort." A cynic would suggest that Biden's attempt to forge another Obama-like "nuclear deal" is designed to ensure that Iran gets a nuclear weapon on the next president's watch. A pessimist believes it's too late.

As a pessimist by nature, I'm afraid that the window of opportunity to prevent Iran from developing a nuclear bomb has closed. Iran is already a nuclear power, and decades of dithering, cajoling, and appeasing by past U.S. administrations from Clinton to Biden (especially Obama) have given it the time and political cover to build several nuclear bombs. Even the International Atomic Energy Agency (IAEA) now estimates that Iran is only several weeks away from having "the approximate amount of nuclear material for . . . manufacturing a nuclear explosive device," which, given the IAEA's spotty record, probably means that threshold was crossed months if not years ago.

The debate over Iran's secretive and illegal nuclear program has always pitted optimists against pessimists.

Optimists emphasize the obstacles Iran has faced conducting secret research and assembling the equipment necessary to produce weapons-grade uranium all under the watchful eye of the "International Community™" and under perpetual threat from Israel's Mossad. They also often point out the difficulty of developing an ICBM capable of delivering nuclear payloads.

Pessimists emphasize uncertainty, insisting that the International Community's eye isn't all that watchful. They counter that there are more ways to deploy a nuclear bomb than by ICBM, and they remind optimists that inspectors were surprised in 1991 at discovering how far along Saddam's nuclear program had progressed, and again in 2003 when Moammar Qaddafi surprised the world by giving up his chemical and nuclear-weapons programs, which had gone largely undetected.

When it came to Iran, the late Bernard Lewis was a pessimist. In the documentary *The Third Jihad* (2008), Lewis said, "We don't know whether Iran has nuclear weapons, but they're certainly making every effort to acquire them, and my guess is that they already have some already or will have them in a very short time." Lewis emphasized that a nuclear Iran could not be contained as the Soviet Union was. In 2011, he told Bari Weiss that the "apocalyptic mindset" of Khomeinism changes the equation because, to Iran, "mutually assured destruction is not a deterrent — it's an inducement." Lewis was referring to what Daniel Pipes calls the "mystical menace" of *Mahdaviat* — the efforts "to lay the foundation for the return of the *Mahdi*," the "rightly guided one" who will rule before the end of time, according to the millenarian beliefs of Shia Islam.

Optimists assure pessimists that Mossad won't let Iran build a nuclear bomb, that Israel prevented both Iraq in 1981 and Syria in 2007 from becoming nuclear powers. They point to successful sabotage of Iran's nuclear infrastructure and to assassinations of its scientists. In turn, pessimists point out that Iran's multifaceted nuclear program is dug in and spread out across the nation. One can acknowledge that Mossad is the best at what it does but still worry about the Fordows we don't know about.

The debate brings up an interesting question: How will we know when Iran has become the tenth member of the "nuclear club"?

After decades of Iran's denying that it was interested in making nuclear weapons — it even produced a phony fatwa allegedly outlawing them — an actual detonation of a nuclear bomb in Iran, deep within a mountain or out in the open, would mark a strategic shift from Tehran's usual pretense that it is always innocent, even of the violence carried out by its proxies. It would also bring the possibility of an immediate Israeli strike.

The most feared "test" would involve a hand-off to Hezbollah, the IRGC, or even Iran's sometime ally al-Qaeda. A small bomb either smuggled through the southern U.S. border or detonated one mile into international waters off the U.S. coast would allow Iran to deny responsibility.

The canniest option would be a test in North Korea, Iran's nuclear partner. The watchdog group United Against Nuclear Iran (UANI) has documented in detail the connections and cooperation between the two programs.

Iran seems to be emulating North Korea's path to the nuclear bomb by stalling agreements through protracted negotiations and then reneging on its obligations. After agreeing to close its plutonium-production program under the 1994 Agreed Framework, North Korea continued clandestine production of uranium and surprised the world by detonating its first nuclear bomb in 2006. After four more successful tests, Barack Obama impotently declared in 2016, "To be clear, the United States does not, and never will, accept North Korea as a nuclear state."

Getting an Iranian nuclear bomb to North Korea poses problems but not insurmountable ones. China imports Iranian oil through a series of "teapot" petrochemical refiners, any one of which could receive and then hand off a device to North Korea as it delivers refined products. And since North Korea does not abide by sanctions against Iranian oil, Tehran's nuclear device could even be put aboard an oil tanker and shipped directly to North Korea.

If North Korea is willing to sell munitions to Russia to use in Ukraine, there's little reason to believe that it would balk at hosting an Iranian nuclear test. In fact, a former head of Iran's nuclear program, Mohsen Fakhrizadeh Mahabadi, was photographed with other Iranian scientists in North Korea at a nuclear test in 2013. Perhaps they were there to test the Iranian bomb.

As John Bolton wrote in 2017, "If Tehran's long collusion with Pyongyang on ballistic missiles is even partly mirrored in the nuclear field, the Iranian threat is nearly as imminent as North Korea's." That threat becomes more imminent every day the Biden administration obsequiously courts Tehran, desperately trying to reach an agreement.

It's tempting to liken a Biden "Iranian nuclear deal" to closing the barn door after the horses have already escaped, but Biden isn't even trying to close the barn door. If he gets his way, JCPOA.2 will compensate the Islamic Republic with cash, lift sanctions, and, like Obama's "Iranian nuclear deal," launder an illegal nuclear program into a legal one. It will also tie the next president's hands by ensuring that the mullahs' nuclear horses are never put back in the barn.

If we pessimists are correct, it's too late to prevent Iran from becoming a nuclear power, but it might not be too late to do something about it. As long as Iran has not demonstrated its capabilities, efforts to destabilize its nuclear capabilities are not futile, but a successful Israeli attack on Iran's nuclear facilities is probably the world's only hope as long as Joe Biden is president.

A.J. Caschetta is a Ginsberg-Milstein fellow at the Middle East Forum and a principal lecturer at the Rochester Institute of Technology.

Escalation Management and Nuclear Employment in Russian Military Strategy

Source: https://www.homelandsecuritynewswire.com/dr20220920-escalation-management-and-nuclear-employment-in-russian-military-strategy

Sep 20 – On 2 June 2022 Russia released the Principles of State Policy of the Russian Federation in the Sphere of Nuclear Deterrence. Michael Kofman and Anya Loukianova Fink write in *War on the Rocks* that characteristically, the long and awkwardly worded title preceded a brief six-page declaratory policy that is intentionally ambiguous on key considerations, substantiating a spectrum of nuclear employment options and strategies. True to its word, the policy offers some basic principles, wrapped in normative language to forearm Russian arms control negotiators, but its contents will not settle the debate on Russian nuclear strategy anytime soon.

Kofman and Loukianova Fink write:

> Russian nuclear strategy has been the subject of vigorous debates in recent years. Some believe it hides a plan to compel war termination through early use of nuclear arms after a case of aggression, i.e., escalate to de-escalate; others see it primarily as a defensive deterrent to be used in exigent circumstances. Analysts have argued that Russia's lowered nuclear threshold is a myth, a temporary measure born out of conventional inferiority. Others believe that "escalate to de-escalate" does not exist as a doctrine, or that the term itself should be terminated because the real strategy is escalation control.
>
> Each perspective offers a kernel of truth, but none of these views captures Russian nuclear strategy and thinking on escalation management in a satisfactory or comprehensive manner. The debate on escalate to de-escalate and Russia's supposed lower nuclear threshold has often missed the plot and degenerated into two camps with broadly divergent interpretations. More importantly, the Russian military's theory of victory and how it developed, or why the military thinks these specific stratagems might work, are often missing considerations.
>
> CNA's Russia Studies Program recently concluded a study on Russia's strategy for escalation management, or intra-war deterrence, across the conflict spectrum from peacetime to nuclear war. The research consulted a representative sample of over 700 Russian-language articles from authoritative military publications over the past three decades. Delving into the current state of Russian military strategy and thinking on these subjects, we found that the Russian defense establishment has developed a mature system of deterrence and a coherent escalation management strategy, integrating conventional, strategic, and nonstrategic nuclear weapons. Russian thinking on deterrence and escalation management is the result of decades of debates and concept development. Official policies, strategies, and doctrines offer glints of the thinking behind Russian nuclear strategy, using refereed terms and concepts whose actual contents are discussed extensively in military writings.

They add:

> In this article we lay out key components of Russia's nuclear strategy and thinking on escalation management, premised on deterrence by what the Russian military calls "fear-inducement" and deterrence through the limited use of force. The simplistic view characterizing Russian strategy as "escalate to de-escalate" or "escalate to win" is not correct, but neither are the commonly

> voiced counterarguments that suggest no Russian strategy for limited nuclear use exists, or that it was simply a stopgap measure born out of conventional inferiority. Russia does have a strategy for escalation management, seeking to dissuade, intimidate, or achieve de-escalation at key transition points and early phases of conflict, from peacetime through large-scale and nuclear war. These stratagems work by integrating the threat to inflict damage with nonnuclear and nuclear capabilities, ideas based on "dosed" damage, and applying force in a progressive manner, in an attempt to raise the adversary's expected costs well above the desired benefits.

Kofman and Loukianova Fink conclude:

> Any conflict with Russia will always be implicitly nuclear in nature. If it is not managed, then the logic of such a war is to escalate to nuclear use. The United States needs to develop its own strategy for escalation management, and a stronger comfort level with the realities of nuclear war.

Going Nuclear

By Lawrence Freedman

Source: https://www.homelandsecuritynewswire.com/dr20220920-going-nuclear

Sep 20 – Supreme leaders achieve their positions and then hold them by controlling events to their advantage. It is natural, therefore, to assume that even when they appear to have lost control, they will find a way to regain it. This assumption is behind the common refrain these days, even heard from people who would dearly like Vladimir Putin to fail, that he will not allow it to happen, that even at this late stage he will find something to do that will turn the tide of the war. That something will have to go beyond adding to the hurt and misery already caused, which we know he can do. It must also stave off Russia's defeat and that is another matter. In addition, therefore, to speculating about what Putin might do next, we also need to ask what good it will do him.

Russia's Way Forward

On Friday 16 September Putin spoke at a news conference at the conclusion of a conference in Uzbekistan. This conference was most memorable for evidence of Russia's increasing isolation, even among countries that might have been expected to be more sympathetic. As there were visible signs of Central Asian states distancing themselves further from Russia, Putin was obliged to acknowledge that both Chinese President Xi Jinping and Indian Prime Minister Narendra Modi had concerns about the war.

Putin sought to explain how he would win the war. Asked about the Ukrainian counter-offensive he said: 'Let's see how it goes and how it ends.' Then, asked if the war plan needed to be adjusted, he stressed Russia's minimum rather than maximum objectives: 'The main goal is the liberation of the entire territory of Donbas'. This is a narrower focus than the one with which he started and with which he was still toying a few weeks ago. He reported that the work to achieve this objective 'continues despite these counteroffensive attempts by the Ukrainian army. The general staff considers some things important, some things secondary, but the main task remains unchanged, and it is being implemented.' Perhaps he appreciates that Kharkiv is lost and Kherson may go soon. Certainly it informs the Russian offensive in Donetsk, which still continues, very much as before, despite the setbacks elsewhere.

While the West worries that Russia might resort to escalation in response to Ukrainian advances, Putin claims to see it the other way round. He spoke of 'attempts to perpetrate terrorist attacks and damage our civilian infrastructure', referring presumably to occasional Ukrainian attacks on the territory of the neighboring Belgorod oblast and of Crimea. He added:

'Terrorist attacks are a serious matter. In fact, it is about using terrorist methods. We see this in the killing of officials in the liberated territories, we even see attempts at perpetrating terrorist attacks in the Russian Federation, including – I am not sure if this was made public – attempts to carry out terrorist attacks near our nuclear facilities, nuclear power plants in the Russian Federation. I am not even talking about the Zaporozhye Nuclear Power Plant.

We are monitoring the situation and will do our best to prevent a negative scenario from unfolding. We will respond if they fail to realize that these approaches are unacceptable. They are, in fact, no different than terrorist attacks.'

Somewhat bizarrely for the head of a country that has been systematically terrorizing people in occupied territories and launching missiles on a regular basis against Ukraine's civilian infrastructure, he insisted that Russia had been 'responding rather restrainedly, but that's for the time being.' Noting that 'a couple of sensitive blows' had been delivered against Ukraine, he added: 'Well, what about that? We will assume that these are warning strikes. If the situation continues to develop in this way, the answer will be more serious.' This was apparently a reference to the strikes that followed Ukraine's successful offensive in Kharkiv, causing widespread blackouts and damaging a dam in the southern city of Kryvyi Rih. The reference to more to come may well have been intended to keep alive fears that at some point along this line nuclear weapons might be used, but that was not explicit and Russia still has means to inflict such damage without resorting to these weapons.

Nuclear Use

Yet the nuclear issue now comes up frequently. It is currently probably the matter for the greatest speculation, including in Kyiv and Washington, when officials and commentators ask what Putin might do next. Rose Gottemoeller, a former top US nuclear policy-maker and NATO's deputy secretary general until 2019, told the BBC of her fear that 'Putin and his coterie' will 'strike back now in really unpredictable ways that may even involve weapons of mass destruction.' She did not expect ICBM launches, but possibly another form of nuclear saber-rattling - 'a single strike over the Black Sea, or perhaps a strike at a Ukrainian military facility' to 'strike terror not only into the hearts of the Ukrainians' and its allies.

This is not a possibility that should be dismissed in a cavalier fashion. Russia has abundant stores of nuclear weapons, in a variety of shapes and sizes, and Putin might be desperate enough to use them. Because he has already done some really stupid things who can say for sure that he won't do anything even stupider. This possibility is not negligible, and that is worrying enough in itself. But it is not enough to answer the question of whether he might give a nuclear order by references to his mental state or assumptions that because he is being humiliated he might respond with a tantrum to end all tantrums. We need to consider exactly what problems, military and/or political this might solve. Matthew Kroenig writing for the Atlantic Council warns that a Russian nuclear strike 'could cause a humanitarian catastrophe, deal a crippling blow to the Ukrainian military, divide the Western alliance, and compel Kyiv to sue for peace.' But will it?

To act this way would break a 'taboo' that has developed around nuclear use since the only time they were used in anger in August 1945. It was a taboo that Putin himself acknowledged with President Biden in June 2021, when they reaffirmed the observation affirmed by Presidents Gorbachev and Reagan in 1985: 'nuclear war cannot be won and must never be fought.'

It would also represent an extreme version of the behavior his forces have already been following. Russia is not short of means of causing hurt and suffering and has shown no reluctance to use them. Ukrainian towns and cities have been pummeled by Russian shells, rockets and missiles, directed against residential buildings, factories, transportation hubs, power plants and much more. Over last weekend the Pivdennoukrainsk nuclear power plant in Mykolaiv oblast was struck. Thankfully the reactor was not hit, although there were explosions only 300 meters away.

Russia's campaign has seen thresholds of violence being passed with disturbing regularity. In addition to the long-distance strikes there have been the more intimate crimes uncovered after the occupying forces have left, of tortures, murders, rapes, abductions, and looting. If these were supposed to have a strategic purpose, and are not just random acts of cruelty and malevolence (some clearly come into this category), then one would suppose the intention would be to make the Ukrainians ready to concede. In practice the effect has been the opposite. It has hardened their resolve and made them even more determined to rid their country of a Russian presence. Despite all that they have been through Ukrainians are showing extraordinary levels of resilience, unity, and determination. When asked, the Ukrainian government says that even nuclear use would have the same effect.

It is especially important to note that just because nuclear weapons have not been employed that does not mean that they have had no influence on the course of this conflict. They have played an important deterrent role. Just before the invasion began Putin took part in an annual drill involving Russian missiles. Then, when he announced the 'special operation' on 24 February, he remarked that 'whoever tries to hinder us' will face 'consequences that you have never faced in your history.' Three days later he publicly ordered his defense minister Shoigu and chief of the general staff Gerasimov 'to transfer the army's deterrence forces to a special mode of combat duty'. This did not amount to much in practice: the point was to underline a deterrence threat.

The threat was directed against any thoughts in NATO countries about directly intervening to support Ukraine. Threats of this type were made in 2014 after Russia annexed Crimea. Then Putin stated that other countries 'should understand it's best not to mess with us,' adding unnecessarily that 'Russia is one of the leading nuclear powers'. At the time, as now, Russian media broadcast regular, lurid descriptions of the terrible things Russia would do to any countries that interfered, neglecting to mention what these countries could do back in return. The aim was to present Russia as a country with unlimited power, a will to use it, and little sense of proportion, so that any minor provocation could result in terror raining down on the perpetrator.

These threats were geared to reinforcing Putin's original message. Take the contributions of Andrei Gurulev, a Lieutenant General, member of the Duma, and regular media commentator, who was directly involved in Russia actions in the Donbas in 2014-15. He is something of a charmer. The Ukrainian authorities have released an intercepted call from him on February 28, 2022, just after the invasion, issuing orders to set Ukrainian households on fire. He instructed an invading unit: 'Burn them, damn it, burn them! Once you've thrown them out of there – finish the house, burn it down! Spit at that f*cking humanism!' He has a thing about destroying Britain. On state television in August, when asked if Britain was readying for war with Russia, Gurulev replied that this was already the case. Russia was fighting both Britain and the US in Ukraine.

'Let's make it super simple. Two ships, 50 launches of Zircon [missiles]—and there is not a single power station left in the UK. Fifty more Zircons—and the entire port infrastructure is gone. One more—and we forget about the British Isles. A Third World country, destroyed and fallen apart because Scotland and Wales would leave. This would be the end of the British Crown. And they are scared of it.'

More recently Gurulyov noted that Biden had warned Russia against using nuclear weapons in Ukraine. He observed that 'we may use them but not in Ukraine.' This time he made particular mention of strikes against decision-making centers in Berlin, threatening Germany with total chaos, along with his familiar theme of turning the British Isles into a 'Martian desert' in 3 minutes flat.' He added, oddly, that this could be done with 'tactical nuclear weapons, not strategic ones,' and, confidently, that the US would not respond. All this was linked to preventing NATO getting directly involved. 'We shouldn't be shy about it or fear it. … They should tuck their tails in and keep up yapping.'

Strip away the absurd rhetoric and braggadocio, and it is clear the focus remains on deterring NATO countries, now including the provision of Ukraine with the means to mount deep strikes against Russian territory. As another recent example, Russian TV presenter Olga Skabeyeva, who regularly describes the current conflict as World War III, made specific threats with regard to the potential delivery of the long-range (300km) Army Tactical Missile System (ATACMS) missile from the US to Ukraine. 'Russia has every right to defend itself. That's to say, to strike Poland or the US's Ramstein base in Germany, for example.' The current narrative in Moscow is that the troubles they now face are not because of the exertions of the Ukrainians but because they are backed by the best Western weapons. It is a familiar refrain that they are at war with NATO.

These threats have not been ignored by NATO. It was determined right at the start that there would be no direct intervention by member states. That was behind their refusal to agree to Kyiv's pleas to set up a non-fly zone to push Russian aircraft from the skies over Ukraine. President Biden has been clear that he does not want to give Putin an excuse to escalate, which is one reason why he has been reluctant to authorize the ATACMS deployment. Another reason is that the Pentagon is unconvinced that this would make a large difference to Ukraine's military performance.

The Americans have also sought to warn the Russians about the risks associated with nuclear escalation. In an interview with CBS, the President explained that turning to nuclear or other unconventional weapons would 'change the face of war unlike anything since World War II. … They'll become more of a pariah in the world than they ever have been.' He added that 'depending on the extent of what they do will determine what response would occur.'

Backed Into a Corner

Yet while the nuclear threats are directed against NATO countries rather than Ukraine, Ukraine is the reason why Russia is in trouble and which now seems to offer the most troubling scenario. Colin H. Kahl, undersecretary of defense for policy, said in a statement to The New York Times that 'Ukraine's success on the battlefield could cause Russia to feel backed into a corner, and that is something we must remain mindful of.' This point was reinforced by the deputy director of the CIA, David S. Cohen, urging not to 'underestimate Putin's adherence to his original objective, which was to control Ukraine' or 'his risk appetite.'

One can note that Russia is not truly backed into a corner. At the moment there is no existential threat to the Russian state, even if one might be developing to Putin's personal position, and that the way to get out of any corner is to cross the border back home. And if he wants to escalate he has other options. To quote the New York Times again:

'more indiscriminate bombardment of Ukrainian cities, a campaign to kill senior Ukrainian leaders, or an attack on supply hubs outside Ukraine — located in NATO countries like Poland and Romania — that are channeling extraordinary quantities of arms, ammunition and military equipment into the country.'

More might be done against critical infrastructure or Ukrainian government buildings.

Yet these are all things he has either done to a degree, tried and failed to do, or simply not attempted because they are too difficult. If the option was there it would have made no sense to wait to interdict the weapon supply lines from the western borders into Ukraine, but Russia has not been able to do this. Attacking Poland or Romania would invoke NATO's Article V. Russian leaders are well aware of this for they refer to it often. This is how nuclear deterrence works in the other direction and keeps the conflict contained.

So if initiating a direct war with NATO is too dangerous, and the value of deterrence lies in limiting the forms of assistance provided to Ukraine, what about using such weapons against Ukrainian targets?

There is a view that Russian forces might hold on until the winter and recreate the sense of stalemate and mutual attrition that was felt last summer while the battle for Luhansk was underway. Another view is that their army is in a shambolic state and will be unable to regain any grip on the situation. Should the Ukrainians start moving against Russian position in the Donbas, or capture the large number of Russian troops defending territory in Kherson and cut off from new supplies, then Putin would face calamity. In the face of such calamity would nuclear use be of any value?

Two possible roles are identified: first, to affect the course of the fighting on the ground, and second, more coercive, to threaten to raise the stakes to terrifying heights, including attacks on cites, persuading the Ukrainians to give up. To a degree this second role is inherent in the first. Once the nuclear threshold has been passed then the barriers to further escalation has been reduced. How might this be done? Options range from a demonstration shot at one end of the spectrum, perhaps against a significant but currently uninhabited site (Snake Island has been mentioned) to make the point that a process has been set in motion with an unpredictable end, to direct strikes against Kyiv at the other end, with battlefield nuclear use in the middle.

The problem with a demonstration is that the message may be unclear. It will show that Russia is ready to ignore the strong normative prohibition on any nuclear use yet is still cautious on making the most of the explosive power. When a similar option was discussed in 1945 prior to the decision to target the city of Hiroshima one concern was that while this could show that the US had a new weapon of unprecedented power, and do so without killing large numbers of people, unless the Japanese could see its destructive effects directly it would make no impression on their leadership.

Another issue was whether the bomb would work. It would be embarrassing to encourage the Japanese to watch and then for the spectacle to turn out to be a dud. It is possible that this could be a non-trivial consideration in any Russian deliberations: while missiles are regularly tested this is not the case with their warheads. The last such test under the Soviet Union was during the early period of the Cold War. As we have seen with other weapons that have been bought out of storage they have not always been well maintained and do not work as advertised.

Another decision made in 1945 was not to warn the Japanese in advance what was coming. Because this would be a lone aircraft they did not want the Japanese to make an effort to shoot it down. As it was, although the air raid sirens sounded over Hiroshima, the absence of a large raiding force meant that it was turned off, and so many people were outside when the bomb exploded. Presumably the Russians would want to add to the shock value of a strike, and to reduce the risks of it being caught by air defenses, by keeping it a surprise. This would mean that any coercive value would have to be extracted after the event, using it as a warning of more to come.

What sort of event? It is assumed, but who can know, that the aim would be to combine any coercive value with a direct military value. This is why the focus is on the short-range low-yield 'battlefield' weapons, sometimes mistakenly described as 'tactical' (any nuclear use has strategic repercussions). This is where the analysis gets tricky.

The Russian armed force have thought long and hard about nuclear strategy. A detailed and subtle analysis by Michael Kofman and Anya Loukianova Fink shows that at least in theory the Russian military do not believe that limited nuclear use necessarily leads to uncontrolled escalation. The potential targets for limited nuclear strikes are those already identified for conventional strikes –critical infrastructure more than cities. How far this would be taken once the first threshold had been passed would depend on the opponent's reaction. Russian thinking on the matter, however, is geared to great power conflicts, and not an attempt to crush a supposedly weaker and smaller neighbor. Moreover, this is the sort of escalation that Putin was talking about in his Uzbekistan press conference for which he does not need nuclear weapons to have the desired effect.

That leaves the question of using the weapons to affect the ongoing battles underway on the ground. Here it is worth noting the issues that surround any attempt to use these as if they were normal weapons of war. In this role they can be seen as uniquely powerful versions of conventional munitions – from bombs, depth charges, shells, and mines, with the added ingredient of radiation. In this regard they are best employed against large targets, for example a gathering of troops preparing for an offensive. The alternative would be a strong defensive position. Ideally this target would be some distance away from Russian troops. (The Americans famously developed a nuclear gun – the Davy Crockett – which had a lethal radius greater than its range).

Given the nature of the fighting in Ukraine this is not at all straightforward. There are rarely massed formations operating in either defense or attack. Units tend to be dispersed. Consider an account (from a Russian source) about the offensive in Kherson. It notes that the Ukrainians have made their impact by messing with the Russian supply lines while advancing not by armored thrusts (unlike Kharkiv) but instead by using small groups of infantry 'creeping' forward over watery ground, for this is an area cut through by irrigation canals. Finding a useful target for nuclear use in such circumstances would be difficult, and, given how little it might achieve, a strange way to start a nuclear war. Moscow has shown no great care for the populations of Luhansk and Donetsk, but as their liberation is supposedly at the heart of Russian war aims it would also be strange to mark this by nuclear detonations.

Conclusion

There is no evidence for now that weapons are being moved into position or being prepared for such strikes. US intelligence, which has been extraordinarily precise so far can be expected to pick up any details (or at least the Russian would need to assume that). No effort has been made to explain to the Russian public why such strikes might be necessary. After all Putin still insists that this is a limited operation and has refused to put the country on a war footing. As we have seen Russian figures talk garrulously about scenarios for nuclear use against NATO countries but not Ukraine. We can also assume that neither of Putin's recent interlocutors - Xi and Modi - would be enthused. This is a scenario largely generated in the West trying to anticipate contingencies that have yet to be reached.

It is true that the prospect of nuclear use might engender panic in Ukraine and NATO. It is also hard to imagine that the news would be greeted calmly in Russia. It could intensify opposition in Moscow to Putin. He would of course need a compliant chain of command to implement an order to go nuclear, especially as part of a complex military operation on the ground. If the wind catches radioactive dust close to the borders it could fall on Russian territory.

Even if use did make a difference the fundamental political problem would still be there: how to pacify a hostile population with a depleted army. Meanwhile nuclear threats do serve an important purpose for Putin, in deterring more direct NATO engagement. Should he use nuclear weapons in a limited and possibly futile way, the threshold would still have been crossed and all bets would be off in terms of a NATO response, which might well include doing exactly those things Putin was trying to deter. This would also be true of possible Ukrainian moves against Belgorod and Crimea.
There is one qualification to this analysis, which is Crimea. This territory was seized from Ukraine in 2014 and Ukraine wants it back. Militarily this would be even more challenging than the other acts of 'de-occupation' that Ukraine wants to achieve. There are ways of making the Russian hold on Crimea more difficult without a military assault, and Zelensky has spoken of this as a problem that might require a diplomatic solution, although if Russia shows no interest in a negotiated withdrawal his forces will keep on going. Rather than fretting about some future craziness, efforts might more usefully be put into preparing for the moment when Putin realizes that he has lost and may seek to hold on to Crimea. At this time all the issues connected with ending this war – sanctions, reparations, war crimes, prisoner exchanges, and security guarantees – would need to be addressed. We may find it difficult to imagine that Putin can lose, and wonder about how well he will cope with his failed aggression, but it is entirely possible that at some point he will run out of options, and have to look failure in the eye.

Lawrence Freedman is Emeritus Professor of War Studies at King's College London. Among his books is The Evolution of Nuclear Strategy.

The EU has delivered 5 million iodine tablets in case of a nuclear emergency

Source: https://hellas.postsen.com/world/amp/117972

Sep 23 – Lithuania's support for refugees from Ukraine was underlined by the Health and Food Safety Commissioner Stella Kyriakidou at a press conference in Vilnius.
"**Our support to Ukraine is ongoing and will continue for as long as needed** Ms. Kyriakidou noted, pointing out that "more than 1,300 Ukrainian patients have been transferred for treatment in European hospitals."
"We have also delivered 5 million iodine tablets in case of a nuclear emergency," the European Commissioner said.
He also mentioned that the EU has created **medical hubs in Poland, Romania and Slovakia,** in order to facilitate the transport of patients fleeing the war in Ukraine.

EDITOR'S COMMENT: There is a strange feeling the EU (and NATO) are dearly wishing for a Russian nuclear attack or a nuclear power plant accident!

How to Deter Russian Nuclear Use in Ukraine—and Respond if Deterrence Fails

Source: https://www.homelandsecuritynewswire.com/dr20220923-how-to-deter-russian-nuclear-use-in-ukraine-and-respond-if-deterrence-fails

Sep 23 – Russia might use nuclear weapons to achieve its goals in the war in Ukraine—a risk that has only grown as Russian forces confront Ukrainian counteroffensives. Such nuclear use could advance the Kremlin's military aims, undermine US interests globally, and set off a humanitarian catastrophe unseen since 1945. Matthew Kroening writes for the Atlantic Council that to deter such a potential disaster, the United States should issue public, deliberately vague threats of serious consequences for any Russian use of nuclear weapons and be prepared to follow through with conventional military strikes on Russian forces if deterrence fails.

Nuclear Weapons in Russian Strategy
Kroening writes that nuclear threats are core to Russia's military strategy, and there is a nonzero chance that Russian President Vladimir Putin will order a nuclear strike on Ukraine.

- Russia's so-called "escalate-to-de-escalate" strategy calls for nuclear threats and, if necessary, limited nuclear use to compel the end to conflict on terms favorable to Moscow.
- Putin has made a series of nuclear threats against the United States and the West, with the aim of preventing them from coming to Ukraine's defense.
- In addition, Russia has employed dual-capable weapons (which can carry both nuclear and conventional warheads) against Ukraine and conducted exercises with its nuclear forces.

- ❖ Putin may believe that he could use nuclear weapons to compel the United States and the West to cease their support for Ukraine.
- ❖ Russia has a wide range of options for conducting nonstrategic nuclear attacks by using one or more of the thousands of low-yield, battlefield nuclear weapons it already possesses. Russia could employ such nuclear weapons in a limited way against Ukrainian forces, bases, logistics hubs, and even cities.

Preventing Russian Nuclear Use

Kroening writes that in order to prevent Russia from employing nuclear weapons in Ukraine, the United States should issue a clearer deterrent threat. It could choose between vague or explicit threats issued publicly or privately.

- ❖ At present, Putin may believe that he could use nuclear weapons without a significant Western response. A clearer US deterrent threat would help disabuse him of that notion.
- ❖ A vague threat (e.g., "Russia's decision to use nuclear weapons in Ukraine would risk the gravest possible consequences") has the benefit of conveying to Russia that there would be repercussions for nuclear use without committing the United States to a particular course of action.
- ❖ A more specific threat (e.g., "It shall be the policy of this nation to regard any nuclear attack against Ukraine as an attack on the United States, requiring a full retaliatory response") would have greater deterrent value but limit US flexibility.
- ❖ While a vague threat could be dismissed as cheap talk, a more specific threat runs the risk of drawing a "red line" that Washington cannot enforce, making a vague threat the better option.
- ❖ These threats could be conveyed privately, but a public threat would likely be more effective in deterring Russia and assuring allies, as US credibility would be on the line for the world to see.

U.S. Response to Russian Nuclear Use

Kroening write that a clearer threat should be sufficient to deter a Russian nuclear attack, but Washington must be prepared to execute its threat if deterrence fails.

Retaliatory option 1: The United States could intensify its current approach: increasing sanctions on Russia, further isolating Moscow internationally, arming Ukraine with more advanced weapons, and redoubling efforts to militarily reinforce Eastern Europe.

Retaliatory option 2: The United States could respond with military force.

- ✓ **Option 2A:** The United States could conduct a limited conventional strike on the Russian forces or bases directly involved in the attack. A more robust version of this option would be to join the war on Ukraine's side.
- ✓ **Option 2B:** The United States could use nuclear weapons to respond to and deter further Russian nuclear use in Ukraine.

Kroening concludes:

> Given the costs and benefits above, the best US response if deterrence fails may be a mix of options 1 and 2A: an intensification of ongoing efforts to counter Russian aggression in Ukraine and a limited conventional strike against the Russian forces or bases that launched the nuclear attack.

Getting Serious About the Threat of High-Altitude Nuclear Detonation

Source: https://www.homelandsecuritynewswire.com/dr20220923-getting-serious-about-the-threat-of-high-altitude-nuclear-detonation

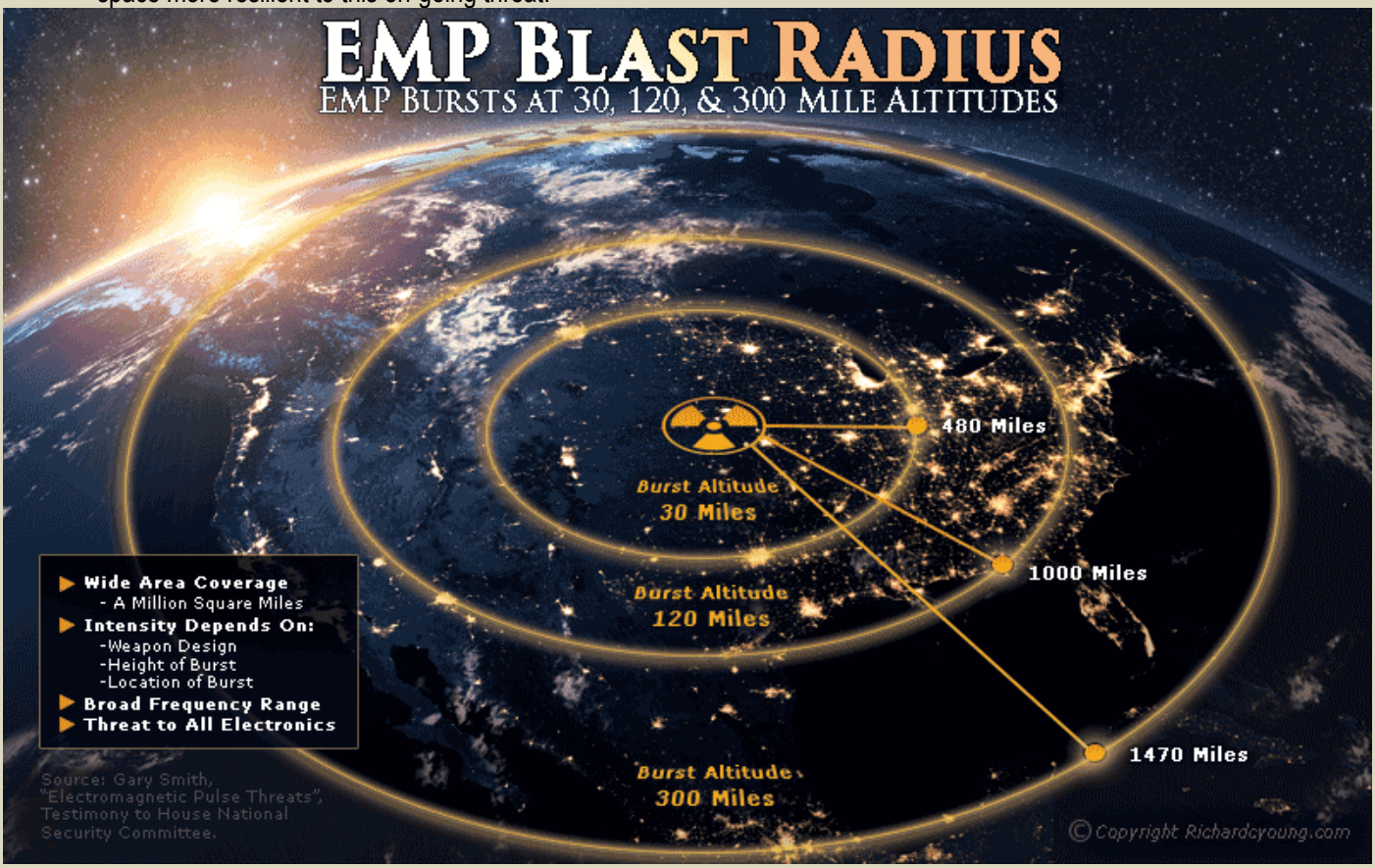
Sep 23 – Aurora Borealis is the scientific term given to the natural light phenomenon of the Northern Lights. On July 9, 1962, the light phenomenon that Hawaiians watched was anything but natural. On that day, the Atomic Energy Commission, in collaboration with the Defense Atomic Support Agency, detonated a thermonuclear device in low Earth orbit. Robert "Tony" Vincent writes in *War on the Rocks* thatthe test, codenamed Starfish Prime, revealed an unfortunate lesson: Even one high altitude nuclear detonation is particularly effective at destroying satellites. Not only were satellites in the line of sight destroyed, but even satellites on the other side of Earth were damaged and rendered inoperable. Starfish Prime damaged or destroyed roughly one third of all satellites in low Earth orbit at the time.

Vincent writes:

> The ongoing commercialization of space with cost effective bulk electronics presents a tantalizing target for nations with a space disadvantage to target long-before a conflict could escalate to nuclear exchange. Therefore, the Department of Defense should get serious about planning for and countering the threat of high-altitude nuclear detonations, starting with its various science and technology funding organizations.

To do so, the Department of Defense should consider developing a coherent research portfolio with consolidated oversight that aims to maximize the survivability of military and commercial satellites from charged particle radiation. The portfolio should focus on rapidly characterizing the space radiation environment, disseminating this information for satellite countermeasures, vectoring excess charged particles out of orbit, and continuing to subsidize the ongoing commercialization of radiation resilient electronic components.

The threat of nuclear explosions in space is marginalized because the potency of their effects is not widely known and the likelihood of nuclear attack in space is assumed to be negligible. Despite this skepticism, war planners should recognize that the growing number of satellites in space may change the incentive structures to disable them in some sort of nuclear attack. The dynamics of escalation are also not straightforward. The use of a nuclear weapon in space may not invite a nuclear response. This means that the traditional way to deter nuclear use — the threat of catastrophic reprisal — may not be as straight forward as many think. Taken together, there is ample incentive to explore making American infrastructure in space more resilient to this on-going threat.



Vincent writes that current risk mitigation of the threat of high altitude nuclear detonations myopically focuses on radiation hardening of electronics, which is insufficient, and simply pretending the likelihood of attack is near zero. "The Department of Defense should invigorate efforts to counter the threat of high altitude nuclear detonations and recognize that the ongoing commercialization of space will lead to an even greater dependency of low Earth orbiting platforms that will remain vulnerable to the charged particle outputs of nuclear explosions," he writes.

Vincent concludes:

The possibility of high-altitude nuclear weapons targeting space assets is not a novel threat, but one that is historically dismissed. The nature of orbiting around Earth means that space assets are periodically exposed in highly predictable patterns. In fact, delivering a nuclear weapon into low earth orbit is an easier engineering challenge for a nation like North Korea than targeting the continental United States because the missile's warhead has to survive the drag and heat of atmospheric reentry. Space assets are not just tempting targets but become more provocative with each supported military operation. Therefore, the Department of Defense needs to form a coherent research and development plan with a dedicated lead to champion the mission of countering high altitude nuclear detonations.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

EXPLOSIVE NEWS

UK to provide underwater drones to help Ukraine demine sea coast

Source: https://english.nv.ua/nation/uk-to-provide-underwater-drones-to-help-ukraine-demine-sea-coast-50266064.html

Aug 27 – The UK is to give Ukraine six underwater drones to help it demine its coast and ensure it is safe for ships to export Ukrainian grain, Sky News reported on Aug. 27.

The UK Ministry of Defense announced that the British Navy is currently teaching Ukrainian sailors to use underwater mine-detecting drones. Around a dozen Ukrainian servicemen have already completed the three-week course, and dozens more are to be trained in the coming months. The UK will provide three drones from its own stocks, and will purchase three more.

The drones are designed to operate in shallow coastal waters at depths of up to 100 meters. They survey the bottom of the sea **using sonar to locate mines**.

According to one of the Ukrainian sailors interviewed by Sky News, the drones will be needed to clean up the sea, "especially in the very critical region near Odesa."

Sky News said under the current circumstances, it could take a decade to completely clear the Ukrainian coastline of mines.

UK Admiral Alan West said the underwater drones would be "a game changer for the Ukrainian Navy" by clearing the main route of ports for further exports.

Earlier, Ukrainian President Volodymyr Zelenskyy said the first million tons of agricultural products from the Ukrainian seaports of Chornomorsk, Odesa and Pivdennyi have been exported after a month of work of the grain export deal. According to him, Ukraine aims to reach an export level of three million tons of grain per month. During a visit to Kyiv on Aug. 24, UK Prime Minister Boris Johnson announced a new £54 million military aid package for Ukraine. It includes drones and anti-tank munitions.

Identifying and Neutralizing New Explosive Threats

Source: https://www.homelandsecuritynewswire.com/dr20220915-identifying-and-neutralizing-new-explosive-threats

Sep 15 – With the Iraq and Afghanistan Wars in the rearview mirror, the Defense Department is preparing for a new era of explosive ordnance disposal which will bring fresh challenges and require new technology solutions. Improvised explosive devices (IEDs) planted by insurgents were one of the top threats during the post-9/11 conflicts. But now, the U.S. military is refocusing on neutralizing bombs

and mines that it could face in future conflicts against more advanced adversaries.

The 2022 EOD/IED & Countermine Symposium will highlight current initiatives toward identifying and neutralizing explosive threats towards the homeland and critical infrastructure. Attendees will have the opportunity to learn of emerging technologies and hear about the capabilities urgently needed to better equip Warfighters for future large scale combat operations, including vehicle-mounted counter-IED systems and unmanned systems.

This symposium will feature senior level-speakers and sessions, including:

- **Developing Adaptive Ordnance Professionals to Effectively Sustain Army Readiness & Win in Multi-Domain Operations**
  BG Michael Lalor, Chief of Ordnance, Commandant, U.S. Army Ordnance School
- **Directing the Overall Planning & Programming for Expeditionary Warfare Systems & Related Manpower, Training & Readiness**
  BGen Marcus Annibale, USMC, Director, Expeditionary Warfare, OPNAV N95
- **Leading USAF EOD Initiatives Toward Preparing for New Era of Explosive Ordnance Disposal**
  Brig Gen Brian S. Hartless, USAF, Deputy Director, Resource Integration, Incoming Air Force Director of Civil Engineers, Deputy Chief of Staff for Logistics, Engineering and Force Protection, HQAF
- **Ensuring Acquisition in Excellence by Delivering Dominating Close Combat Capabilities to the Warfighter to Win in MDO**
  COL Russell Hoff, USA, Project Manager, Close Combat Systems, Joint Program Executive Office Armaments & Ammunition
- **Guiding 71st Ordnance Group Efforts to Ensure an Effective Response to all CBRNE and WMD Threats**
  COL Michael Schoonover, USA, Commander, 71st Ordnance Group
- **Conducting NAVSEA's R&D Efforts Toward Finding Ordnance, Energetics, & EOD Solutions to the Warfighter**
  CAPT Eric C. Correll, USN, Commanding Officer, Naval Surface Warfare Center Indian Head Division

To allow for actionable discussion and dialogue amongst speaker and attendees, seating will be limited. Register now to reserve your seat. Active military and government and state personnel attend complimentary.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

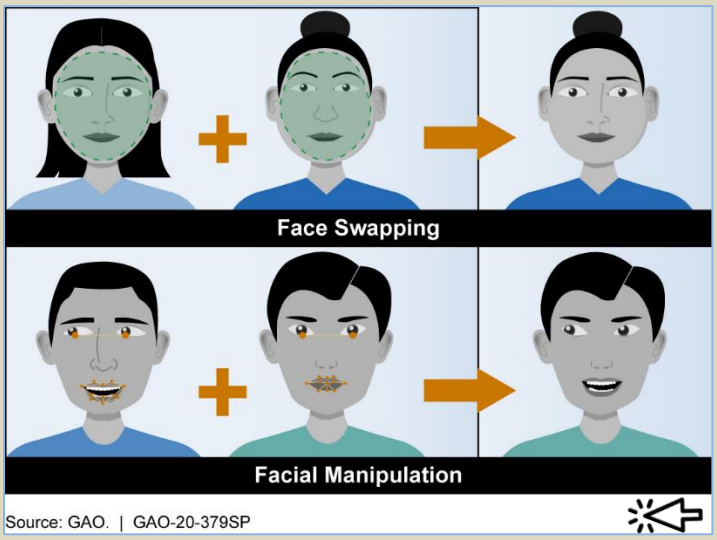
Meet the company working with the Air Force to detect deepfakes

By Hayden Field

Source: https://www.emergingtechbrew.com/stories/2022/08/22/meet-the-company-working-with-the-air-force-to-detect-deepfakes

Aug 22 – Two of the ways DeepMedia makes money: by creating deepfakes and by detecting them.

Rijul Gupta, a former machine learning engineer, co-founded the Bay Area startup in 2017 with Emma Brown as a way to communicate in Hindi with his extended family. The tool they built, DubSync, currently allows someone to appear to be speaking any one of 10 languages, using translation, vocal synthesis, dubbing, and facial animation.



Now, the company claims it's working with some of the biggest names in streaming, but would not share specific clients or partnerships. According to Gupta, it's currently on track to generate between $300,000 and $500,000 in revenue this year.

In the years since DeepMedia's debut, the team—now a group of about 20—has also begun pursuing its other mission: *detecting* synthetic audio and video. And they're doing it via partnerships, including one with the Air Force Research Laboratory, the division's primary science R&D arm and part of the Department of Defense. Announced in April, the grant involves developing deepfake detectors for faces, voices, and aerial imagery. One of the ways DeepMedia trains these detector tools is by constantly creating datasets of advanced deepfakes, using the company's own generation tools.

By December 2022 or early 2023, DeepMedia plans to release a public deepfake detection product: a web-based tool that allows individual consumers or enterprises—for example, political candidates looking to verify or prove video authenticity—to pay to upload content and receive a report explaining whether the content is falsified, the algorithm that was initially used to create the deepfake, and how the company came to that conclusion.

As of now, Gupta said, the company's deepfake detectors work at about 95% accuracy across "most deepfake modalities on synthetic faces, voices and aerial imagery." He said the company won't release them until they're at 99% accuracy.

"The worst thing for us would be to release a tool, and it says something's fake when it's actually real, or it says something's real, when it's actually fake," Gupta said, noting that "no machine learning algorithm is ever 100% accurate—those types of issues will always be present."

Diving into detection

There are already a range of deepfake detection tools out there, so DeepMedia had competition for the DOD grant. To win, the team demonstrated that the deepfakes it had generated could only be detected by the company's own detectors and not by other existing tools. Gupta attributes its success, in part, to how quickly overall deepfake quality is advancing, and that existing deepfake datasets—like Deepfake Detection Challenge Dataset (DFDC), DeeperForensics, and FaceForensics—can become obsolete in just a few years' time.

"[Existing datasets] don't represent the modern quality of deepfakes that we're seeing, like deepfake Zelenskyy video, for example," Gupta told us, referencing a viral synthetic video of Vladimir Zelenskyy from March, in which the Ukrainian president appears to tell the country's troops to surrender. "The algorithms used to create that deepfake are not in the deepfake datasets that are publicly available."

Those datasets also are significantly lacking in data for Black and Latino individuals, and the data skews male, Gupta said—meaning that tools trained solely on those datasets could tend to classify videos of minorities as authentic, even when they're synthetic.

DeepMedia uses those existing datasets as benchmarking tools for its model training.

The company's AI detection process starts with a lot of pre-processing steps. Say you uploaded a video that seemed to feature President Biden and wanted to check its authenticity: First, the models would need to detect the president's face in that video, analyze facial landmarks, pick out the voice and extract it from background noise, and more—all before the deepfake detection begins. Next, the content is run through a series of detectors, including a binary classifier of real versus fake for both video and audio. Finally, the content is

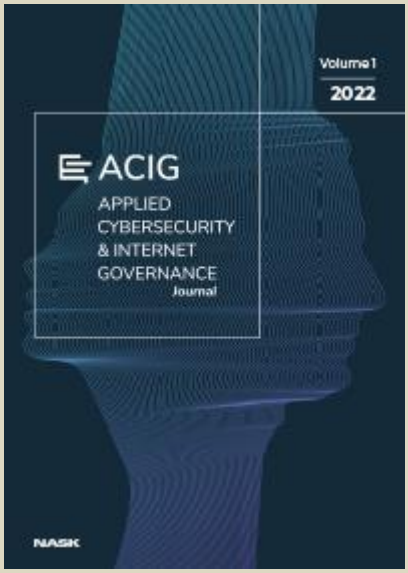
examined by convolutional neural networks, which attempt to pick out which algorithm, or algorithms, were used to create a deepfake. DeepMedia is also beginning to use vision-based Transformer models—the same model architecture Google uses to pull up relevant search results—to build detection networks. Transformer models can train 10 times faster than the convolutional neural networks that the company currently uses, Gupta said, and end up with similar accuracy metrics.

The company is still building out its detectors' capabilities by developing new datasets, but there's still the potential for bias against vulnerable communities. "It's not perfect—we don't have an exact equal number between all different races," he said. "But it's close enough to being equal, where we can get accuracy metrics that do work. So as opposed to having 100 videos of people of color and 100,000 of white people, it might be 50,000 [of] white people and 55,000 [of] people of color."

Hayden Field is a NYC-based journalist. She reports on AI, shifting power dynamics in the tech industry, and all things emerging technology. She writes Emerging Tech Brew, a reported newsletter about cutting-edge technology, as well as longer-form feature articles. Nearly 300,000 readers turn to Emerging Tech Brew for the latest on AI, robotics, self-driving cars, and everything else shaping the future of business. Hayden's work has also appeared in Protocol, MIT Technology Review, WIRED UK, Entrepreneur, Fortune, and more.

Applied Cybersecurity & Internet Governance

Source: https://acigjournal.com/resources/html/cms/MAINPAGE

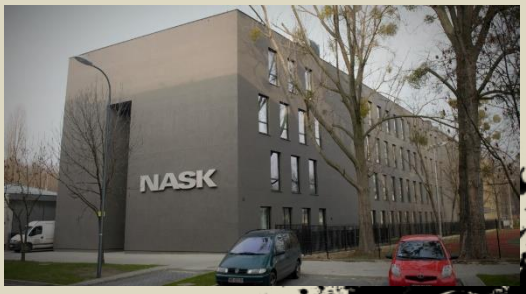


Applied Cybersecurity & Internet Governance is a peer-reviewed, open-access journal that provides a platform for debate on crucial and strategic cyber challenges facing both national institutions and multinational corporations. The Editorial Board does not charge the authors for the submission and publication of papers. The journal aims to create an open space to publish cybersecurity research from various regional, sectoral, and thematic perspectives. Such multifaceted knowledge lends a voice to the ongoing debate on the importance and role of cybersecurity in social, political, and technological settings. ACIG's mission is not only to highlight the fundamental role that cyber technology plays today, but also to emphasize the interdisciplinary nature of research that provides a fresh take on the nature of modern cybersecurity challenges. It is an opportunity to present scientific achievements, as well as studies of academic communities in Central Europe, but also to strengthen the harmonization of global cooperation. Thus, the papers published in the journal contribute to increasing knowledge and gaining a better understanding of the ongoing processes of digital technologies today. The editors welcome original research papers that extend the existing knowledge in the field of cybersecurity, both theoretically and empirically.

Scope

- Network and Critical Infrastructure Security;
- Cybersecurity Data Analysis;
- Privacy Enhancing Technologies for Anonymity;
- IoT Security;
- AI Security;
- Digital Infrastructure;
- Security and Crime Science;
- Security Economics;
- Human Factors and Psychology;
- Cybersecurity Education;
- Legal Aspects of Information Security;
- Perspectives on Cybersecurity Policy;
- Strategy and International Relations;
- Cybersecurity Policy.

Publisher



NASK is a National Research Institute whose mission is to develop and implement solutions that facilitate the development of information and communication networks in Poland, in addition to improving their effectiveness and security. They carry out research and development projects as well as projects aimed at improving the security of Polish civilian cyberspace. Another of NASK's important activities is educating users and promoting the concept of an information society. NASK is the Polish national registry of Internet names in the .pl domain. It also serves as the data networks operator. In the framework of

NASK operates CERT Polska – a team dedicated to responding to network security breaches. NASK is the institution that connected Poland to the Internet in 1991.

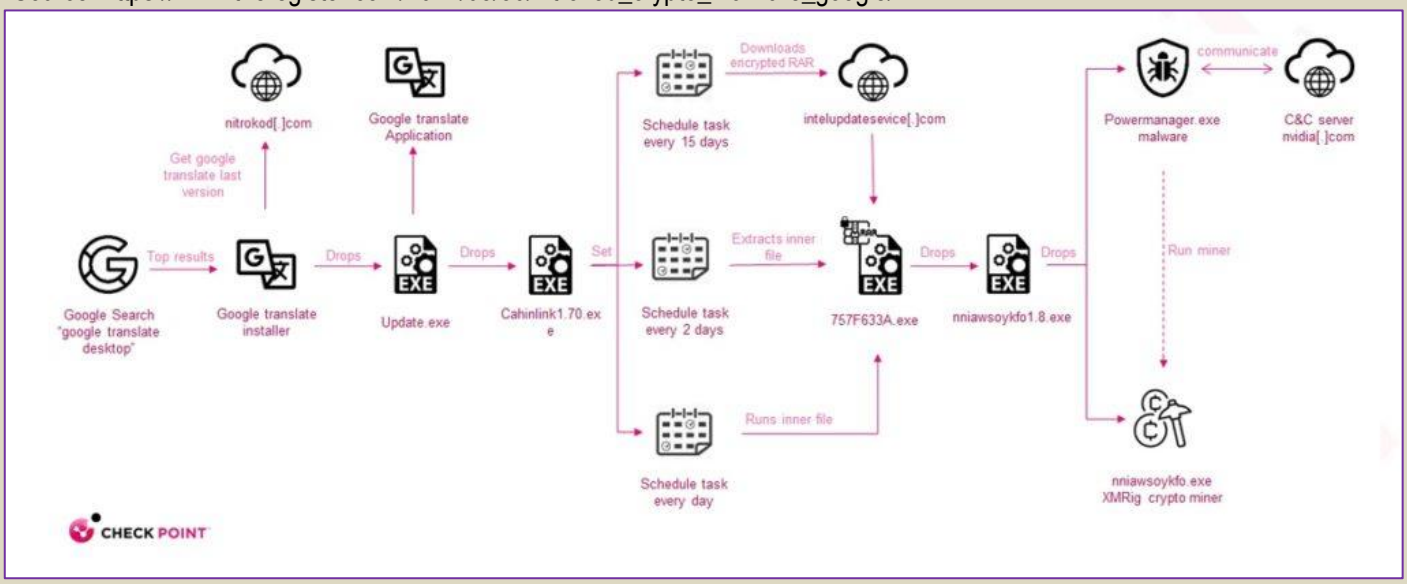
Why Is No One Talking About This Threat?

Source: https://i-hls.com/archives/112006

Sep 03 – **USB drives** are the cyber threat vector no one talks about. Industrial control systems (ICS) and operational technology (OT) environments face cyber threats from malicious USB devices capable of circumventing the air gap to disrupt operations from within. 79% of USB drive attacks can potentially disrupt the operational technologies that power industrial processing plants.
Ransomware attackers rely on USBs to deliver malware, jumping the air gap that all industrial distribution, manufacturing, and utilities rely on as their first line of defense against cyberattacks.
The study finds the incidence of malware-based USB attacks is one of the fastest-growing and most undetectable threat vectors that process-based industries such as public utilities face today.
Industrial Control Systems are among the most porous and least secure enterprises systems, a fact that makes them a prime target for ransomware.
USB-based threats rose from 19% of all ICS cyberattacks in 2019 to just over 37% in 2020, the second consecutive year of significant growth, according to the report.
Ransomware attackers prioritize USBs as the primary attack vector and delivery mechanism for processing manufacturing and Utility targets.
AI and machine learning (ML) technologies can help create and fine-tune continuously learning anomaly detection rules and analytics of events, so they can identify and respond to incidents and avert attacks. ML is also used to identify a true incident from false alarms, according to venturebeat.com.
The report was based on aggregated cybersecurity threat data from hundreds of industrial facilities globally during a 12-month period.
Along with USB attacks, research shows a growing number of cyber threats including remote access, Trojans and content-based malware have the potential to cause severe disruption to industrial infrastructure.

That 'clean' Google Translate app is actually Windows crypto-mining malware

Source: https://www.theregister.com/2022/08/30/nitrokod_crypto_malware_google/



Aug 30 – Watch out: someone is spreading cryptocurrency-mining malware disguised as legitimate-looking applications, such as Google Translate, on free software download sites and through Google searches.
The cryptomining Trojan, known as Nitrokod, is typically disguised as a clean Windows app and works as the user expects for days or weeks before its hidden Monero-crafting code is executed.
It's said that the **Turkish-speaking group behind Nitrokod** – which has been active since 2019 and was detected by Check Point Research threat hunters at the end of July – may already have infected

thousands of systems in 11 countries. What's interesting is that the apps provide a desktop version to services generally only found online.
"The malware is dropped from applications that are popular, but don't have an actual desktop version, such as Google Translate, keeping the malware versions in demand and exclusive," Check Point malware analyst Moshe Marelus wrote in a report Monday.
"The malware drops almost a month after the infection, and following other stages to drop files, making it very hard to analyze back to the initial stage."
Along with Google Translate, other software leveraged by Nitrokod include other translation applications – including Microsoft Translator Desktop – and MP3 downloader programs. On some sites, the malicious applications will boast about being "100% clean," though they are actually loaded with mining malware.
Nitrokod has been successful using download sites such as Softpedia to spread its naughty code. According to Softpedia, the Nitrokod Google Translator app has been downloaded more than 112,000 times since December 2019.
According to Check Point, the Nitrokod programmers are patient, taking a long time and multiple steps to cover up the malware's presence inside an infected PC before installing aggressive cryptomining code. Such lengthy, multi-stage infection efforts allowed the campaign to run undetected by cybersecurity experts for years before finally being discovered.
"Most of their developed programs are easily built from the official web pages using a Chromium-based framework," he wrote. "For example, the Google translate desktop application is converted from the Google Translate web page using the CEF [Chromium Embedded Framework] project. This gives the attackers the ability to spread functional programs without having to develop them."
After the booby-trapped program is downloaded and the user launches the software, an actual Google Translate app, built as described above using Chromium, is installed and runs as expected. At the same time, quietly in the background the software fetches and saves a series of executables that eventually schedule one particular .exe to run every day once unpacked. This extracts another executable that connects to a remote command-and-control server, fetches configuration settings for the Monero miner code, and starts the mining process, with generated coins sent to miscreants' wallets. Some of the early-stage code will self destruct to cover its tracks.
"At this point, all related files and evidence are deleted and the next stage of the infection chain will continue after 15 days by the Windows utility schtasks.exe," Marelus wrote. "This way, the first stages of the campaign are separated from the ones that follow, making it very hard to trace the source of the infection chain and block the initial infected applications."
One stage also checks for known virtual-machine processes and security products, which might indicate the software is being analyzed by researchers. If one is found, the program will exit. If the program continues, it will add a firewall rule to allow incoming network connections.
Throughout the multiple stages, the attackers use password-protected RAR encrypted files to deliver the next stage to make them more difficult to detect.
Check Point researchers were able to study the cryptomining campaign through the vendor's Infinity extended detection and response (XDR) platform, Marelus claimed.

Warning: cyber criminals are launching phishing attacks on LinkedIn

Source: https://www.yahoo.com/now/warning-cyber-criminals-launching-phishing-033334123.html

Aug 25 – Regular users of LinkedIn, the professional networking and social working platform, have noticed an increase of threat actors trying to steal critical personal information through phishing attacks. These cyber criminals are using false LinkedIn accounts to trick unsuspecting victims into giving up confidential information.
How are they doing it? Threat actors start by creating fraudulent LinkedIn profiles and generate vast networks with multiple other accounts to make their fake accounts seem more credible. At this point, they begin targeting active accounts with phishing emails acting as recruiters or as individuals who want to help expand other networks. With these phishing emails, some create false recruitment documents which have you input critical information. These documents may also have dangerous links that send you to a webpage where you are asked to download files that are harmful and have hidden payloads.
So, what can you do to mitigate the risk? If you currently have and use an active LinkedIn account, whenever receiving emails from a person you personally do not know, be skeptical of anything they send you. Do not download anything unless you are sure it holds no negative payloads, and hover over each link provided to verify it is taking you to a location you expect.
It may take extra time and diligence to vet every LinkedIn invitation or email, but you can't be too careful when it comes to protecting your valuable information and assets.

●▶ For more information, contact Javier Young at javier.young@CLAconnect.com or 704-816-8470. For more information on CliftonLarsonAllen LLP, visit CLAconnect.com.

French hospital hit by $10M ransomware attack, sends patients elsewhere

Source: https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/

Aug 23 – The Center Hospitalier Sud Francilien (CHSF), a 1000-bed hospital located 28km from the center of Paris, suffered a cyberattack on Sunday, which has resulted in the medical center referring patients to other establishments and postponing appointments for surgeries.

CHSF serves an area of 600,000 inhabitants, so any disruption in its operations can endanger the health, and even lives, of people in a medical emergency.

"This attack on the computer network makes the hospital's business software, the storage systems (in particular medical imaging), and the information system relating to patient admissions inaccessible for the time being," explains CHSF's announcement (translated).

The hospital's administration has not provided further updates on the situation, and the IT system outage that enforced reduced operations still plagues the establishment.

Those in need of emergency care will be evaluated by CHSF's doctors, and if their condition requires medical imaging for treatment, they will be transferred to another medical center.

According to Le Monde, which has info from the country's law enforcement agencies, the ransomware actors that hit CHSF demanded the payment of a **ransom of $10,000,000 in exchange for a decryption key.**

"An investigation for intrusion into the computer system and for attempted extortion in an organized gang has been opened to the cybercrime section of the Paris prosecutor's office," a police source told Le Monde, also specifying that "the investigations were entrusted to the gendarmes of the Center fight against digital crime (C3N)".

The LockBit 3.0 hypothesis

French cybersecurity journalist Valéry Riess-Marchive identified signs of a LockBit 3.0 infection, mentioning that the handling by the national gendarmerie is a clue pointing to that direction, as that service deals with Rangar Locker and LockBit attacks.

As Riess-Marchive explains at LegMagIT, Ragnar Locker is unlikely to be behind the attack due to a different focus on the economic size of its victims, whereas LockBit 3.0 demonstrates a broader targeting scope.

If LockBit 3.0 is responsible for the attack on CHSF, it will violate the RaaS program's rules, which prohibit affiliates from encrypting systems of healthcare providers.

At this time, the attribution to the particular threat group hasn't been confirmed yet, and LockBit 3.0's extortion site contains no entry for CHSF yet, so their involvement remains a hypothesis.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

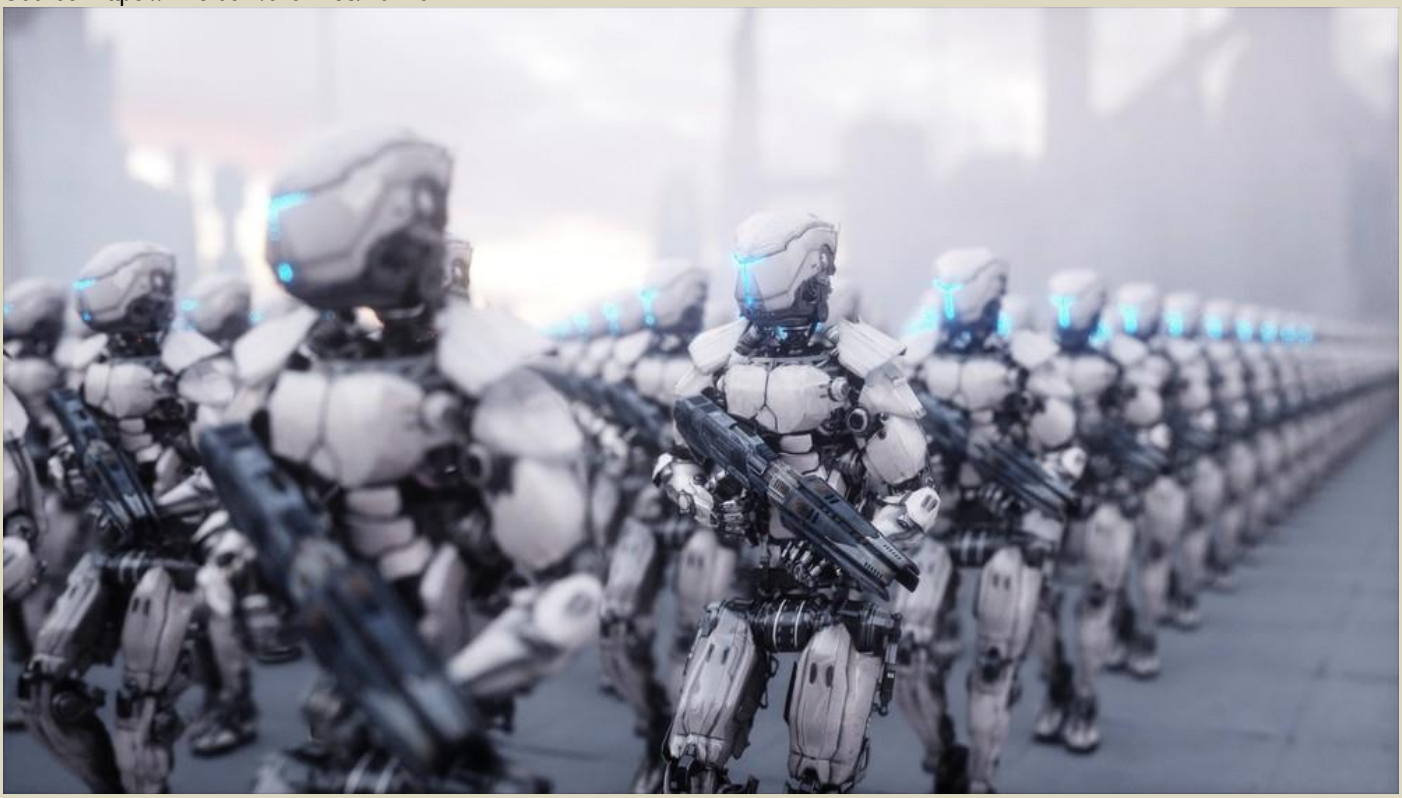
C²BRNE DIARY

& Robotic

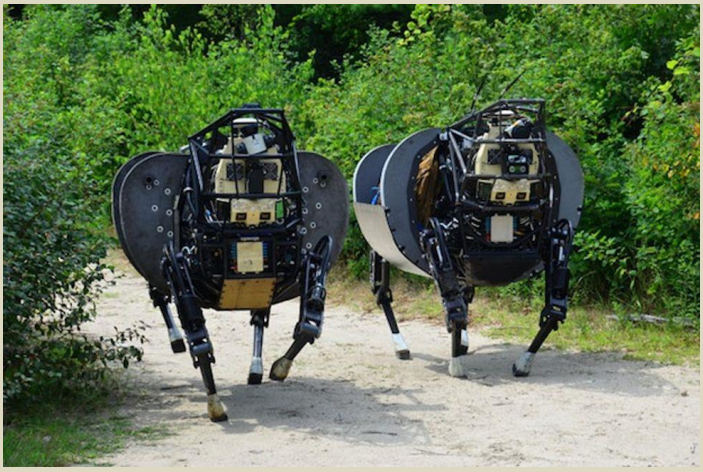
DRONE NEWS

British Army Looking To Replace Soldiers With Robots

Source: https://i-hls.com/archives/107791



Apr 23 – Over the next decades, the British army may enlist tens of thousands of robotic soldiers. In the face of new emerging technologies and changing military landscapes, and as part of a major military overhaul, the United Kingdom's Army is about to



shrink by 10,000 soldiers. Part of the move to restructure the military is to invest more heavily in military robots, drones, and other tools of high-tech combat. Overall, the update represents an adaptation to the changing face of warfare — with more of an emphasis on cyberwarfare than ground troops.

UK Defence Secretary Ben Wallace said "increased deployability and technological advantage" meant greater effect could be delivered by fewer people, setting out plans for new capabilities such as electronic warfare and drones in the Commons.

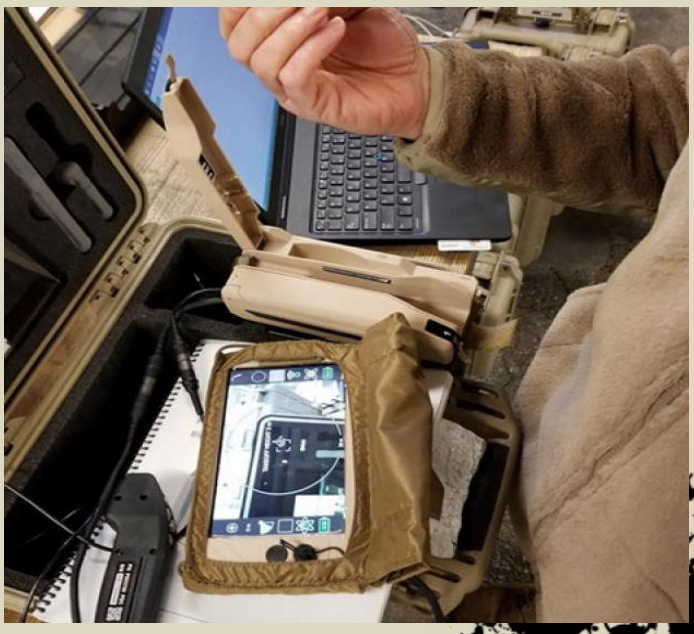
The UK's Army had about 80,000 troops — considerably fewer than a decade ago. The plan now is to bring that number even further down to about 70,000, mostly by letting soldiers retire or leave and choosing to not replace them, according to the BBC.

Meanwhile, the Army is investing more heavily in drones and combat robots — something that a British general previously suggested could make up a large fraction of the armed forces.

General Nick Carter, chief of defense staff for the British army, said that a massive push for a robotic military, in which large numbers of autonomous or remote-controlled robotic soldiers replace human fighters, could be operational by the 2030s.
The shift also means putting more resources into cyberwarfare by expanding the military's national cyber force and establishing a space command that sounds like it will function similarly to the US Space Force, as reported by futurism.com.

Norway and Great Britain to transfer to Ukraine Black Hornet micro unmanned aerial vehicles and NightFighter anti-drone systems

Source: https://mil.in.ua/en/news/norway-and-great-britain-to-transfer-to-ukraine-black-hornet-micro-unmanned-aerial-vehicles-and-nightfighter-anti-drone-systems/



Aug 24 – Norway and Great Britain are joining efforts to acquire the Norwegian micro-drone Black Hornet and donate it to Ukraine.
The Ministry of Defense of Norway reported this.
Ukrainian authorities have asked for this type of equipment in the fight against the Russian invasion.
The price will be up to NOK 90 million ($9.1 million). The package includes Black Hornet units, spare parts, transportation and training costs.
The Norwegian Ministry of Defense noted this assistance will be financed by the British-led fund to which Norway has contributed NOK 400 million.
The Norwegian-developed drone is a global market leader. It is used in a number of allied countries, including the United States and Great Britain. The drone is used for reconnaissance and target identification, says Norway's Defense Minister Bjørn Arild Gram. The Black Hornet is easy to operate, robust, difficult to detect, and particularly well suited for combat in urban areas.

The Black Hornet is a micro helicopter unmanned aerial vehicle weighing 18 g that can operate without recharging for 25 minutes. **Having a diameter of the main screw of 120 mm, the drone reaches a speed of more than 20 km/h, while the operating range is about 2 km.**
The kit consists of two drones, a charger and a control tablet. **The weight of the set is about 1.3 kg**.
The fund will also purchase a system for combating drones for approximately NOK 100 million. Nightfighter by British SteelRock Technologies was chosen as the system.
An anti-drone system will also be purchased for approximately 100 million of the Norwegian funds for the fund. The system chosen is the **anti-drone system Nightfighter** from British SteelRock Technologies.

NightFighter anti-drone system. Photo credits: SteelRock Technologies

The SteelRock Nightfighter is a portable system that provides protection against drones through effective jamming.
The system is particularly suitable for protecting smaller patrols, artillery positions, and other important resources.

The Guardian view of medals for drone pilots: morally ambiguous

Source: https://www.theguardian.com/commentisfree/2017/sep/21/the-guardian-view-of-medals-for-drone-pilots-morally-ambiguous

2017 – It seems obvious that members of the armed forces win their medals for facing danger bravely, but this belief would not long survive exposure to a photograph of Prince Charles in uniform. Four of his 11 medals were awarded for simply being alive while his mother was on the throne. There is a long military tradition of handing out decorations to people who have not fought at all.
In this light, the proposal by the Ministry of Defence to strike a medal for the campaign against Islamic State, which would be given to drone operators among other recipients, makes a kind of sense. But it is still morally disturbing. A similar proposal, in the US in 2013, was withdrawn after outrage from fighting soldiers. Their obvious objection is that a drone operator runs no personal risk at all. The same could be said of many specialists on whom a modern army depends, from technicians to staff officers, but most of them are at least in the theatre of war, even if behind the lines. That's why they earn campaign medals even though medals for bravery are reserved for the fighting troops.

Prince Charles poses for an official portrait to mark his 60th birthday in 2008. 'His example does show that there is a long military tradition of handing out decorations to people who have not fought at all.' Photograph: Getty Images

The drone pilots sit thousands of miles from the action, killing people with the press of a button. Rewarding them tends to reinforce the terrible delusion that modern war, as fought by our armed forces, is a hygienic business in which only consenting adults are killed. No drone pilot anywhere seems to have been punished for killing civilians; the British Ministry of Defence argues that none of our 4,000 strikes ever have. But then the only evidence for the effects of most strikes are gathered by the self-same drones.
This is part of the wider moral ambiguity that has always attended killing people from the air. The drone controller 2,000 miles from his victim is different in degree, but not in kind, from the jet pilot who fires a cruise missile from friendly airspace over the horizon at his target. Nor is danger a guarantee of moral purity. The allied airmen who carried out the bombing of German cities in the second world war were undoubtedly heroic. They faced very high odds of death over long tours of duty, but they often set out deliberately to kill as many civilians as possible. Perhaps we should admire more those who were less brave – and less lethal with it.

Air Force recognizes drone pilots with new medal

Source: https://www.stripes.com/air-force-recognizes-drone-pilots-with-new-medal-1.605089

2019 – The Air Force's new Remote Combat Effects Campaign Medal is intended to recognize drone pilots and other airmen who make contributions to combat from a remote location. (Sahara Fales/U.S. Air Force)
A new Air Force campaign medal will recognize drone operators and other airmen who directly supported a combat operation from a remote location.
The Remote Combat Effects Campaign medal is part of an effort to better recognize the combat contributions of airmen who are not deployed, the Air Force said in a statement announcing the award's criteria Monday.
Former Air Force Secretary Heather Wilson established the decoration earlier this year.
Airmen serving in the following career fields are eligible for the award: remotely piloted aircraft; cyber; space or intelligence; surveillance and reconnaissance. Airmen from other career fields may be considered for the medal on a case-by-case basis, service officials said.
To be eligible, an airman's contributions must have occurred on or after Sept. 11, 2001, while assigned or attached to a unit directly in support of a Pentagon combat operation, the criteria states.

An airman must have "personally provided" hands-on employment of a weapon system that has a direct and immediate effect on combat operations, the Air Force said. The airman also cannot have been physically exposed to hostile actions or at risk of exposure to hostile action, though that could qualify them for other awards.

Qualifying combat operations involve several in the Middle East and elsewhere in Asia: Enduring Freedom, Iraqi Freedom, New Dawn, Nomad Shadow, Freedom's Sentinel, Inherent Resolve, Odyssey Lightning and Pacific Eagle – Philippines.

The Pentagon for years has grappled with how to recognize the contributions of service members who influence a military operation thousands of miles away from the front lines.

Drone pilots have played a central role in U.S. efforts targeting extremists, often putting in long hours. The Air Force has struggled to retain drone pilots, with some developing symptoms of post-traumatic stress disorder, studies have shown.

A Pentagon effort in 2013 to recognize "extraordinary actions" of drone pilots and other off-site troops performing noteworthy deeds far away from the battlefield was scrapped due to criticism. Veterans groups objected because the medal would have outranked some awards for troops serving in harm's way, such as the Purple Heart and the Bronze Star with Valor. The new medal is worn lower — above the Air and Space Campaign Medal and below the Military Outstanding Volunteer Service Medal.

In 2016, the Pentagon approved a new distinguishing device that can be affixed to previously awarded medals, including one for engaging an enemy through remote actions.

Will the Drone War Come Home? Ukraine and the Weaponization of Commercial Drones

By Benjamin Fogel and Andro Mathewson

Source: https://mwi.usma.edu/will-the-drone-war-come-home-ukraine-and-the-weaponization-of-commercial-drones/

Aug 22 – Hours after Russia's invasion of Ukraine began in February, Ukraine's Ministry of Defense appealed for civilian drone owners to donate or fly their commercially bought drones to help defend Kyiv. Donations poured in and consumer unmanned aerial vehicles (UAVs) took to the skies amid Russia's advance. Throughout the war, commercial UAVs have been used by Ukrainian regular and special operations forces, Belarusian partisans, Russian infantry, and Russian-led separatists; they demonstrate the challenges, opportunities, and threats emerging from the proliferation of consumer drones. The most common are small, light, and inexpensive rotary-wing quadcopters produced by the Chinese drone maker DJI.

Commercial off-the-shelf (COTS) and homemade drones can offer low-cost and low-risk intelligence, surveillance, and reconnaissance capabilities and are commonly used for target acquisition and for directing artillery or mortar fire. These drones can also be converted into delivery vehicles for improvised explosive devices (IEDs), capable of precision impacts and profound psychological effects. Shortly into the conflict, videos emerged of Ukrainian forces dropping munitions on Russian targets from commercial UAVs, including one popular example where a bomblet was dropped through the sunroof of a Russian

vehicle. These aerial attacks employed modernized RKG-3 antitank grenades and VOG-17 fragmentation grenades and successfully targeted and destroyed mechanized and infantry forces.

Ukraine established an impromptu UAV unit following the 2014 Russian invasion when volunteer IT professionals and drone hobbyists came together to form the Aerorozvidka unit. While primarily used for intelligence collection, Aerorozvidka also modifies commercial drones for kinetic strikes, marking Ukraine as one of the first states to develop and use such a tactic. Employment of lethal COTS drones is neither new nor unique to Ukraine or the region. For example, in 2020, Ukrainian forces reported an attack in Donetsk from a COTS drone–dropped grenade, and in the fall of 2021 the Belarusian resistance claimed to have bombed a Minsk police station with a COTS UAV.

The proliferation of small commercial drones represents a dangerous asymmetric threat that Western governments are ill-prepared to counter. The post-9/11 era coincided with information and digital technology revolutions that lowered the barriers of entry for the modification and use of COTS drones. In turn, smaller states and nonstate actors—including terrorist groups, guerrillas, and lone wolves—have developed precision capabilities previously monopolized by advanced militaries. The very nature of commercially available technology means that innovation is diffusing and any creative actor can develop this capability, eroding the advantage of large states and posing new military and security challenges. Cheap commercial drones carrying self-fashioned explosive devices will not remain limited to theaters of war. In essence, these types of drones have become aerial vehicle-borne improvised explosive devices (AVBIEDs).

Counter-AVBIED capabilities are few and far between and existing techniques have not been effectively tested. The materials to create AVBIEDs are cheap, readily accessible, and easily concealed, and can be legally purchased or effortlessly smuggled into Riga, Prague, Stockholm, or Brussels. A malicious actor could attempt a high-profile attack on a busy intersection or crowded marketplace to achieve the psychological effects of a London- or Nice-style terrorist attack that could leave civilians looking to the skies in terror for the rest of their lives. Western governments must learn a critical technical lesson from Ukraine: how to counter AVBIEDs once unleashed on civilian population centers.

The AVBIED: When the Drone Hobbyist Seeks Terror

Terrorist attacks primarily rely on readily available weapons and materials such as small arms and improvised explosives. Remotely detonated IEDs and vehicle-borne IEDs—car bombs—were two attempts to innovate new asymmetric weapons. Since the development of modern drones in the mid to late twentieth century, their use has been monopolized by national militaries. As small drones entered commercial markets in the early 2000s, the remote precision targeting gap has narrowed.

With the emergence of commercially available drones, a new terrorist tool was created—the AVBIED. Unlike their grounded counterparts, AVBIEDs can target remote and restricted areas by navigating a

permissive air environment. They are cheap, mobile, and flexible, and in the hands of a relatively skilled operator they can be precise and deadly. Importantly, their missions are not necessarily suicidal for machine or operator. While drones can be employed in single-use, one-way missions (*direct AVBIEDs*), they can also be outfitted with remotely released explosive ordnance and deployed for multiple missions (*indirect AVBIEDs*). These latter AVBIEDs can be built with simple, independent release mechanisms to deliver a payload on target and return to a staging area to be resupplied and reused.

Direct AVBIEDs

Direct AVBIEDs conduct kamikaze-style attacks in which the machine is expected to detonate on impact. This crude delivery mechanism dates back to the Cold War, when, in 1971, the Jewish Defense League planned to use a "drone airplane" to target the Soviet Mission to the UN. Another early attempt came in 1977, when according to German media, the Red Army Faction sought to target German politician Franz Josef Strauss with a remote-controlled aircraft.

Many cases of planned attacks with direct AVBIEDs have surfaced over the past two decades, but they were often dismissed as unrealistic or exaggerated. For example, months before he orchestrated the September 11 attacks, Osama bin Laden was believed by some intelligence officials to have been planning an attack on the July 2001 G8 Summit in Italy, targeting President George W. Bush and other world leaders. In another example, during the Second Intifada, the Palestinian Authority reportedly redirected hundreds of toy planes intended for Palestinian children to bomb makers for AVBIED research and development. Both the Revolutionary Armed Forces of Colombia (FARC) and Hamas also began to explore AVBIED programs, though neither became operational. The most significant plot was disrupted in 2011, when al-Qaeda sympathizer Rezwan Ferdaus became the first terrorist convicted and imprisoned for attempting to use a direct AVBIED in an attack on American soil. Ferdaus sought to equip multiple remote-controlled aircraft with explosives to target the US Capitol and Pentagon buildings.

It was not until the Syrian Civil War and the rise of the Islamic State that weaponized drones were successfully deployed by nonstate actors. Although ISIS's drone program dates back to early 2013, it accelerated rapidly beginning in 2015, when the group stood up a dedicated research and development division. In 2016, ISIS carried out several drone attacks in Iraq, killing two Kurdish fighters and injuring two French soldiers. The tactics spread to groups in Syria, where rebels have attempted to mass direct AVBIED attacks against government forces, and to Mexico, where cartels have adopted AVBIEDs as a tool of intimidation and targeted assassination.

Indirect AVBIEDs

Indirect AVBIEDs are distinguished by the use of an independent release mechanism that enables the drone to drop its munitions and return to the operator. It can thus be reequipped and reused. These AVBIEDs can deliver conventional munitions or can serve as platforms to mount other weapons such as firearms or aerosolized spraying devices. Indirect AVBIEDs are more likely to be used in attacks against smaller or weaker targets due to limited payload, though as demonstrated in Ukraine, they can be effective against vehicles.

The first attempt to develop indirect AVBIEDs occurred in 1995, when Japanese doomsday cult Aum Shinrikyo acquired "at least two radio controlled drone aircraft" in a plan to disperse sarin gas or aerosolized anthrax throughout Tokyo. The next supposed case arose in 2003, when alleged al-Qaeda associate Moazzam Begg was accused of plotting to use a drone for a chemical weapons attack on the British House of Commons. A decade later, Iraq arrested five men planning to use a remote-controlled helicopter to release mustard gas.

Although early attempts to develop indirect AVBIEDs focused on turning UAVs into weapons platforms, today they are primarily used to release conventional munitions. In 2016, Hezbollah first employed commercial UAVs in Aleppo and dropped Chinese-manufactured MZD-2 cluster munitions on Syrian rebel positions. On the other side, Syrian jihadists were also mastering indirect AVBIEDs and modified drones to drop ordnance on proregime forces in Hama. More recently, in Myanmar, the People's Defense Force has targeted government police stations and training camps by grenades with stabilizing tail fins resembling 3D-printed shuttlecocks from drones, while Houthis have bombed progovernment forces in Yemen with grenade-carrying, DJI Mavic 2 quadcopters.

Commercial Drones in Ukraine

The war in Ukraine has advanced commercial drone war. Even before 2022, Aerorozvidka, the Ukrainian drone unit, was integrated into Ukraine's armed forces and formally brought weaponized COTS drones into state military services. It developed two types of indirect AVBIEDs: quadcopters generally designed for smaller munitions, such as antipersonnel hand grenades, and octocopters capable of carrying heavier antitank grenades or mortars. Smaller quadcopters can cost less than $1,000, while larger octocopters cost between $5,000 and $20,000. By 2020, Aerorozvidka announced it had successfully attached 3D-printed stabilization fins to RKG-3 antitank grenades to create the RKG-1600. The newly printed tail increased the accuracy of the munitions and enabled the user to drop them from a greater height, reducing the threat of detection, and with greater precision.

Since the war began, innovation in indirect AVBIED capabilities has accelerated, as both sides have found new ways to independently release munitions from COTS UAVs. For example, some Ukrainian units began modifying a piece of fishing gear called tackle feeders to act as a release mechanism for grenades to prevent premature detonation, while Russian-led fighters in the Donbas have begun dropping grenades held in plastic cups. AVBIEDs were used to attack Russian convoys outside of Kyiv and improvised fixed-wing UAVs have also been found. Russian Telegram channels, which have boasted about Russia's indirect AVBIED capabilities since the start of the war, frequently share videos of Russian service members crudely modifying DJI quadcopters to carry grenades. Large quantities of DJIs have been captured. The conflict has inspired others to create new AVBIED capabilities: Dutch engineers, for example, have designed drum magazine release mechanisms for dropping mortar shells. But the conflict also highlights the need to create counter–small UAV capabilities as states begin to respond to the threat of weaponized consumer drones.

Capabilities to Counter the Threat

Countering these emerging capabilities involves two broad elements: monitoring and countermeasures. Monitoring equipment can be active, passive, or a combination that detects, classifies, locates, and tracks drones in range. Small commercial UAVs are hard to monitor because they are often no bigger than a large bird and possess a low radar signature. Monitoring gear generally cannot distinguish between armed and surveillance drones, but detecting drones and their movement is the first step to providing effective AVBIED responses. Countermeasures aim to neutralize or destroy a hostile drone. Drones can be neutralized with directional radio frequency jammers, GPS spoofers, or high-power microwave devices; they can be destroyed by high-energy lasers, small arms fire, net guns, or even trained birds of prey. While these are effective against unarmed commercial drones, it becomes more complex with AVBIEDs, depending on payload and range from the target. Since AVBIEDs carry explosive munitions, they are likely to cause damage and casualties unless neutralized or destroyed at a significant distance from an intended target and away from populated areas. The Ukrainian front lines are seeing the first widespread battlefield testing of counter-AVBIED capabilities. Both small arms fire and directional jammers are being used, with Ukrainian forces introducing the DroneDefender, manufactured by the US company Dedrone, and the Lithuanian "Sky Wiper" EDM4S as nonlethal antidrone jamming guns. Specific counter-AVBIED tactics, techniques, and procedures cannot be found in publicly available sources. The UK Counter-Unmanned Aircraft Strategy does not mention the word "explosive," while the US Department of Homeland Security Counter-Unmanned Aircraft Systems Technology Guide only references that commercial drones *can* carry explosives. The US Department of Defense Counter-Small Unmanned Aircraft Systems Strategy recognizes the importance of responding to the threat of commercial drones but does not explicitly mention the danger of AVBIEDs. With the increasing use of COTS drones for targeted attacks, developing cost-efficient and sustainable countermeasures must become a priority. Additionally, as advances in commercial technologies continue, we will see increased use of unmanned and autonomous systems. For example, underwater drones are already being used as vehicles for IEDs; last year Hamas attempted to destroy Israeli offshore installations with an explosives-carrying uncrewed submersible. Developing precise and specific countermeasures is a necessity to prevent both targeted attacks against authorities and indiscriminate attacks against civilians.

Moving Forward

As commercial drones become increasingly advanced, accessible, and cheap, the threat from direct and indirect AVBIEDs will become more acute. It is only a matter of time before a state proxy, terrorist group, or lone wolf launches another attack on a high-ranking government official, as a group of rebels attempted in Venezuela in 2018, or an iconic target using an AVBIED. Even if the assault causes minimal casualties, such an event would leave a lasting effect on the public psyche. Large public gatherings and celebrations from the Super Bowl to a Wembley Stadium concert would become instant targets necessary to defend. More sophisticated actors could stage massed and coordinated attacks on the battlefield or on Broadway, where AVBIEDs could swarm a target from multiple directions and overwhelm security forces. NATO and the governments of its member states should capitalize on recent momentum to organize a study of defensive systems and identify vulnerabilities. NATO could establish a dedicated center of excellence to research, educate, and train member and partner nations on responding to AVBIEDs. Governments must look no further than Ukraine to learn lessons on the threats AVBIEDs will pose in the future of irregular war.

Benjamin Fogel is a graduate student at Johns Hopkins SAIS, with experience at the UN, European Union, and NATO Allied Air Command on Ramstein Air Base. He was named junior ambassador to the 2020 Munich Security Conference and 2022 GLOBSEC young leader.

Andro Mathewson is a research officer at the HALO Trust, focusing on the conflict in Ukraine. He completed his master's degree in international relations at the University of Edinburgh where he explored the proliferation of underwater drones. Before that, he was a fellow at Perry World House at the University of Pennsylvania. He is starting his PhD in War Studies at Kings College London in September 2022.

Pentagon Reveals Details of VAMPIRE Counter-Unmanned Aerial Systems Supplies to Ukraine

Source: https://militaryleak.com/2022/08/25/pentagon-reveals-details-of-vampire-counter-unmanned-aerial-systems-supplies-to-ukraine/

Aug 25 – On the 31st anniversary of Ukraine's independence, the United States is reinforcing its long-term commitment to the nation **with $2.98 billion to train and equip the Ukrainian armed forces for their struggle against the Russian invasion**. President Joe Biden said the people of the world have been awed and inspired by Ukrainian resistance and pledged the United States will stand with the people of Ukraine as they fight to defend their sovereignty. The Pentagon will buy newly announced air defense systems, counter-drone systems, radars, artillery systems and munitions from industry over months and years with Ukraine Security Assistance Initiative funding and apart from billions in equipment it has sent Ukraine from its

stockpiles.

The package, which marks the single largest tranche since Russia launched an invasion of Ukraine six months ago includes six more of the National Advanced Surface-to-Air Missile Systems (NASAMS), Puma and ScanEagle drones. Also included are Vampire counter-unmanned aerial systems. L3Harris' Vehicle-Agnostic Modular Palletized ISR Rocket Equipment (VAMPIRE) is a portable kit that can be installed on most vehicles with a cargo bed for the launching of the advanced precision kill weapons system (APKWS) or other laser-guided munitions. The Vampire is a kinetic system that uses a small missile, essentially, to shoot UAVs out of the sky. This L3Harris suitcase-type APKWS launcher and designator kit provides a rapid solution for arming non-tactical vehicles (NTV).

The AGR-20 Advanced Precision Kill Weapon System (APKWS) is a design conversion of Hydra 70 unguided rockets with a laser guidance kit to turn them into precision-guided munitions (PGMs). APKWS is approximately one-third the cost and one-third the weight of the current inventory of laser-guided

weapons have a lower yield more suitable for avoiding collateral damage and takes one-quarter of the time for ordnance personnel to load and unload. The APKWS II uses the Distributed Aperture Semi-Active Laser Seeker (DASALS) technology. This system

allows a laser seeker to be located on the leading edge of each of the forward control canards, working in unison as if they were a single seeker.

The APKWS configuration allows existing warheads from the Hydra 70 system to be used without the need for a laser seeker in the missile nose. An APKWS-equipped rocket was fitted with a proximity fuze and destroyed a Class 2 UAS. The proximity fuze enables it to intercept UAS at a lower cost than other methods, and due to the rocket's laser guidance that activates on launch, it does not

EFFECTIVE FOR AIRBORNE TARGETS

EFFECTIVE FOR GROUND TARGETS

require locking on to the target before launch. VAMPIRE is designed to complement the low-cost, low-signature, and availability of common NTVs and fit in any pickup or vehicle with a cargo bed. Installation can be completed in approximately two hours by two people using common tools. The power supply eliminates the need for a 24-volt alternator on the vehicle.

These Drones Are Equipped With AI Based Cybersecurity

Source: https://i-hls.com/archives/106720

Aug 25 – Drones can now be equipped with cybersecurity powered by artificial intelligence (AI). SkyGrid, a joint venture between Boeing and SparkCognition, has recently announced a world-first plan to deploy an AI-powered cybersecurity system on drones. Its DeepArmor product, a patented machine-learning cybersecurity technology is designed for the UAV industry at a time when never-before-seen cyberattacks are expected as more drones take flight.

The new software uses sophisticated AI models to protect a wide range of endpoints, designed to alleviate any potential zero-day threats.

According to aerospace-technology.com, the technology can be used both in the commercial sector and on UAVs within the defense industry to counter national security threats. Incidents such as the capture of RQ- 170 UAV by Iran back in 2015, which was subsequently reverse-engineered, could now be avoided.

The **DeepArmor Aerial product** can be deployed directly on drone hardware to provide protection even when network connectivity is impaired or non-existent. The ability to autonomously monitor and act on all payloads and processes is vital.

According to the company, the technology "is unique in how it classifies threats. It uses sophisticated AI models to analyze thousands of characteristics of payloads in memory or permanent storage. As a result, DeepArmor does not need prior knowledge of a specific threat to make a classification and has been very successful at catching advanced zero-day threats. This is especially important in the UAV industry where we expect to see never-before-seen cyberattacks emerge as more drones take flight," the company was cited by aviationtoday.com.

AI technologies are becoming ubiquitous for both protecting against cyberattacks and also as an instrument for launching them. AI systems used as cyber offensive tools create a worrying vulnerability for militaries, as new autonomous technologies can increase the anonymity of cyberattacks, which can also be executed at much larger scale and at faster speeds. Securing unmanned systems against such attacks is critical as breaches can offer attackers access to vast amounts of data that could pose an immediate risk to military operations.

This Drone Will Save Lives When All Hope Is Lost

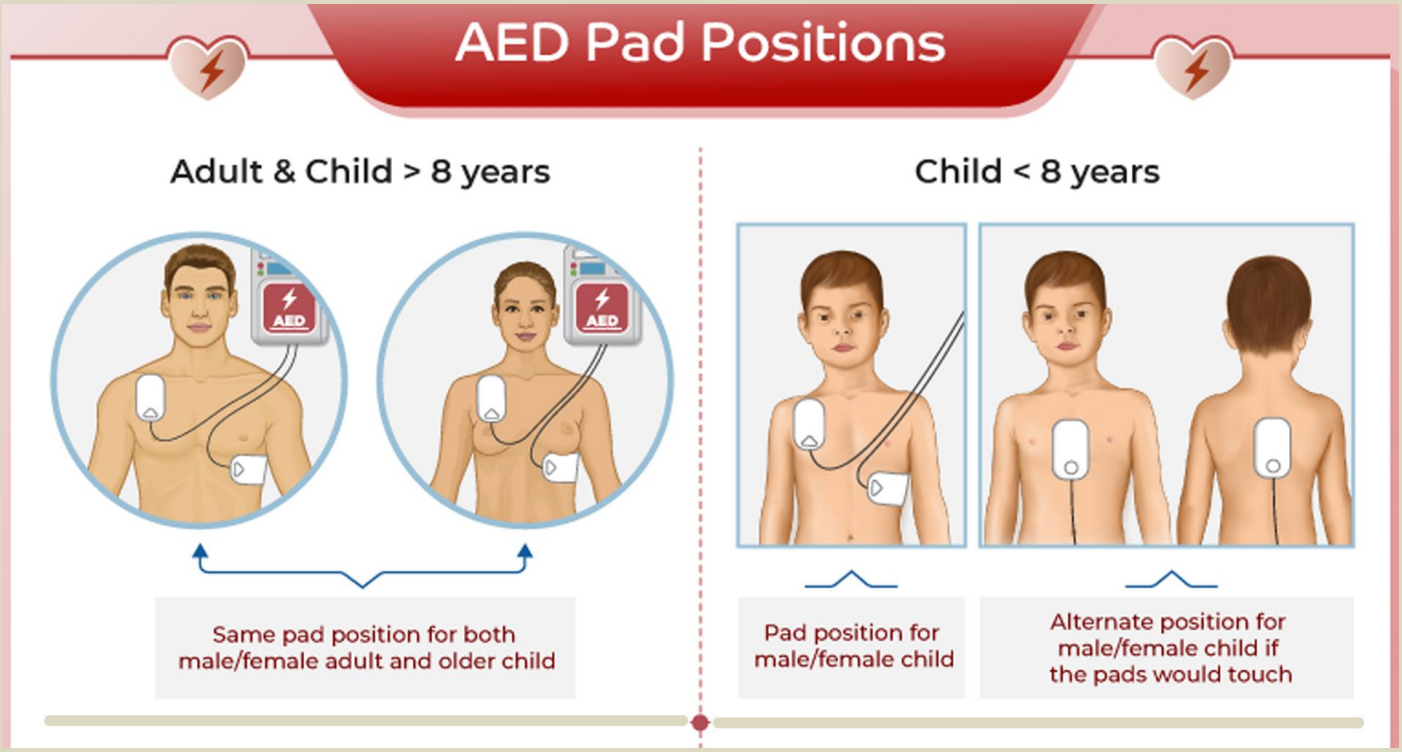
Source: https://i-hls.com/archives/105051

Aug 26 – The survival rate for people with cardiac arrest depends on the time patients get defibrillation. The defibrillator is a portable electronic device that automatically diagnoses life-threatening cardiac arrhythmias and is able to treat them through defibrillation, the application of electrical therapy.

A new drone solution could save lives in cases where patients are far away from hospitals. Specially-designed drones developed by the Sweden-based **FlyPulse** will address this challenge through LifeDrone AED – a transportation drone, equipped with an automated external defibrillator (AED).

According to the company, the system "can improve the survival rate for people with cardiac arrest, where it is difficult to arrive with an AED in time with ambulances or other transportation."

The technology includes the mechanical drone system, its payload, electronics, and the software to manage complete operations, with a high level of automation. Software plays a critical role in the success of this application, as several major modules have to be integrated, including flight control and safety, payload management, cloud connectivity for remote telemetry and control, fleet management through a centralized dashboard, and more.
Live video streaming for situational awareness and remote patient monitoring is also provided, as well as collision avoidance and airspace management.
The company has partnered with FlytBase, which offers an advanced drone software development platform, with "intelligence" and "connectivity" as its core features.
FlytOS, its operating system for drones, is compatible with the widest range of drones and computer hardware platforms. This enables developers to make their applications agnostic to hardware. It provides a number of other capabilities, like, navigation and control, computer vision, payload management, authentication and security, machine learning, a simulator for testing, SDKs for web/mobile, according to suasnews.com.
FlytBase Cloud extends a number of these capabilities to the cloud. It helps developers manage large fleets of drones, connect over wifi/4G networks, and easily integrate drones with other business applications.



What Military Robots Do When Communication Is Lost

Source: https://i-hls.com/archives/115902

Aug 30 – A new technique allows robots to remain resilient when faced with intermittent communication losses on the battlefield. The α-shape, provides an efficient method for resolving goal conflicts between multiple robots that may want to visit the same area during missions including unmanned search and rescue, robotic reconnaissance, perimeter surveillance and robotic detection of physical phenomena, such as radiation and underwater concentration of lifeforms. Army.mil reports that researchers from the US Army Combat Capabilities Development Command, known as DEVCOM, Army Research Laboratory and the University of Nebraska, Omaha Computer Science Department collaborated regarding this topic.
In environments where the robots cannot communicate widely due to needing to stay covert, clutter leading to radios not working for long distance communications, or to preserve battery or bandwidth for more important messages, the robots will need a method to coordinate with as few communications as

possible. This coordination is accomplished through sharing their next task with the team, and select team members will remember this information, allowing other robots to ask if any other robot will perform that task without needing to communicate directly with the robot that selected the task. "This research enables coordination between robots when each robot is empowered to make decisions about its next tasks without requiring it to check in with the rest of the team first," Army researcher Dr. Bradley Woosley said.
The technique uses a geometric approximation called α-shape to group together regions of the environment that a robot can communicate with other robots using multi-hop communications over a communications network. This technique is integrated with an intelligent search algorithm over the robots' communication tree.

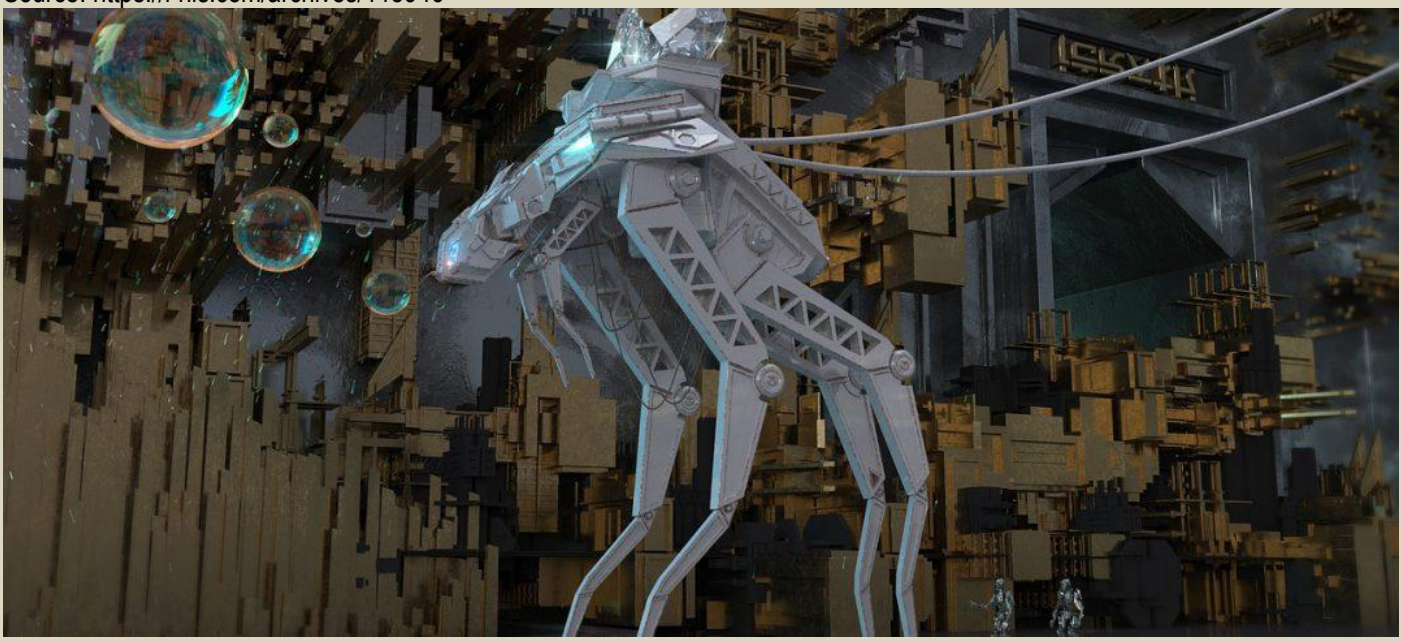
Amazing Solution For Drone Noise Cancellation

Source: https://i-hls.com/archives/115955

Sep 01 – Taking camera shots from drones has become a common practice among videographers. However, one limitation of taking videos on drones is limited camera audio due to the sound of the drone. The noise caused by the operation of the drone renders any audio captured from the drone useless, especially when the audio of the surroundings can be a very important part of what is trying to be captured. A patent granted to GoPro refers to a system to provide noise cancellation for an aerial vehicle. The system includes an audio signal filter that utilizes operational condition input parameters from components of the vehicle. These parameters act as a baseline of noise (i.e. vibrational and air noise) from the audio signal. The audio signal filter combines the analysis of vehicle component operational conditions and distances of the components from the microphone to filter the noise information from the operation of the drone. With the ability to identify and process the additional noise sources the system can generate a baseline noise profile for the vehicle to be used by the audio filter. This baseline provides the user with a general starting point to further tune the noise parameters filtered by the system. The implementation of an audio signal filter demonstrates an innovative way to pair two systems together creating an innovative approach to solve this particular problem, according to founderslegal.com.

Meet China's Cyber Dog – The Future Of Robotics

Source: https://i-hls.com/archives/115946



Aug 31 – China has developed the world's largest electric-powered quadruped bionic robot, which is expected to join logistics delivery and reconnaissance missions in complex environments that have proven too challenging for human soldiers, including remote border regions and highly risky combat zones, analysts said.
In December, China announced that it would work to become a leading global player in robotics by 2025 under a five-year plan.
The robot (dubbed the "mechanical yak") can carry up to 160 kilograms, and despite its large size, it can run at up to 10 kilometers an hour, CCTV reported. It is equipped with sensors to be aware of the surrounding terrain and environment, and it has displayed a very strong adaptative ability to various types

of terrains including steps, trenches and cliffs, not to mention muddy roads, grasslands, deserts and snow fields, the report said.
The robot can be deployed to deliver supplies including munitions and food in environments like plateaus, mountains, deserts and forests where normal vehicles have difficult time traversing.
Another potential use is close-in reconnaissance, as it can persistently gather battlefield intelligence and monitor target movements even in complex environments that have proven to be too challenging for human soldiers.
The robot is a very good choice for missions in remote border regions where constant monitoring is needed but conditions do not favor a constant human presence, for example, in high altitude plateaus, icy regions and dense forests, a Chinese military expert who requested anonymity told globaltimes.cn.
Last year, Chinese tech giant Xiaomi had unveiled the "CyberDog," a bionic quadruped robot with a high-precision environmental sensing system and 11 high-precision sensors distributed throughout its body. Other Chinese tech companies may have also developed quadruped bionic robots for various applications.

The THeMIS UGV

Source: https://milremrobotics.com/defence/

Operationally proven during several exercises, experiments, and the anti-insurgency mission Operation Barkhane in Mali – the THeMIS is a multi-role unmanned ground vehicle (UGV) intended to reduce the number of troops on the battlefield. THeMIS' open architecture enables it to be rapidly configured from having a transport function to being weaponized, performing ordnance disposal, or supporting intelligence operations according to the nature of the mission. THeMIS UGVs have been acquired by 11 countries, 7 of which are members of NATO, including Estonia, Germany, the Netherlands, Norway, the UK, and the US.
Carrying supplies and equipment in combat is often difficult for dismounted units. Due to the soldier's physical limitations, the weight of additional equipment and heavy weapons often restrict what the soldier can take into battle. The purpose of the THeMIS Cargo is to reduce the cognitive load of soldiers and provide a means to carry and utilize extra gear and firepower. The THeMIS Cargo will increase the mobility of dismounted units and make them more effective against the adversary. The THeMIS Cargo can also be used to support on-base logistical activities and for last-mile resupply.

THeMIS Cargo

The THeMIS Cargo is intended to support dismounted troops by carrying everything a soldier would normally carry, thus letting the fighter concentrate on the mission at hand. It can be outfitted with various types of tie downs and restraints to prevent load shift.

THeMIS Cargo Mortar carrier

The THeMIS Mortar carrier has been adjusted to accommodate a mortar up to 81 mm. The Cargo platform is equipped with a specially designed suspension system for safe transportation and utilization of the mortar, extra equipment and ammunition, making it rapidly deployable on harsh terrain.The main purpose of this system is to enable logistical supportand indirect fire for manoeuvre forces .

THeMIS Cargo CASEVAC

The purpose of the CASEVAC platform is to provide rapid evacuation for urgent casualties from the point of injury to higher-level medical facilities. It reduces the need for manpower usually used for casualty evacuation.The vehicle facilitates most NATO stretchers used in the armed forces.

THeMIS with GroundEye

The THeMIS GroundEye system is the first explosive ordinance detection and disposal unit that has been developed in partnership with Raytheon UK.

THeMIS Combat with ADDER DM

The ADDER was the first remote weapon station integrated into the THeMIS. This system has been tested in the cold Estonian winter in partnership with weapon station developer and manufacturer Singapore Engineering Land Systems under the supervision of the Estonian Defence Forces.

THeMIS Combat with R400S-MK2-D-HD

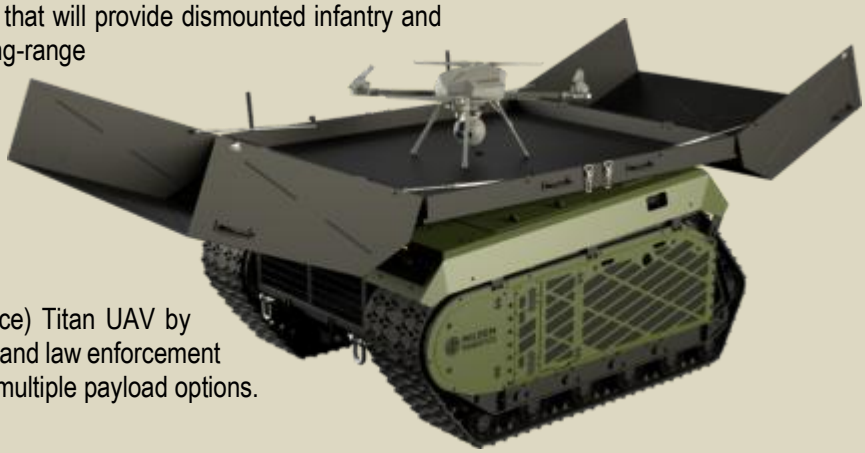
The THeMIS Combat with the EOS R400S-MK2-D-HD 30 mm autocannon remote weapon system provides direct fire support for manoeuvre forces acting as a force multiplier. The stabilized weapon system provides higher precision over wide areas, day and night, increasing stand-off distance, force protection and survivability. Reducing logistical footprint and enabling light infantry units to deploy with a heavy weapon system.

THeMIS Combat with GUARDIAN 2.0

The GUARDIAN 2.0 by Escribano Mechanical & Engineering provides defence capabilities over short and medium ranges with high firing accuracy and it is a cost-effective solution for defence against asymmetric threats. The system is stabilized and can operate by day and by night. Operational functions include surveillance, target identification and tracking. Ballistic calculations for shooting are programmed into the main comp uter unit, allowing improved shooting accuracy.

THeMIS Combat with Hero-120

The THeMIS Combat with the Hero-120 by UVision can be equipped with up to six Loitering Munition systems that will provide dismounted infantry and Special Forces units with long-range ISR and firepower combination. Ideal for anti-tank missions or other strategic objectives, the Hero-120 is the largest of UVision's short-range systems. It carries a 3.5 kg warhead and can endure an extended flight time of 60 minutes.



THeMIS Observe with the KX-4 LE Titan

The THeMIS Observe with the KX-4 LE (Long Endurance) Titan UAV by Threod Systems is the perfect tool for surveillance, rescue and law enforcement missions. The system features a heavy-lift multirotor with multiple payload options.

EDITOR'S COMMENT: According to the CAST Telegram channel "Due to the fact that this device is of undeniable technical interest, the Center for Strategic and Technological Analysis is announcing a reward of 1 million rubles, to any military or officer or a group, who manage to deliver the THEMIS platform to Ukraine more or less intact situation and make it available to the Ministry of Defense of Russia"

Living Organic Robots – US Army Amidst Developments

Source: https://i-hls.com/archives/106512

Sep 09 – "Today's robot's primary limitation is power, strength and versatility. They can perform limited tasks for a certain amount of time. But it's not really on the order of magnitude that an organism can do the same thing," claims Dean Culver, an Army Research Laboratory research scientist. "We still don't have robots that can go into an unknown space and adapt to what they sense. These are all ultimately problems that we feel that either a bio-hybrid or a bioinspired engineering design can tackle."
This is the reason why the US Army is interested in developing a robot with living, organic muscles to build robots that may be able to gain the agility and versatility of living creatures. The ARL's Combat Capabilities Development Command has teamed up with universities in North Carolina to develop studies in bio-hybrid robotics in order to fuse living tissue with cold metal.
According to federalnewsnetwork.com, the ARL wants to grow tissue in a lab and then connect it between linkages in a robot's joints. This technology could allow robots to adapt faster to terrains instead of relying on the static joints made of synthetic materials.The muscles can come from any animal depending on what the Army needs. The first applications of biohybrid robots will focus on the legged platforms. Right now, the Army has a Legged Locomotion and Movement Adaptation research platform that serves as a perfect example for the type of robot the service could work on.
ARL is currently finding more partners for the projects. "At the moment, we have a great theoretical basis for what we're trying to do," Culver said. "Some of the tools that we want to use to improve the design of muscle tissue for use in robots have been tested on lots of other proteins and molecules, and they're proven to be effective. What we really need now is some time and support to get these tools directed at the molecules relevant in muscles. There's a lot of learning to do before we produce prototypes."
Until then the Army will continue using robots for smaller tasks. For example, Boston Dynamics and the military have made great strides in using robots with bomb diffusion and intelligence gathering.

3D printing drones work like bees to build and repair structures while flying

Source: https://www.imperial.ac.uk/news/239973/3d-printing-drones-work-like-bees/

Sep 21 – Imperial College London and Empa researchers have created a fleet of bee-inspired **flying 3D printers** for building and repairing structures in-flight.
The technology could ultimately be used for manufacturing and building in difficult-to-access or dangerous locations such as tall buildings or help with post-disaster relief construction, say the researchers, who publish their work in *Nature*.

We've proved that drones can work autonomously and in tandem to construct and repair buildings, at least in the lab. Professor Mirko Kovac Department of Aeronautics & Empa
3D printing is gaining momentum in the construction industry. Both on-site and in the factory, static and mobile robots print materials for use in construction projects, such as steel and concrete structures.
This new approach to 3D printing uses flying robots, known as drones, that use collective building methods inspired by natural builders like bees and wasps.
The drones in the fleet, known collectively as Aerial Additive Manufacturing (Aerial-AM), work co-operatively from a single blueprint, adapting their techniques as they go. They are fully autonomous while flying but are monitored by a human controller who checks progress and intervenes if necessary, based on the information provided by the drones.
Lead author Mirko Kovac, Professor at Imperial's Department of Aeronautics and Head of Empa's Materials and Technology Center of Robotics, said: "We've proved that drones can work autonomously and in tandem to construct and repair buildings, at least in the lab. Our solution is scalable and could help us to construct and repair building in difficult-to-reach areas in the future."

BuilDrones (R) 3D print their material during flight, and ScanDrones (L) continuously measure their output for quality control.

Printing 3D geometries

Aerial-AM uses both a 3D printing and path-planning framework to help the drones adapt to variations in geometry of the structure as a build progresses. The fleet consists of BuilDrones, which deposit materials during flight, and quality-controlling ScanDrones that continually measure the BuilDrones' output and inform their next manufacturing steps.

"Our fleet of drones could help reduce the costs and risks of construction in the future, compared to traditional manual methods." Professor Mirko Kovac Department of Aeronautics & Empa

To test the concept, the researchers developed four bespoke cementitious mixtures for the drones to build with.

Throughout the build, the drones assessed the printed geometry in real time and adapted their behaviour to ensure they met the build specifications, with manufacturing accuracy of five millimetres.

The proof-of-concept prints included a 2.05-metre high cylinder (72 layers) with a polyurethane-based foam material, and an 18-centimetre high cylinder (28 layers) with a custom-designed structural cementitious material.

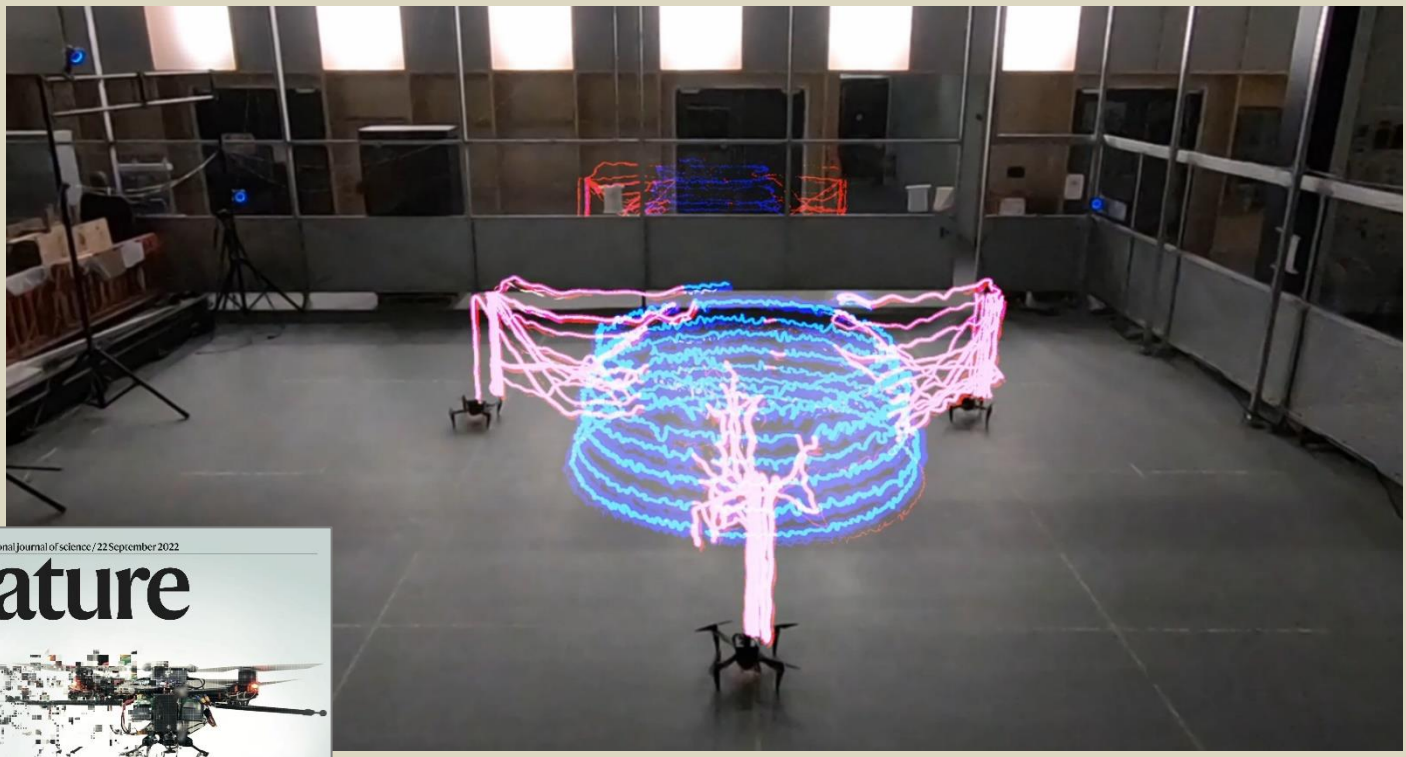
The technology offers future possibilities for building and repairing structures in tall or other hard-to-access locations. Next, the researchers will work with construction companies to validate the solutions and provide repair and manufacturing capabilities.

Professor Kovac said: "We believe our fleet of drones could help reduce the costs and risks of construction in the future, compared to traditional manual methods."

Co-investigators include Robert Stuart-Smith, Stefan Leutenegger, Vijay Pawar, Richard Ball, Chris Williams and Paul Shepherd, and their research teams at UCL, University of Bath, University of Pennsylvania, Queen Mary University of London, and Technical University of Munich (TUM). It was launched by Assistant Professor Stuart-Smith at UCL and University of Pennsylvania and Professor Kovac at Imperial and Empa after a pilot research collaboration and award for a demonstration on pipeline repair.

This work was funded by the Engineering and Physical Sciences Research Council (part of UKRI), the Royal Society, the European Commission's Horizon 2020 Programme, Royal Thai Government

Scholarship and a University of Bath Research Scholarship. The project is also supported by Industrial Partners Skanska, Ultimaker, Buro Happold, and BRE.



A simulation of potential future building projects. Credit: Autonomous Manufacturing Lab, UCL

The drones could be used to help building projects in hard-to-access locations

"Aerial Additive Manufacturing with Multiple Autonomous Robots" by Zhang *et al.*, published 21 September 2022 in *Nature*.
Credit: Videos taken at the Imperial College London Aerial Robotics Laboratory by all partners (Imperial College London, University College London, University of Bath).
The research is featured on the cover of Nature's September edition

International CBRNE INSTITUTE

AI - NEWS

C2BRNE DIARY

This Technology Can Uncover Hidden Weapons

Source: https://i-hls.com/archives/109003

Aug 22 – A new scanning solution uses **advanced sensors and artificial intelligence** to detect a wide range of concealed weapons and threats, such as firearms, metallic weapons and improvised explosive devices, on a visitor entering a premise. Motorola Solutions has unveiled the newest addition to its video security and analytics portfolio, Concealed Weapon Detection (CWD), through an agreement with Evolv Technologies.

AI technology enables the automation and unification of workflows to better protect people against the threat of violence.

The solution is designed to allow up to 3600 visitors to walk through one of the scanning systems per hour without having to conduct pat downs or empty pockets as the technology can distinguish between personal items and weapons. If a threat is detected, an alert is displayed on an Express tablet showing the location of the potential threat on the person's body, or in their bag, to security operators.

Alerts are sent directly to Motorola Solutions' video management system, Avigilon Control Center (ACC), which automatically notifies and shares live video with the facility's security team so they have precise awareness of the situation and can support an immediate response.

The sensitivity levels on the CWD solution can be adjusted to align with the safety needs of a facility based on their anticipated threat-scenarios. This capability allows for the technology to identify and flag new threat profiles over time, and enables security personnel to manage data and insights that help to provide a safe and positive experience for visitors and staff, according to the company's announcement.

The Potential of AI-Human Teaming

Source: https://i-hls.com/archives/100944

Aug 21 – Artificial intelligence will be an integral part of the future battlefield. AI Technologies will eventually reduce the number of soldiers in harm's way, however, they will not simply replace soldiers one-for-one. Success in future operations will require soldiers to interact with multiple, advanced technologies at once.

The US Army wants to improve the interactions between humans and AI tools. In a presolicitation notice, the Army Research Laboratory is looking for a Human-Agent Teaming Research and Engineering Services contract to study how soldiers interact with AI and improve the training regimen for humans and machines.

According to the RFI, the Army wants to "develop and field systems requiring soldiers to team with AI technologies by facilitating the exchange of information between the soldier, system, and environment."

"Development of AI technologies to support teams of soldiers and autonomy will change the way that team members, both human and autonomous, interact with the environment, the enemy, and with each other. AI technologies will be able to learn, not only how to interact with individuals and teams, but how to

collaboratively make decisions and solve problems as part of teams, maximizing the strengths and minimizing the weaknesses of individual team members—human or autonomous."

The technical and engineering support are required in order to develop training simulations and integrating those into existing regimens.

New test and evaluation methods will be required for measuring the effectiveness of human-AI teams and integrating those with the Army's Next Generation Combat Vehicle program. The program will also iterate on existing methods and develop new ways of mapping soldiers' brain functions, psychology and behavior when interacting with AI teammates.

According to defenseone.com, the Army plans to award the contract to DCS Corporation but released a request for information to hear from other potential vendors capable of delivering on this contract.

Artificial Intelligence and Democratic Values: Next Steps for the United States

By Marc Rotenberg and Merve Hickok

Source: https://www.homelandsecuritynewswire.com/dr20220826-artificial-intelligence-and-democratic-values-next-steps-for-the-united-states

Aug 26 – More than fifty years after a research group at Dartmouth University launched work on a new field called "Artificial Intelligence," the United States still lacks a national strategy on artificial intelligence (AI) policy. The growing urgency of this endeavor is made clear by the rapid progress of both U.S. allies and adversaries.

Europe is moving forward with two initiatives of far-reaching consequence. The EU Artificial Intelligence Act will establish a comprehensive, risk-based approach for the regulation of AI when it is adopted in 2023. Many anticipate that the EU AI Act will extend the "Brussels Effect" across the AI sector as the earlier European data privacy law, the General Data Privacy Regulation, did for much of the tech industry.

The Council of Europe is developing the first international AI convention aiming to protect fundamental rights, democratic institutions, and the rule of law. Like the Council of Europe Convention on Cybercrime (COE) and the Privacy Convention, the AI Convention will be open for ratification by member and non-member states. The COE remains influential, as Canada, Japan, the United States, and several South American countries have signed on to the COE.

China is also moving forward with an aggressive regulatory strategy to complement its goal to be the "world leader in AI by 2030." China recently matched the GDPR with the Personal Information Protection Law and a new regulation on recommendation algorithms with similar provisions to the EU's Digital Services Act. The Chinese regulatory model will likely influence countries in Africa and Asia, part of the Belt and Road Initiative, and give rise to a possible "Beijing Effect."

The United States has done an admirable job maintaining a coherent policy in the Executive Branch over the Obama, Trump, and Biden administrations, highlighting key values and promoting an aggressive research agenda. In the 2019 Executive Order on Maintaining American Leadership in AI, the United States said it would "foster public trust and confidence in AI technologies and protect civil liberties, privacy,

and American values in their application." Promoting the Use of AI in the Federal Government established the principles for the "development and use of AI consistent with American values and are beneficial to the public."
The United States also played a leading role at the Organization for Economic Cooperation and Development (OECD) with the development and adoption of the OECD AI Principles, the first global framework for AI policy. Those principles, which emphasize "human-centric and trustworthy" AI, were later adopted by the G-20 nations, and are now endorsed by more than 50 countries, including Russia and China.
But the United States was out of the loop when the UN Educational, Scientific, and Cultural Organization (UNESCO) adopted the Recommendation on AI Ethics, now the most comprehensive framework for global AI policy which addresses emerging issues, such as AI and climate and gender equity.
"Democratic values" is a key theme as the United States seeks to draw a sharp distinction between the deployment of technologies that advance open, pluralist societies and those that centralize control and enable surveillance. As Secretary Blinken explained last year, "More than anything else, our task is to put forth and carry out a compelling vision for how to use technology in a way that serves our people, protects our interests and upholds our democratic values." But absent a legislative agenda or clear statement of principles, neither allies nor adversaries are clear about the U.S. AI policy objectives.
The United States has run into similar problems with the Trade and Technology Council (TTC), an effort to align U.S. and EU tech policy around shared values. The inaugural Joint Statement laid a foundation for cooperation on AI for the EU and the United States in the fall of 2021, but Ukraine has upended transatlantic priorities, and it remains unclear at this point whether the TTC will regain focus on a common AI policy.
A similar challenge confronts EU and U.S. leaders on new rules for transatlantic data flows. After two earlier decisions from the high court in Europe, finding that the United States lacked adequate privacy protection for the transfer of personal data, lawmakers on both sides of the Atlantic worried that data flows could be suspended, as the Irish privacy commissioner has recently threatened. President Biden and President von der Leyen announced an agreement in principle in May, but several months later there is still no public text for review.
To restore leadership in the AI policy domain, the United States should move forward the policy initiative launched last year by the Office of Science and Technology Policy (OSTP). The science office outlined many of the risks of AI, including embedded bias and widespread surveillance, and called for an AI Bill of Rights. OSTP said, "Our country should clarify the rights and freedoms we expect data-driven technologies to respect."The White House supported the initiative and encouraged Americans to "Join the Effort to Create A Bill of Rights for an Automated Society."
We strongly support this initiative. After an extensive review of the AI policies and practices in 50 countries, we identified the AI Bill of Rights as possibly the most significant AI policy initiative in the United States. But early progress has stalled. The delay has real consequences for Americans who are subject to automated decision-making in their everyday lives, with little transparency or accountability. Foreign governments are also looking for U.S. leadership in this rapidly evolving field. Progress on the AI Bill of Rights initiative will help build trust and restore U.S. leadership.
Last year, the Office of Science and Technology Policy stated clearly, "Powerful technologies should be required to respect our democratic values and abide by the central tenet that everyone should be treated fairly." That should be the cornerstone of a U.S. national AI policy, and that policy will advance international norms for the governance of AI.

Marc Rotenberg is President of the Center for *AI* and Digital Policy (*CAIDP*), author the forthcoming *Law of Artificial Intelligence* (West Academic 2023), and a Life Member of *CFR*.
Merve Hickok is the Research Director of *CAIDP* and founder of the AIethicist.org.

The Military Cannot Rely on AI for Strategy or Judgment

Source: https://www.homelandsecuritynewswire.com/dr20220826-the-military-cannot-rely-on-ai-for-strategy-or-judgment

Aug 26 – Using artificial intelligence (AI) for warfare has been the promise of science fiction and politicians for years, but new research from the Georgia Institute of Technology argues only so much can be automated and shows the value of human judgment.
"All of the hard problems in AI really are judgment and data problems, and the interesting thing about that is when you start thinking about war, the hard problems are strategy and uncertainty, or what is well known as the fog of war," said Jon Lindsay, an associate professor in the School of Cybersecurity & Privacy and the Sam Nunn School of International Affairs. "You need human sense-making and to make moral, ethical, and intellectual decisions in an incredibly confusing, fraught, scary situation."
AI decision-making is based on four key components: data about a situation, interpretation of those data (or prediction), determining the best way to act in line with goals and values (or judgment), and action.

Machine learning advancements have made predictions easier, which makes data and judgment even more valuable. Although AI can automate everything from commerce to transit, judgment is where humans must intervene, Lindsay and University of Toronto Professor Avi Goldfarb wrote in the paper, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," published in *International Security*.

Many policy makers assume human soldiers could be replaced with automated systems, ideally making militaries less dependent on human labor and more effective on the battlefield. This is called the substitution theory of AI, but Lindsay and Goldfarb state that AI should not be seen as a substitute, but rather a complement to existing human strategy.

"Machines are good at prediction, but they depend on data and judgment, and the most difficult problems in war are information and strategy," he said. "The conditions that make AI work in commerce are the conditions that are hardest to meet in a military environment because of its unpredictability."

An example Lindsay and Goldfarb highlight is the Rio Tinto mining company, which uses self-driving trucks to transport materials, reducing costs and risks to human drivers. There are abundant, predictable, and unbiased data traffic patterns and maps that require little human intervention unless there are road closures or obstacles.

War, however, usually lacks abundant unbiased data, and judgments about objectives and values are inherently controversial, but that doesn't mean it's impossible. The researchers argue AI would be best employed in bureaucratically stabilized environments on a task-by-task basis.

"All the excitement and the fear are about killer robots and lethal vehicles, but the worst case for military AI in practice is going to be the classically militaristic problems where you're really dependent on creativity and interpretation," Lindsay said. "But what we should be looking at is personnel systems, administration, logistics, and repairs."

There are also consequences to using AI for both the military and its adversaries, according to the researchers. If humans are the central element to deciding when to use AI in warfare, then military leadership structure and hierarchies could change based on the person in charge of designing and cleaning data systems and making policy decisions. This also means adversaries will aim to compromise both data and judgment since they would largely affect the trajectory of the war. Competing against AI may push adversaries to manipulate or disrupt data to make sound judgment even harder. In effect, human intervention will be even more necessary.

Yet this is just the start of the argument and innovations.

"If AI is automating prediction, that's making judgment and data really important," Lindsay said. "We've already automated a lot of military action with mechanized forces and precision weapons, then we automated data collection with intelligence satellites and sensors, and now we're automating prediction with AI. So, when are we going to automate judgment, or are there components of judgment cannot be automated?"

Until then, though, tactical and strategic decision making by humans continues to be the most important aspect of warfare.

Artificial Intelligence and Policing: It's a Matter of Trust

By Nick Evans

Source: https://www.homelandsecuritynewswire.com/dr20220830-artificial-intelligence-and-policing-it-s-a-matter-of-trust

Aug 30 – From *Robocop* to *Minority Report*, the intersection between policing and artificial intelligence has long captured attention in the realm of high-concept science fiction. However, only over the past decade or so has academic research and government policy begun to focus on it.

Teagan Westendorf's ASPI report, *Artificial intelligence and policing in Australia*, is one recent example. Westendorf argues that Australian government policy and regulatory frameworks don't sufficiently capture the current limitations of AI technology, and that these limitations may 'compromise [the] principles of ethical, safe and explainable AI' in the context of policing.

My aim in this article is to expand on Westendorf's analysis of the potential challenges in policing's use of AI and offer some solutions. Westendorf focuses primarily on a particular kind of policing use of AI, namely, statistical inferencing used to make (or inform) decisions—in other words, technology that falls broadly into the category of 'predictive policing'.

While predictive policing applications pose the thorniest ethical and legal questions and therefore warrant serious consideration, it's important to also highlight other applications of AI in policing. For example, AI can assist investigations by expediating the transcription of interviews and analysis of CCTV footage. Image-recognition algorithms can also help detect and process child-exploitation material, helping to limit human exposure. Drawing attention to these applications can help prevent the conversation from becoming too focused on a small but controversial set of uses. Such a focus could risk poisoning the well for the application of AI technology to the sometimes dull and difficult (but equally important) areas of day-to-day police work.

That said, Westendorf's main concerns are well reasoned and worth discussing. They can be summarised as being the problem of bias and the problem of transparency (and its corollary, explainability).

Like all humans, police officers can have both conscious and unconscious biases that may influence decision-making and policing outcomes. Predictive policing algorithms often need to be trained on datasets capturing those outcomes. Yet, if algorithms are trained on historical datasets that include the results of biased decision-making, it can result in unintentional replication (and in some cases amplification) of the original biases. Efforts to ensure systems are free of bias can also be hampered by 'tech-washing', where AI outputs are portrayed (and perceived) as based solely on science and mathematics and therefore inherently free of bias.

Related to these concerns is the problem of transparency and explainability. Some AI systems lack transparency because their algorithms are closed-source proprietary software. But it can be difficult to render even open-source algorithms explainable—particularly those used in machine learning—due to their complexity. After all, a key benefit of AI lies in its ability to analyse large datasets and detect relationships that are too subtle for the human mind to identify. Making models more comprehensible by simplifying them may require trade-offs in sensitivity, and therefore also in accuracy. Together these concerns are often referred to as the 'AI black box' (inputs and outputs are known, but not what goes on in the middle). In short, a lack of transparency and explainability makes the detection of bias and discriminatory outputs more difficult. This is both an ethical concern and a legal one when justice systems require that charging decisions be understood by all parties to avoid discriminatory practices. Indeed, research suggests that when individuals trust the process of decision-making, they are more likely to trust the outcomes in justice settings, even if those outcomes are unfavourable. Explainability and transparency can therefore be important considerations when seeking to enhance public accountability and trust in these systems. As Westendorf points out, steps can be taken to mitigate bias, such as pre-emptively coding against foreseeable biases and involving human analysts in the processes of building and leveraging AI systems. With these sorts of safeguards in place (as well as deployment reviews and evaluations), use of AI may have the upshot of establishing built-in objectivity for policing decisions by reducing reliance on heuristics and other subjective decision-making practices. Over time, AI use may assist in debiasing policing outcomes.

While there's no silver bullet for enhancing explainability, there are plenty of suggestions, particularly when it comes to developing AI solutions to enhance AI explainability. Transparency challenges generated by proprietary systems can also be alleviated when AI systems are owned by police and designed in house. Yet the need for explainability is only one consideration for enhancing accountability and public trust in the use of AI systems by police, particularly when it comes to predictive policing. Recent research has found that people's level of trust in the police (which is relatively high in Australia) correlates with their level of acceptance of changes in the tools and technology used by police. In another study, participants exposed to purportedly successful policing applications of AI technology were more likely to support wider police use of such technologies than those exposed to unsuccessful uses, or not exposed to examples of AI application at all. In fact, participants exposed to purportedly successful applications even judged the decision-making process involved to be trustworthy. This suggests that focusing on broader public trust in policing will be vital in sustaining public trust and confidence in the use of AI in policing, regardless of the degree of algorithmic transparency and explainability. The goal of transparent and explainable AI shouldn't neglect this broader context.

Nick Evans is a lecturer and researcher at the Tasmanian Institute of Law Enforcement Studies at the University of Tasmania.

Spirals of Delusion – How AI Distorts Decision-Making and Makes Dictators More Dangerous

By Henry Farrell, Abraham Newman, and Jeremy Wallace

September/October 2022

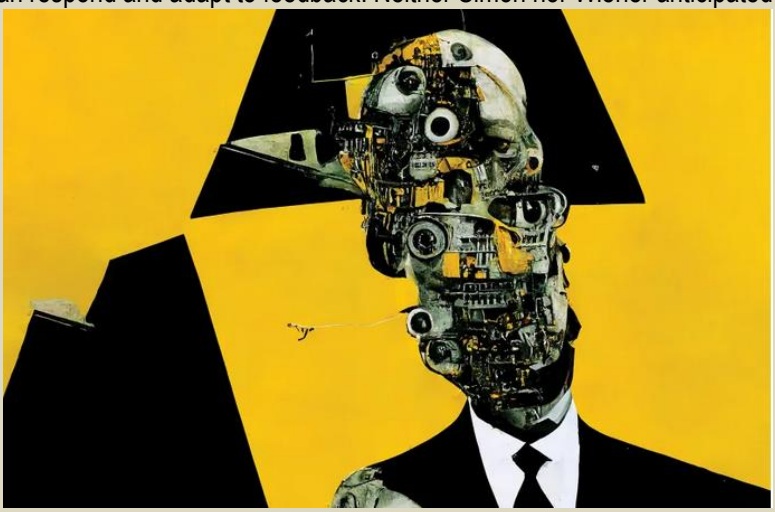
Source: https://www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making

In policy circles, discussions about artificial intelligence invariably pit China against the United States in a race for technological supremacy. If the key resource is data, then China, with its billion-plus citizens and lax protections against state surveillance, seems destined to win. Kai-Fu Lee, a famous computer scientist, has claimed that data is the new oil, and China the new OPEC. If superior technology is what

provides the edge, however, then the United States, with its world class university system and talented workforce, still has a chance to come out ahead. For either country, pundits assume that superiority in AI will lead naturally to broader economic and military superiority.

But thinking about AI in terms of a race for dominance misses the more fundamental ways in which AI is transforming global politics. AI will not transform the rivalry between powers so much as it will transform the rivals themselves. The United States is a democracy, whereas China is an authoritarian regime, and machine learning challenges each political system in its own way. The challenges to democracies such as the United States are all too visible. Machine learning may increase polarization—reengineering the online world to promote political division. It will certainly increase disinformation in the future, generating convincing fake speech at scale. The challenges to autocracies are more subtle but possibly more corrosive. Just as machine learning reflects and reinforces the divisions of democracy, it may confound autocracies, creating a false appearance of consensus and concealing underlying societal fissures until it is too late.

Early pioneers of AI, including the political scientist Herbert Simon, realized that AI technology has more in common with markets, bureaucracies, and political institutions than with simple engineering applications. Another pioneer of artificial intelligence, Norbert Wiener, described AI as a "cybernetic" system—one that can respond and adapt to feedback. Neither Simon nor Wiener anticipated how machine learning would dominate AI, but its evolution fits with their way of thinking. Facebook and Google use machine learning as the analytic engine of a self-correcting system, which continually updates its understanding of the data depending on whether its predictions succeed or fail. It is this loop between statistical analysis and feedback from the environment that has made machine learning such a formidable force.



What is much less well understood is that democracy and authoritarianism are cybernetic systems, too. Under both forms of rule, governments enact policies and then try to figure out whether these policies have succeeded or failed. In democracies, votes and voices provide powerful feedback about whether a given approach is really working. Authoritarian systems have historically had a much harder time getting good feedback. Before the information age, they relied not just on domestic intelligence but also on petitions and clandestine opinion surveys to try to figure out what their citizens believed.

Now, machine learning is disrupting traditional forms of democratic feedback (voices and votes) as new technologies facilitate disinformation and worsen existing biases—taking prejudice hidden in data and confidently transforming it into incorrect assertions. To autocrats fumbling in the dark, meanwhile, machine learning looks like an answer to their prayers. Such technology can tell rulers whether their subjects like what they are doing without the hassle of surveys or the political risks of open debates and elections. For this reason, many observers have fretted that advances in AI will only strengthen the hand of dictators and further enable them to control their societies.

The truth is more complicated. Bias is visibly a problem for democracies. But because it is more visible, citizens can mitigate it through other forms of feedback. When, for example, a racial group sees that hiring algorithms are biased against them, they can protest and seek redress with some chance of success. Authoritarian countries are probably at least as prone to bias as democracies are, perhaps more so. Much of this bias is likely to be invisible, especially to the decision-makers at the top. That makes it far more difficult to correct, even if leaders can see that something needs correcting.

Contrary to conventional wisdom, AI can seriously undermine autocratic regimes by reinforcing their own ideologies and fantasies at the expense of a finer understanding of the real world. Democratic countries may discover that, when it comes to AI, the key challenge of the twenty-first century is not winning the battle for technological dominance. Instead, they will have to contend with authoritarian countries that find themselves in the throes of an AI-fueled spiral of delusion.

Bad feedback

Most discussions about AI have to do with machine learning—statistical algorithms that extract relationships between data. These algorithms make guesses: Is there a dog in this photo? Will this chess strategy win the game in ten moves? What is the next word in this half-finished sentence? A so-called objective function, a mathematical means of scoring outcomes, can reward the algorithm if it guesses correctly. This process is how commercial AI works. YouTube, for example, wants to keep its users engaged, watching more videos so that they keep seeing ads. The objective function is designed to maximize user engagement.

The algorithm tries to serve up content that keeps a user's eyes on the page. Depending on whether its guess was right or wrong, the algorithm updates its model of what the user is likely to respond to.
Machine learning's ability to automate this feedback loop with little or no human intervention has reshaped e-commerce. It may, someday, allow fully self-driving cars, although this advance has turned out to be a much harder problem than engineers anticipated. Developing autonomous weapons is a harder problem still. When algorithms encounter truly unexpected information, they often fail to make sense of it. Information that a human can easily understand but that machine learning misclassifies—known as "adversarial examples"—can gum up the works badly. For example, black and white stickers placed on a stop sign can prevent a self-driving car's vision system from recognizing the sign. Such vulnerabilities suggest obvious limitations in AI's usefulness in wartime.
Diving into the complexities of machine learning helps make sense of the debates about technological dominance. It explains why some thinkers, such as the computer scientist Lee, believe that data is so important. The more data you have, the more quickly you can improve the performance of your algorithm, iterating tiny change upon tiny change until you have achieved a decisive advantage. But machine learning has its limits. For example, despite enormous investments by technology firms, algorithms are far less effective than is commonly understood at getting people to buy one nearly identical product over another. Reliably manipulating shallow preferences is hard, and it is probably far more difficult to change people's deeply held opinions and beliefs.
General AI, a system that might draw lessons from one context and apply them in a different one, as humans can, faces similar limitations. Netflix's statistical models of its users' inclinations and preferences are almost certainly dissimilar to Amazon's, even when both are trying to model the same people grappling with similar decisions. Dominance in one sector of AI, such as serving up short videos that keep teenagers hooked (a triumph of the app TikTok), does not easily translate into dominance in another, such as creating autonomous battlefield weapons systems. An algorithm's success often relies on the very human engineers who can translate lessons across different applications rather than on the technology itself. For now, these problems remain unsolved.
Bias can also creep into code. When Amazon tried to apply machine learning to recruitment, it trained the algorithm on data from résumés that human recruiters had evaluated. As a result, the system reproduced the biases implicit in the humans' decisions, discriminating against résumés from women. Such problems can be self-reinforcing. As the sociologist Ruha Benjamin has pointed out, if policymakers used machine learning to decide where to send police forces, the technology could guide them to allocate more police to neighborhoods with high arrest rates, in the process sending more police to areas with racial groups whom the police have demonstrated biases against. This could lead to more arrests that, in turn, reinforce the algorithm in a vicious circle.
The old programming adage "garbage in, garbage out" has a different meaning in a world where the inputs influence the outputs and vice versa. Without appropriate outside correction, machine-learning algorithms can acquire a taste for the garbage that they themselves produce, generating a loop of bad decision-making. All too often, policymakers treat machine learning tools as wise and dispassionate oracles rather than as fallible instruments that can intensify the problems they purport to solve.

Call and response

Political systems are feedback systems, too. In democracies, the public literally evaluates and scores leaders in elections that are supposed to be free and fair. Political parties make promises with the goal of winning power and holding on to it. A legal opposition highlights government mistakes, while a free press reports on controversies and misdeeds. Incumbents regularly face voters and learn whether they have earned or lost the public trust, in a continually repeating cycle.
But feedback in democratic societies does not work perfectly. The public may not have a deep understanding of politics, and it can punish governments for things beyond their control. Politicians and their staff may misunderstand what the public wants. The opposition has incentives to lie and exaggerate. Contesting elections costs money, and the real decisions are sometimes made behind closed doors. Media outlets may be biased or care more about entertaining their consumers than edifying them.
All the same, feedback makes learning possible. Politicians learn what the public wants. The public learns what it can and cannot expect. People can openly criticize government mistakes without being locked up. As new problems emerge, new groups can organize to publicize them and try to persuade others to solve them. All this allows policymakers and governments to engage with a complex and ever-changing world.
Feedback works very differently in autocracies. Leaders are chosen not through free and fair elections but through ruthless succession battles and often opaque systems for internal promotion. Even where opposition to the government is formally legal, it is discouraged, sometimes brutally. If media criticize the government, they risk legal action and violence. Elections, when they do occur, are systematically tilted in favor of incumbents. Citizens who oppose their leaders don't just face difficulties in organizing; they risk harsh penalties for speaking out, including imprisonment and death. For all these reasons, authoritarian governments often don't have a good sense of how the world works or what they and their citizens want.
Such systems therefore face a tradeoff between short-term political stability and effective policymaking; a desire for the former inclines authoritarian leaders to block outsiders from expressing political opinions, while the need for the latter requires them to have some idea of what is happening in the world and in their societies. Because of tight controls on information, authoritarian rulers cannot rely on citizens, media,

and opposition voices to provide corrective feedback as democratic leaders can. The result is that they risk policy failures that can undermine their long-term legitimacy and ability to rule. Russian President Vladimir Putin's disastrous decision to invade Ukraine, for example, seems to have been based on an inaccurate assessment of Ukrainian morale and his own military's strength.

Even before the invention of machine learning, authoritarian rulers used quantitative measures as a crude and imperfect proxy for public feedback. Take China, which for decades tried to combine a decentralized market economy with centralized political oversight of a few crucial statistics, notably GDP. Local officials could get promoted if their regions saw particularly rapid growth. But Beijing's limited quantified vision offered them little incentive to tackle festering issues such as corruption, debt, and pollution. Unsurprisingly, local officials often manipulated the statistics or pursued policies that boosted GDP in the short term while leaving the long-term problems for their successors.

The world caught a glimpse of this dynamic during the initial Chinese response to the COVID-19 pandemic that began in Hubei Province in late 2019. China had built an internet-based disease-reporting system following the 2003 SARS crisis, but instead of using that system, local authorities in Wuhan, Hubei's capital, punished the doctor who first reported the presence of a "SARS-like" contagion. The Wuhan government worked hard to prevent information about the outbreak from reaching Beijing, continually repeating that there were "no new cases" until after important local political meetings concluded. The doctor, Li Wenliang, himself succumbed to the disease and died on February 7, triggering fierce outrage across the country.

Beijing then took over the response to the pandemic, adopting a "zero COVID" approach that used coercive measures to suppress case counts. The policy worked well in the short run, but with the Omicron variant's tremendous transmissibility, the zero-COVID policy increasingly seems to have led to only pyrrhic victories, requiring massive lockdowns that have left people hungry and the economy in shambles. But it remained successful at achieving one crucial if crude metric—keeping the number of infections low.

Data seem to provide objective measures that explain the world and its problems, with none of the political risks and inconveniences of elections or free media. But there is no such thing as decision-making devoid of politics. The messiness of democracy and the risk of deranged feedback processes are apparent to anyone who pays attention to U.S. politics. Autocracies suffer similar problems, although they are less immediately perceptible. Officials making up numbers or citizens declining to turn their anger into wide-scale protests can have serious consequences, making bad decisions more likely in the short run and regime failure more likely in the long run.

It's a trap?

The most urgent question is not whether the United States or China will win or lose in the race for AI dominance. It is how AI will change the different feedback loops that democracies and autocracies rely on to govern their societies. Many observers have suggested that as machine learning becomes more ubiquitous, it will inevitably hurt democracy and help autocracy. In their view, social media algorithms that optimize engagement, for instance, may undermine democracy by damaging the quality of citizen feedback. As people click through video after video, YouTube's algorithm offers up shocking and alarming content to keep them engaged. This content often involves conspiracy theories or extreme political views that lure citizens into a dark wonderland where everything is upside down.

By contrast, machine learning is supposed to help autocracies by facilitating greater control over their people. Historian Yuval Harari and a host of other scholars claim that AI "favors tyranny." According to this camp, AI centralizes data and power, allowing leaders to manipulate ordinary citizens by offering them information that is calculated to push their "emotional buttons." This endlessly iterating process of feedback and response is supposed to produce an invisible and effective form of social control. In this account, social media allows authoritarian governments to take the public's pulse as well as capture its heart.

But these arguments rest on uncertain foundations. Although leaks from inside Facebook suggest that algorithms can indeed guide people toward radical content, recent research indicates that the algorithms don't themselves change what people are looking for. People who search for extreme YouTube videos are likely to be guided toward more of what they want, but people who aren't already interested in dangerous content are unlikely to follow the algorithms' recommendations. If feedback in democratic societies were to become increasingly deranged, machine learning would not be entirely at fault; it would only have lent a helping hand.

There is no good evidence that machine learning enables the sorts of generalized mind control that will hollow out democracy and strengthen authoritarianism. If algorithms are not very effective at getting people to buy things, they are probably much worse at getting them to change their minds about things that touch on closely held values, such as politics. The claims that Cambridge Analytica, a British political consulting firm, employed some magical technique to fix the 2016 U.S. presidential election for Donald Trump have unraveled. The firm's supposed secret sauce provided to the Trump campaign seemed to consist of standard psychometric targeting techniques—using personality surveys to categorize people—of limited utility.

Indeed, fully automated data-driven authoritarianism may turn out to be a trap for states such as China that concentrate authority in a tiny insulated group of decision-makers. Democratic countries have correction mechanisms—alternative forms of citizen feedback that can check governments if they go off

track. Authoritarian governments, as they double down on machine learning, have no such mechanism. Although ubiquitous state surveillance could prove effective in the short term, the danger is that authoritarian states will be undermined by the forms of self-reinforcing bias that machine learning facilitates. As a state employs machine learning widely, the leader's ideology will shape how machine learning is used, the objectives around which it is optimized, and how it interprets results. The data that emerge through this process will likely reflect the leader's prejudices right back at him.

As the technologist Maciej Ceglowski has explained, machine learning is "money laundering for bias," a "clean, mathematical apparatus that gives the status quo the aura of logical inevitability." What will happen, for example, as states begin to use machine learning to spot social media complaints and remove them? Leaders will have a harder time seeing and remedying policy mistakes—even when the mistakes damage the regime. A 2013 study speculated that China has been slower to remove online complaints than one might expect, precisely because such griping provided useful information to the leadership. But now that Beijing is increasingly emphasizing social harmony and seeking to protect high officials, that hands-off approach will be harder to maintain.

Chinese President Xi Jinping is aware of these problems in at least some policy domains. He long claimed that his antipoverty campaign—an effort to eliminate rural impoverishment—was a signature victory powered by smart technologies, big data, and AI. But he has since acknowledged flaws in the campaign, including cases where officials pushed people out of their rural homes and stashed them in urban apartments to game poverty statistics. As the resettled fell back into poverty, Xi worried that "uniform quantitative targets" for poverty levels might not be the right approach in the future. Data may indeed be the new oil, but it may pollute rather than enhance a government's ability to rule.

This problem has implications for China's so-called social credit system, a set of institutions for keeping track of pro-social behavior that Western commentators depict as a perfectly functioning "AI-powered surveillance regime that violates human rights." As experts on information politics such as Shazeda Ahmed and Karen Hao have pointed out, the system is, in fact, much messier. The Chinese social credit system actually looks more like the U.S. credit system, which is regulated by laws such as the Fair Credit Reporting Act, than a perfect Orwellian dystopia.

More machine learning may also lead authoritarian regimes to double down on bad decisions. If machine learning is trained to identify possible dissidents on the basis of arrest records, it will likely generate self-reinforcing biases similar to those seen in democracies—reflecting and affirming administrators' beliefs about disfavored social groups and inexorably perpetuating automated suspicion and backlash. In democracies, public pushback, however imperfect, is possible. In autocratic regimes, resistance is far harder; without it, these problems are invisible to those inside the system, where officials and algorithms share the same prejudices. Instead of good policy, this will lead to increasing pathologies, social dysfunction, resentment, and, eventually, unrest and instability.

Weaponized AI

The international politics of AI will not create a simple race for dominance. The crude view that this technology is an economic and military weapon and that data is what powers it conceals a lot of the real action. In fact, AI's biggest political consequences are for the feedback mechanisms that both democratic and authoritarian countries rely on. Some evidence indicates that AI is disrupting feedback in democracies, although it doesn't play nearly as big a role as many suggest. By contrast, the more authoritarian governments rely on machine learning, the more they will propel themselves into an imaginary world founded on their own tech-magnified biases. The political scientist James Scott's classic 1998 book, *Seeing Like a State*, explained how twentieth-century states were blind to the consequences of their own actions in part because they could see the world through only bureaucratic categories and data. As sociologist Marion Fourcade and others have argued, machine learning may present the same problems but at an even greater scale.

This problem creates a very different set of international challenges for democracies such as the United States. Russia, for example, invested in disinformation campaigns designed to sow confusion and disarray among the Russian public while applying the same tools in democratic countries. Although free speech advocates long maintained that the answer to bad speech was more speech, Putin decided that the best response to more speech was more bad speech. Russia then took advantage of open feedback systems in democracies to pollute them with misinformation.

One rapidly emerging problem is how autocracies such as Russia might weaponize large language models, a new form of AI that can produce text or images in response to a verbal prompt, to generate disinformation at scale. As the computer scientist Timnit Gebru and her colleagues have warned, programs such as Open AI's GPT-3 system can produce apparently fluent text that is difficult to distinguish from ordinary human writing. Bloom, a new open-access large language model, has just been released for anyone to use. Its license requires people to avoid abuse, but it will be very hard to police.

These developments will produce serious problems for feedback in democracies. Current online policy-comment systems are almost certainly doomed, since they require little proof to establish whether the commenter is a real human being. Contractors for big telecommunications companies have already flooded the U.S. Federal Communications Commission with bogus comments linked to stolen email addresses as part of their campaign against net neutrality laws. Still, it was easy to identify subterfuge

when tens of thousands of nearly identical comments were posted. Now, or in the very near future, it will be trivially simple to prompt a large language model to write, say, 20,000 different comments in the style of swing voters condemning net neutrality.
Artificial intelligence–fueled disinformation may poison the well for autocracies, too. As authoritarian governments seed their own public debate with disinformation, it will become easier to fracture opposition but harder to tell what the public actually believes, greatly complicating the policymaking process. It will be increasingly hard for authoritarian leaders to avoid getting high on their own supply, leading them to believe that citizens tolerate or even like deeply unpopular policies.

Shared threats

What might it be like to share the world with authoritarian states such as China if they become increasingly trapped in their own unhealthy informational feedback loops? What happens when these processes cease to provide cybernetic guidance and instead reflect back the rulers' own fears and beliefs? One self-centered response by democratic competitors would be to leave autocrats to their own devices, seeing anything that weakens authoritarian governments as a net gain.
Such a reaction could result in humanitarian catastrophe, however. Many of the current biases of the Chinese state, such as its policies toward the Uyghurs, are actively malignant and might become far worse. Previous consequences of Beijing's blindness to reality include the great famine, which killed some 30 million people between 1959 and 1961 and was precipitated by ideologically driven policies and hidden by the unwillingness of provincial officials to report accurate statistics. Even die-hard cynics should recognize the dangers of AI-induced foreign policy catastrophes in China and elsewhere. By amplifying nationalist biases, for instance, AI could easily reinforce hawkish factions looking to engage in territorial conquest.
Perhaps, even more cynically, policymakers in the West may be tempted to exploit the closed loops of authoritarian information systems. So far, the United States has focused on promoting Internet freedom in autocratic societies. Instead, it might try to worsen the authoritarian information problem by reinforcing the bias loops that these regimes are prone to. It could do this by corrupting administrative data or seeding authoritarian social media with misinformation. Unfortunately, there is no virtual wall to separate democratic and autocratic systems. Not only might bad data and crazy beliefs leak into democratic societies from authoritarian ones, but terrible authoritarian decisions could have unpredictable consequences for democratic countries, too. As governments think about AI, they need to realize that we live in an interdependent world, where authoritarian governments' problems are likely to cascade into democracies.
A more intelligent approach, then, might look to mitigate the weaknesses of AI through shared arrangements for international governance. Currently, different parts of the Chinese state disagree on the appropriate response to regulating AI. China's Cyberspace Administration, its Academy of Information and Communications Technology, and its Ministry of Science and Technology, for instance, have all proposed principles for AI regulation. Some favor a top-down model that might limit the private sector and allow the government a free hand. Others, at least implicitly, recognize the dangers of AI for the government, too. Crafting broad international regulatory principles might help disseminate knowledge about the political risks of AI.
This cooperative approach may seem strange in the context of a growing U.S.-Chinese rivalry. But a carefully modulated policy might serve Washington and its allies well. One dangerous path would be for the United States to get sucked into a race for AI dominance, which would extend competitive relations still further. Another would be to try to make the feedback problems of authoritarianism worse. Both risk catastrophe and possible war. Far safer, then, for all governments to recognize AI's shared risks and work together to reduce them.

Henry Farrell is the Stavros Niarchos Foundation Agora Professor of International Affairs at Johns Hopkins University.
Abraham Newman is Professor of Government in the Edmund A. Walsh School of Foreign Service at Georgetown University.
Jeremy Wallace is Associate Professor of Government at Cornell University and the author of *Seeking Truth and Hiding Facts: Information, Ideology, and Authoritarianism in China*.

AI model detects COVID-19 infection in people's voices

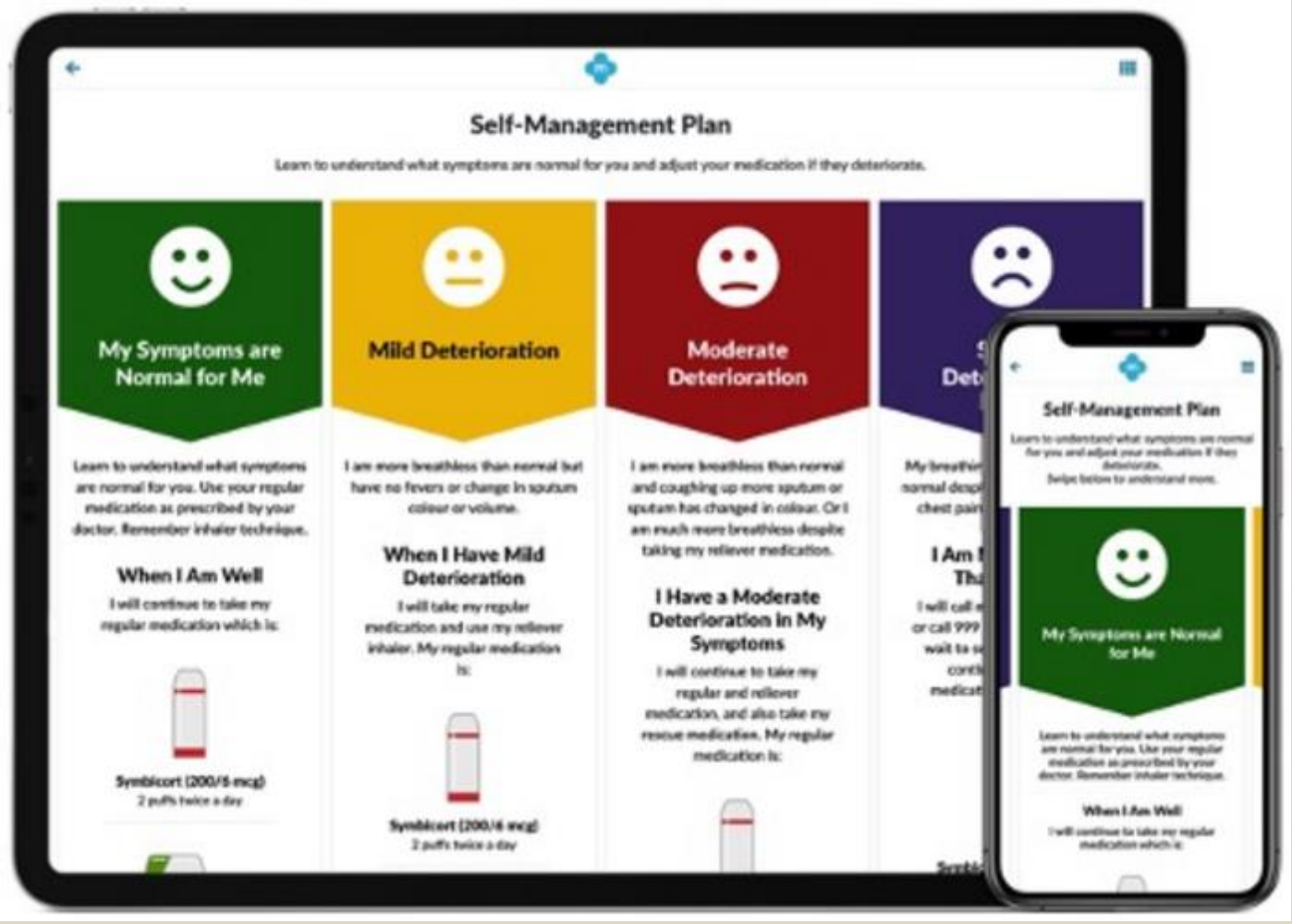
Source: https://www.news-medical.net/news/20220905/AI-model-detects-COVID-19-infection-in-peoplee28099s-voices.aspx

Sep 05 – Artificial intelligence (AI) can be used to detect COVID-19 infection in people's voices by means of a mobile phone app, according to research to be presented on Monday at the European Respiratory Society International Congress in Barcelona, Spain.
The AI model used in this research is more accurate than lateral flow/rapid antigen tests and is cheap, quick and easy to use, which means it can be used in low-income countries where PCR tests are expensive and/or difficult to distribute.
Ms Wafaa Aljbawi, a researcher at the Institute of Data Science, Maastricht University, The Netherlands, told the congress that the AI model was accurate 89% of the time, whereas the accuracy of lateral flow

tests varied widely depending on the brand. Also, lateral flow tests were considerably less accurate at detecting COVID infection in people who showed no symptoms.

"These promising results suggest that simple voice recordings and fine-tuned AI algorithms can potentially achieve high precision in determining which patients have COVID-19 infection. Such tests can be provided at no cost and are simple to interpret. Moreover, they enable remote, virtual testing and have a turnaround time of less than a minute. They could be used, for example, at the entry points for large gatherings, enabling rapid screening of the population."

Wafaa Aljbawi, Researcher, Institute of Data Science, Maastricht University



COVID-19 infection usually affects the upper respiratory track and vocal cords, leading to changes in a person's voice. Ms Aljbawi and her supervisors, Dr Sami Simons, pulmonologist at Maastricht University Medical Centre, and Dr Visara Urovi, also from the Institute of Data Science, decided to investigate if it was possible to use AI to analyze voices in order to detect COVID-19.

They used data from the University of Cambridge's crowd-sourcing COVID-19 Sounds App that contains 893 audio samples from 4,352 healthy and non-healthy participants, 308 of whom had tested positive for COVID-19. The app is installed on the user's mobile phone, the participants report some basic information about demographics, medical history and smoking status, and then are asked to record some respiratory sounds. These include coughing three times, breathing deeply through their mouth three to five times, and reading a short sentence on the screen three times.

The researchers used a voice analysis technique called Mel-spectrogram analysis, which identifies different voice features such as loudness, power and variation over time.

"In this way we can decompose the many properties of the participants' voices," said Ms Aljbawi. "In order to distinguish the voice of COVID-19 patients from those who did not have the disease, we built different artificial intelligence models and evaluated which one worked best at classifying the COVID-19 cases."

They found that one model called Long-Short Term Memory (LSTM) out-performed the other models. LSTM is based on neural networks, which mimic the way the human brain operates and recognizes the

underlying relationships in data. It works with sequences, which makes it suitable for modeling signals collected over time, such as from the voice, because of its ability to store data in its memory.
Its overall accuracy was 89%, its ability to correctly detect positive cases (the true positive rate or "sensitivity") was 89%, and its ability to correctly identify negative cases (the true negative rate or "specificity") was 83%.
"These results show a significant improvement in the accuracy of diagnosing COVID-19 compared to state-of-the-art tests such as the lateral flow test," said Ms Aljbawi. "The lateral flow test has a sensitivity of only 56%, but a higher specificity rate of 99.5%. This is important as it signifies that the lateral flow test is misclassifying infected people as COVID-19 negative more often than our test. In other words, with the AI LSTM model, we could miss 11 out 100 cases who would go on to spread the infection, while the lateral flow test would miss 44 out of 100 cases.
"The high specificity of the lateral flow test means that only one in 100 people would be wrongly told they were COVID-19 positive when, in fact, they were not infected, while the LSTM test would wrongly diagnose 17 in 100 non-infected people as positive. However, since this test is virtually free, it is possible to invite people for PCR tests if the LSTM tests show they are positive."
The researchers say that their results need to be validated with large numbers. Since the start of this project, 53,449 audio samples from 36,116 participants have now been collected and can be used to improve and validate the accuracy of the model. They are also carrying out further analysis to understand which parameters in the voice are influencing the AI model.
In a second study, Mr Henry Glyde, a PhD student in the faculty of engineering at the University of Bristol, showed that AI could be harnessed via an app called myCOPD to predict when patients with chronic obstructive pulmonary disease (COPD) might suffer a flare-up of their disease, sometimes called acute exacerbation. COPD exacerbations can be very serious and are associated with increased risk of hospitalization. Symptoms include shortness of breath, coughing and producing more phlegm (mucus).
"Acute exacerbations of COPD have poor outcomes. We know that early identification and treatment of exacerbations can improve these outcomes and so we wanted to determine the predictive ability of a widely used COPD app," he said.
The myCOPD app is a cloud-based interactive app, developed by patients and clinicians and is available to use in the UK's National Health Service. It was established in 2016 and, so far, has over 15,000 COPD patients using it to help them manage their disease.
The researchers collected 45,636 records for 183 patients between August 2017 and December 2021. Of these, 45,007 were records of stable disease and 629 were exacerbations. Exacerbation predictions were generated one to eight days before a self-reported exacerbation event. Mr Glyde and colleagues used these data to train AI models on 70% of the data and test it on 30%.
The patients were "high engagers", who had been using the app weekly over months or even years to record their symptoms and other health information, record medication, set reminders, and have access to up-to-date health and lifestyle information. Doctors can assess the data via a clinician dashboard, enabling them to provide oversight, co-management and remote monitoring.
"The most recent AI model we developed has a sensitivity of 32% and a specificity of 95%. This means that the model is very good at telling patients when they are not about to experience an exacerbation, which may help them to avoid unnecessary treatment. It is less good at telling them when they are about to experience one. Improving this will be the focus of the next phase of our research," said Mr Glyde.
Speaking before the congress, Dr James Dodd, Associate Professor in respiratory medicine at the University of Bristol and project lead, said: "To our knowledge, this study is the first of its kind to model real world data from COPD patients, extracted from a widely deployed therapeutic app. As a result, exacerbation predictive models generated from this study have the potential to be deployed to thousands more COPD patients after further safety and efficacy testing. It would empower patients to have more autonomy and control over their health. This is also a significant benefit for their doctors as such a system would likely reduce patient reliance on primary care. In addition, better-managed exacerbations could prevent hospitalization and alleviate the burden on the healthcare system. Further study is required into patient engagement to determine what level of accuracy is acceptable and how an exacerbation alert system would work in practice. The introduction of sensing technologies may further enhance monitoring and improve the predictive performance of models."
One of the limitations of the study is the small number of frequent users of the app. The current model requires a patient to input a COPD assessment test score, fill out their medication diary and then report they are having an exacerbation accurately days later. Usually, only patients who are highly engaged with the app, using it daily or weekly, can provide the amount of data needed for the AI modeling. In addition, because there are significantly more days the users are stable than when they are having an exacerbation, there is a significant imbalance between the exacerbation and non-exacerbation data available. This results in even further difficulty in the models correctly predicting events after training on this imbalanced data.
"A recent partnership between patients, clinicians and carers to set research priorities in COPD found that the highest-rated question was how to identify better ways to prevent exacerbations. We have focused on this question ,and we will be working closely with patients to design and implement the system," concluded Mr Glyde.
Chair of the ERS Science Council, Professor Chris Brightling, is the National Institute for Health and Care Research (NIHR) Senior Investigator at the University of Leicester, UK, and was not involved with the research. He commented: "These two studies show the potential of artificial intelligence and apps on

mobile phones and other digital devices to make a difference in how diseases are managed. Having more data available for training these artificial intelligence models, including appropriate control groups, as well as validation in multiple studies, will improve their accuracy and reliability. Digital health using AI models presents an exciting opportunity and is likely to impact future health care."

Russia Initiates Plan To Dominate AI Operations

Source: https://i-hls.com/archives/108719

Sep 16 – As Russian leadership attempts to come to terms with technology's impact on its military power and role in the world, artificial intelligence and autonomy stand out as an area of particular growth and potential for influence. According to a new paper from a US Navy-linked think tank, the Center for Naval Analyses (CNA), the United States isn't the only major military power trying to digitally link all of its weapons and execute operations faster with artificial intelligence. Russia has been making gains in its own version of centralized command and control across land, sea, space, and cyberspace,

Russian military leaders have steadily advanced an AI-linked concept called automated control systems, or ACS, says the paper. The concept bears an uncanny resemblance to the U.S. military's own vision for AI-fueled, network-centric operations. In 2017, U.S. service chiefs began speaking about digitally linking planes, ships, drones, satellites and troops in a comprehensive data web. The idea was to allow any "shooter" on the battlefield to hit any target. Artificial intelligence would play a key role, analyzing rapidly incoming data streams about targets and the state of U.S. forces and then determining best courses of action for commanders to execute.

The Russian military began testing ACS concepts in 2019, even simulating a (presumably NATO-led) attack on the Crimean Peninsula. Russian forces combined an S-400 anti-aircraft radar and battery with a Pantsir-S missile system to shoot down dozens of enemy cruise missiles, at least in state media accounts. Like the US JADC2, ACS would use AI to find targets and build strike plans. Unlike JADC2, ACS might leave humans out of the loop. "The [Ministry of Defense] thinks that in the future, this system will be equipped with AI in order to independently detect potential targets and distribute missile strikes without human intervention," the CNA paper said.

No Detail Missed – Body Cameras With Artificial Intelligence

Source: https://i-hls.com/archives/111892

Sep 15 – Nowadays, body camera footage is essential for any proper execution of a security mission. It is a rarity to find a police officer not adoring a body camera. How about a body camera enhanced with AI? The next generation of the **AI body camera VEMO** was launched by Iveda and Clearview Asset Protection. The device is integrated with IvedaAI intelligent video search technology, featuring face recognition, license plate recognition, object search and other AI functions. VEMO can stream directly into the IvedaAI platform for real-time video analytics.

Using 4G, VEMO streams live video to headquarters and doubles as a walkie-talkie with push-to-talk feature (PTT). PTT allows communication from the bodycam to headquarters or to other VEMO devices in the same group. The device is WiFi-enabled which is ideal for city-wide deployments. This saves the city cellular data cost where WiFi infrastructure exists.

The camera will be 5G ready when the network is widely available.

It can serve criminal justice practitioners, first responders, public safety professionals and the general public. Applications beyond law enforcement include remote site surveys, medical, health and safety applications, etc. It may also be used as in-vehicle surveillance for taxi and rideshare services.

Iveda recently joined the Emergency Response Training and Certification Association (ERTCA) to develop new standardized applications for the public safety industry, along with more than 20 other member organizations.

Study looks at impact of artificial intelligence on primary health care

Source: https://medicalxpress.com/news/2022-09-impact-artificial-intelligence-primary-health.html

Sep 22 – Whether we're ready or not, artificial intelligence (AI) already plays a role in many health care settings. However, cautiously developing, deploying and even defining further AI advancements will determine its impact and efficacy in the years ahead, according to a new University of Western Ontario study.

Interdisciplinary researchers from family medicine, computer science and epidemiology have identified key issues regarding the use of AI tools in primary health care by connecting directly with family physicians, nurses, nurse practitioners and digital health stakeholders.

Overwhelmingly, the responses show AI could have a positive impact in clinical practice, but many factors must be considered regarding its implementation.

"We are ready for AI, but we must be thoughtful about how and when we use it," said Dan Lizotte, an associate professor in computer science and the Schulich School of Medicine & Dentistry and senior author on the study. "So let me amend and say, 'I think we're ready to start the process of successful implementation.'"

AI and machine learning (a subfield of AI where patterns are learned from data) encompass a variety of techniques loosely focused on computers performing human-like "intelligent" tasks. AI methods are already used in applications ranging from advanced web search engines (Google) and recommendation systems (Netflix, Amazon) to understanding human speech (Siri and Alexa) and self-driving cars (Tesla). In primary health care settings, AI could be used for predicting patient outcomes based on anonymous electronic medical record (EMR) data or forecasting trends and identifying patterns too complex for humans to discern (e.g., infectious disease outbreaks in a community.)

For this study, former graduate student Jaky Kueper, Lizotte and co-principal investigator Amanda Terry conducted 14 in-depth interviews with primary health care and digital health stakeholders in Ontario. Kueper, now a TechForward Fellow in AI at The College of Family Physicians of Canada, is the first-ever Western student to complete a combined Ph.D. in epidemiology and computer science.

In the interviews, there was general positivity about the introduction of AI in primary health care settings, but there were also several apprehensions, including cost and availability of new technology, privacy concerns, threats to clinical skills and capacity, loss of human control over decision making, and broader ethical, legal and social implications.

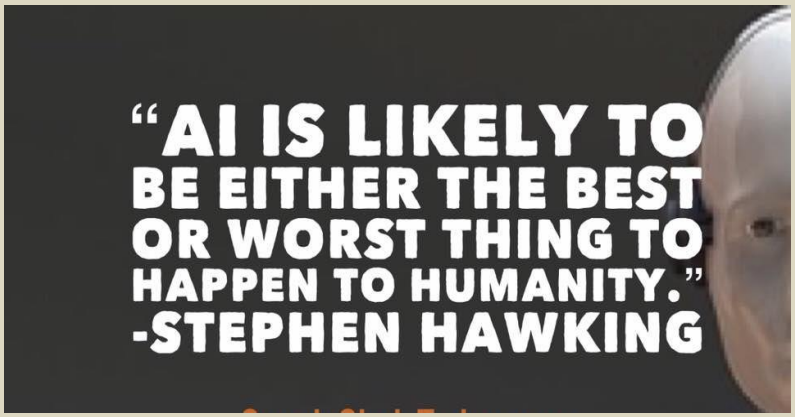
"There's a readiness in terms of people looking for solutions using technology including AI that can help support primary health care practitioners, but there are a lot of things that need to be in place first, in terms of transparency, assurances of privacy and cost," said Terry, director of the Center for Studies in Family Medicine at Schulich Medicine and Dentistry.

When considering the use of AI in primary health care settings, the practitioners need to be comfortable with the implementation and application but so do the patients.

Lizotte said the introduction of AI triggers as many questions as answers for doctors, nurses, and nurse practitioners but that's an important step to consider as the digitization of health care is here to stay.

"Is AI going to enhance the things I care about doing in my practice? Or is it going to supplant them in a way that's not going to be good for me and not going to be good for my patients? These are the questions on everyone's mind," said Lizotte. "I think overall there is cautious optimism about AI implementation, but the key word is cautious."

●▶ **The study appears in** *BMC Medical Informatics and Decision Making*.




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

The Expanding Role of Tactical Medicine

By Ian Pleet

Source: https://www.domesticpreparedness.com/healthcare/the-expanding-role-of-tactical-medicine/

Aug 10 – Since the mass shooting at Columbine High School in 1999, the paradigm for responding to an active shooter has shifted from a reactive to a proactive response to stop the killing (by stopping the shooter or shooters) and stop the dying (by stopping external hemorrhage and treating other life-threatening injuries). To prevent the dying, trained first responders with the correct equipment and the courage to use it must be present at the point of wounding, almost immediately, to stop the bleeding. While this may be the principal responsibility of a tactical medic, there is much more involved to be effective in this role.

The Role of a Tactical Medic

The American College of Emergency Physicians describes Tactical Medical Providers (TMPs) as those who "render medical care during training and at high-threat deployments where normal EMS and Fire personnel cannot safely respond." Today, tactical emergency medical care has evolved into a highly specialized discipline within the field of prehospital emergency medical care. The Vietnam War demonstrated the value of rapidly transporting casualties to higher echelons of care via helicopter. Furthermore, the global war on terrorism – with combat operations in Iraq and Afghanistan – has confirmed the lifesaving effects of tourniquets and hemostatic agents. Although there has been and continues to be ongoing development in new and better ways to kill in combat, there are also improved ways to treat combat injuries with higher survivability rates. As a result, casualty fatality rates have decreased by almost 10%, from 19.1% in WWII to 9.4% in the Iraq and Afghanistan conflicts.

Tactical medicine plays a significant role in reducing deaths associated with active assailant incidents.

Unfortunately, the wounding patterns previously seen primarily on the battlefield now occur in neighborhood streets, subways, busses, and schools. Mass shootings and active assailant attacks have become frequent headlines in the daily news. Further, there is the ever-present threat of a chemical, biological, radiological, nuclear, or high-yield explosive (CBRNE) attack. As a result, tactical medicine has become a discipline and specialty within EMS and law enforcement circles using the principles of tactical combat casualty care (TCCC) and tactical emergency casualty care (TECC), now widely taught to first responders.

When the U.S. Department of Defense realized that the leading cause of preventable death on the battlefield was exsanguination due to bleeding from an extremity, it and the Uniformed Services University of the Health Sciences reevaluated battlefield trauma care. From 1993 to 1996, a three-year study produced the TCCC guidelines. TCCC is a set of evidence-based, best-practice prehospital trauma care guidelines and the standard taught to the members of the U.S. military. TCCC is the standard taught to the members of the U.S. military. Medical personnel (MP), such as U.S. Navy Hospital Corpsman, U.S. Army Medics, and U.S. Air Force Pararescuemen, receive 16 hours of TCCC-MP training. Nonmedical personnel deploying in support of combat operations receive 40 hours of combat lifesaver (CLS) training (TCCC-CLS). All service members (ASM) receive 7 hours of TCCC-ASM. The civilian version is 16 hours of classroom training (TECC). Both TCCC and TECC emphasize:

- Bleeding control, using tourniquets high and tight on the extremity, over the clothing, and wound packing with hemostatic gauze;
- Airway and breathing control with needle decompression and surgical airways;
- Techniques for removing a patient from a vehicle; and
- Assessment and treatment of the patient in a nontraditional environment (e.g., under or behind cover, in low light, no light, or under night vision).

Lack of Standardization

There is no national standard on what training or certification must be considered to become a tactical medic. They may or may not have tactical training, be sworn law enforcement officers, or even be armed. However, several organizations offer training or certification in tactical medicine:

- The Counter Narcotics and Terrorism Operational Medical Support (CONTOMS) course, which has existed since 1990;
- The Tactical Paramedic-Certified (TP-C), offered by the International Board of Specialty Certifications;
- Emergency Medical Technician-Tactical (EMT-T) certification, offered by Rescue Training Incorporated;
- The TCCC and TECC courses, offered by the National Association of EMTs.

In addition to these classes, prehospital trauma life support (PHTLS), advanced trauma life support (ATLS), and the trauma nurse core course (TNCC) offer valuable education for the tactical medic. Tactical

medics practice the full scope of prehospital paramedical care. So, while these instructional programs focus on trauma, an officer can just as quickly die from an exacerbation of his underlying asthma. Therefore, it is critically important for the tactical medic to stay current on their knowledge, skills, and abilities to recognize and treat medical conditions.

Tactical medical skills are perishable. They require many hours of direct patient care experience and regular exercises to maintain competency and proficiency, like any other medical skill. A full-time tactical medic assigned to the tactical team would train officers or agents in the basics of self-care and buddy care, focusing on bleeding control. A 12-month training calendar would include periods of classroom instruction, clinical rotations at the local trauma center, cadaver and live tissue labs, and operating room time to maintain their airway skills and techniques. In addition, the agency must allocate funds in the annual budget to support attendance at local and national professional development and training conferences.

There is currently no nationwide standard practice for how law enforcement and EMS agencies integrate tactical medics. For example, some law enforcement agencies have tactical medics assigned to their tactical teams full-time, while others utilize them part-time for callouts. In some cases, the tactical medic is a sworn police officer, but they are not required to have full police powers. Additionally, there are times that transport capabilities exist, such as an ambulance staged inside the hot zone. But there are other circumstances in which that capacity does not exist.

Many law enforcement agencies depend on the local civilian EMS agency to provide EMTs or paramedics and the transport vehicle. However, relying on civilian EMS agencies poses several challenges. For example, the EMT or paramedics may or may not have tactical medical training and may not be familiar with the tactical team's techniques, procedures, or equipment. Additionally, it is standard practice for civilian EMS to stage in the cold zone with the ambulance. While this keeps the civilian EMTs and paramedics safe, it requires precious time for them to be brought up to the injured officer or bring the wounded officer to the ambulance.

Some jurisdictions opt to use a hospital car or "h-car," which is a police car that takes an injured police officer to the hospital. As reported in a January 25, 2021 article from the Penn Medicine News, Philadelphia Police transport as many as two-thirds of penetrating trauma victims to the hospital using their police cars. While this may be a practical way to get an injured person to definitive care, there is little to no lifesaving en-route care.

Additional Benefits of TMPs

A vital part of any tactical medic program is medical control. If a civilian EMS agency supplies the tactical medic, they already have medical control. However, if the tactical medic is organic to the law enforcement agency, they would most likely fall under the operational medical control of the same doctor directing the local civilian EMTs and paramedics – but would most likely need some kind of agreement between the

law enforcement agency the medical director. Getting medical control could be as simple as a memorandum of understanding or a memorandum of agreement with the local hospital or authority having jurisdiction.

EDITOR'S COMMENT: A strange combination of surgical gloves, tactical gloves, different canisters, and PPE (?) and a victim in PPE without respiratory protection – a thematic photo added to this article

Law enforcement agencies with tactical medics should use them to maximize their value to the team. When taking part in a pre-planned event or callout, the tactical medic could be consulted or personally author the medical plan. They could assist in identifying the vehicle(s) used for transport and the primary and secondary evacuation routes to the nearest trauma center. Part of the contingency planning for any event should also be identifying where the landing zone would be. The tactical medic should go with an officer to the hospital to provide en-route care, be the medical advocate for the officer, and liaise between the hospital and law enforcement agency. When attending training or at high-threat deployments, the tactical medic can provide value when not directly participating in the training or deployment – for example, distributing bottles of water to keep the officers hydrated or monitoring for weather extremes in heat or cold to help the officers avoid hyperthermia or hypothermia. The tactical medic is also trained in canine medicine and provides medical support in remote or austere environments such as a fugitive hunt.

The tactical medic can provide emergency medical contingency planning and administrative support when not deployed on a tactical operation. Medical contingency planning, more commonly known as the behind-the-scenes work, is an often-overlooked and underappreciated aspect of tactical medicine until an officer is wounded. They can help buy medical supplies, create a budget for medical equipment, training, and resources, and provide medical and logistical support. They should advocate for policy standardizing the contents and location of the individual first aid kit (IFAK). While commercial off-the-shelf (COTS) IFAKs can be well-stocked, the tactical medic can add value by customizing them for their officers, including pre-sized nasal pharyngeal airways. Officers should be required to carry their IFAK on their support side, opposite their handgun, so that other officers know where to locate the device in an emergency.

Tactical training is traditionally a high-risk training event, which carries a higher risk of injury to the participating officers. A tactical medic on-site during training allows them to provide immediate lifesaving

care if needed. It also enables the tactical medic to gain a basic understanding of movement and tactics. Another administrative procedure is creating a medical *file* for each officer, tactical or not. This file could be a laminated index card listing the past medical history, known allergies, next of kin contact information, and medications. The tactical medic can reference this card if the officer cannot speak or is unconscious. Officers should keep this on their persons in a pre-determined location, for instance, in the breast pocket on their support side.

With the increased awareness and threat of CBRNE attacks, the tactical medic can train officers to identify the signs and symptoms of a nerve agent attack and use a nerve agent antidote kit. With the rise of Fentanyl-related calls and reported exposures, the organic tactical medic can provide officers with procedures to screen for exposure and immediate care if necessary. They can also give the officers current and accurate procedures and practices to screen for actual exposure and coordinate with the local fire department or hazmat team to provide appropriate decontamination. The agency's public relations can be bolstered by having the tactical medic teach CPR and Stop the Bleed® classes to the public. With the rise in violence, it is prudent for law enforcement leaders to work with EMS leaders to codify how they will integrate tactical medics within their ranks before the next active shooter opens fire or the terrorist pushes the plunger.

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

Preparedness – A Constant Juggle

By Catherine L. Feinman

Domestic Preparedness Journal | Volume 18, Issue 8, August 2022

Source: https://www.domesticpreparedness.com/journals/august-2022/

It is impressive to see how emergency preparedness professionals across disciplines constantly juggle numerous tasks and projects while balancing the needs of everyone they serve. In addition to managing their teams, leaders must educate and train personnel for many scenarios and help ensure the team members' physical and mental well-being.

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

Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the Domestic Preparedness Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Because international CBRNE First Responders need a common roof!

https://www.ici-belgium.be/