C²BRNE DIARY

Dedicated to Global First Responders

March 2022

03\22

PART B

WAR

ВОЙНА

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

C2BRNE DIARY

DIRTY R-NEWS

Russian Forces Capture Chernobyl Nuclear Power Plant, Says Ukrainian PM

Source: https://www.rferl.org/a/ukraine-invasion-russian-forces-chernobyl-/31721240.html

A shelter construction covers the exploded reactor at the Chernobyl nuclear plant, in Chernobyl, April 27, 2021

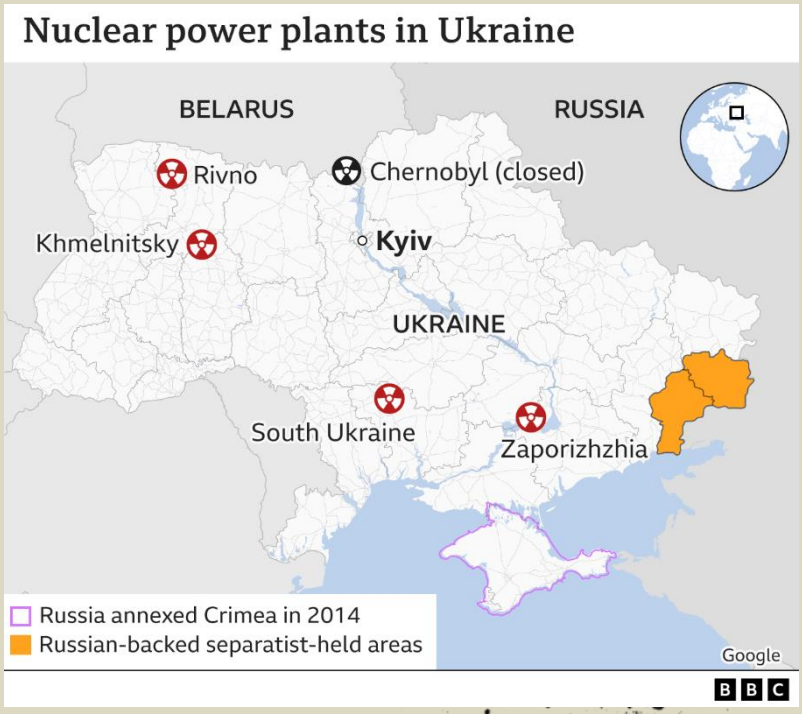
Feb 24 – The Chernobyl nuclear power plant and the exclusion zone around it has been captured by Russian forces, Prime Minister Denys Shmygal said on February 24.

"Unfortunately, I have to say that, as of now, the Chernobyl zone, the so-called exclusion zone, and all Chernobyl facilities have been taken under control by Russian armed groups," Shmygal told a news briefing after an extraordinary cabinet meeting in Kyiv. "According to the leadership of the Chornobyl Exclusion Zone, there are no victims at the moment," he said, adding the further information will released after clarification.

Russian forces captured the power plant, the site of the world's worst nuclear disaster, after a "fierce" battle on the first day of Russia's invasion of Ukraine, an adviser to the head of the president's office said.

"After the absolutely senseless attack of the Russians in this direction, it is impossible to say that the Chernobyl nuclear power plant is safe. This is one of the most serious threats to Europe today," said the adviser, Mykhailo Podolyak.

The Vienna-based International Atomic Energy Agency (IAEA) said it had been told of the takeover by Ukraine. IAEA Director General Rafael Mariano Grossi called for "maximum restraint" to avoid actions that could put Ukraine's nuclear facilities at risk.



The State Nuclear Regulatory Inspectorate of Ukraine (SNRCU) informed the (IAEA) that all Chernobyl facilities, including storage facilities for spent nuclear fuel, in the exclusion zone were **taken under armed control**.
The military unit that had been assigned to guard the facilities has been disarmed, the SNRCU said.
There were no deaths or injuries, and no changes in the radiation situation have been observed, the regulator said. It also said the integrity of the protective barriers of nuclear facilities was not violated.
Some Russian military massed in the Chernobyl exclusion zone before crossing into Ukraine early on February 24, a Russian security source said, according to Reuters.
Russia wants to control the Chernobyl nuclear reactor to signal to NATO not to interfere militarily, the source told the agency.
Ukrainian President Volodymyr Zelenskiy announced earlier that Russian forces were trying to seize the Chernobyl nuclear plant.
"Russian occupying forces are trying to take over the Chernobyl Nuclear Power Plant. Our soldiers are giving their lives so that the tragedy of 1986 does not happen again," Zelenskiy said on Twitter.
He said Kyiv's forces are fighting off Russian troops for control of the Chernobyl plant, which spewed radioactive waste across Europe when one of its nuclear reactors exploded in April 1986.
Fighting in the exclusion zone **raised fears** it could trigger a large-scale environmental disaster, Ukrainian officials said.
The plant, which lies 130 kilometers north of Kyiv, has been decommissioned, and the reactor that exploded has been covered by a protective shelter to prevent radiation from leaking.
Interior Ministry adviser Anton Herashchenko said earlier that Russian troops entered the zone of the Chernobyl nuclear power plant from Belarus.
“If as a result of the occupiers' artillery strikes the nuclear waste storage facility is destroyed, the radioactive dust may cover the territories of Ukraine, Belarus and the EU countries,” he said.

Chernobyl's Radiation Spiked 20 Times Above Usual Levels as Russian Forces Arrive

Source: https://www.sciencealert.com/chernobyl-radiation-levels-have-increased-20-times-above-usual-levels-following-combat-and-military-movement

Feb 25 – The Chernobyl nuclear power plant and its surrounding area are showing increased radiation levels after heavy fighting between Ukrainian and Russian troops in the region, Ukrainian officials said Friday (Feb. 25)
Online data from the Chernobyl exclusion zone's automated radiation-monitoring system shows that gamma radiation has increased 20 times above usual levels at multiple observation points, which officials from the Ukrainian nuclear agency attributed to radioactive dust thrown up by the movement of heavy military equipment in the area.
The defunct Chernobyl nuclear power plant has been under occupation by attacking Russian soldiers since Thursday (Feb. 24) after Russian president Vladimir Putin launched a full-scale invasion of Ukraine in the early hours of the morning.
Workers at the facility, stationed there to monitor and maintain radiation levels within safe bounds, have been taken hostage by Russian troops, according to Anna Kovalenko, a Ukrainian military expert.
"The station staff is being held hostage. This threatens the security of not only Ukraine but also a significant part of Europe," Kovalenko wrote on Facebook.
White House press secretary Jen Psaki said in a news briefing on Thursday (Feb. 24) that the Biden administration was "outraged" by reports of Russian troops holding Chernobyl plant staff against their will and demanded their release.
She warned that the action "could upend the routine civil service efforts required to maintain and protect the nuclear waste facilities."
As one of the most radioactive places in the world, large parts of the Chernobyl exclusion zone have been closed off since the disastrous meltdown of Ukraine's Chernobyl nuclear power plant in 1986.
In that year, two enormous explosions inside the plant's reactor flipped its 2,000-ton (1,800 metric tons) lid like a coin, blanketing the surrounding 1,000-square-mile (2,600 square kilometers) with radioactive dust and reactor chunks.
Following evacuation and the dousing of the nuclear fire – which cost many firefighters their lives – the reactor was sealed off and the area deemed uninhabitable by humans for the next 24,000 years.
Heavy fighting around the plant on Thursday (Feb. 24) led to **concerns that stray munitions** could accidentally pierce the exploded reactor's two layers of protection – consisting of a new, outer safe-confinement structure and an inner concrete sarcophagus – and release the deadly radioactive fallout trapped inside.

In a contradictory statement, Igor Konashenkov, the spokesman for the Russian Defense Ministry, said that radiation around the plant was within normal levels and that Russian forces were working with the facilities' staff to ensure the area's safety.

Oleksiy Arestovych, an advisor to Ukrainian president Volodymyr Zelenskyy, believes that the Chernobyl site was seized as part of a "possible blackmail" tactic against the West.
"Chernobyl has been seized and I think they will blackmail the West. The President's Office is preparing a response to possible blackmail through Chernobyl," Arestovych said in a statement.
The site, which is just 60 miles (97 km) north of the Ukrainian capital Kyiv, lies on a direct invasion route between Kyiv and the Russian forces' northern entry point to Ukraine at the Belarusian border.
Claire Corkhill, a professor of nuclear material degradation at the University of Sheffield in the UK, wrote on Twitter that the gamma radiation around the Chernoybl plant "looks to have increased by around 20 times compared with a few days ago."
However, caution should be taken "not to over-interpret at this stage," she said.
"This appears to be based on a single data point," Corkhill added in a separate tweet. "What is intriguing is that the level of radiation has increased mostly around the main routes in and out of the Chernobyl exclusion zone, as well as the reactor. This would tend to suggest that increased movement of people or vehicles may have disturbed radioactive dust."
The highly radioactive fuel inside the Chernobyl reactor is buried deep beneath the defunct plant and is unlikely to be released unless the reactor is directly targeted, Corkhill said.
Fighting around the plant was just a small part of a much wider ongoing Russian invasion of Ukraine, the biggest on a European nation since World War II.

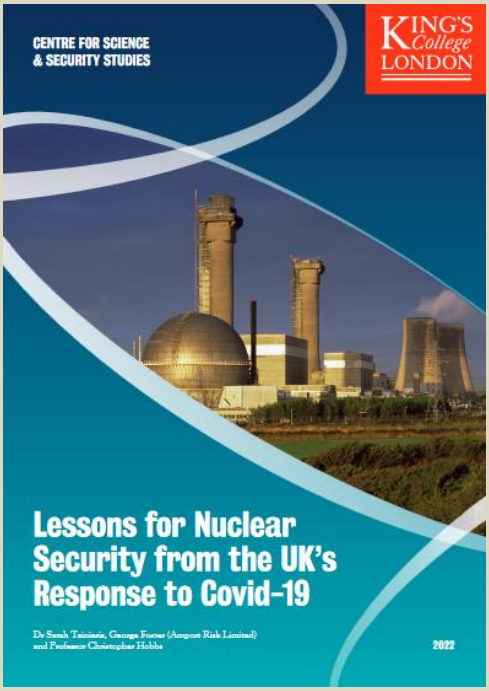
Experience the power of a nuclear blast in your area

Source 1: https://outrider.org/nuclear-weapons/interactive/bomb-blast
Source 2: https://nuclearsecrecy.com/nukemap/

Exploring the Impact of the COVID-19 Pandemic on Nuclear Security

Source: https://www.homelandsecuritynewswire.com/dr20220225-exploring-the-impact-of-the-covid19-pandemic-on-nuclear-security

Feb 25 – King's College London academics have published new research exploring how the UK's civil nuclear sector has responded to challenges posed by Covid-19.



The study, from the Nuclear Security Culture Program in the Centre for Science and Security Studies (CSSS), King's College London, and run in partnership with industry and supported, identifies a series of lessons learnt in maintaining nuclear security. It also provides recommendations for managing the continuing impact of the pandemic and preparing for future crises.
The Covid-19 pandemic has had a significant impact on the nuclear sector and its critical national infrastructure. Challenges have included an increase in worker absenteeism due to infections and enforced isolation, constraints on numbers of staff at facilities, physical restrictions for those onsite to minimize disease transmission, and a large-scale transition to remote working.
This has complicated the delivery of security, in an environment where threats are continually evolving, both from malicious actors taking advantage of perceived weaknesses, and as a by-product of the broader uncertainty generated by the pandemic.
The nuclear industry therefore had to adapt to changing security risks. In order to generate insights into successful adaptations, the researchers conducted semi-structured interviews with practitioners from eight different UK nuclear organizations spanning government, the Office for Nuclear Regulation (ONR), transport, nuclear research and energy production. The interviews were conducted over a period of six months from early- to mid-2021.
The study's key findings emphasize the importance of developing information gathering systems to respond to government decision-making on risk and security. Although, these must be carefully constructed so as not to place unnecessary burden on nuclear operators. Organizations should also regularly update their internal risk registers to account for new emerging threats and vulnerabilities. In the context of COVID-19 relatively few

nuclear companies had a pandemic scenario within their top-10 risks, despite its clear prominence as a high-probability high-consequence event in the UK's national risk register.
The study further calls for an outcome focused regulatory regime, which researchers believe offers advantages when responding to a crisis, as this can provide nuclear organizations within an important level of flexibility and autonomy to modify security arrangements at sites to meet changing operational requirements.
They also advocate an increased focus on security culture during a crisis, given the rapid changes operations and the uncertainty this generates within a workforce. With the rapid move to home working precipitated by the COVID-19 pandemic, there was therefore a need to raise awareness of potential security risks in relation to remote information management and digital communications, while also maintaining staff morale through developing new approaches to protect the wellbeing of staff.
Professor Christopher Hobbs, Director of King's Institute for Applied Security Studies (KIASS) and one of the authors of the study said:
'This research, provides new insights into how nuclear security has been implemented at the operational level, following the on-set of Covid-19.
It is clear that the pandemic has both presented challenges to the delivery of nuclear security and opportunities for organizations to advance a range of alternative security solutions. Here it is essential that innovation is balanced with pragmatism and the consideration of broader risks.'

Dirty bomb efforts and uranium seizure in Ukraine may be less than meets the eye

By Artur Saradzhyan
Source: https://www.belfercenter.org/publication/dirty-bomb-efforts-and-uranium-seizure-ukraine-may-be-less-meets-eye

August 2015 – Ukraine-based journalist Maxim Tucker has just published two articles to claim that pro-Russian rebels in Eastern Ukraine are plotting to manufacture a dirty bomb with the help of Russian scientists, using radioactive waste from a storage facility at the Donetsk Chemical Factory. The journalist has published two versions of the story, in *The Times of London* and *Newsweek*. Meanwhile, in an apparently unrelated incident, Ukrainian authorities have arrested four men for attempting to smuggle what reports suggest was natural uranium.
There are four key elements to this story, with varying degrees of evidence for each. **First**, Tucker reports that there is an old bunker storing radioactive materials in areas controlled by the Donetsk separatists. That is clearly correct, and has been reported on multiple occasions before. Leaders of the Donbass separatists have confirmed its existence, report that OSCE monitors have visited the storage to measure radiation, and have offered to allow OSCE monitors to return.
Second, there is the claim that the bunker has been opened and material removed. This seems more doubtful, given the separatists' denial and willingness to have OSCE monitors check.
The **third** element is the idea that the separatists are working with Russian scientists to do something with the radioactive materials. Tucker describes a Ukrainian "security dossier" which contains what are said to be documents from the separatists ordering certain people to escort Russian specialists to the bunker this past July. Another part of the order reportedly directs the rebel Ministry of Emergency Situations to evacuate a "two-mile zone" around the site and help transport the materials away. Given the strong Ukrainian incentives to release information unflattering to Russia, this seems somewhat suspect. It's also not specified what the purpose of the Russian specialists' visit is: from the information provided, it could easily be to improve the safety or security of the waste site and remove particularly dangerous materials.
The **fourth** and most frightening element of the story is the claim that the rebels are using some of the materials stored at the Donetsk facility to build a radiological weapon. This seems highly unlikely, for several reasons. First, the only source for this claim in the ostensible Ukrainian security dossier seems to be a single conversation, described as "vodka-soaked," between an undercover Ukrainian agent and a rebel, in which the rebel claimed that the commander of this unit, Mikhail Tolstykh (nome de guerre: Givi) has boasted to his comrades-in-arms that the self-proclaimed Donetsk People's Republic (DNR) "would soon have an atomic weapon." Tostykh is widely known as a big talker and a loose cannon, and both the rebel talking to the agent and Tolstykh have every reason to exaggerate the military power of the rebels. The entire story comes from the Ukrainian government, which has been accused of doctoring evidence to back their claims on Eastern Ukraine in the past. (Remarkably, the Ukrainian defense minister has even claimed that Russia has already used tactical nuclear weapons in Luhansk.) Finally, it's difficult to see how detonation of a dirty bomb would give the rebels any significant advantage. They would have the same problems operating in the contaminated area as Ukrainian tropps would, so it seems unlikely they would use such a weapon on the front lines. It could be used to spread panic within Ukraine, but that would generate a lot of bad

publicity for the rebels, who are already under fire over allegations of their involvement in the downing of the Malaysian airliner last year, reinforcing Kiev's narrative that they are 'terrorists.' More information will be needed before any definite conclusions can be drawn about what is going on with the radioactive materials stored in Ukraine.
Meanwhile, on August 5, the Ukrainian Security Service announced that it had arrested four men it had caught "red-handed" attempting to **smuggle nuclear material "most likely to be uranium-238."** Natural uranium, when mined, is more than 99 percent U-238. U-238 cannot support the nuclear chain reaction needed for a nuclear bomb, and is not radioactive enough to be very useful for a dirty bomb. Nor is it an especially precious commodity: the price of natural uranium oxide on international markets is currently in the range of $40 a pound. These initial reports suggest this was another in a long string of small-time hustlers and smugglers attempting to make money from nuclear material they did not understand very well.

EDITOR'S COMMENT: This could have been a prophetic article that might materialize anytime today (if accurate).

Feb 26, 2022 – The assumption that Ukraine is preparing to drop a "dirty bomb" on the territory of the Russian Federation is a sick fake, Ukraine does not have nuclear weapons, does not carry out any work on their creation or acquisition, Ukrainian Foreign Minister Dmytro Kuleba said. "Russian propaganda has gone off the rails and speculates Ukraine might be preparing to drop a 'dirty bomb' on the Russian territory. **This is a sick fake.** Ukraine doesn't have nuclear weapons, doesn't conduct any work to create/acquire them. We are a responsible member of the NPT," Kuleba wrote on Twitter on Saturday.

Video: How Far Away Would You Need to Be to Survive a Nuclear Blast?

Source: https://www.sciencealert.com/video-explains-how-far-away-would-you-need-to-be-to-survive-a-nuclear-blast

Blast radius of a bomb targeting NYC's Central Park. (AsapSCIENCE/Facebook)

Feb 28 – It's been nearly 80 years since two nuclear bombs were detonated over the Japanese cities of Hiroshima and Nagasaki, killing at least 129,000 people, and causing devastating, long-term health effects.
To date, those are the only instances of nuclear weapons being used for warfare, but the reality is there are roughly 12,700 warheads remaining in the world today. So, what would happen if nuclear war broke out tomorrow?
Don't panic – this is just a hypothetical. But in the video below, the team from AsapSCIENCE breaks down the science of nuclear bombs to predict how likely you'd be to survive. Let's just say, in the case of a nuclear blast, you would want to be wearing white.
First, let's get this out of the way – there is no clear-cut way to estimate the impact of a single nuclear bomb, because it depends on many factors, including the weather on the day it's dropped, the time of day it's detonated, the geographical layout of where it hits, and whether it explodes on the ground or in the air.
But, generally speaking, there are some predictable stages of a nuclear bomb blast that can affect the likelihood of your survival. (You can also explore this chilling interactive to find out how a nuclear blast would spread through the area where you live.)

As the video above explains, approximately 35 percent of the energy of a nuclear blast is released in the form of thermal radiation. Since thermal radiation travels at approximately the speed of light, the first thing that will hit you is a flash of blinding light and heat. The light itself is enough to cause something called flash blindness – a usually temporary form of vision loss that can last a few minutes.

The AsapSCIENCE video considers a 1 megaton bomb, which is 80 times larger than the bomb detonated over Hiroshima, but much smaller than many modern nuclear weapons. For a bomb that size, people up to 21 km (13 miles) away would experience flash blindness on a clear day, and people up to 85 km (52.8 miles) away would be temporarily blinded on a clear night. Heat is an issue for those closer to the blast. Mild, first-degree burns can occur up to 11 km (6.8 miles) away, and third-degree burns – the kind that destroy and blister skin tissue – could affect anyone up to 8 km (5 miles) away. Third-degree burns that cover more than 24 percent of the body would likely be fatal if people don't receive medical care immediately.

Those distances are variable, depending not just on the weather, but also on what you're wearing – white clothes can reflect some of the energy of a blast, while darker clothes will absorb it.

That's unlikely to make much difference for those unfortunate enough to be at the center of the explosion, though.

The temperatures near the site of the bomb blast during the Hiroshima explosion were estimated to be 300,000 degrees Celsius (540,000 degrees Fahrenheit) – which is roughly 300 times hotter than the temperature bodies are cremated at, so humans were almost instantly reduced to the most basic elements, like carbon.

But for those slightly farther away from the center of the blast, there are other effects to consider aside from heat. The blast of a nuclear explosion also drives air away from the site of the explosion, creating sudden changes in air pressure that can crush objects and knock down buildings.

Within a 6-km (3.7-mile) radius of a 1-megaton bomb, blast waves would produce 180 metric tons of force on the walls of all two-story buildings, and wind speeds of 255 km/h (158 mph). In a 1-km (0.6-mile) radius, the peak pressure is four times that amount, and wind speeds can reach 756 km/h (470 mph).

Technically, humans can withstand that much pressure, but most people would be killed by falling buildings.

If you somehow survive all of that, there's still the radiation poisoning to deal with – and the nuclear fallout. AsapSCIENCE touches on this in the video above, but the ongoing effects on the planet are longer-lasting than you might expect.

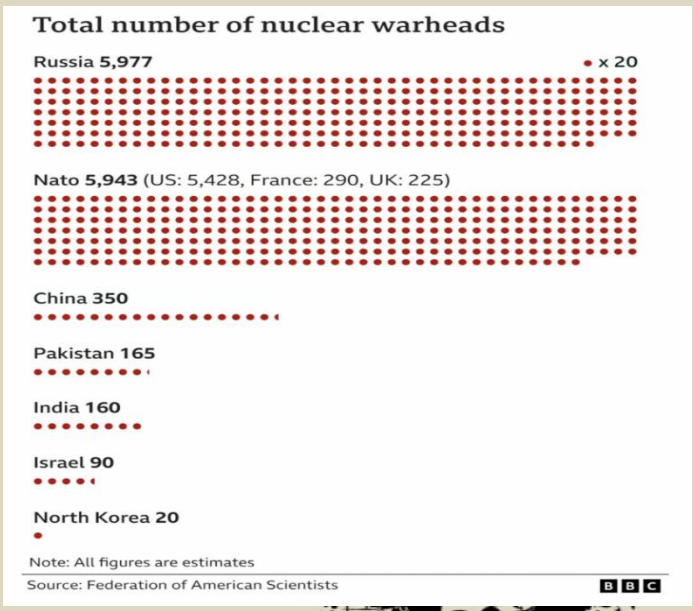
For example, a simulation study published in 2019 found that a nuclear war between the United States and Russia would plunge Earth into a nuclear winter within days, due to the levels of smoke and soot released into the atmosphere.

We also know that radioactive particles can travel remarkably far; a recent study found that remnants of radioactive carbon from Cold War nuclear bomb tests have been found all the way down in the Mariana Trench, the deepest point of the world's oceans.

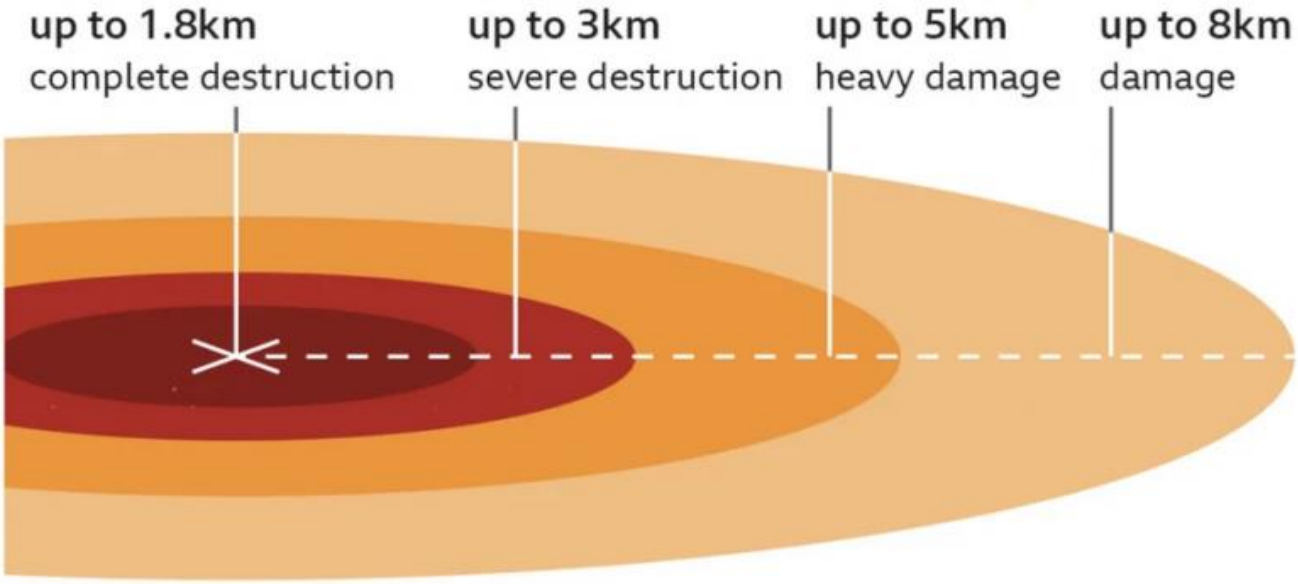
Again, all of this is hypothetical – there are international treaties in place to stop the spread and use of nuclear weapons, so we hope you never need to know any of this information for real.

However, to find out more about the current state of nuclear weaponry in the world, including the scale of the bombs, you can visit the Nuclear Notebook at the Bulletin of the Atomic Scientists.

Ukraine war nukes



Damage zones from 100kT nuclear weapon



Fireball
Destroys buildings, objects and people

Blast wave
Death, injury and damage to buildings

Radiation
Damage to body's cells can lead to radiation sickness

Electromagnetic pulse
Damages electronics several kilometers from detonation

Fallout
Radioactive dust and debris falling to ground about 15 minutes after blast can cause sickness

Source: SGR, Fema

BBC

Russian military surrounds Europe's largest nuclear power plant as Ukrainians' block access roads

By Jessica McKenzie

Source: https://thebulletin.org/2022/03/russian-military-surrounds-europes-largest-nuclear-power-plant-as-ukrainians-block-access-roads/

Ukrainians block the access road to Zaporizhzhya Nuclear Power Plant, the largest in Europe. (Photo: Ministry of Internal Affairs of Ukraine)

Mar 02 – Russian military forces have taken control of the territory around the Zaporizhzhia Nuclear Power Plant in Ukraine, which contains six of country's 15 nuclear reactors, heightening concerns that the safety of the plant and its workers could be at risk.

"The situation in Ukraine is unprecedented and I continue to be gravely concerned," the director general of the International Atomic Energy Agency (IAEA), Rafael Mariano Grossi, told the organization in an emergency meeting on Wednesday. "It is the first time a military conflict is happening amidst the facilities of a large, established nuclear power program."

"The safety and security of nuclear facilities, and nuclear and other radioactive material, in Ukraine must under no circumstances be endangered," Grossi told the organization's board of governors. "I have called for restraint from all measures or actions that could jeopardize the security of nuclear and other radioactive material, and the safe operation of any nuclear facilities in Ukraine."

Grossi also reminded the 173 member states of the IAEA, including Russia and Ukraine, that in 2009 they unanimously affirmed that "any armed attack on and threat against nuclear

facilities devoted to peaceful purposes constitutes a violation of the principles of the United Nations Charter, international law and the Statute of the Agency."

Russia informed the IAEA that it was in control of the region around Zaporizhzhia Nuclear Power Plant in a letter dated March 1. That same day, the State Nuclear Regulatory Inspectorate of Ukraine (SNRIU) asked IAEA to provide assistance in maintaining the safety and security of the Chernobyl disaster site, which was captured by Russian forces last week, and other nuclear facilities. As of Tuesday, the SNRIU said all nuclear power facilities remained under control.

Speaking to the press on Wednesday, Grossi clarified that Russia is in control of the area around the Zaporizhzhia Nuclear Power Plant and its general environs but has not taken control of the plant itself. "They have the physical control of the perimeter, including the village where most of the employees live," he said.

Social media footage verified by CNN shows Ukrainian civilians and power plant workers blocking the access roads to the plant to prevent the Russian military from entering.

Nuclear power plants have not been designed to sustain the kind of damage that wars can inflict on people and infrastructure, Edwin Lyman, an expert on nuclear proliferation and nuclear terrorism, told the Bulletin. "In peacetime," Lyman said, "the most severe threats are severe weather."

The most significant risk is that damage from munitions could prevent the plant from maintaining cooling of the highly radioactive fuel in the core or of the spent fuel. This could also happen if the plant loses access to the grid and the back-up generators fail or the plant is otherwise unable to continue delivering power to the cooling system.

"That's the situation they faced at Fukushima, in Japan, in 2011, where the plant lost both off-site and on-site power," Lyman said. "In that case, there were very few means the operators had to try to keep the fuel from melting down, and the result was three core meltdowns. So it is critical that you keep cooling, however you can."

Each nuclear reactor at Zaporizhzhia has three backup generators and seven days' worth of diesel fuel to keep them running, Lyman said. In the wake of the Fukushima disaster, many nuclear power plant facilities around the globe, including in Ukraine, added measures to prevent disasters like Fukushima from happening. "Those measures could potentially be brought to bear in a crisis at one of Ukraine's plants, but then that additional equipment is only as good as it's protected," Lyman added. "It's only good if it's available."

The other risk at Ukraine's nuclear facilities, active or not, is of human error. The people responsible for maintaining the safety and security of the facilities are working long hours under tense and dangerous conditions. Valentin Geiko, the head of the shift at Chernobyl, celebrated his 60th birthday on March 2, after working nonstop for six consecutive days to maintain the Russian-occupied plant. "He can't hand over his shift and can't leave his post," SNRIU said.

"That's the other issue is the plant personnel," Lyman said. "If the enemy controls the plant and all the access points, are the personnel who were not on duty, are they going to report to work? And if not, then you have the shifts that are there now, they ordinarily will not have to work, nonstop, and can't work nonstop."

In theory, these facilities were designed by the Soviet Union, so Russia probably could bring in its own personnel to run them, but that just adds another wrinkle, Lyman said.
Grossi has called for nothing to prevent nuclear facilities workers from doing their jobs. "In this context, it is also imperative to ensure that the brave people who operate, regulate, inspect and assess the nuclear facilities in Ukraine can continue to do their indispensable jobs safely, unimpeded and without undue pressure," he told his IAEA colleagues Wednesday. "I want to emphasize there is nothing normal about the circumstances under which the professionals at Ukraine's four nuclear power plants are managing to keep the reactors that produce half of Ukraine's electricity working."

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.

UN atomic watchdog: Iran further raising nuclear stockpile

Source: https://www.ivpressonline.com/news/world/un-atomic-watchdog-iran-further-raising-nuclear-stockpile/article_934902b6-c957-5a7f-b57c-9dd7c6267214.html

Activity at Imam Khomeini Spaceport (Semnan Province, Iran) | Feb 27, 2022 (Maxar Technologies sat photo)

Mar 03 — The United Nations' atomic watchdog said Thursday that it believes Iran has significantly increased its stockpile of highly enriched uranium in breach of a 2015 accord with world powers.

The International Atomic Energy Agency told member nations in its confidential quarterly report that Iran has an estimated 33.2 kilograms (73.1 pounds) of uranium enriched to up to 60% fissile purity, an increase of 15.5 kilograms since November.

Such highly enriched uranium can be easily refined to make atomic weapons, which is why world powers have sought to contain Tehran's nuclear program. The 33.2-kilogram figure brings Iran closer to having enough weapons-grade uranium to produce a nuclear weapon.

In a report to member states about its work in Iran seen by The Associated Press, IAEA estimated that as of Feb. 19, Iran's stockpile of **all enriched uranium was 3197.1 kilograms**, an increase of 707.4 kilograms.

The Vienna-based agency said it was unable to verify the exact size of Iran's stockpile of enriched uranium due to limitations Tehran imposed on U.N. inspectors last year. IAEA's monitoring and verification activities in Iran continue to be "seriously affected" by Iran's decision to stop letting inspectors access the agency's monitoring equipment, the report states.

Senior diplomats from Britain, China, France, Germany, and Russia have been meeting with Iranian officials in Vienna since November to discuss bringing Tehran back into compliance with the 2015 Joint Comprehensive Plan of Action. The pact eased sanctions on Iran in return for curbs on its nuclear program.

The United States pulled out of the accord under former President Donald Trump and reimposed sanctions on Iran, prompting Tehran to resume its uranium enrichment.

The IAEA announced earlier Thursday that Director General Rafael Mariano Grossi would travel to Tehran for meetings with senior Iranian officials on Saturday.

Asked to characterize the cooperation with Iranian officials and whether there had been any progress, Grossi said at a Wednesday press conference in Vienna, "We are working very hard."

EDITOR'S COMMENT: It will come a day when Iran will say "*Hei! We have two bombs*!" It has been done before and history repeats itself!

Potassium Iodide (KI)

Source: https://www.cdc.gov/nceh/radiation/emergencies/ki.htm

KI (potassium iodide) is a salt of stable (not radioactive) iodine that can help block radioactive iodine from being absorbed by the thyroid gland, thus protecting this gland from radiation injury.

The thyroid gland is the part of the body that is most sensitive to radioactive iodine.

People should take KI (potassium iodide) only on the advice of public health or emergency management officials. There are health risks associated with taking KI.

KI (potassium iodide) does not keep radioactive iodine from entering the body and cannot reverse the health effects caused by radioactive iodine once the thyroid is damaged.

- KI (potassium iodide) only protects the thyroid, not other parts of the body, from radioactive iodine.

KI (potassium iodide) cannot protect the body from radioactive elements other than radioactive iodine—if radioactive iodine is not present, taking KI is not protective and could cause harm.

Table salt and foods rich in iodine do not contain enough iodine to block radioactive iodine from getting into your thyroid gland. **Do not use table salt or food as a substitute for KI.**

Do not use dietary supplements that contain iodine in the place of KI (potassium iodide). They can be harmful and non-efficacious. Only use products that have been approved by the U.S. Food and Drug Administration (FDA).

How does KI (potassium iodide) work?

The thyroid gland cannot tell the difference between stable and radioactive iodine. It will absorb both.

KI (potassium iodide) blocks radioactive iodine from entering the thyroid. When a person takes KI, the stable iodine in the medicine gets absorbed by the thyroid. Because KI contains so much stable iodine, the thyroid gland becomes "full" and cannot absorb any more iodine—either stable or radioactive—for the next 24 hours.

KI (potassium iodide) may not give a person 100% protection against radioactive iodine. Protection will increase depending on three factors.

- **Time after contamination:** The sooner a person takes KI, the more time the thyroid will have to "fill up" with stable iodine.

- **Absorption:** The amount of stable iodine that gets to the thyroid depends on how fast KI is absorbed into the blood.
- **Dose of radioactive iodine:** Minimizing the total amount of radioactive iodine a person is exposed to will lower the amount of harmful radioactive iodine the thyroid can absorb.

Who can take KI (potassium iodide)?

The thyroid glands of a fetus and of an infant are most at risk of injury from radioactive iodine. Young children and people with low amounts of iodine in their thyroid are also at risk of thyroid injury.

Infants (including breast-fed infants)

Infants have the highest risk of getting thyroid cancer after being exposed to radioactive iodine. All infants, including breast-fed infants, need to be given the dosage of KI (potassium iodide) recommended for infants.

- Infants (particularly newborns) should receive a single dose of KI. More than a single dose may lead to later problems with normal development. Other protective measures should be used.
- In cases where more than one dose is necessary, medical follow-up may be necessary.

Children

The U.S. Food and Drug Administration (FDA) recommends that all children internally contaminated with (or likely to be internally contaminated with) radioactive iodine take KI (potassium iodide) unless they have known allergies to iodine (contraindications).

Young Adults

The FDA recommends that young adults (between the ages of 18 and 40 years) internally contaminated with (or likely to be internally contaminated with) radioactive iodine take the recommended dose of KI (potassium iodide). Young adults are less sensitive to the effects of radioactive iodine than are children.

Pregnant Women

Because all forms of iodine cross the placenta, pregnant women should take KI (potassium iodide) to protect the growing fetus. Pregnant women should take only one dose of KI following internal contamination with (or likely internal contamination with) radioactive iodine.

Breastfeeding Women

Women who are breastfeeding should take only one dose of KI (potassium iodide) if they have been internally contaminated with (or are likely to be internally contaminated with) radioactive iodine. They should be prioritized to receive other protective action measures.

Adults

Adults older than 40 years should not take KI (potassium iodide) unless public health or emergency management officials say that contamination with a very large dose of radioactive iodine is expected.

- Adults older than 40 years have the lowest chance of developing thyroid cancer or thyroid injury after contamination with radioactive iodine.
- Adults older than 40 are more likely to have allergic reactions to or adverse effects from KI.

How is KI (potassium iodide) given?

The FDA has approved two different forms of KI (potassium iodide), tablets and liquid, that people can take by mouth after a radiation emergency involving radioactive iodine.

Tablets come in two strengths, 130 milligram (mg) and 65 mg. The tablets have lines on them so that they may be cut into smaller pieces for lower doses.

For the oral liquid solution, each milliliter (mL) contains 65 mg of KI (potassium iodide).

According to the FDA, the following doses are appropriate to take after internal contamination with (or likely internal contamination with) radioactive iodine:

- Newborns from birth to 1 month of age should be given 16 mg (¼ of a 65 mg tablet or ¼ mL of solution). This dose is for both nursing and non-nursing newborn infants.
- Infants and children between 1 month and 3 years of age should take 32 mg (½ of a 65 mg tablet OR ½ mL of solution). This dose is for both nursing and non-nursing infants and children.
- Children between 3 and 18 years of age should take 65 mg (one 65 mg tablet OR 1 mL of solution). Children who are adult size (greater than or equal to 150 pounds) should take the full adult dose, regardless of their age.
- Adults should take 130 mg (one 130 mg tablet OR two 65 mg tablets OR two mL of solution).

- Women who are breastfeeding should take the adult dose of 130 mg.

Age Group	KI Dosage	Number of 130mg Tablets	Number of 65mg Tablets
Adults and Adolescents* (Over 150 lbs.)	130mg	1 tablet	2 tablets
Children 3-18 yrs (Under 150 lbs.)**	65mg	½ tablet	1 tablet
Infants (1 month – 3 yrs)**	32mg	¼ tablet Liquid form preferred	½ tablet
Infants (Birth – 1 month)	16mg	⅛ tablet Liquid form preferred	¼ tablet Liquid form preferred

* Adolescents approaching adult size (150 pounds) should receive the adult dose (130mg).
** KI tablets may be crushed to form a powder. Powdered KI or liquid KI may be mixed in milk, water, formula, or soft foods.
Source

How often should KI (potassium iodide) be taken?
Taking a stronger dose of KI (potassium iodide), or taking KI more often than recommended, does not offer more protection and can cause severe illness or death.
A single dose of KI (potassium iodide) protects the thyroid gland for 24 hours. A one-time dose at recommended levels is usually all that is needed to protect the thyroid gland.
In some cases, people can be exposed to radioactive iodine for more than 24 hours. If that happens, public health or emergency management officials may tell you to take one dose of KI (potassium iodide) every 24 hours for a few days.
Avoid repeat dosing with KI (potassium iodide) for pregnant and breastfeeding women and newborn infants.

What are the side effects of KI (potassium iodide)?
Side effects of KI (potassium iodide) may include stomach or gastro-intestinal upset, allergic reactions, rashes, and inflammation of the salivary glands.
When taken as recommended, KI (potassium iodide) can cause rare adverse health effects related to the thyroid gland.
These rare adverse effects are more likely if a person:

- Takes a higher than recommended dose of KI
- Takes the drug for several days
- Has a pre-existing thyroid disease.

Newborn infants (less than 1 month old) who receive more than one dose of KI (potassium iodide) are at risk for developing a condition known as hypothyroidism (thyroid hormone levels that are too low). If not treated, hypothyroidism can cause brain damage.

- Infants who receive more than a single dose of KI should have their thyroid hormone levels checked and monitored by a doctor.
- **Avoid repeat dosing of KI to newborns.**

Will Putin Use Nuclear Weapons?

By Rod Lyon

Source: https://www.homelandsecuritynewswire.com/dr20220304-will-putin-use-nuclear-weapons

Mar 04 – It's still early days in the Russian invasion of Ukraine, but so far nuclear issues have enjoyed a much higher profile than might have been expected. A strategic missile exercise formed part of the lead-up to the invasion. And when first launching the military operation last Thursday, Putin warned darkly that any country that stood in Russia's way would suffer 'consequences that you have never encountered in your history'.

Since then, we've had statements that allege the invasion was motivated in part by a concern that Ukraine was a proliferation threat. We've had a Russian spokesman say that the reason Chernobyl was seized so early in the campaign was to deny Ukraine the option of making a 'dirty' bomb. And we've had voters in Belarus—in a disputed referendum—renounce the anti-nuclear clause in its constitution, opening up the possible deployment of Russian nuclear weapons there.

Perhaps most worryingly, on Sunday Putin instructed his defense minister and chief of the general staff to raise the alert level of Russian deterrence forces by putting them on a 'special regime of combat duty'. It's not clear what he meant. US defense officials observed that this was not a term of operational art with which they were familiar and stated that they had seen no subsequent 'muscle movement' in the status of the Russian nuclear arsenal.

The Russian ministry of defense confirmed on Monday that its nuclear missile forces and the Northern and Pacific fleets had been placed on 'enhanced' combat duty. Some reports spoke of Russia boosting staff at its nuclear sites—which might mean that all leave has been cancelled.

All of this has made for a hectic time in the world of nuclear strategists. Nuclear signaling is woven through the invasion of Ukraine in a way we haven't seen since the days of the Cuban missile crisis. Naturally, it has fed a wave of speculation on social media about the potential crossing of the nuclear threshold, either deliberately or inadvertently.

In early June 2020, Russia published an official outline of the principles underpinning Russian nuclear deterrence. (The online English translation seems currently inaccessible, perhaps as a result of the attack by the group called Anonymous against Russian governmental internet sites, but a quick summary can be found here.) **The document lists four instances in which Russia might resort to use of nuclear weapons:**

- ✓ in response to the use of nuclear and other types of weapons of mass destruction against it and/or its allies
- ✓ in the event of aggression against the Russian Federation with the use of conventional weapons when the very existence of the state is in jeopardy
- ✓ when there is reliable data on a launch of ballistic missiles attacking the territory of the Russian Federation and/or its allies
- ✓ in the event of an attack by an adversary against critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces' response options.

Some of Putin's comments suggest an effort to make out a case under the second of those provisions. That's a stretch. The transfer to Ukraine of lethal conventional military equipment from NATO members and other countries, at a time when a daunting array of sanctions are hitting the regime and its supporters, certainly isn't seen in Washington, European capitals, or Canberra, as 'aggression' jeopardizing the 'very existence' of the Russian state. True, some commentators do see those actions as jeopardizing the future of Putin's regime, but most see them simply as incentives for Moscow to change course in relation to its intended subjugation of Ukraine.

Still, Putin's behavior has been more than a little odd lately—including his apparent fascination with long-distance seating arrangements. Driven by a long list of perceived grievances, a burning ambition to recreate Greater Russia, and wounded pride, Putin might well see his own role in more sweeping historical terms.

That means, of course, that escalation is still more likely than de-escalation. Might that escalation involve nuclear weapons? Yes. But, from the Cold War days, Western intelligence probably still has available to it a good-sized list of warning indicators for imminent nuclear use. I don't think we're close to that.

And remember that Putin has a range of other, more likely, options. Those include a more vigorous prosecution of his current strategy—the toppling of the current government in Kiev, the installation of a more compliant regime in its place, and the gradual incorporation of Ukraine back under Moscow's control. Easier said than done, certainly, but Moscow has form in that regard. He might also choose to strike—with conventional weapons—at the supply lines through which military equipment is finding its way into Ukraine. Or he might have in mind a more distant target set, again without necessarily resorting to nuclear weapons.

Strategic deterrence today doesn't turn merely upon the old division of weapons into the conventional and the nuclear. Conflict has become multi-domain. Long-range precision-strike conventional weapons, options in the cyber realm, and space and counterspace weaponry are all possibilities.

In short, nuclear weapons have so far played a larger role in the crisis than expected—but there are still many paths forward.

Rod Lyon is a senior fellow at *ASPI.*

The Dangers Following Russia's Attack on the Zaporizhzhia Nuclear Power Plant

By Ross Peel

Source: https://www.homelandsecuritynewswire.com/dr20220304-the-dangers-following-russia-s-attack-on-the-zaporizhzhia-nuclear-power-plant

Mar 04 – Following recent news of Russian shelling of Zaporizhzhia nuclear power plant in southern Ukraine, which is the largest in Europe, there is great concern over the potential for a Chernobyl-esque release of radioactive material. Several security personnel at the plant were injured by the attack.

With six large nuclear power reactors, there is a significant quantity of nuclear material at the site. While these are not the same type of reactor as those at the Chernobyl plant, and are of a much safer design, this does not make them any less vulnerable to weapons of war.

The building which suffered the attack and ensuing fire was located approximately 500 metres from the block of six reactors. It contained no nuclear material, as it was used solely for training and administration purposes. No increase in radiation levels has been detected.

While Ukrainian staff remain in control of the reactors, Russian forces have effectively taken control of the wider power plant. From CCTV footage, this does not seem to have been an accidental strike, but a deliberate attack. The Russian forces are sending a message – they can attack the plant at any time, but for the moment are choosing not to do so. The fire may have been quickly extinguished, but the threat of what could come next looms larger than ever.

The situation is almost unprecedented. Nuclear materials have previously fallen under threat of attack during times of armed conflict, as they did during Israel's bombing of a secret Syrian reactor. However, as the Syrian reactor was still under construction at the time and nuclear fuel had yet to be loaded, we are effectively in uncharted waters.

This is a threat that I myself, only a few days ago, thought highly unlikely. To attack a nuclear power plant, especially one so close to one's own territory, is a highly risky strategy. The negative consequences are likely to far outweigh any potential benefits. However, experts such as myself have consistently been proved wrong when assessing what Vladimir Putin will and will not do.

At the time of the attack, only one of the six reactors was operating: Unit 4 at 60% power. All other units were either already shut down for maintenance or in a low-power standby state. The plant is thus continuing to operate as normal to some extent, albeit in the most abnormal of circumstances.

Keeping the Site Safe

Unfortunately, Ukraine's nuclear power plants remain at risk. Even shutting down a nuclear reactor does not immediately render it safe. Once nuclear fuel has been placed into a reactor, it will continue to generate its own heat long after shutdown. Older reactors, such as those in Ukraine, require active measures to maintain the fuel in a safe state. Water must be circulated in storage pools and the reactor even after shutdown, which means a source of electricity is required, as well as staff to monitor and manage the plant.

While the power required for this can be provided by Unit 4, trained operators will still require ready access to the site to assure this, and access to cooling water taken from the Dnieper River. Without this cooling, a range of accident scenarios can occur, from a nuclear fuel meltdown to a reactor core explosion.

If Unit 4 were to be shut down, the required electricity would have to be brought in from off site. However, in the current situation, off-site power may not be reliable, or even available. Furthermore, once a nuclear plant is shut down, it cannot be restarted for several days. As such, shutting down the plant would make it dependent on a potentially unreliable source of power to maintain safety functions. This being the case, keeping Unit 4 operational in a low power state may be the best course of action.

Any attack on a nuclear facility is a major breach of international norms. However, the attack could have been much worse. In the extreme, a breach of a fuelled and operating reactor could be disastrous, releasing vast quantities of hazardous nuclear material into the air. This plume of material could be blown over a large area by wind, contaminating vast areas of land and water supplies. Such a scenario is not limited to a nuclear reactor either. If a used fuel storage pool were to be damaged and the fuel could not be cooled, a similar scenario could result, albeit at a smaller scale.

The above is, however, an unlikely worst case scenario. If Russia's decision to target an administrative building was indeed deliberate, we can hope that this means they will not target the reactors. It seems likely, at least currently, that the planners of Russia's "special military operation" will seek to capture the plant as a piece of critical national infrastructure.

However, should the conflict continue to drag on past Moscow's original expectation of three to four days, more extreme measures may be taken.
In a press conference on the morning after the attack, the International Atomic Energy Agency's Director General, Rafael Mariano Grossi, stated that the agency would not idly monitor the situation from Vienna. Grossi expressed an intention to travel for talks with both Ukraine and Russia. We must hope that he can reach an agreement that will minimise further danger to the power plant and allow Ukraine's nuclear reactors to operate safely until the crisis can be resolved.

Ross Peel is Research and Knowledge Transfer Manager, King's College London.

It is feasible, but is it ethical for a nation invaded by another nation to use radiological dispersal devices as an area denial weapon to counter a mightier opponent?

Editor's question

Ukraine Making Nuclear "Dirty Bomb" In Chernobyl, Alleges Russia

Source: https://www.ndtv.com/world-news/russia-without-evidence-says-ukraine-making-nuclear-dirty-bomb-2806345

Mar 06 – Russian media cited an unnamed source on Sunday as saying that Ukraine was close to building a plutonium-based "dirty bomb" nuclear weapon, although the source cited no evidence.
Russian President Vladimir Putin ordered an invasion of Ukraine on February 24, with the aim to "demilitarise" and "denazify" its pro-Western neighbor and prevent Kyiv from joining NATO.
The West, dismissing that rationale as a pretext, has responded with harsh sanctions on Moscow and heavy military and other aid to Kyiv.
The TASS, RIA and Interfax news agencies quoted "a representative of a competent body" in Russia on Sunday as saying Ukraine was developing nuclear weapons at the destroyed Chernobyl nuclear power plant that was shut down in 2000.
Ukraine's government has said it had no plans to rejoin the nuclear club, having given up its nuclear arms in 1994 following the break-up of the Soviet Union.
Shortly before the invasion, Putin said in a grievance-filled speech that Ukraine was using Soviet know-how to create its own nuclear weapons, and that this was tantamount to preparation for an attack on Russia. He cited no evidence for his claim.

List of crossings of the Dnieper River in Ukraine

By the Editor

This is a list of all current crossings of the Dnieper River which begins at the Dnieper River's crossing a Belarus-Ukraine border and extends to its river delta near the Dnieper Estuary at Kherson.

- Upper stream (Chernihiv, Kyiv oblasts and Kyiv city): 19
- Mid-stream (Cherkasy, Kirovohrad, Poltava and Dnipropetrovsk oblasts): 13
- Lower stream (Zaporizhia and Kherson oblasts): 11

All these crossings are ideal for radiological area denial that will significantly slow the Russian military advance.

Ukrainian military to blow up experimental nuclear reactor at Kharkov Institute - ministry

Source: https://tass.com/defense/1418059

Mar 07 – The Ukrainian Security Forces and the nationalist Azov battalion are planning to blow up a reactor at the National Research Center of the Kharkov Institute of Physics and Technology and accuse the Russian Armed Forces of launching projectiles at an experimental nuclear reactor, says Russia's Defense Ministry on Monday.

"The Security Forces of Ukraine along with the militants of the Azov battalion are plotting a provocation with possible radioactive contamination of the area near the city of Kharkov. Nationalists mined a reactor at an experimental nuclear system located at the [National Research Center of] Kharkov Institute of Physics and Technology. The Ukrainian military and the Azov battalion militants are planning to blow up the reactor and accuse the Russian Armed Forces of allegedly launching a missile strike on an experimental nuclear system," the statement says.

The Russian Defense Ministry noted that "on March 6, foreign journalists arrived in Kharkov to register the consequences of the provocation, followed by accusing Russia of creating an environmental disaster.".

EDITOR'S COMMENT: If you are a group of fanatic nationalists who do not care about the consequences to their own fellow citizens then yes, it can be done although it would be very difficult to stage the destruction as a Russian missile attack.

Ukraine: Chernobyl nuclear plant off power grid, generators running instead

Source: https://www.dw.com/en/ukraine-chernobyl-nuclear-plant-off-power-grid-generators-running-instead/a-61063591

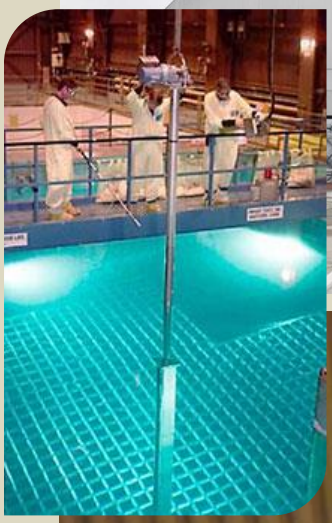
Mar 09 – The Chernobyl nuclear power plant and its security systems were shut down on Wednesday as fears began to grow that radioactive substances could be released from the site where the world's worst nuclear disaster occurred.
Ukraine's energy operator Ukrenerho said the plant "was fully disconnected from the power grid," adding that military operations meant "there is no possibility to restore the lines."
The International Atomic Energy Agency said that Ukraine had informed it of the power outage, but said that although the development "violates [a] key safety pillar," in this case it saw "no critical impact on safety."
The site is currently being powered by generators instead, with electricity needed primarily for water cooling to control the heat of spent fuel at the site.

Chernobyl Nuclear Plant Reported to Have Lost Electricity. Here's What That Means

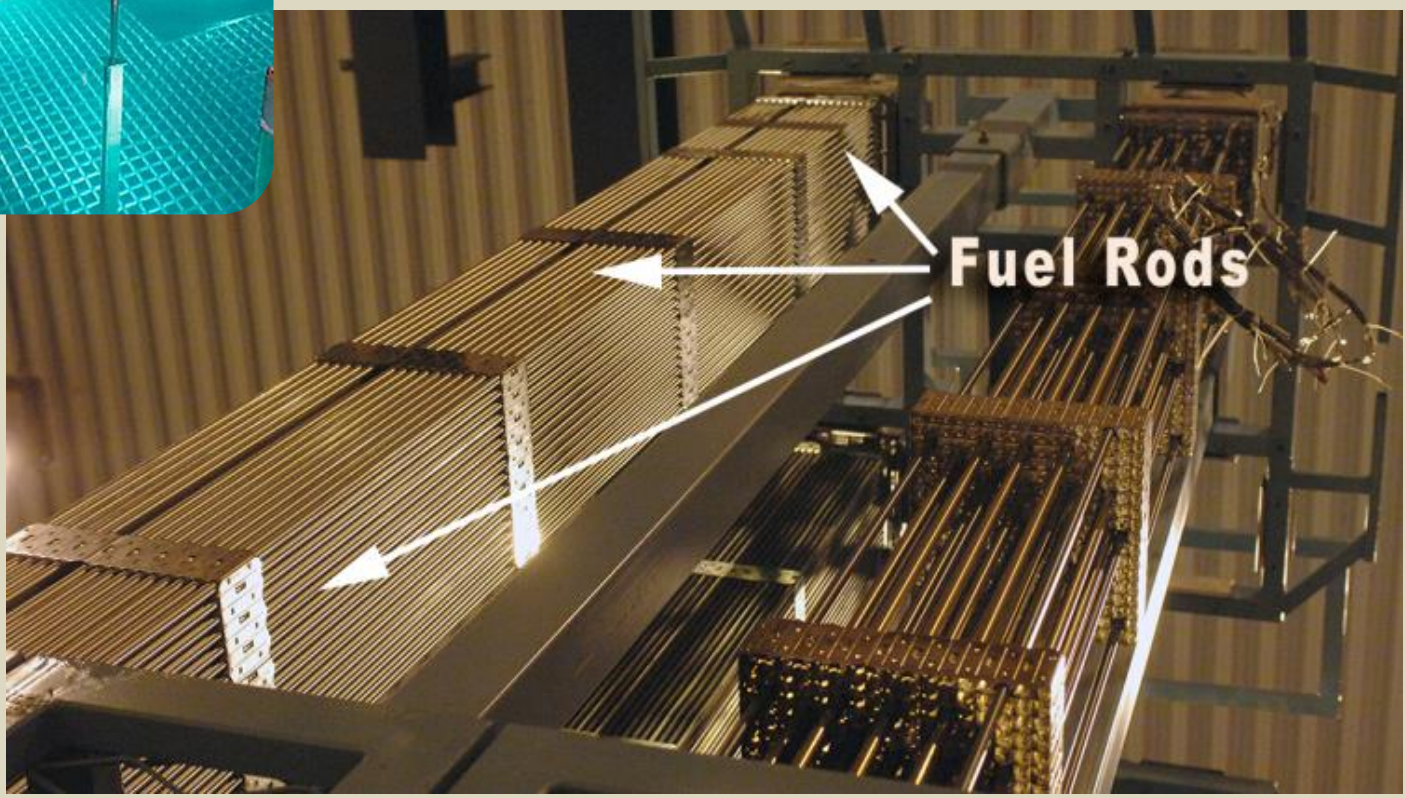
Source: https://www.sciencealert.com/chernobyl-s-nuclear-plant-is-now-without-electricity-and-officials-are-concerned

Mar 10 – Chernobyl's nuclear power plant and all the facilities in the Chernobyl exclusion zone have been completely disconnected and are now without electricity, Ukraine's state energy company has announced.
Russian forces attacked the defunct nuclear facility on the very first day of the invasion (Feb. 24), seizing it after heavy fighting and taking its roughly 210 staff hostage, Live Science previously reported. Now that the plant has been disconnected from the electrical grid, the roughly 20,000 spent nuclear fuel units held in the plant's cooling tanks will no longer receive active cooling.
Ukrainian officials have warned that this could increase the likelihood of the evaporation and discharge of nuclear material, and give a dangerous dose of radioactive material to the plant's personnel. Some nuclear energy experts, however, have cautioned that, as the **spent fuel rods are now 22 years old and much colder than they were**, this event is unlikely.

"The spent fuel rods are at minimum 22 years old. They have very little heat to dissipate," Mark Nelson, the managing director of the Radiant Energy Fund, which advises companies and nonprofits about nuclear energy, wrote on Twitter.
"Their heat is low enough that experts I've talked to expect weeks or even months to heat the water enough to dry out the pool. Even then, natural air circulation should be sufficient."
The Ukrainian State Service of Special Communications and Information Protection of Ukraine (SSSCIP) has blamed the power outage on "damage caused by the occupiers," although there has yet to be any independent verification of the cause.



Ukraines foreign minister Dmytro Kuleba said that the Chernobyl plant's reserve diesel generators had a 48-hour capacity, and called for a ceasefire to restore the electricity.
Meanwhile, officials from the UN's International Atomic Energy Agency (IAEA) have expressed increasing concern for the well-being of the staff at Chernobyl, who have been held hostage at the plant for two weeks. Workers would usually leave the radioactive plant after work hours ended but have now been forced to live at the site.



Systems set up to monitor the nuclear material at Chernobyl's radioactive waste facilities stopped transmitting data to the UN's nuclear watchdog on Tuesday (March 8).
Safeguards are the technical measures that the IAEA uses to keep track of nuclear material and ensure it doesn't fall into the wrong hands. With these offline, the agency has no way of knowing the location of the plant's nuclear material, increasing the possibility that it could fall into the wrong hands.
The IAEA said in a statement that "remote data transmission from safeguards monitoring systems installed at the Chernobyl NPP had been lost," and that while workers have "access to food and water, and medicine to a limited extent", the "situation for the staff was worsening."
Staff at the facility are responsible for decommissioning the site and ensuring the safe disposal of the radioactive material inside the plant's defunct reactors. However, since the

Russian occupation of Chernobyl, that work has been put on hold. Prior to the power outage, workers could only be contacted via email.
"I'm deeply concerned about the difficult and stressful situation facing staff at the Chernobyl nuclear power plant and the potential risks this entails for nuclear safety," IAEA Director General Rafael Grossi said in the statement.
"I call on the forces in effective control of the site to urgently facilitate the safe rotation of personnel there."
Eight of Ukraine's 15 operational nuclear reactors are still online, Ukraine's nuclear regulator said in the statement, including two at the Zaporizhzhya plant that was captured by Russian forces last week, Live Science previously reported. Staff at the Zaporizhzhya plant, which briefly caught fire after being shelled during its capture, are working in shifts.
Radiation at both Chernobyl and Zaporizhzhya has been reported to be at normal levels.
▶ **UPDATE:** Electricity problem was restored by a team of Belarus technicians (Mar 10, 2022)

Russian nuclear and biological disinformation undermines treaties on weapons of mass destruction

By Milton Leitenberg
Source: https://thebulletin.org/2022/03/russian-nuclear-and-biological-disinformation-undermines-treaties-on-weapons-of-mass-destruction/

The Lugar Center for Public Health Research in Tbilisi, Georgia, was built with US government support. Credit: Q9k2C6J3 via Wikimedia Commons.

Mar 10 – A long study published in October 2021 argued that the Russian government, through an unprecedented and extraordinary biological weapons disinformation campaign aimed primarily at the United States and secondarily at the government of Georgia, displayed an open disdain and disregard for the Biological Weapon Convention, an international treaty with 183 member states.
In March 2022, the lies regarding biological laboratories in Ukraine are deliberate and knowing. The Russian government knows with absolute certainty that none of the charges leveled at any of the facilities in Ukraine, or at the United States, are true—in the same way it knew with absolute certainty that the similar charges that it leveled for many years at Georgia's Lugar Laboratory were not true.
False allegations undermine the authority and legitimacy of international treaties such as the Biological Weapons Convention, whose purpose is to prevent the proliferation of weapons of mass destruction, in this case, biological weapons.
Similarly, the Russian government has shown its equal disdain and disregard for the Chemical Weapons Convention, an international treaty with 193 member states. The Russian government did this through its years of support for the government of Syria, its denial of the Syrian government's use of the chemical nerve agent sarin against its own citizens, and its efforts to undermine the efforts of the Organization for the Prohibition of Chemical Weapons (OPCW) to carry out investigations of the Syrian government's use of chemical munitions. It is the responsibility of the OPCW to protect the Chemical Weapon Convention and to see that it is not violated.

Now, in March 2022, as an unnecessary and superfluous accompaniment to its invasion of Ukraine, the Russian government has initiated yet another disinformation campaign, this time involving nuclear weapons and radiation munitions. Russia alleged variously that Ukraine had planned to develop and produce nuclear weapons, that Ukraine was preparing to make "dirty bombs" composed of radioactive materials to be scattered by high explosives, and that the United States may have supplied plutonium to Ukraine, from which nuclear weapons can be produced. With these false charges, the Russian government has demonstrated the same destructive disregard for the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) as it previously showed for the BWC and the CWC. The Soviet Union played an instrumental role in achieving the NPT in July 1968, a treaty that presently has 191 member states.

Perhaps, one might think, only a former KGB agent who had become a head of state would think that these scurrilous disinformation campaigns were appropriate behavior for a major world power. President Putin has, after all, turned Russia into an empire of disinformation. But Putin is not alone. In the very same week, one sees the same lies—those concerning biological weapons and the United States—becoming a staple of the statements by the spokesman of the Ministry of Foreign Affairs of China, Zhao Lijian.

In one tweet, Zhao stated: **Yes, 336 facilities have received funding support under the US Biological Threat Reduction Program.** This program was initiated in 1997 to demilitarize former Soviet biological weapon research, development, and production facilities in Russia and the newly independent states formed on dissolution of the Soviet Union and to convert them to civilian public-health facilities.[1] The program was subsequently expanded to improve the capabilities of public-health facilities in many other countries. *None* of the 336 facilities are "US … labs" and *none* are "under its control." In their joint statement on February 5, 2022, Presidents Xi Jinping and Vladimir Putin stated: "The sides emphasize that domestic and foreign bioweapons activities by the United States and its allies raise serious concerns and questions for the international community regarding their compliance with the BWC. The sides share the view that such activities pose a series threat to the national security of the Russian Federation and China and are detrimental to the security of the respective regions. The sides call on the U.S. and its allies to act in an open, transparent, and responsible manner by properly reporting on their military biological activities conducted overseas and on their national territory…The sides, reaffirming their commitment to the goal of a world free of chemical weapons, call upon all parties to the Chemical Weapons Convention to work together to uphold its credibility and effectiveness." It is of enormous significance—and perhaps unprecedented in post-Cold War diplomacy—that the heads of state of Russia and China included such false and hypocritical remarks in a major statement.

Two of the most important countries in the world have made a mockery of truth, turned disinformation into a plaything, and are undermining all three international treaties—the BWC, the CWC, and the NPT—whose purposes are to dissuade countries from obtaining weapons of mass destruction.

Notes

[1] 2020 Meeting Geneva, 22-25 November 2021, Item 6 of the provisional agenda, Consideration of the factual reports of the Meetings of Experts reflecting their deliberations, including possible outcomes. Article X Cooperation and Laboratory Support: The Example of the Biological Threat Reduction Program, Submitted by the United States of the America, 22 November 2021

Milton Leitenberg is a senior research associate at the Center for International and Security Studies at the University of Maryland (CISSM). His research is concentrated in three disparate areas of study: biological weapons; actual wars and conflicts of the past two decades and the issue of international intervention in these; and the history of nuclear weapons between the United States and Soviet Union and Russia between 1945 and 1995. CISSM published his major monograph, *Biological Weapons Arms Control,* in 1996. Since 1992, he has published over 30 papers in the area of biological weapons. Several of these papers concern the biowarfare program of the former Soviet Union, and *The Soviet Biological Weapons Program: A History* was published by Harvard University Press in 2013. Leitenberg published two other recent books on the subject of biological weapons: *The Problem of Biological Weapons* (National Defense College, Stockholm, 2004) and *Assessing the Biological Weapons and Bioterrorism Threat* (US Army War College, December 2005).

Is Putin Irrational? Nuclear Strategic Theory on How to Deter Potentially Irrational Opponents

By Edward Geist

Source: https://www.homelandsecuritynewswire.com/dr20220309-is-putin-irrational-nuclear-strategic-theory-on-how-to-deter-potentially-irrational-opponents

Mar 09 – Vladimir Putin's astonishing lapse of judgment in invading Ukraine has fueled speculation that the Russian president may have taken leave of his senses. Former Secretary of Defense and CIA director Robert Gates commented in a recent CNN interview

that Putin has "gone off the rails." Sen. Marco Rubio, the ranking Republican on the Senate Intelligence Committee, tweeted after the invasion began that, "I wish I could share more, but for now I can say it's pretty obvious to many that something is off with Putin. He has always been a killer, but his problem now is different & significant. It would be a mistake to assume this Putin would react the same way he would have 5 years ago." If these assessments are accurate, then the world faces a highly disturbing situation: a mad king in possession of the world's largest nuclear arsenal, as he reminded the world when announcing an alert of his strategic deterrent forces February 27. If Putin is not a rational adversary, then the policies that would deter a more-reasonable man may fail or even backfire. As nuclear strategists recognized decades ago, deterrence is necessary—but it isn't always sufficient. The analysts and theorists who worked on these issues were bedeviled, in particular, by the problem of nonrational opponents. As the nuclear strategist Herman Kahn put it in 1962, "We want to deter even the mad." Kahn took comfort in his conclusion that "irrationality is a matter of degree," so scaling up nuclear deterrence might still impress a "need for caution" upon irrational adversaries. Furthermore, "if the irrationality is sufficiently bizarre, the irrational decisionmaker's subordinates are likely to step in."

Theorist Patrick Morgan preferred the term "sensible" over "rational" to make it clear that an adversary doesn't have to be perfectly rational to be understood and his actions anticipated. Sensible actors may have goals that are anathema to our own, but they pursue them in ways that appear likely to attain those objectives. They also may commit human errors. But even Morgan acknowledged that not every opponent will be "sensible" enough to respect a deterrent threat. Nuclear deterrence theorists never identified a robust solution. Fortunately, during the Cold War, the problem of irrational leaders wielding nuclear weapons never became acute. But now Putin's behavior may be turning it into an immediate concern.

Critics of nuclear deterrence theory find the whole framework baseless. Real-world humans, these critics say, are almost never "rational" by the stringent definitions of economics and game theory, under which a competent leader can pursue arbitrary or bizarre goals, but appear more "rational" than one who makes errors while aiming for goals that make sense to us.

So is Putin just making mistakes, or irrational? His claim that the Ukrainian government, which is headed by a Jewish former comedian, is somehow "fascist" and "Nazi" was preposterous. His invasion appears to have been based on a completely misguided assumption that Ukrainians would welcome Russian soldiers as liberators. Even more unaccountable is how Putin seems not to have anticipated how rapidly his actions would alienate world opinion. Yet all this doesn't mean that Putin is necessarily too irrational to be convinced to change course. (Or, per Kahn, his subordinates might intervene as the situation continues to deteriorate.) At the same time, the United States and its allies must account for the possibility that even in the face of credible deterrent threats—military or economic—Putin might double down and lash out. It is a mistake to assume that a nonsensible opponent necessarily suffers from some diagnosable psychopathology. Autocratic rulers like Putin and North Korean dictator Kim Jong-un have incentives so different from those of an ordinary person as to warp their "rational" goals. They tend to conflate the continuation of their rule with their personal survival, with good reason. Perpetuating their own rule at any cost or risk of nuclear war is insensible to everyone else, but rational for them. Therefore, while Putin's apocalyptic rhetoric might be alarming, it is not necessarily a symptom of a deranged mind. For instance, Putin declared in a 2018 interview that "if someone decides to annihilate Russia, we have the legal right to retaliate. Yes, it will be a catastrophe for humanity and for the world…but we will ascend to heaven as martyrs, while they will just croak before they know what hit them." On another occasion, the Russian president asked, "What use to us is a world without Russia?"

Of course, a previously competent ruler could suffer a psychotic break or a stroke that changed their personality, but other mechanisms can make rulers defy expectations. Dictators, particularly those who have been in power for a long time like Putin, often come to exist within information bubbles where no one is willing to tell them "no" or to challenge their beliefs. Erroneous beliefs can inspire poor-quality decisions without rising to the level of outright delusions.

Still, if Putin is not a sensible man, then cost-imposing strategies such as the devastating economic sanctions that are continuing to pile up may fail to temper his misbehavior. Instead, other, more-rational Russians may need to be the targets of sanctions and other cost-imposing measures designed to influence Russia's policies in Ukraine. Increasingly isolated and desperate, Putin might still try to suddenly escalate the conflict rather than back down, potentially imperiling countless innocent people. To account for this treacherous possibility, Western leaders need to plan for the worst while hoping for the best.

Edward Geist is a policy researcher at the nonprofit, nonpartisan RAND Corporation.

Can Ukraine Be Saved Without Triggering a Nuclear Response?

By Brendan Nicholson

Source: https://www.homelandsecuritynewswire.com/can-ukraine-be-saved-without-triggering-nuclear-response

Mar 09 – Nations in and near Eastern Europe have long feared the sort of brutal onslaught Russia's Vladimir Putin is visiting upon Ukraine. That fear is heightened by the horrifying

prospect that if, against the odds, they manage to bring the Russians to the point of defeat, Putin will launch a 'battlefield' or 'tactical' nuclear weapon to destroy them or their NATO allies.
That will be exercising the minds of Polish leaders conscious that their nation is a vital supply route to its beleaguered neighbor which is using weapons supplied by allies to inflict undreamed-of damage on the Russian invaders.
In 2016, I attended a military exercise in Poland involving 31,000 troops from the United States and other NATO countries along with nations that were once members of the Warsaw Pact. On a vast stretch of rolling meadow scattered with trees in northern Poland, a combined team of US Apache attack helicopters and Soviet-era Hind gunships blasted a 'Red' army force trapped in a valley below. No one on the 'Blue' army side, or among the watching politicians and NATO officials, acknowledged that the 'Red' force that had been cut off after invading from the north represented the Russians—but that's clearly who it was.
The exercise was driven by rising fears of Putin's Russia and its willingness to use force to threaten, weaken and ultimately invade weaker nations on its borders. This included regular reminders from Moscow that it had a nuclear arsenal.
By 2016, Russia wasn't 'red' anymore, but a succession of events in Europe had breathed new life into a Cold War most of the world thought was long dead.
In 2014, Russia's neighbors were appalled by its forced annexation of the Crimean peninsula which had been part of Ukraine. After that success, Russia infiltrated thousands of its regular troops, the so-called 'little green men', into Ukraine's Donbas region until the war there reached a stalemate.
By then, Putin's bullyboy tactics, his threats and his unpredictability had his country's former allies, and the rest of Europe, badly spooked. Russia said it was merely reacting to NATO's expansion eastwards and the installation of missile defense systems across nations that once were part of the Soviet bloc. Having a protective moat of acquiescent nations had long provided Moscow with a measure of comfort.
To achieve what it wanted in Eastern Europe, Moscow engaged in a multifaceted strategy some in the West tagged 'hybrid warfare'. That worked best in countries on Russia's borders where there was already some political instability or ethnic tension.
Russia builds up opposition to the status quo, ideally by working with members of an ethnic Russian minority, triggering demonstrations and targeting people such as journalists who raise the alarm to put them out of work by damaging their reputations and swamping their email systems to shut them down.
When the situation is destabilized, regular Russian troops can be sent to train and stiffen violent opposition groups and destabilize, disorientate and weaken the country. The next step is to make the opponent look like the aggressor so there's an excuse to send in forces who look as if they are defending legitimate interests.
London's Chatham House says this type of hybrid warfare is not new or substantially different from past Russian and Soviet doctrine. It's just the Russian way of achieving its policy objectives and waging war using a range of weapons, some of them non-military.
The 2016 Exercise Anakonda led by Poland was designed to demonstrate to Moscow that the US and Western and central European nations were willing to come to the aid of one-time Russian satellite nations monstered by the Kremlin.
With them were forces from non-NATO nations Sweden and Finland. Poland, Lithuania, Latvia and Estonia, on the alliance's vulnerable eastern flank, were former members of the Warsaw Pact that joined NATO after the collapse of the Soviet Union. All of these nations are now watching events in Ukraine with horror and disbelief. But they are also playing a part in supporting the Ukrainian government and forces with weapons to use in their defense. These newer NATO members have turned out to have influential voices in shaping the re-energized NATO we are starting to see.
Putin's use of language is as chilling as his approach to nuclear weapons and is also an echo of past Russian doctrine and policy. As part of a 'de-escalation strategy' in the event of a conflict, Russian military chiefs could order the use of a relatively small and low-yield nuclear bomb fired by artillery or launched on a missile.
The intention would be to leave the NATO nations that have nuclear weapons—the US, Britain and France—with the unspeakable choice of using a similar bomb against Russian forces and embarking on a nuclear war or pulling back their forces to avoid possible annihilation.
Polish officials said in 2016 that even if Russia didn't carry out such a threat, leaving the very possibility dangling was a weapon in its own right designed to create fear and uncertainty among allied nations and weaken their resolve to act.
Poland's then defense minister, Antoni Macierewicz, said that he was less worried about the threat from Russia because his nation was assured of support from other NATO countries. Addressing a future that looked much like the current Russian war against Ukraine, Macierewicz told me that if a neighbor such as Ukraine were threatened by Russia, Poland would keep its promise to help 'restore its territorial integrity'.
At the time, concerns focused on the area known as the Suwalki Gap along Poland's border with Lithuania. This is the 100-kilometre-long strip of land between the Russian exclave of Kaliningrad and close Russian ally Belarus. Polish military leaders feared that if NATO forces advanced into Lithuania through that gap to help one of the Baltic nations, Russia could set off a nuclear blast to stop or discourage the allied advance.

As Russia continues to attack Ukraine's cities with bombs, shells and missiles, its long military convoy on the road to Kyiv would make an enticing target for allied air forces.
Putin has shown off his army in action and, apart from what it's done to Ukraine's cities, NATO commanders must be wondering why they feared the Soviet and Russian conventional forces for seven decades—although those forces have demonstrated their traditional willingness to unleash massive firepower on 'soft' targets.
Some of the Russian troops have been so lacking in education, training or any sense of self-preservation that they used a tank to fire on a Ukrainian nuclear power plant, setting sections of it on fire.
With poor-quality tires unable to deal with boggy ground, the formidable looking Russian troop transports and rocket launchers have had trouble crossing terrain that could be traversed by enthusiasts from any serious four-wheel-drive club.
That appears to be forcing the attackers to line up their vehicles side by side and bumper to bumper on whatever tarseal is available.
In a war against any peer adversary, the Russian force locked onto that road to Kyiv would long ago have been a smoldering ruin.
The restraint of NATO military planners is explained by their fear that too much military success might invite a nuclear response.
That restraint on NATO's part also demonstrates why it never posed any sort of existential threat to Russia.

Brendan Nicholson is executive editor of The Strategist.

What Are the Risks at the Chernobyl Nuclear Plant?

By Ajit Niranjan

Source: https://www.homelandsecuritynewswire.com/dr20220309-what-are-the-risks-at-the-chernobyl-nuclear-plant

Mar 09 – In late February Russian troops invading Ukraine occupied the defunct Chernobyl nuclear power plant, site of the worst nuclear disaster in history, and took over an exclusion zone that houses decommissioned reactors and radioactive waste facilities.
Since then, the 210 technicians and guards responsible for keeping it safe have not taken a proper break. The International Atomic Energy Agency (IAEA), the United Nations body responsible for nuclear security, says a key pillar of nuclear safety is giving operating staff

the capacity to make decisions free of "undue pressure." But overworked staff at Chernobyl are trying to fulfil their duties amid an invasion that has already forced 2 million people to flee.

Two nuclear containment specialists inside the main control center at the New Safe Confinement (NSC). Some 3,000 people work at the site, including several foreign specialists.

A combination of factors has increased fears of radioactive leaks from the Chernobyl site. But there is no chance of a nuclear meltdown — the last reactor was closed more than two decades ago. For now, the main concerns are for staff.
"I'm deeply concerned about the difficult and stressful situation facing staff at the Chernobyl nuclear power plant and the potential risks this entails for nuclear safety," said IAEA Director General Rafael Grossi in a press statement Tuesday. "I call on the forces in effective control of the site to urgently facilitate the safe rotation of personnel there."

Communications and Power Failures

Compounding the concerns are problems with communications and electricity.
On Tuesday, the IAEA said data transmission from monitoring systems installed at Chernobyl had been lost and Ukraine's regulatory authority could only communicate with the plant via email. State-run nuclear energy company Ukrenergo reported Wednesday that a high-voltage electricity line connecting Kyiv and Chernobyl had been disconnected. That has forced workers to rely on diesel generators for electricity and there are concerns it could disrupt the cooling pumps for spent fuel.
Radioactive fuel rods continue to heat up after they have been taken out of reactors and need to be chilled in water for years before they can be moved to dry storage facilities. More than 20,000 spent fuel rods are sitting in wet and dry storage facilities at the site.
If the cooling pools were to dry out, the radiation could hurt workers. But experts said a large release of radiation akin to the 1986 disaster is unlikely and would not "have consequences outside the plant site."
"It is also important to note that drying out of the ponds will not cause a nuclear reaction or explosion to occur," said Mark Foreman, associate professor of nuclear chemistry at Chalmers University of Technology in Sweden, in a statement.
A report from the Ukrainian state regulator in 2011 stress-tested different scenarios that could lead to failure. It found that if electricity were cut, the loss of the pool water cooling function would raise temperatures — but not by enough to cause an accident.
In a tweet on Wednesday, the IAEA confirmed the heat load of the spent fuel storage pool and the volume of cooling water was enough to effectively remove heat without the need for electricity.

"The spent fuel there is so old that evaporation will not likely be the problem," said Jan Haverkamp, a nuclear expert at environmental campaign group Greenpeace. Still, he added, "an explosion hitting the pool could cause overheating."
The loss of electricity could also hit the ventilation system and make it harder to manage radioactive dust.
"It may become much harder for workers to enter some parts of the site without full protective clothing," said Foreman. "They may also have greater difficulty in changing in and out of their protective clothing. Some parts of the site might become off limits to the workers until the power is restored."

Workers and visitors must test their radiation levels before being allowed to leave Chernobyl's New Safe Confinement (NSC)

Nuclear Safety
Russian President Vladimir Putin's decision to fully invade Ukraine in February has thrown the security of nuclear power into the spotlight. "If there is a nuclear accident the cause will not be a tsunami brought on by mother nature," said Grossi on Monday, referring to the earthquake that flooded the reactor of the Fukushima Daiichi nuclear power plant in Japan in 2011. "Instead, it will be the result of human failure to act when we knew we could."
Chernobyl is a powerful symbol of nuclear catastrophe. In 1986, a sudden surge of power during a reactor test destroyed Unit 4 of the poorly designed nuclear power station, in what was then part of the Soviet Union. The fire that followed released clouds of radioactive material into the environment that led to authorities setting up an exclusion zone and evacuating hundreds of thousands of people. Dozens are thought to have died as a direct result of the disaster. Radiation levels have since fallen. Some residents of the exclusion zone have returned to their homes and live in areas with levels that are above average but not fatal. Radiation unexpectedly spiked in February when Russian troops entered the area, possibly because of heavy vehicles raising a layer of topsoil and kicking dust up into the air. The IAEA found the levels pose no danger to the public. But the unprecedented reality of war in a country operating nuclear power stations has raised the specter of nuclear catastrophe.
The Russian army shelled Europe's largest nuclear power plant last week before taking over the site. Though there was no safety incident, it was the first time that military explosives have hit an operating nuclear facility.
"We've entered something that that the industry was in complete denial of," said Haverkamp. "Nuclear power is just not an energy source that belongs in a war situation."

Ajit Niranjan is Environment and Globalization reporter at *DW*.

●▶ **Source of photos**

Prominent Ukrainian physics institute imperiled by Russian attacks

Source: https://physicstoday.scitation.org/do/10.1063/PT.6.2.20220307a/full/

The main building of the National Science Center, Kharkiv Institute of Physics and Technology, last year. Kharkiv is located in northeast Ukraine and is the country's second-largest city. Credit: Sergiy Bobok, via Wikimedia Commons, CC BY-SA 4.0

Mar 07 – The National Science Center, Kharkiv Institute of Physics and Technology (KIPT), which was a hotbed of early nuclear research in the former Soviet Union and currently hosts a newly installed neutron source, has suffered significant damage from Russia's relentless attack on Kharkiv, Ukraine's second-largest city. Rockets and bombs have damaged buildings and left civilians wounded, says Oleksandr Bakai, who heads the department of condensed matter and nuclear theory at KIPT and lives near the institute.

The damaged facilities include the constructed but not fully operational Ukraine Neutron Source, according to the State Nuclear Regulatory Inspectorate of Ukraine. After saying in a 7 March press briefing that the neutron source had been destroyed, International Atomic Energy Agency director general Rafael Mariano Grossi said in a statement that Ukraine had informed the IAEA that the facility was "damaged by shelling."

Despite reports of concerns about a nuclear accident, the facility is an accelerator-driven subcritical assembly and not a critical nuclear reactor. The assembly cannot sustain a chain reaction without neutrons from the accelerator, says Harvard proliferation researcher Matthew Bunn, and it generates virtually zero fission products. In addition, there is no highly

enriched uranium onsite. "The danger is from bullets and bombs, not from radiation from this facility," he says. Both Grossi and Ukraine's nuclear regulator said on 7 March that there has been no release of radiation.

Since the start of the invasion on 24 February, the Russian military has been attacking both Kharkiv neighborhoods where KIPT is located: the city center and the Piatykhatky area to the north. On the first day of the war, at least one building in the Piatykhatky neighborhood near the institute caught fire, and a 10-foot-long rocket struck an apartment complex but did not detonate, Bakai says. But what had been sporadic attacks became a concentrated "bombardment" on 6 March, he reports. The Kharkiv branch of Ukraine's Security Service wrote that the Russians were using Grad multiple rocket launchers. The US Department of Defense is looking into reports of a rocket attack on KIPT, a senior defense official said on 7 March, but at that time was not independently able to verify them.

More than 400 scientists conduct research at KIPT in condensed matter, plasma physics, nuclear physics, and theoretical physics, according to the institute's website. Eugene Chudnovsky, a cochair of the Committee of Concerned Scientists who received his physics education at the institute and worked at a university department associated with it, says he has had trouble reaching even close acquaintances in the battered city. The people he has heard from "told me that they were hiding inside underground facilities."

A substation at the Ukraine Neutron Source was destroyed by Russian attacks on 6 March, according to Ukraine's nuclear regulatory agency. Credit: State Nuclear Regulatory Inspectorate of Ukraine

The 6 March shelling heavily damaged the Ukraine Neutron Source. Ukraine's nuclear regulatory agency reported a destroyed substation, damaged heating and cooling systems, and broken windows.

The Neutron Source was developed in collaboration with the US Department of Energy's Argonne National Laboratory and is designed for research and medical isotope production. Several institutes in Russia were involved in the systems engineering, equipment making, and construction, which was completed in 2018, says Mark Hibbs, a senior fellow in the nuclear policy program of the Carnegie Endowment for International Peace. An electron linear accelerator generates neutrons that hit a tungsten or low-enriched uranium target. The unit is considered a research reactor by the IAEA, which maintains a database of both critical assemblies and subcritical ones like KIPT's.

Staff at the Kharkiv Institute of Physics and Technology load the first fuel assemblies into a container at the launch of the institute's neutron source in October. Credit: Press Service of the National Academy of Sciences of Ukraine

Staff at KIPT loaded the first fuel assemblies last October, according to the National Academy of Sciences of Ukraine, and since then researchers had been preparing for operation and working to secure necessary licenses. The source of the uranium oxide fuel, enriched to about 19% ^{235}U, has been the Russian vendor TVEL, Hibbs says. Ukraine's nuclear regulator reports that the reactor contained fresh fuel as recently as the eve of the Russian invasion. However, the agency adds that by 24 February the reactor had been "transferred to a deep subcritical state," which Hibbs says suggests that the fuel was proactively removed.

On 6 March DOE's National Nuclear Security Administration received reports from its Ukrainian partners that the facility "sustained damage due to an explosion," says NNSA

spokeswoman Kate Hewitt. She says that NNSA "is in frequent contact with facility staff and is monitoring the situation closely," and that KIPT has reported no casualties at the site.
In describing the attack on KIPT, Ukraine's Security Service said that the Neutron Source has 37 loaded nuclear fuel elements and that the destruction of the facility "could lead to a large-scale ecological disaster." Bunn, however, says the risk of widespread radiation contamination is "nearly zero" because of the subcritical nature of the facility. Hibbs agrees, adding that even when operational, there would be only grams of uranium fuel in the core. Russian military action at nuclear power plants such as Zaporizhzhya in southeastern Ukraine is of much greater concern, Bunn adds.

A rich but turbulent history

Founded by physicist Abram Ioffe in 1928, when Kharkiv was the capital of the Ukrainian Soviet Republic, the institute stood out for the "high quality of its personnel from the start," says Russian and Soviet historian Paul Josephson of Colby College in Maine. Early alumni included theoretical physicists Lev Landau and Ilya and Evgeny Lifshitz and low-temperature experimentalist Lev Shubnikov. In 1932 physicists at the institute reproduced the splitting of an atom by fast protons, which had been demonstrated by John Cockcroft and Ernest T. S. Walton at the Cavendish Laboratory earlier that year.
"KIPT has a glorious history," Josephson says, "but also a very painful one." In the late 1930s numerous scientists at the institute were arrested as part of the Stalin regime's Great Purge; Shubnikov, the codiscoverer of type II superconductivity, was executed in 1937. Then came World War II and the German occupation of Ukraine.

Physicists gather at the then-Ukrainian Physical-Technical Institute in Kharkiv in 1934. First row, from left: Lev Shubnikov, Aleksandr Leipunski, Lev Landau, and Pyotr Kapitsa. Second row, from left: Nisson Finkelstein, Olga Trapeznikova, Kirill Sinelnikov, and J. N. Rjabinin. Credit: AIP Emilio Segrè Visual Archives

Following the war, scientists at the institute turned their attention to the Soviet atomic bomb project. KIPT was known as Laboratory No. 1; Moscow's Kurchatov Institute became Laboratory No. 2 and took the lead in developing the Soviet Union's first nuclear weapons. In subsequent years, a number of KIPT physicists turned their attention to fusion energy projects, with some research informing the ITER project that is under construction in France, Josephson says.
Ukrainian science suffered from the severe funding cuts that followed the collapse of the Soviet Union, and KIPT was no exception. Still, the institute possessed dozens of kilograms of highly enriched uranium left over from the Cold War—"the biggest and most worrisome single cache" of highly enriched uranium in Ukraine, says Bunn, who as a White House nonproliferation policy adviser tried unsuccessfully to get the US to purchase the uranium in 1994. As part of a 2011 agreement with the Obama administration, the Ukrainian government agreed to remove the remainder of the highly enriched uranium at KIPT and received funding and support to build the neutron source.
Ukraine hosts three other operational research reactors, according to the IAEA. One is in Kyiv, at the Science Center Institute for Nuclear Research. The other two are in Sevastopol, a city that has been controlled by Russia since it annexed Crimea in 2014.

How to avoid nuclear catastrophe—and a costly new arms race

By Daryl G. Kimball
Source: https://thebulletin.org/2022/03/how-to-avoid-nuclear-catastrophe-and-a-costly-new-arms-race/

Mar 11 – If Russian President Vladimir Putin's premeditated, illegal attack on Ukrainian cities, towns, nuclear power stations, hospitals, and civilians wasn't shocking enough, his recent nuclear saber-rattling is a crude reminder that the risk of nuclear war still looms. To respond effectively, those looking for a safer, saner world must rethink the nuclear deterrence policies and practices that have led the nuclear weapons countries to this point and push them toward new approaches and policies that move the world away from nuclear catastrophe.
"Western countries aren't only taking unfriendly economic actions against our country, but leaders of major NATO countries are making aggressive statements about our country,"

Putin said in a February 27 in a meeting with Russian defense officials. "So, I order to move Russia's deterrence forces to a special regime of combat duty."
According to a senior Russian official I have spoken with in recent days, Putin's statement was probably designed to reinforce his earlier implied threats of nuclear use—threats clearly meant to ward off outside military interference in his attack on Ukraine. Nuclear threats and alerts were not uncommon during the Cold War, before the 1962 Cuban missile crisis and after. But Putin's overt nuclear saber-rattling is unprecedented—and unacceptable—in the post-Cold War era. Since the Soviet Union dissolved, no US or Russian leader has raised the alert level of nuclear forces to try to coerce the other side's behavior.
Such actions are dangerous for all sides. Nuclear threat rhetoric and orders to raise the operational readiness of Russian or US nuclear forces could be also misinterpreted in ways that lead to other side to make nuclear countermoves that lead to a dangerous escalation of tensions and fears of attack.
The idea that nuclear weapons can be "used" provide cover for a major conventional military intervention against a nonnuclear weapon state is, unfortunately, not a new one nor uniquely Russian. Adm. Charles Richard, head of US Strategic Command, said in February 2021 that "[w]e must acknowledge the foundational nature of our nation's strategic nuclear forces, as they create the 'maneuver space' for us to project conventional military power strategically."
In this case, Putin's nuclear brinksmanship, while unnerving and dangerous, has not stopped NATO members from providing defensive weapons to Ukraine and deploying sweeping sanctions against Russia's leadership, oligarchs, and financial and economic systems.
Putin's invasion also underscores a reality: Contrary to myth, nuclear weapons don't prevent major wars. Rather, they can facilitate aggression by nuclear-armed states and make wars waged by nuclear-armed states far more dangerous—especially when nuclear-armed states become pitted against one another, dangerously increasing the risk of miscalculation and miscommunication.
President Joe Biden has wisely not engaged in inflammatory nuclear rhetoric or raised the alert status of US nuclear forces. The Pentagon even postponed a scheduled Minuteman III intercontinental ballistic missile test flight to avoid the possibility that Putin might use it as a pretext for further nuclear escalation.
So long as NATO and Russian forces don't begin fighting each other, the risk of nuclear escalation may be kept in check. But a close encounter between NATO and Russian warplanes (which would result if NATO imposed a "no fly zone" over Ukraine's airspace) could become a flashpoint that leads to a direct and wider conflict.
Unlike the more severe and acute risk of nuclear war between the United States and the Soviet Union during the 13 day-long Cuban missile crisis of October 1962, Russia's brutal war in Ukraine will likely lasts many weeks, if not months or more. In other words, the world will remain in a condition of heightened nuclear danger for some time. The situation demands restraint and a diplomatic solution. But once warfare in Ukraine has stopped, there must be a serious reckoning with the role nuclear weapons play in the military strategies of nuclear countries around the world, and renewed pressure for action toward their elimination.

Needed: changes in military doctrine

Today, US and Russian military strategies reserve the option to use nuclear weapons first in extreme circumstances and even sometimes against nonnuclear threats. Russia's formal nuclear doctrine describes two main scenarios that might trigger the use of nuclear weapons: in response to an attack with weapons of mass destruction, or in the face of a conventional war that threatens the "very existence of the state."
The viability of the Russian state is clearly not under imminent threat from either Ukraine or from NATO. But if the Kremlin thought an attack from the United States or NATO was under way, Putin might well consider going nuclear, perhaps beginning with the use of short-range, "tactical" nuclear weapons, to try to tip the balance in Russia's military favor or to try to end the conflict.
But the notion that a nuclear war can be "limited" is dangerous. In practice and in the fog of war, once nuclear weapons are used in a conflict involving nuclear-armed adversaries, there is no guarantee it would not quickly become an all-out nuclear conflagration.
As the head of US Strategic Command General John Hyten said in 2018 after the annual Global Thunder wargame: "It ends bad. And the bad meaning it ends with global nuclear war."
To illustrate the dangers, in 2020 researchers at Princeton's Program on Science and Global Security published an analysis of what might happen if Russian or NATO leaders chose to use nuclear weapons first in a conflict in Europe. After an initial volley of "tactical" nuclear detonations, it could escalate and involve a massive exchange of thermonuclear weapons involving Russia's arsenal of some 1,450 strategic warheads and the U.S. arsenal of 1,350 strategic warheads on its missiles and bombers.
In that scenario, more than 91 million people were projected to die in just the first few hours of the conflict. In the days, weeks, and years that follow, millions more would die from exposure to radiation. Health, financial, and economic systems would collapse around the globe.
We can ill afford to live with nuclear weapons policies that could lead to such catastrophic outcomes. New approaches are essential.

New approaches to the nuclear threat

In 2017, more than 120 nonnuclear weapon states negotiated the Treaty on the Prohibition of Nuclear Weapons. Although that treaty has to date been dismissed by nuclear-armed countries because it challenges their nuclear deterrence doctrines, it bolsters the global taboo against nuclear weapons and builds-up the legal framework for their eventual elimination.

Many American politicians, mainly Republicans but also some Democrats, however, want to double down on insanity by funding even more nuclear firepower. Former Secretary of State Mike Pompeo has argued that "advanced weapons must be pursued if they are necessary to match potential belligerents" like Russia. These include new types of lower-yield nuclear weapons to provide a president with "more credible" nuclear use options and, if necessary, use in a future conflict in the Baltic region, or some other dispute with Russia, or perhaps China. But there are no winners in such a costly new arms race, and certainly no winners in a nuclear war.

Instead of reverting to extremely risky and absurd Cold War-era nuclear behaviors, US leaders need to embrace new thinking that begins to move us out from under the shadow of nuclear catastrophe, beginning with the Biden administration's nearly completed Nuclear Posture Review.

To start, Biden should draw a strong distinction between Putin's irresponsible nuclear threats and US behavior and clarify that the sole purpose of the U.S. nuclear weapons arsenal deter the first use of nuclear weapons by others as he pledged to do in 2020. A "sole purpose" policy would rule out the use of nuclear weapons in a preemptive strike or in response to a non-nuclear attack on the United States or its allies, increase stability, reduce Russia's perception of the threat from NATO, and decrease the overall risk of nuclear war.

Even after the eventual end of Putin's war on Ukraine, the risk of further NATO-Russia conflict will persist. The United States and Russia (with or without Putin), along with France, and the United Kingdom, will still possess deadly nuclear arsenals poised to retaliate within minutes in response to nuclear attack or a false warning. In the wake of the conflict in Ukraine, we can expect that many in the security establishments of the United States, Europe, and Russia will argue for new nuclear weapons capabilities to counter each other, and perhaps for the first time in decades, an increase in the number of US and Russian deployed nuclear weapons.

The more prudent path is to freeze the qualitative arms race, further reduce the role nuclear weapons, and reverse the race through renewed US and Russian action on nuclear arms control and disarmament—and eventually to involve the other major nuclear-armed states, particularly China, in the nuclear arms control and disarmament enterprise.

To reduce tensions in Europe, Russia and NATO member states will need avoid the temptation to introduce new offensive strike weapons, particularly nuclear weapons. For example, the offer from Russia's client state, Belarus, to host Russian nuclear weapons, if pursued by Putin, would further undermine Russian and European security, and increase the risk of nuclear war. It would also be highly destabilizing if NATO and/or Russia reintroduce once-banned intermediate-range missiles, which can reach their targets in minutes and with little warning.

Still more can and must be done reduce nuclear risks. With an enormous number of their nuclear forces deployed on invulnerable strategic submarines, neither Washington nor Moscow needs to keep their land-based missiles ready for launch within minutes of a warning of attack, as current plans require. Both countries could reduce the day-to-day high alert status of their land-based intercontinental missiles and they would still be capable of launching a devastating retaliatory nuclear attack.

The need for continued arms control and disarmament negotiations

Although Putin's regime must suffer international isolation now, Russia and the West have a strong interest (and an obligation under the 1968 Treaty on the Nonproliferation of Nuclear Weapons) to resume negotiations on verifiable agreements that significantly cut the still bloated strategic nuclear stockpiles on both sides.

Despite reckless behavior on the part of Russia, as well as China's effort to fortify its nuclear arsenal array, the size of the US nuclear arsenal still exceeds what is necessary to maintain an effective deterrent.

President Obama announced in 2013 that the United States could safely reduce its deployed strategic nuclear weapons by up to one-third below the current New START levels. The analysis concluded the United States could independently reduce is deployed arsenal to this level and still hold adversary targets at risk so as to deter nuclear attack. But the Obama administration made a political decision to pursue such reductions bilaterally with Russia. The rationale for a smaller force still holds.

An up-to-one-third reduction in deployed strategic forces would leave the United States (and Russia) with nuclear capability with which to trade as part of new arms control arrangements with Russia (or in the future China).

Any increase in the number of US or Russian strategic nuclear weapons above New START levels, or any increase in nonstrategic weapons arsenals, would not enhance deterrence against one another. Rather it would lead to a dangerous action-reaction that increases tensions and the risk of miscalculation and catastrophe.

US efforts to further limit Russian strategic nuclear weapons and bring China into the arms control process are unlikely to gain traction unless Washington agrees to seriously discuss constraints on its long-range missile defense capabilities. Fielding sufficient numbers of U.S.

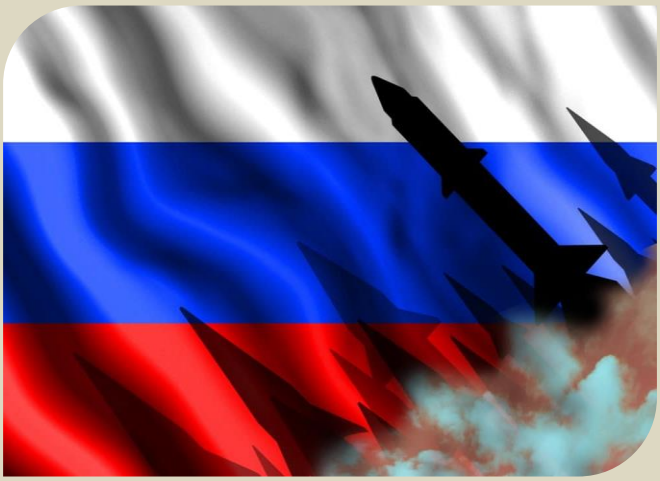
missile interceptors to mitigate the threat of a limited ballistic attack from North Korea or Iran and agreeing to binding limits on the quantity, location, and capability of missile defense systems should not be mutually exclusive.
Whenever the US-Russian arms control dialogue resumes again, the two countries will also need to explore options to prevent a new intermediate-range missile race and to regulate and reduce existing stockpiles of shorter-range "battlefield" nuclear arsenals, including Russia's stockpile of approximately 1,000 weapons that are kept at centralized storage sites and the 160 US nuclear gravity bombs stationed at five NATO bases in Europe. Before Russia's war on Ukraine, both sides indicated they want to prevent the redeployment of intermediate-range, ground-launched missiles that could threaten Europe and Russia.
The last remaining nuclear arms control agreement regulating the world's two largest arsenals, New START, expires early in 2026. In the absence of commonsense nuclear arms control guardrails, the risk of costly, unconstrained global nuclear arms race will grow. Putin's recent nuclear threats highlight the existential dangers posed by nuclear weapons. Ultimately, the only way to eliminate those dangers to verifiably eliminate all nuclear weapons. Even if that goal is a long way off, moving steadily in that direction, while preserving the taboo against nuclear weapons use, is essential to our survival.

Daryl G. Kimball has studied and written about nuclear weapons policy issues for 26 years as an analyst with Physicians for Social Responsibility, at the Coalition to Reduce Nuclear Dangers, and, since 2001, as the executive director of the non-partisan, independent Arms Control Association, in Washington, DC. He is publisher of and a contributor to the monthly journal *Arms Control Today*.

Russia's nuclear weapon use policy

By David Holloway
Source: https://thebulletin.org/2022/03/read-the-fine-print-russias-nuclear-weapon-use-policy/

Mar 10 – The risk of nuclear war casts a dark shadow over the already-tragic events in Ukraine. On February 19, Vladimir Putin launched an exercise involving Russian strategic forces. On February 24—the day Putin invaded Ukraine—he warned that Russia would respond immediately to those who stood in its way, with consequences that "will be such as you have never seen in your entire history." On February 27, he publicly ordered his minister of defense and chief of the general staff to transfer Russia's "deterrence forces" to "special combat readiness." Putin's aim was evidently to deter outside intervention and to signal Russia's determination to achieve its goals.



But another, more troubling, aspect to Putin's recent comments has received little or no attention. It has to do with the circumstances under which Russia might use nuclear weapons.
In June 2020, Putin signed a decree—the Basic Principles of the Russian Federation's State Policy in the Domain of Nuclear Deterrence—that specifies two conditions under which Russia would use nuclear weapons. The first is unsurprising: "The Russian Federation retains the right to use nuclear weapons in response to the use of nuclear weapons and other types of weapons of mass destruction against it and/or its allies…" But that sentence ends with an unusual statement: ***"… and also in the case of aggression against the Russian Federation with the use of conventional weapons, when the very existence of the state is put under threat"*** [emphasis added].
In his February 24 speech, Putin echoed that unusual language to describe his Ukraine invasion. The United States, he claimed, was creating a hostile "anti-Russia" next to Russia and in Russia's historic land. "For the United States and its allies, it is a policy of containing Russia, with obvious geopolitical dividends," he said. "For our country, it is a matter of life and death, a matter of our historical future as a nation. This is not an exaggeration; this is a fact. *It is not only a very real threat to our interests but to the very existence of our state and to its sovereignty*" [emphasis added]. Putin has defined the current situation as one in which, in line with the principles of its deterrence policy, Russia retains the right to use nuclear weapons.
This does not mean that Russia will use such weapons, and deterrence at the strategic level appears to be robust. At the tactical level, however, the situation is different. The 2018 US Nuclear Posture Review ascribed to Russia the view that "the threat of nuclear escalation or even first use of nuclear weapons would serve to de-escalate a conflict on terms favorable to Russia." Russian military theorists have certainly discussed this idea of "escalating to de-

escalate," though whether it is a part of Russian doctrine is disputed among students of Russian strategy. "Escalating to de-escalate" in a war with NATO would run the serious risk of escalation rather than de-escalation. In a local war with a non-nuclear adversary, however, the small-scale tactical use of nuclear weapons might be a serious temptation, especially if the war were not going according to plan. In short, the impulse to escalate in a tight corner could be strong.

There are two reasons for drawing attention to Putin's recent words. **First,** in echoing the Basic Principles of Russian Federation's State Policy in the Domain of Deterrence, Putin provides a frame of reference for his thinking about nuclear weapon use. This, in turn, provides context for assessing the risk that he will escalate to the use of nuclear weapons.

Second, in a period of high tension, a miscalculation could have catastrophic consequences, as Russia's recent decisions arguably show. World leaders should do as much as possible to dissuade Putin from using of nuclear weapons, not so much by the threat of retaliation in kind, since that could lead to dangerous escalation. Rather they should prepare the ground for a massive political response to a potential decision Putin might make to cross the nuclear threshold.

David Holloway is the Raymond A. Spruance Professor of International History at Stanford University, a professor of political science, and a Freeman Spogli Institute of International Studies senior fellow. He was co-director of the Center for International Security and Cooperation from 1991 to 1997 and director of the Freeman Spogli Institute from 1998 to 2003. His research focuses on the international history of nuclear weapons, on science and technology in the Soviet Union, and on the relationship between international history and international relations theory. His book *Stalin and the Bomb: The Soviet Union and Atomic Energy, 1939-1956* (Yale University Press, 1994) was chosen by the *New York Times Book Review* as one of the 11 best books of 1994. Holloway also wrote *The Soviet Union and the Arms Race* (1983) and co-authored *The Reagan Strategic Defense Initiative: Technical, Political and Arms Control Assessment* (1984).

From Hiroshima and Nagasaki to Fukushima 2

Health effects of radiation and other health problems in the aftermath of nuclear accidents, with an emphasis on Fukushima

Arifumi Hasegawa, Koichi Tanigawa, Akira Ohtsuru, Hirooki Yabe, Masaharu Maeda, Jun Shigemura, Tetsuya Ohira, Takako Tominaga, Makoto Akashi, Nobuyuki Hirohashi, Tetsuo Ishikawa, Kenji Kamiya, Kenji Shibuya, Shunichi Yamashita, Rethy K Chhem

437 nuclear power plants are in operation at present around the world to meet increasing energy demands. Unfortunately, five major nuclear accidents have occurred in the past—ie, at Kyshtym (Russia [then USSR], 1957), Windscale Piles (UK, 1957), Three Mile Island (USA, 1979), Chernobyl (Ukraine [then USSR], 1986), and Fukushima (Japan, 2011). The effects of these accidents on individuals and societies are diverse and enduring. Accumulated evidence about radiation health effects on atomic bomb survivors and other radiation-exposed people has formed the basis for national and international regulations about radiation protection. However, past experiences suggest that common issues were not necessarily physical health problems directly attributable to radiation exposure, but rather psychological and social effects. Additionally, evacuation and long-term displacement created severe health-care problems for the most vulnerable people, such as hospital inpatients and elderly people.

Lancet 2015; 386: 479–88

This is the second in a Series of three papers about Hiroshima and Nagasaki to Fukushima

Department of Radiation Disaster Medicine (Prof A Hasegawa MD), Fukushima Global Medical Science Center (Prof K Tanigawa MD), Department of Radiation

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

By Hans M. Kristensen and Matt Korda

Source: https://thebulletin.org/premium/2022-02/nuclear-notebook-how-many-nuclear-weapons-does-russia-have-in-2022/

Feb 23 – Russia is in the late stages of a decades-long modernization of its strategic and nonstrategic nuclear forces to replace Soviet-era weapons with newer systems. In December 2021, Russian Defense Minister Sergei Shoigu reported that modern weapons and equipment now make up 89.1 percent of Russia's nuclear triad, an increase from the previous year's 86 percent (Russian Federation 2021a; Russian Federation 2020a). The 2021 modernization activities apparently exceeded the projected gains for this year, as President Putin's 2020 end-of-year address estimated

Table 1. Russian nuclear forces, 2022

Type/name	Russian designation	Launchers	Year deployed	Warheads x yield (kilotons)	Total warheads
Strategic offensive weapons					
ICBMs					
SS-18 M6 Satan	RS-20V	40	1988	10 x 500/800 (MIRV)	400[1]
SS-19 M3 Stiletto	RS-18 (UR-100NUTTH)	0	1980	6 x 400 (MIRV)	0[2]
SS-19 M4	? (Avangard)	6	2019	1 x HGV	6
SS-25 Sickle	RS-12M (Topol)	9[3]	1988	1 x 800	9
SS-27 Mod 1 (mobile)	RS-12M1 (Topol-M)	18	2006	1 x 800?	18
SS-27 Mod 1 (silo)	RS-12M2 (Topol-M)	60	1997	1 x 800	60
SS-27 Mod 2 (mobile)	RS-24 (Yars)	153	2010	4 x 100? (MIRV)	612[4]
SS-27 Mod 2 (silo)	RS-24 (Yars)	20	2014	4 x 100? (MIRV)	80
SS-X-29 (silo)	RS-28 (Sarmat)	–	(2022)	10 x 500? (MIRV)	–
Subtotal		**306**			**1,185[5]**
SLBMs					
SS-N-18 M1 Stingray	RSM-50	0/0	1978	3 x 50 (MIRV)	0[6]
SS-N-23 M2/3	RSM-54 (Sineva/Layner)[7]	5/80	2007	4 x 100 (MIRV)	320[8]
SS-N-32	RSM-56 (Bulava)	5/80	2014	6 x 100 (MIRV)	480[9]
Subtotal		**10/160[10]**			**800[11]**
Bombers/weapons					
Bear-H6/16	Tu-95MS6/MS16/MSM	55	1984/2015	6-16 x AS-15A ALCMs or 14 x AS-23B ALC	448
Blackjack	Tu-160/M	13	1987/2021	12 x AS-15B ALCMs or AS-23B ALCM, bombs	132
Subtotal		**68[12]**			**580[13]**
Subtotal strategic offensive forces		**534[14]**			**2,565[15]**
Nonstrategic and defensive weapons					
ABM/Air/Coastal defense					
S-300/S-400 (SA-20/SA-21)		~750	1992/2007	1 x low	~290
53T6 Gazelle		68	1986	1 x 10	68[16]
SSC-1B Sepal (Redut)		8[17]	1973	1 x 350	4
SSC-5 Stooge (SS-N-26) (K-300P/3M-55)		60	2015	(1 x 10)[18]	25
Land-based air					
Bombers/fighters (Tu-22M3(M3M)/Su-24M/Su-34/MiG-31K)		~300	1974-2018	ASMs, ALBM, bombs	~500
Ground-based					
SS-26 Stone SSM (9K720, Iskander-M)		144	2005	1 x 10-100	70[19]
SSC-7 Southpaw GLCM (R-500/9M728, Iskander-M)[20]					
SSC-8 Screwdriver GLCM (9M729)[21]		20[22]	2017	1 x 10-100	20
Naval					
Submarines/surface ships/air				LACM, SLCM, ASW, SAM, DB, torpedoes	~935
Subtotal nonstrategic and defensive forces					**~1,912[23]**
TOTAL					**~4,477**
Deployed					1,588
Reserve					2,889
Retired warheads awaiting dismantlement					**1,500**
Total inventory					**5,977**

ABM = antiballistic missile; ALCM = air-launched cruise missile; AS = air-to-surface; ASM = air-to-surface missile; ASW = antisubmarine weapon; DB = depth bomb; GLCM= ground-launched cruise missile; ICBM = intercontinental ballistic missile; LACM = Land-Attack Cruise Missile; MIRV = multiple independently targetable reentry vehicle; SAM = surface-to-air missile; SLBM = submarine-launched ballistic missile; SLCM = sea-launched cruise missile; SRAM = short-range attack missile; SSM = surface-to-surface missile

that the modernization percentage would be 88.3 percent by the end of 2021 (Russian Federation 2020a). In previous years, Putin's remarks have emphasized the need for Russia's nuclear forces to keep pace with Russia's competitors: "It is absolutely unacceptable to stand idle. The pace of change in all areas that are critical for the Armed Forces is unusually fast today. It is not even Formula 1 fast—it is supersonic fast. You stop for one second and you start falling behind immediately" (Russian Federation 2020a).

Table 1. Russian nuclear forces, 2022 (view PDF for full table with notes)

In his 2021 end-of-year speech, Putin also noted that he is "extremely concerned about the deployment of elements of the US global missile defense system near Russia." In particular, he accused the United States of using its missile defense deployments as a guise to deploy offensive systems targeted at Russia: "The Mk 41 launchers located in Romania and planned for deployment in Poland have been adapted to the use of the Tomahawk strike systems" (Russian Federation 2021a). Officials from the United States and NATO deny that the launchers have been adapted for use of Tomahawk missiles.

Putin also noted his disappointment with the deterioration of the US-Russia arms control regime, and stated that Russia needed "long term, legally binding guarantees […] because the United States easily withdraws from all international treaties, which for one reason or another become uninteresting to them—easily, explaining something or nothing at all without explaining how it was with the Anti-Ballistic Missile Treaty, [the Treaty] on Open Skies" (Russian Federation 2021a).

Russia's nuclear modernization programs, combined with an increase in the number and size of military exercises and occasional explicit nuclear threats against other countries, contribute to uncertainty about Russia's long-term intentions and growing international debate about the nature of its nuclear strategy. These concerns, in turn, stimulate increased defense spending, nuclear modernization programs, and political opposition to further nuclear weapons reductions in Western Europe and the United States.

As of early 2022, we estimate that Russia has a stockpile of approximately 4,477 nuclear warheads assigned for use by long-range strategic launchers and shorter-range tactical nuclear forces, which is a slight decrease from last year. Of the stockpiled warheads, approximately 1,588 strategic warheads are deployed: about 812 on land-based ballistic missiles, about 576 on submarine-launched ballistic missiles, and possibly 200 at heavy bomber bases. Approximately another 977 strategic warheads are in storage, along with about 1,912 nonstrategic warheads. In addition to the military stockpile for operational forces, a large number—approximately 1,500—of retired but still largely intact warheads await dismantlement, for a total inventory of approximately 5,977 warheads.[1] (See Table 1).

With only two days remaining until its expiration in March 2021, Russia and the United States mutually agreed to an extension of New START that will keep it in force through February 4, 2026. In advance of New START coming into force in 2018, Russia significantly reduced (downloaded) the number of warheads deployed on its ballistic missiles to meet the treaty limit of no more than 1,550 deployed strategic warheads. Russia achieved the required reduction by the February 5, 2018 deadline, when it declared 1,444 strategic warheads attributed to 527 launchers (Russian Federation Foreign Affairs Ministry 2018). The most recent data exchange, declared on September 1, 2021, listed Russia with 1,458 deployed warheads attributed to 527 strategic launchers (US State Department, Bureau of Arms Control, Verification and Compliance 2021a). These numbers differ from the estimates presented in this Nuclear Notebook because the New START counting rules artificially attribute one warhead to each deployed bomber, even though Russian bombers do not carry nuclear weapons under normal circumstances. Additionally, this Nuclear Notebook counts weapons stored at bomber bases that can quickly be loaded onto the aircraft as "deployed."

Russia (like the United States) could potentially upload several hundreds of extra warheads onto their launchers but is prevented from doing so by the New START treaty limit. The treaty provides an important node of transparency for both Russia's and the United States' strategic nuclear forces: as of January 2022, the United States and Russia have completed a combined 328 on-site inspections and exchanged 23,100 notifications (US State Department, Bureau of Arms Control, Verification and Compliance 2022). Due to the ongoing COVID-19 pandemic, on-site Type One and Type Two inspections were paused in April 2020. Inspections were set to restart on November 1, 2021 (Post 2021), but that did not happen. The first meeting of the Bilateral Consultative Commission since the pandemic began took place in October 2021 (US State Department, Bureau of Arms Control, Verification and Compliance 2021b).

Due to New START limitations, Russia appears to have been forced to reduce the warhead loading on some of its missiles to less than maximum capacity. We do not know the breakdown of the loading because Russia, unlike the United States, does not publish an unclassified overview of its strategic forces. However, the reduction may have involved scaling back the number of warheads on each SS-18 and SS-27 Mod 2 intercontinental ballistic missile (ICBM), as well as on each SS-N-32 submarine-launched ballistic missile (SLBM). This demonstrates that New START places real constraints on Russia's deployed strategic forces. The result appears to be an increased reliance on a strategic reserve of non-deployed warheads that can be loaded onto missiles in a crisis to increase the size of the force—a strategy similar to the one the United States has relied on for several decades.

Russia's nuclear modernization program is motivated in part by the Kremlin's strong desire to maintain overall parity with the United States and by national prestige, but also by the Russian leadership's apparent conviction that the US ballistic missile defense system constitutes a real future risk to the credibility of Russia's retaliatory capability. Policy and strategy aside, the development of multiple weapon systems, rather than focusing resources on one or two, also indicates the strong influence of the military-industrial complex on Russia's nuclear posture planning (Luzin 2021).

What is Russia's nuclear strategy?

The international debate about Russia's nuclear strategy has reached a new level of intensity, particularly after the Trump administration published its Nuclear Posture Review in February 2018. The Nuclear Posture Review claimed that "Russian strategy and doctrine emphasize the potential coercive and military uses of nuclear weapons. It mistakenly assesses that the threat of nuclear escalation or actual first use of nuclear weapons would serve to 'de-escalate' a conflict on terms favorable to Russia" (US Defense Department 2018, 8). Specifically, the document claimed, "Moscow threatens and exercises limited nuclear first use, suggesting a mistaken expectation that coercive nuclear threats or limited first use could paralyze the United States and NATO and thereby end a conflict on terms favorable to Russia." This so-called "escalate to de-escalate" doctrine "follows from Moscow's mistaken assumption of Western capitulation on terms favorable to Moscow" (US Defense Department 2018, 30).

The former head of the US Strategic Command, Gen. John Hyten, reacted to "Russia's destabilizing doctrine on what some call escalate to deescalate" by saying: "I really hate that discussion. I've looked at the Russian doctrine. I've looked at Russian writings. It's not escalate to de-escalate, it's escalate to win. Everybody needs to understand that" (Hyten 2017). Some have suggested that Russian leaders are signaling a willingness to use nuclear weapons even before an adversary retaliates against a Russian conventional attack by "employing the threat of selective and limited use of nuclear weapons to *forestall opposition to potential aggression*" (emphasis added) (Miller 2015). The implication is that Russia would potentially use nuclear weapons first to scare an adversary into not even defending itself.

Such characterizations conflict with Russia's publicly stated policy. In June 2020, President Putin approved an update to the "Basic Principles of State Policy of the Russian Federation on Nuclear Deterrence," which notes that "The Russian Federation considers nuclear weapons exclusively as a means of deterrence." The policy lays out four conditions under which Russia could launch nuclear weapons:

1. "arrival of reliable data on a launch of ballistic missiles attacking the territory of the Russian Federation and/or its allies;

2. use of nuclear weapons or other types of weapons of mass destruction by an adversary against the Russian Federation and/or its allies;
3. attack by adversary against critical governmental or military sites of the Russian Federation, disruption of which would undermine nuclear forces response actions; and
4. aggression against the Russian Federation with the use of conventional weapons when the very existence of the state is in jeopardy" (Russian Federation Foreign Affairs Ministry 2020).

The document's emphasis on deterrence by punishment, as well as the "defensive" nature of Russia's nuclear weapons, is likely intended to be a response to the aforementioned US claims of a Russian "escalate-to-deescalate" policy. The updated policy is also consistent with remarks that President Putin made to the Valdai Club in October 2018, when he stated that "Our nuclear weapons doctrine does not provide for a pre-emptive strike." Rather, he continued, "our concept is based on a reciprocal counter strike … This means that we are prepared and will use nuclear weapons only when we know for certain that some potential aggressor is attacking Russia, our territory" (Russian Federation 2018a). This is additionally consistent with previous iterations of Russian nuclear policy, which has largely remained unchanged since President Putin came to power in 2000 (Russian Federation 2014, 2010). Although some initial reports interpreted Putin's 2018 Valdai Club comments to mean that Russia might be adopting a nuclear no-first-use policy, this does not seem to be the case; his remarks were more likely meant to respond to the US Nuclear Posture Review's claim that Russia has lowered its threshold for first use of nuclear weapons in a conflict (Stowe-Thurston, Korda, and Kristensen 2018). Because Putin's comments imply that Russia would only use nuclear weapons in retaliation against an existential threat, independent analysts have challenged the Nuclear Posture Review's characterization of the Russian strategy as overblown and a misreading of Russia's nuclear doctrine.[2]

Whatever Russia's nuclear strategy is, Russian officials have made many statements about nuclear weapons that appear to go beyond the published doctrine, threatening to potentially use them in situations that do not meet the conditions described. For example, officials explicitly threatened to use nuclear weapons against ballistic missile defense facilities, and in regional scenarios that do not threaten Russia's survival or involve attacks with weapons of mass destruction (The Local 2015).

Moreover, the fact that Russian military planners are pursuing a broad range of upgraded and new versions of nuclear weapons suggests that the real doctrine goes beyond basic deterrence and toward regional war-fighting strategies, or even weapons aimed at causing terror. One widely-cited example involves the so-called Status-6—known in Russia as "Poseidon" and in the United States as "Kanyon"—a long-range nuclear-powered torpedo that a Russian government document described as intended to create "areas of wide radioactive contamination that would be unsuitable for military, economic, or other activity for long periods of time" (Podvig 2015). A diagram and description of the proposed weapon, first revealed in a Russian television broadcast, can still be seen on YouTube (YouTube 2015). The weapon, which is under development, appears designed to attack harbors and cities to cause widespread indiscriminate collateral damage in violation of international law.

Intercontinental ballistic missiles

Russia's Strategic Rocket Force currently deploys several variants of silo-based and mobile ICBMs. The silo-based ICBMs include the SS-18, SS-19, SS-27 Mod 1, SS-27 Mod 2, and the mobile ICBMs include the SS-25, SS-27 Mod 1, and SS-27 Mod 2. In December 2021, Chief of the General Staff Valery Gerasimov declared that 95 percent of Russia's strategic missile forces are continuously ready for combat use (RIA Novosti 2021a). In December 2021, the commander of the country's Strategic Rocket Forces, Col. Gen. Sergei Karakaev, stated in an interview with *Krasnay Zvezda* ("Red Star"), the official newspaper of the Russian Ministry of Defense, that the ratio between mobile and siloed launchers in each regiment is "approximately equal;" however, the number of nuclear warheads assigned to each silo-based missile regiment is "currently somewhat larger" than the mobile regiments because of the siloed SS-18 ICBM, which can carry large numbers of multiple independently targetable reentry vehicles (MIRVs). In total, the ICBMs carry about 60 percent of Russian deployed strategic warheads (*Krasnaya Zvezda* 2021a).

Based on what we can observe via satellite images, combined with information published under New START by various US government sources, Russia appears to have approximately 400 nuclear-armed ICBMs, which we estimate can carry up to 1,185 warheads (see Table 1). The size of the force that we can observe, however, is difficult to square with statements made by Russian officials. Since 2016, and again most recently in December 2019, Karakaev has stated to Russian news agencies such as TASS that Russia had approximately 400 ICBMs on combat duty (TASS 2016a; Andreyev and Zotov 2017; Karakaev 2019). But since Russia declared 527 deployed strategic launchers in total as of September 2021, a force of 400 ICBMs would mean Russia only deployed 127 SLBMs and bombers, which seems unlikely (US State Department, Bureau of Arms Control, Verification and Compliance 2021a). It is possible that Karakaev is referring to all ICBMs in the inventory (including those in storage), not just those that are deployed. Modernization of the ICBM force also involves equipping upgraded silos with new air- and perimeter-defense systems, and the new Peresvet laser has been deployed with at least five road-mobile ICBM divisions for the

purpose of "covering up their maneuvering operations" (Russian Federation Defense Ministry 2019a; Sanders 2021).

Table 2. Estimated status of Russian ICBM forces, 2022

Locations	Divisions	Regiments	Launchers*	Status
Barnaul	35th MD	307th MR (53.3128, 84.5080)	9 SS-27 Mod 2 TEL[1]	Active
		479th GMR (53.7709, 83.9580)	9 SS-27 Mod 2 TEL	Active
		480th MR (53.3054, 84.1459)	9 SS-27 Mod 2 TEL	Active
		867th GMR (53.2255, 84.6706)	(9 SS-27 Mod 2 TEL)	Upgrading
Dombarovsky	13th MD[2]	368th MR (51.0934, 59.8446)	6 SS-18 silos	Active
		494th MR (51.0628, 60.2119)	6 SS-18 silos	Active
		767th MR (51.2411, 60.6069)	6 SS-18 silos	Active
		621st MR (51.0618, 59.6081)	6 SS-19 Mod 4 silos[3]	Active
Irkutsk	29th GMD	92nd GMR (52.5085, 104.3933)	9 SS-27 Mod 2 TEL	Active
		344th GMR (52.6694, 104.5199)	9 SS-27 Mod 2 TEL	Active
		586th GMR (52.5505, 104.1584)	9 SS-27 Mod 2 TEL	Active
Kozelsk	28th GMD	74th MR (53.7982, 35.8039)	10 SS-27 Mod 2 silos	Active
		168th MR (54.0278, 35.4589)	10 SS-27 Mod 2 silos	Active
		214th MR (53.7641, 35.4866)	(2 SS-27 Mod 2 silos)	Upgrading
Novosibirsk	39th GMD	357th GMR (55.3270, 82.9417)	9 SS-27 Mod 2 TEL	Active
		382nd GMR (55.3181, 83.1676)	9 SS-27 Mod 2 TEL	Active
		428th GMR (55.3134, 83.0291)	9 SS-27 Mod 2 TEL	Active
Nizhny Tagil	42nd MD	308th MR (58.2298, 60.6773)	9 SS-27 Mod 2 TEL	Active
		433rd MR (58.1015, 60.3592)	9 SS-27 Mod 2 TEL	Active
		804th MR (58.1372, 60.5366)	9 SS-27 Mod 2 TEL	Active
Tatishchevo	60th MD[4]	31st MR (51.8792, 45.3368)	10 SS-27 Mod 1 silos	Active
		104th MR (51.6108, 45.4970)	10 SS-27 Mod 1 silos	Active
		122nd MR (52.1589, 45.6404)	10 SS-27 Mod 1 silos	Active
		165th MR (51.8062, 45.6550)	10 SS-27 Mod 1 silos	Active
		322nd MR (52.0449, 45.4458)	10 SS-27 Mod 1 silos	Active
		626th MR (51.7146, 45.2278)	10 SS-27 Mod 1 silos	Active
Teykovo	54th GMD	235th GMR (56.7041, 40.4403)	9 SS-27 Mod 1 TEL	Active
		285th GMR (56.8091, 40.1710)	9 SS-27 Mod 2 TEL	Active
		321st MR (56.9324, 40.5440)	9 SS-27 Mod 1 TEL	Active
		773rd MR (56.9167, 40.3087)	9 SS-27 Mod 2 TEL	Active
Uzhur[5]	62nd MD	229th MR (55.2453, 89.9194)	6 SS-18 silos	Active
		269th MR (55.2077, 90.2526)	6 SS-18 silos	Active
		302nd MR (55.1147, 89.6311)	(6 SS-29 silos)	Upgrading
		735th MR (55.2720, 89.5783)	10 SS-18 silos	Active
Vypolsovo	7th GMD	41st MR (57.8620, 33.6500)	(9 SS-27 Mod 2 TEL)	Upgrading[6]
		510th GMR (57.7889, 33.8660)	9 SS-25 TEL	Active
Yoshkar-Ola	14th MD	290th MR (56.8328, 48.2370)[7]	9 SS-27 Mod 2 TEL	Active
		697th MR (56.5601, 48.2144)	9 SS-27 Mod 2 TEL	Active
		779th MR (56.5821, 48.1550)[8]	9 SS-27 Mod 2 TEL	Active
11 Nuclear ICBM Divisions		**39 regiments**	**306 ICBMs[9]**	
Yurya	4th MD	76th MR (59.21946, 49.4256)	9 SS-25 TEL[10]	Active; non-nuclear
12 Total ICBM Divisions		**40 regiments**	**315 ICBMs**	

GMD = Guards Missile Division; GMR = Guards Missile Regiment; MD = Missile Division; MR = Missile Regiment; TEL = Transporter Erector Launcher

* Uses US/NATO missile designations. SS-18 (RS-20 V), SS-19 (RS-18), SS-25 (Topol), SS-27 Mod 1 (Topol-M), SS-27 Mod 2 (RS-24).

Table 2. Estimated status of Russian ICBM forces, 2022 (view PDF for full table with notes)

The ICBMs are organized under the Strategic Rocket Forces in three missile armies with a total of 12 divisions consisting of approximately 40 missile regiments (see Table 2). The regiment in the missile division at Yurya operates ICBMs that are believed to serve as a back-up launch code transmitter and are therefore not nuclear-armed. The ICBM force has been declining in number for three decades, and Russia claims to be 83 percent of the way through a modernization program to replace all Soviet-era missiles with newer types by the early 2020s on a less-than-one-for-one basis (*Krasnaya*

Zvezda 2021a). Currently, the remaining Soviet-era ICBMs include the SS-18 and the SS-25. According to Col. Gen. Karakaev, 36 missile regiments are now equipped with modern strategic missile systems—20 of which are mobile regiments and 16 of which are siloed regiments (*Krasnaya Zvezda* 2021a). However, Karakaev may be including siloed regiments which are currently undergoing infrastructure upgrades to prepare them for future Sarmat deployments. In 2022, Russia plans to place four more missile regiments on combat duty, which will amount to a scheduled increase of 21 launchers: the first SS-X-29 Sarmat regiment at Uzhur, one silo-based SS-19 Mod 4 Avangard regiment at Dombarovsky, and two mobile SS-27 Mod 2 Yars regiments in Vypolsovo and in the Kirov region, possibly at Yurya (*Krasnaya Zvezda* 2021a; Russian Federation 2021a).

The SS-18 (RS-20 V or R-36 M2 Voevoda) is a silo-based, 10-warhead heavy ICBM first deployed in 1988. It is reaching the end of its service life, with approximately 40 SS-18s that can carry up to 400 warheads remaining in the 13th Missile Division at Dombarovsky and the 62nd Missile Division at Uzhur. We estimate that the number of warheads on each SS-18 has been reduced for Russia to meet the New START limit for deployed strategic warheads. The SS-18 is scheduled to formally begin retiring in 2022, when the SS-X-29 (Sarmat or RS-28) ICBM will begin to replace it at the Uzhur missile field (*Krasnaya Zvezda* 2021a). Commercial satellite imagery indicates that the 302nd Missile Regiment at Uzhur has already been disarmed in order to accommodate for Sarmat-related upgrades to the regiment's silos (Figure 1).

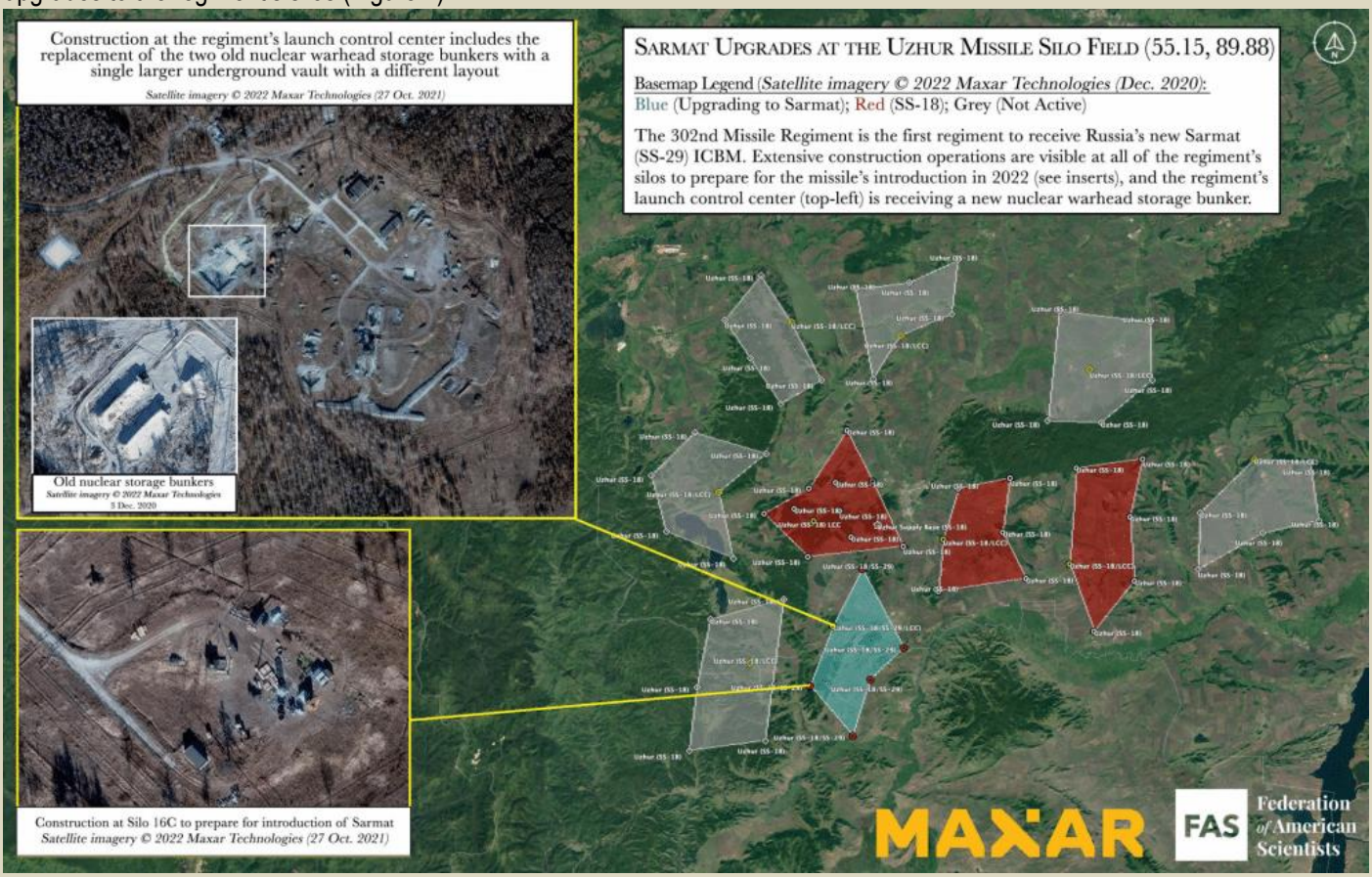


Figure 1. Upgrade of SS-18 silos at Uzhur ICBM division began in 2021 in preparation for conversion to the new SS-29 (RS-28, Sarmat) missile. Satellite imagery © 2022 Maxar Technologies.

The silo-based, six-warhead SS-19 (RS-18 or UR-100NUTTKh), which entered service in 1980, appears to have been retired from combat duty. A small number of converted SS-19s are being deployed with two regiments of the 13th Missile Division at Dombarovsky as the SS-19 Mod 4 with the new Avangard hypersonic glide vehicles (see below). In October 2021, Russian officials announced that the service life of the SS-19 had been extended until at least 2023; this is probably to allow the missile's boosters to be used for the Mod 4 Avangard deployment (RIA Novosti 2021b).

Russia continues to retire its SS-25 (RS-12 M or Topol) road-mobile missiles at a rate of one or two regiments (nine to 18 missiles) each year, replacing them with the SS-27 Mod 2 (RS-24). Eighteen SS-25s were scheduled to be dismantled by November 2022 (*Weaponews* 2017; RIA Novosti 2020b). There remains some uncertainty about how many SS-25s are fully operational. Garrison upgrades used to involve significant rebuilding, but satellite images indicate that

Russia has started to upgrade the garrisons by simply replacing the SS-25s with the new SS-27 launchers and their service vehicles, which are maintained under camouflage nets. We estimate that as few as nine SS-25s remain in the active force, and it is believed that the last SS-25 missile will be removed from service by the end of 2024 (TASS 2021b).

The new ICBMs include two versions of the SS-27: the Mods 1 and 2. We estimate that these two versions now carry more warheads than all the remaining SS-18s. The SS-27 Mod 1 is a single-warhead missile, known in Russia as Topol-M, that comes in either mobile (RS-12 M1) or silo-based (RS-12 M2) variants. Deployment of the SS-27 Mod 1 was completed in 2012 with a total of 78 missiles: 60 silo-based missiles with the 60th Missile Division in Tatishchevo, and 18 road-mobile missiles with the 54th Guards Missile Division at Teykovo. Russian officials indicated in 2019 that the Topol-M units eventually will be upgraded to RS-24 Yars as well.

The focus of the current and larger phase of Russia's modernization is the SS-27 Mod 2, known in Russia as the RS-24 (Yars), which is a modified SS-27 Mod 1 (or Topol-M) that can carry up to four multiple independently targetable reentry vehicles (MIRVs). During an interview with Col. Gen. Sergei Karakaev in December 2020, the Russian Defense Ministry's TV channel declared that approximately 150 mobile- and silo-based Yars had been deployed by the Strategic Rocket Force (Zvezda 2020). We estimate that as of January 2022, this number has grown to approximately 173 mobile- and silo-based Yars missiles. SS-27 Mod 2 upgrades now appear to be complete at the 39th Guards Missile Division at Novosibirsk, the 42nd Missile Division at Nizhny Tagil, the 14th Missile Division at Yoshkar-Ola, and the 29th Guards Missile Division at Irkutsk. Although these divisions now all have been equipped with the SS-27 Mod 2, some of the garrisons are not equipped to accommodate all the vehicles required to support the launchers and will continue to undergo construction for several years. After several years of temporarily basing the 382nd Guards Missile Regiment at a temporary open-air location, commercial satellite imagery now indicates that the possible permanent garrison is nearing completion (Figure 2).

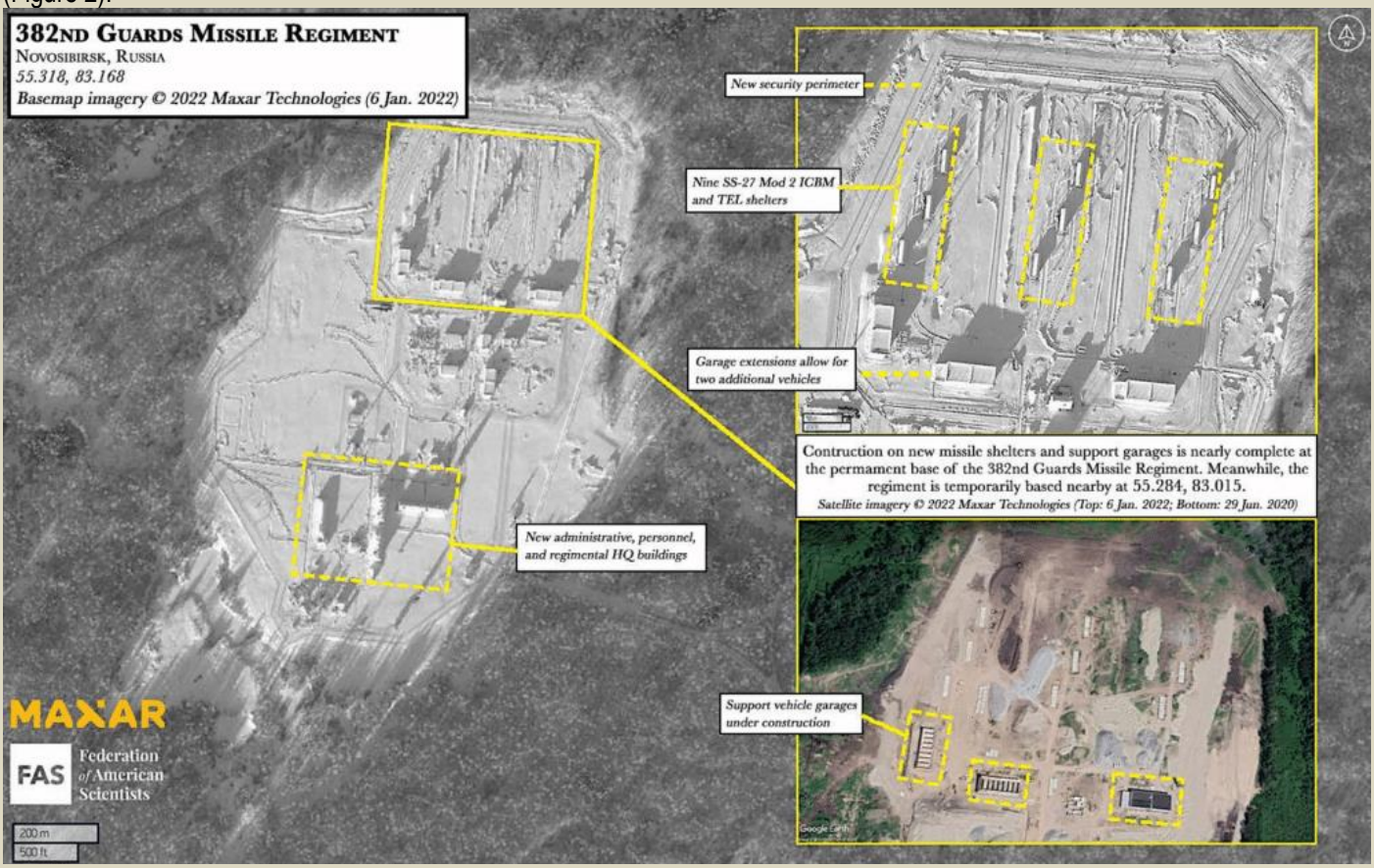


Figure 2. Construction of a new SS-27 Mod 2 (RS-24, Yars) garrison at the Novosibirsk road-mobile ICBM division is nearly complete. Satellite imagery © 2022 Maxar Technologies.

The 35th Missile Division at Barnaul appears to be nearing completion of its rearmament to the SS-27 Mod 2. The first regiment at Barnaul (the 479th Guards Missile Regiment) went on preliminary combat alert duty with the Yars in September 2019 and full combat duty in December 2019 (Russian Federation Defense Ministry 2019c). The Barnaul division formally accepted its second Yars regiment (the 480th Missile Regiment) in December 2020 (RIA

Novosti 2020a). In March 2021, Col. Gen. Karakaev announced that the entire Barnaul division would be re-armed with Yars ICBMs by the end of the year, and given that Karakaev did not include further plans for the Barnaul division in his 2022 rearmament schedule, it is possible that rearmament at this division is now largely complete (Russian Federation Defense Ministry 2021b).

The next mobile ICBM division to be upgraded is the 7th Missile Division at Vypolsovo. The Vypolsovo division, which is the smallest ICBM division with only 18 launchers, started early preparations for the upgrade in 2019 (Tikhonov 2019), and it is possible that one of its two regiments has already stood down its SS-25 launchers. In January 2022, the Russian Ministry of Defense announced that the Vypolsovo division would be rearmed with SS-27 Mod 2 missiles in 2022 (Interfax 2022).

The 28th Guards Missile Division at Kozelsk is the only silo division with SS-27 Mod 2 and continues to expand: the first regiment (the 74th Missile Regiment) officially began combat duty with its full complement of 10 missiles in November 2018, after initially being declared operational (likely with just six missiles) in 2015 (Russian Federation Defense Ministry 2018b). Satellite pictures show that upgrades of the second regiment (the 168th Missile Regiment) are complete, as was confirmed by Col. Gen. Karakaev at the end of 2020. (TASS 2020l). In December 2021, Col. Gen. Karakaev stated that the third missile regiment at Kozelsk (the 214th Missile Regiment) had been placed on combat alert; however, satellite imagery suggests that the necessary infrastructure upgrades have only taken place at a couple of silos and are still ongoing. His statement might indicate that a portion of the regiment has reached some prelimary readiness status. Given the time it took to complete the upgrades of the first two regiments at Kozelsk, it remains to be seen whether the Yars upgrade can be fully completed by 2024 as scheduled.

Apart from the missiles and silos themselves, the ICBM upgrade involves extensive modification of external fences, internal roads, and support facilities. Each site is also receiving a new "Dym-2" perimeter defense system including automated grenade launchers, small arms fire, and remote-controlled machine gun installations (*Krasnaya Zvezda* 2021a; Russia Insight 2018).

Final development and deployment of a compact SS-27 version, known as Rubezh (Yars-M or RS-26), appears to have been delayed at least until the next armament program in the late 2020s (TASS 2018a). A rail-based version known as Barguzin appears to have been canceled.

Russia is also developing the heavy SS-X-29, or Sarmat (RS-28), which will begin replacing the SS-18 (RS-20V) at Uzhur in 2022. Three ejection tests were conducted in December 2017, March 2018, and May 2018 at the Plesetsk Space Center, involving the cold launch and test firing of the Sarmat's first stage and booster engine. The closing test stages, which will include a test launch with the 62nd Missile Division at Uzhur, were supposed to be completed by the end of 2020; however, this has been continuously delayed, partly due to a manufacturing delay for the missile's command module (War Bolts 2022). The first Sarmat flight test is now scheduled for the first quarter of 2022 at the new Severo-Yeniseysky proving ground (TASS 2021a) and will be followed by several more tests. If these tests are successful, Sarmat will officially be handed over to the military and serial production will begin. As of March 2020, Sarmat's industrial production line reportedly had completed all the necessary upgrades to prepare for serial production (TASS 2020a).

There are many rumors about the SS-X-29, which some in the media have dubbed the "Son of Satan" because it is a follow-on to the SS-18, which the United States and NATO designated "Satan"—presumably to reflect its extraordinary destructive capability. Rumors that the SS-X-29 could carry 15 or more MIRV warheads, though, seem exaggerated. We expect that it will carry about the same number as the SS-18 plus penetration aids. It is likely that a small number will be equipped to carry the Avangard hypersonic glide vehicle, which are currently being installed on a limited number of SS-19 Mod 4 boosters at Dombarovsky. If the SS-X-29 replaces all current SS-18s, it will be installed in a total of 46 silos of the three regiments at the Dombarovsky missile field and four regiments at the Uzhur missile field (six regiments of six missiles and one regiment of 10 missiles). In December 2020, Col. Gen. Sergei Karakaev announced that the first Sarmat missiles would be "put on alert" at Uzhur sometime in 2022 (*Krasnaya Zvezda* 2020a). It appears that the first regiment to receive Sarmat might be the 302nd Missile Regiment; upgrades to the regiment's silos are clearly visible on commercial satellite imagery, indicating that the regiment's SS-18s have already been removed (see Figure 1).

The new Avangard hypersonic glide vehicle is designed to evade missile defenses and is initially being fitted atop modified SS-19 missiles (SS-19 Mod 4) at Dombarovsky and possibly later on SS-X-29 missiles at Uzhur. Russia is currently deploying the new weapon at a rate of two per year: the first two missiles at Dombarovsky began combat duty on December 27th, 2019, followed by another two in December 2020 (TASS 2019f; Russian Federation Defense Ministry 2020a). The regiment received its final two missiles—achieving a full complement of six missiles—in December 2021 (Russian Federation 2021a). The first two missiles in the second Avangard regiment will reportedly be placed on combat duty in 2022 or 2023, with the entire regiment completing its rearmament by the end of 2027 to coincide with the completion of the current state armament program (*Krasnaya Zvezda* 2021a; TASS 2021c). Similar to the new silos at Kozelsk, the modified Dombarovsky silos appear to have some form of perimeter defense system.

In December 2021, Karakaev stated that "a new mobile ground-based missile system" is being developed (*Krasnaya Zvezda* 2021a). It is possible that this refers to the Osina-RV ICBM, a follow-on system reportedly derived from the Yars ICBM (War Bolts 2021). Flight

tests of the siloed system are expected within the next couple of years. Russia has also recently commenced work on its strategic "Kedr" project; however, it remains unclear whether Kedr refers to a specific type of next-generation ICBM, or whether it is the name of the overall campaign to develop a new suite of next-generation strategic missile systems (TASS 2021p).

While the 2018 Nuclear Posture Review anticipated that Russian missile forces will increase over time, the evidence for this still is not clear. The US National Air and Space Intelligence Center predicted in 2020 that "the number of missiles in the Russian ICBM force will continue to decrease because of arms control agreements, aging missiles, and resource constraints" (US Air Force 2020, 26). With the ongoing modernization, the force level will likely level out as the modernization program is completed, although the modernized force will be able to deliver more warheads if all the single-warhead Topol-M (SS-27 Mod 1) ICBMs are replaced with MIRVed Yars (SS-27 Mod 2).

According to Col. Gen. Karakaev, Russia has conducted more than 25 ICBM test launches over the past five years, and plans to conduct at least ten ICBM launches in 2022, indicating a significant increase in test frequency (*Krasnaya Zvezda* 2021a). The Strategic Rocket Force often test-launches its missiles to the Sary-Shagan test site in Kazakhstan. However, given that Kazakhstan is a state party to the Treaty on the Prohibition of Nuclear Weapons—which entered into force in January 2021—it is unclear whether the country will continue to allow Russia to use its test site at Sary-Shagan for its ICBM launches. Article 4(2) of the treaty notes that each state party must ensure "the elimination or irreversible conversion of all nuclear-weapons-related facilities" (United Nations 2017). This would necessarily include Sary-Shagan, which would be considered nuclear weapons-related infrastructure if it is still being used for ICBM testing. This means that Kazakhstan faces a tough decision over whether to fully comply with the treaty and risk souring relations with Russia, or whether to dilute its compliance. This potential compliance issue could be the reason why Russia is building a new proving ground for its Sarmat tests at Severo-Yeniseysky, a decision which was announced in December 2020 (Russian Federation 2020a).

Russia is also developing a nuclear-powered, ground-launched, nuclear-armed cruise missile, known as 9M730 Burevestnik (NATO's designation is SSC-X-9 Skyfall). This missile has faced serious setbacks: According to US military intelligence, it has failed nearly a dozen times since its testing period began in June 2016 (Panda 2019a). In November 2017, a failed test resulted in the missile being lost at sea, which required a substantial recovery effort (Macias 2018). A similar recovery effort in August 2019 resulted in an explosion that killed five scientists and two soldiers at Nenoksa; the explosion's connection to Skyfall was confirmed by US State Department officials in October 2019 (DiNanno 2019). Due to these setbacks, it is possible that the Burevestnik program has been put on pause; there were no declared tests of the system in 2020 or 2021 and, unlike other elements of Russia's nuclear forces, it was not mentioned in Defense Minister Shoigu's year-end remarks in either year. In August 2021, satellite imagery appeared to indicate that Russia was preparing for another test of the Burevestnik system at Novaya Zemlya; however, it is unclear whether such a test actually took place (Lewis 2021; Cohen 2021).

Submarines and submarine-launched ballistic missiles

The Russian Navy operates 10 nuclear-powered nuclear-armed ballistic missile submarines (SSBNs) of two classes: five Delta IV (Project 667BRDM) and five Borei (Project 955), two of which are improved Borei-A (Project 955A) submarines.[3] Each submarine can carry 16 SLBMs, and each SLBM can carry several MIRVs, for a combined maximum loading of approximately 800 warheads. However, not all of these submarines are fully operational, and the warhead loading on some of the missiles may have been reduced as part of New START implementation; the total number of warheads carried is possibly around 608.

For the next couple of years, the backbone of Russia's nuclear submarine force will continue to be the five third-generation Delta IVs built between 1985 and 1992, each equipped with 16 SLBMs. All Delta IVs are part of the Northern Fleet and based at Yagelnaya Bay (Gadzhiyevo) on the Kola Peninsula. Russia has upgraded the Delta IVs to carry modified SS-N-23 SLBMs, known as Layner (or Liner), each of which might carry four warheads (Podvig 2011). Normally three or four of the five Delta IVs are operational at any given time, with the other one or two in various stages of maintenance. In March 2021, three SSBNs—possibly two Delta IV SSBNs and one Borei SSBN—simultaneously surfaced alongside each other near the North Pole during Russia's "Umka-2021" major Arctic exercise (Russian Federation Defense Ministry 2021a). Russia previously possessed six Delta IV SSBNs, but in April 2021, defense sources suggested that one of Russia's Delta IV SSBNs—*Yekaterinburg (K-84)*—would be withdrawn from the Northern Fleet and decommissioned in 2022 after 36 years of service (TASS 2021f).

All remaining Delta III SSBNs have been withdrawn from strategic service. Two *(K-223 Podolsk* and *K-433 Svyatoy Georgiy Pobedonosets)* were decommissioned in 2018 (Podvig 2018), and the commander of the Russian Pacific Fleet submarine force, Vice-Admiral Vladimir Dmitriev said in late-2021 that the Delta III SSBN—*Ryazan (K-44)*—had been converted from a missile submarine cruiser to an attack (general-purpose) submarine (*Krasnaya Zvezda* 2021b).

Each Borei (Project 955/A) SSBN is armed with 16 SS-N-32 (Bulava) SLBMs that can carry up to six warheads each. It is possible that the missile payload has been lowered to four warheads each to meet the New START limit on deployed strategic warheads. In May 2018, one of the new boats, *Yuri Dolgoruki (K-535)*, salvo-fired four Bulavas as part of a test launch

(Russian Federation Defense Ministry 2018a). In December 2020, another Borei, *Vladimir Monomakh (K-551*), salvo-fired four Bulavas during a test launch from the Sea of Okhotsk—the 35th-38th tests of the Bulava SLBM, and the first Bulava launch from a Pacific Fleet submarine (Russian Federation Defense Ministry 2020b; Podvig 2020). Five Boreis are currently in service, with another five in various stages of construction, for a total of 10 planned Borei SSBNs. The first boat, *Yuri Dolgoruki*, is based at Yagelnaya in the Northern Fleet. The second boat, *Alexander Nevsky (K-550)*, arrived at its home base at Rybachiy near Petropavlovsk in September 2015, where it was joined by the third Borei, *Vladimir Monomakh (K-551)*, in September 2016.

The first of the improved Borei-A/II (Project 955A) SSBNs, and the fourth Borei submarine in total, *Knyaz Vladimir (K-549)*, was after much delay finally accepted into the Navy on June 12, 2020 (Russian Federation Defense Ministry 2020c).

The fifth Borei—*Knyaz Oleg (K-552)*—underwent hull pressure tests in November 2016 and was originally scheduled for delivery in 2018 but was delayed for several years before finally being launched in July 2020 (TASS 2020g). The boat began its sea trials in June 2021 and launched a MIRVed Bulava SLBM—the 39th Bulava test-launch—in October 2021 (TASS 2021d; Lindemann 2021). *Knyaz Oleg* was delivered to the Navy in December 2021 and will join the Pacific Fleet (Sevmash 2021a), bringing the total number of Borei SSBNs in the Pacific Fleet to three. Significant upgrades are underway at the Pacific SSBN base (see Figure 3).

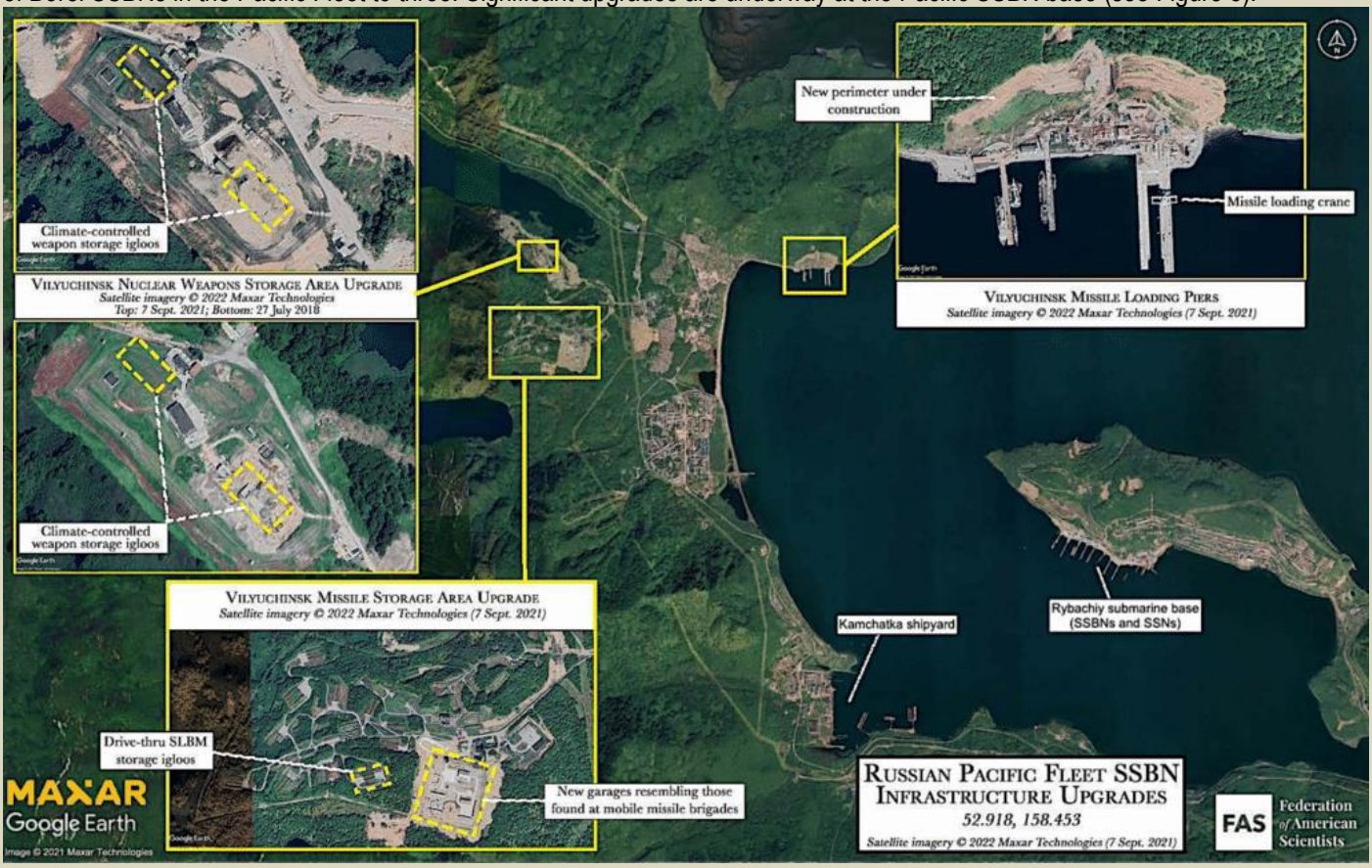


Figure 3. The Russian Pacific Fleet SSBN base complex on the Kamchatka Peninsula is undergoing extensive upgrades to accommodate new submarines and weapons. Satellite imagery © 2022 Maxar Technologies.

The keel of the sixth boat—*Generalissimus Suvorov*—was laid down in December 2014 for possible completion in 2018 but has also been delayed. In December 2020, Defense Minister Sergei Shoigu declared that the Navy was expected to receive the *Generalissimus Suvorov* in 2021 (Russian Federation 2020a). However, the boat was only launched in December 2021, meaning that it is not expected to be delivered to the Navy before December 2022 (Sevmash 2021b; Russian Federation 2021a).

The keel for the seventh boat—*Emperor Alexander III*—was laid down in December 2015 for scheduled delivery in 2019 but has also been delayed. It is now expected that the boat will be launched in December 2022, begin sea trials in the second half of 2023, and be delivered to the Navy's Pacific Fleet in December 2023 (TASS 2021e).

The keel for the eighth Borei SSBN—*Knyaz Pozharsky*—was laid in December 2016 for potential delivery between 2021 and 2023 (Russian Federation Defense Ministry 2016).

The keels for the ninth and tenth Borei SSBNs—*Dmitry Donskoy* and *Knyaz Potemkin*—were laid in August 2021 (Sevmash 2021c). Given that the *Dmitry Donskoy* shares its name with Russia's only remaining operational *Typhoon*-class SSBN—which now only operates

as a weapons testing platform—it seems likely that the older Typhoon SSBN will be removed from service before the delivery of the newer Borei SSBN. These two SSBNs are scheduled to be delivered by the completion of the State Armaments Program in 2027, bringing the total fleet up to 10 boats (Russian Federation 2021b). Eventually, five SSBNs will be assigned to the Northern Fleet, and five will be assigned to the Pacific (TASS 2018b).

In December 2020, Russia conducted its annual nuclear force readiness exercise, during which a Delta-IV SSBN launched a Sineva or Layner SLBM from the Barents Sea (Russian Federation Defense Ministry 2020f). In 2019, technical malfunctions during the strategic exercises prompted aborted launches—in the case of planned SLBM launches—or required the use of backup launch systems, in the case of 3M-54 Kalibr cruise missile launches (Sidorkova and Kanaev 2019).

The Russian Navy is also developing the Status-6 Poseidon mentioned above—a nuclear-powered, very long range, nuclear-armed torpedo. Underwater trials began in December 2018. The weapon is scheduled for delivery in 2027 and will be carried by specially configured submarines (TASS 2018f). The first of these special submarines—the Project 09852 *Belgorod* (K-329)—was launched in April 2019 and was originally scheduled for delivery to the Navy by the end of 2020; however, it only began sea trials in June 2021 and returned to dry dock in October 2021 (Sutton 2021a; Sutton 2021b). State trials are scheduled for 2022, which could indicate that delivery to the Navy could be delayed until late 2022 (TASS 2021o). *Belgorod* will become Russia's largest submarine and reportedly will be capable of carrying up to six Poseidon torpedoes (TASS 2019d). The launch of the second Poseidon-capable submarine—Project 09851 *Khabarovsk*—was expected to take place in the autumn of 2021, but appears to have been delayed until 2022 (TASS 2021g). *Khabarovsk* will reportedly also be capable of carrying up to six Poseidon torpedoes (TASS 2020b).

Strategic bombers

Russia operates two types of nuclear-capable heavy bombers: the Tu-160 Blackjack and the Tu-95MS Bear-H. We estimate that there are 60 to 70 bombers in the inventory, of which perhaps only 50 are counted as deployed under New START. Both bomber types can carry the nuclear AS-15 Kent (Kh-55) air-launched cruise missile and upgraded versions are being equipped to carry the new AS-23B (Kh-102) nuclear cruise missile. Two versions of the Tu-95 are thought to exist: Tu-95H6, which can carry up to six missiles internally, and Tu-95H16, which was built to carry missiles both internally and on wing-mounted pylons for a total of 16 missiles. The Tu-95 modernization program is equipping the Tu-95s to carry eight AS-23B missiles externally for a maximum of 14 missiles per aircraft. The Tu-160s are also being modernized to carry up to 12 AS-23B internally. The new AS-23B being added during bomber modernization will likely replace the AS-15.

It is unclear how many nuclear weapons are assigned to the heavy bombers. Each Tu-160 can carry up to 40,000 kilograms (about 44 tons) of ordnance, including 12 nuclear AS-15B air-launched cruise missiles. The Tu-95MS can carry six to 16 cruise missiles, depending on configuration. Combined, the bombers could potentially carry over 800 weapons, but we estimate weapons only exist for deployed bombers for a total of approximately 580 bomber weapons. The Tu-160 may also have a secondary mission with nuclear gravity bombs, but it seems unlikely that the old and slow Tu-95 would stand much of a chance against modern air defense systems.[4] According to Defense Minister Sergei Shoigu, Russian strategic bombers performed 50 flights on preset routes in 2020 (Russian Federation 2020a). Most of the nuclear weapons assigned to the bombers are thought to be in central storage, with only a couple hundred deployed at the two bomber bases. Modernization of the nuclear weapons storage bunker at Engels Air Base continues.[5]

The aging Tu-160s and most of the Tu-95MSs have also been undergoing various minor upgrades for several years. The first seven upgraded Tu-160s and Tu-95MSs returned to service in 2014, another nine followed in 2016, and five more were added in 2018. Only a few dozen of the Tu-95MSs—perhaps around 44—will be modernized, while at least 10 Tu-160s were slated to be modernized by 2019, although there has been some delay. Two additional Tu-160s and five Tu-95MS bombers were reportedly upgraded in 2020, followed by four additional Tu-95MS bombers in 2021 (Russian Federation 2020a; Russian Federation 2021a).

In addition to these minor upgrades, Russia is conducting a significant modernization campaign for its aging Tu-160 force; however, there is some confusion with regards to the nomenclature of the upgraded planes, with various news outlets using Tu-160, Tu-160M, Tu-160M1, and Tu-160M2 designations interchangeably. It appears that there are two distinct modernization programs for the Tu-160 taking place simultaneously: one program involving a "deep modernization" of existing Tu-160 airframes to incorporate next-generation engines, as well as new avionics, navigation, and radar systems, and another program involving the incorporation of similar next-generation systems onto completely new airframes (*Krasnaya Zvezda* 2020b; Butowski 2016; TASS 2018g).

The first public flight of the Tu-160M (sometimes referred to as Tu-160M1) prototype with its older engine was conducted in January 2018 at the Gorbunov Aviation Factory in Kazan, during a visit by President Putin. Immediately after the visit, a 160 billion ruble contract (approximately $2.13 billion) was signed for the modernization of 10 "deeply modernized" Tu-160M aircraft using existing airframes by 2027 (Russian Federation 2018b). The Tu-160M "deep modernization" campaign appears to be separate from the Tu-160M2 project, which requires serial production of completely new airframes in order to accommodate the 50-aircraft order made by the Russian Aerospace Force. During Putin's

2018 factory visit in Kazan, he described the requirement for the new aircraft: "The older version of this plane was discontinued in 1993. In 2015, we decided to modernize it and resume production. This, in fact, is a completely different aircraft, including avionics and everything else. […] It may look the same, but the engine, the flight range and the capacity are different" (Russian Federation 2018b).

Both the Tu-160M and Tu-160M2 aircraft will reportedly include a new engine—the NK-32-02—that is said to increase the aircraft's range by approximately 1,000 kilometers, or about 621 miles (TASS 2017). The Tu-160M's first flight with its older engine was conducted in February 2020, and the aircraft's first flight with its next-generation engine took place in November 2020, although the United Aircraft Corporation declined to show pictures of the November test flight due to classification concerns, instead electing to couple its announcement with pictures of an older version of the plane (United Aircraft Corporation 2020). A second Tu-160M, converted from an older Tu-160 airframe, began ground tests at the Gorbunov factory in December 2020 (TASS 2020e). In January 2019, Defense Minister Sergei Shoigu announced that the first Tu-160M aircraft would be delivered to the Russian Aerospace Force in 2021; however, this has been postponed by at least a year (Russian Federation Defense Ministry 2019b; Russian Federation 2020a). In December 2021, Defense Ministry Shoigu announced plans to deliver two Tu-160M bombers to the Russian Air Force in 2022 (Russian Federation 2021a).

The first newly-manufactured Tu-160M2 bomber conducted its maiden flight in January 2022 (United Aircraft Corporation 2022). The Tu-160M2 is expected to include a communications suite drawn from the fifth-generation Su-57 fighter (TASS 2020c, 2020g). It is possible that the eventual target of 50 new Tu-160M2 bombers might be exaggerated, but if it is accurate, it would probably result in the retirement of most, if not all, of the remaining Tu-95MSs, which are expected to be retired no later than 2035.

The Tu-160 modernization program, meanwhile, is only a temporary bridge to the next-generation bomber known as PAK-DA, the development of which has been underway for several years. The Russian government signed a contract with manufacturer Tupolev in 2013 to construct the PAK-DA at the Kazan factory. Research and development work on the PAK-DA has reportedly been completed, and the aircraft is expected to share many systems with the Tu-160M2 (TASS 2019h). Construction of the first aircraft's cockpit reportedly began in the spring of 2020, and final assembly has been postponed from 2021 to 2023 in advance of flight trials (TASS 2020f; TASS 2021h). Preliminary tests of the PAK-DA are scheduled for April 2023 (to be completed by fall 2025), and state tests are scheduled for February 2026. Initial production is expected to begin in 2027, with serial production beginning in 2028 or 2029 (Izvestia 2020; TASS 2019a). However, it is unclear whether the Russian aviation industry has enough capacity to develop and produce two strategic bombers at the same time, and as such this development schedule could face delays.

Nonstrategic nuclear weapons

Russia is updating many of its shorter-range, so-called "nonstrategic" nuclear weapons and introducing new types. This effort is less clear and comprehensive than the strategic forces modernization plan but also involves phasing out Soviet-era weapons and replacing them with newer but fewer weapons. New systems are being added, which prompted the Trump administration's Nuclear Posture Review to accuse Russia of "increasing the total number of [nonstrategic nuclear] weapons in its arsenal, while significantly improving its delivery capabilities" (US Defense Department 2018, 9). In the longer term, though, the emergence of more advanced conventional weapons could potentially result in reduction or retirement of some existing nonstrategic nuclear weapons.

Regardless of the number, the Russian military continues to attribute importance to nonstrategic nuclear weapons for use by naval, tactical air, and air- and missile-defense forces, as well as on short-range ballistic missiles. Part of the rationale is that nonstrategic nuclear weapons are needed to offset the superior conventional forces of NATO and particularly the United States. Russia also appears to be motivated by a desire to counter China's large and increasingly capable conventional forces in the Far East, and by the fact that having a sizable inventory of nonstrategic nuclear weapons helps Moscow keep overall nuclear parity with the combined nuclear forces of the United States, the United Kingdom, and France.

After the 2018 Nuclear Posture Review was published, defense sources distributed inaccurate and exaggerated information in Washington that attributed nuclear capability to several Russian systems that had either been retired or were not, in fact, nuclear. Moreover, although the Nuclear Posture Review claims that Russia has increased its nonstrategic nuclear weapons over the past decade, the inventory has in fact declined significantly—by about one-third—during that period (Kristensen 2019). Moreover, although the Trump Nuclear Posture Review stated that Russia has "up to 2,000" nonstrategic nuclear weapons and defense officials frequently have claimed it has more than 2,000, the US Defense Intelligence Agency's Worldwide Threat Assessment in 2021 stated that "Russia probably possesses 1,000 to 2,000 nonstrategic nuclear warheads" (US Defense Intelligence Agency 2021, 54). The range reflects difference estimates within the US intelligence community; the military uses the higher number. Rumors emerged in early-2022 that some in the Intelligence Community believe the number of Russian non-strategic nuclear weapons could increase significantly—potentially doubling—by 2030 (Bender 2022, Kristensen 2022).[6]

We estimate that Russia today has approximately 1,912 nonstrategic nuclear warheads, potentially fewer, assigned for delivery by air, naval, ground, and various defensive

forces. Although there are many rumors about additional nuclear systems, there is little authoritative public information available. This estimate, and the categories of Russian weapons that we have been describing in the Nuclear Notebook for years, was echoed by the Nuclear Posture Review, which stated:

"Russia is modernizing an active stockpile of up to 2,000 nonstrategic nuclear weapons, including those employable by ships, planes, and ground forces. These include air-to-surface missiles, short range ballistic missiles, gravity bombs, and depth charges for medium-range bombers, tactical bombers, and naval aviation, as well as anti-ship, anti-submarine, and anti-aircraft missiles and torpedoes for surface ships and submarines, a nuclear ground-launched cruise missile in violation of the 1987 Intermediate-Range Nuclear Forces Treaty, and Moscow's antiballistic missile system (US Defense Department 2018, 53)."

The Nuclear Posture Review also said:

"Russia possesses significant advantages in its nuclear weapons production capacity and in nonstrategic nuclear forces over the US and allies. It is also building a large, diverse, and modern set of nonstrategic systems that are dual-capable (may be armed with nuclear or conventional weapons). These theater- and tactical-range systems are not accountable under the New START Treaty and Russia's nonstrategic nuclear weapons modernization is increasing the total number of such weapons in its arsenal, while significantly improving its delivery capabilities. This includes the production, possession, and flight testing of a ground-launched cruise missile in violation of the Intermediate-Range Nuclear Forces Treaty. Moscow believes these systems may provide useful options for escalation advantage. Finally, despite Moscow's frequent criticism of US missile defense, Russia is also modernizing its long-standing nuclear-armed ballistic missile defense system and designing a new ballistic missile defense interceptor (US Defense Department 2018, 9)."

These paragraphs constituted the first substantial official US public statement on the status and composition of the Russian nonstrategic nuclear arsenal in more than two decades, even though the paragraphs also raise questions about assumptions and counting rules. Most of the nonstrategic weapon systems are dual-capable, which means not all platforms may be assigned nuclear missions, and not all operations are nuclear. Moreover, many of the delivery platforms are in various stages of overhaul and would not be able to launch nuclear weapons at this time.

Sea-based nonstrategic nuclear weapons

As far as we can ascertain, the biggest user of nonstrategic nuclear weapons in the Russian military is the navy, which we estimate has roughly 935 warheads for use by land-attack cruise missiles, anti-ship cruise missiles, anti-submarine rockets, anti-aircraft missiles, torpedoes, and depth charges. These weapons may be used by submarines, aircraft carriers, cruisers, destroyers, frigates, corvettes, and naval aircraft. This number may be lower because not all vessels with dual-capable weapon systems may actually be assigned nuclear warheads.

Major naval modernization programs focus on the next class of nuclear attack submarines, known in Russia as Project 885/M or Yasen/-M. The program is progressing very slowly. The first of these boats, known as *Severodvinsk*, finally entered service in 2015 after 16 years of construction and is thought to be equipped with a nuclear version of the Kalibr land-attack sea-launched cruise missile (the SS-N-30A) (Gertz 2015). It can also launch the SS-N-26 (3M-55) anti-ship/land-attack cruise missile, which the US National Air and Space Intelligence Center says is "nuclear possible" (US Air Force 2020, 36). The second boat, and the lead ship of the improved Yasen-M class—known as *Kazan*—was originally scheduled to join the Northern Fleet in late 2019 (TASS 2018c); however, the boat was delayed due to the poor results of its dockside trials, which indicated that "some of the ship's auxiliary sub-assemblies and mechanisms do not meet the requirements of the specifications set by the Defense Ministry" (TASS 2019b). The *Kazan* underwent sea trials in late 2020, successfully hitting a target over 1,000 kilometers (621 miles) away with a Kalibr cruise missile (TASS 2020h). The *Kazan* was delivered to the Navy in May 2021 and is now operational with the Northern Fleet (TASS 2021k). The next Yasen-M boat—the *Novosibirsk*—began sea trials in July 2021, was delivered to the Navy's Pacific Fleet in December 2021, and may become operational in 2022 (Manaranche 2021; Sevmash 2021a).

Six additional Yasen-M SSGNs—named *Krasnoyarsk, Arkhangelsk, Perm, Ulyanovsk, Voronezh,* and *Vladivostok*—are under various stages of construction. The *Krasnoyarsk* was launched in July 2021 and will likely conduct its sea trials in late 2022 (TASS 2021l). The five other boats were laid down in 2015, 2016, 2017, 2020, and 2020, respectively (RIA Novosti 2015; TASS 2016b; TASS 2020m).

The first Yasen submarine is reportedly 10 to 12 meters (about 33 to 39 feet) longer than the improved Yasen-M submarine and can therefore accommodate 40 Kalibr missiles, eight more than its successors (Gady 2018). The Yasen-M boats reportedly also have improved reactors and sonar systems, which may enhance their ability to evade detection (Kaushal et al. 2021).

In addition to dual-capable Kalibr land-attack cruise missiles, the Yasen-class submarines will also be able to deliver the SS-N-26 anti-ship cruise missile, SS-N-16 (Veter) nuclear anti-submarine rockets, as well as nuclear torpedoes. Additionally, in October 2021 the *Severodvinsk* successfully test-launched the Tsirkon hypersonic missile from surface and sub-surface positions—the first tests of the new system from a submarine (TASS 2021i).

According to Russian military officials, the Yasen-M submarines are able to salvo-launch several different types of missiles through the use of "universal launchers" that can accommodate multiple systems (Interfax 2021; TASS 2021j).
Other upgrades of naval nonstrategic nuclear-capable platforms include those planned for the Sierra class (Project 945), the Oscar II class (Project 949A), and the Akula class (Project 971). While the conventional version of the Kalibr is being fielded on a wide range of submarines and ships, the nuclear version will likely replace the current SS-N-21 nuclear land-attack cruise missile on select attack submarines. There is also speculation that Russia might consider building a new type of cruise missile submarine based on the Borei SSBN design, which would be called Borei-K. The Borei-Ks could potentially carry nuclear-armed cruise missiles instead of ballistic missiles, and if they were approved then they would be scheduled for delivery after 2027 (TASS 2019c). However, given that the incoming Yasen-M submarines are also capable of delivering nuclear-armed cruise missiles, there may be no need for a new type of SSGN.

Air-based nonstrategic nuclear weapons
The Russian Air Force is the military's second-largest user of nonstrategic nuclear weapons, with roughly 500 such weapons assigned for delivery by Tu-22M3 (Backfire) intermediate-range bombers, Su-24M (Fencer-D) fighter-bombers, the new Su-34 (Fullback) fighter bomber, and the MiG-31K. All types can deliver nuclear weapons. A total of four regiments are now equipped with the new Su-34, which is replacing the Su-24, with more than 125 aircraft delivered so far. Russia is also purchasing an additional 76 upgraded units of the Su-34M with improved avionics, resulting in a total future fleet of approximately 200 Su-34s (Lavrov and Krezul 2020).
The Tu-22M3 can also deliver Kh-22 (AS-4 Kitchen) air-launched cruise missiles, which is being replaced by an upgraded missile known as Kh-32. The Tu-22M3 and Su-24M are also being upgraded, and the new Tu-22M3M—which reportedly contains 80 percent entirely new avionics and shares a communications suite with the new Su-57 fighter—conducted its maiden flight in December 2018 (United Aircraft Corporation 2018; TASS 2020d). The second prototype of the upgraded Tu-22M3M conducted its first flight in March 2020, and has since conducted four additional flight tests—one of which tested the plane's resilience at supersonic speeds (TASS 2020i). The Tu-22M3M—in addition to the Tu-160M and future PAK-DA strategic bombers—will eventually be equipped with a new Kh-95 hypersonic missile, a prototype of which has reportedly already been tested (RIA Novosti 2021c).
It is possible that the Russian Air Force also has various types of other guided bombs, air-to-surface missiles, and air-to-air missiles with nuclear capability. If they exist, however, these systems would probably already be included in the Defense Intelligence Agency's estimate of 1,000-2,000 nonstrategic warheads.
Russia has also developed a new long-range, dual-capable, air-launched ballistic missile system known as the 9-A-7760 Kinzhal. The missile, which appears similar to the ground-launched SS-26 short-range ballistic missile used on the Iskander system, allegedly has a range of up to 2,000 kilometers (about 1,243 miles) if launched from a specially modified MiG-31K (Foxhound) designated as MiG-31IK, and up to 3,000 kilometers (about 1,864 miles) if launched from the Tu-22M3 bomber (the range is the combined combat range of the aircraft plus the missile). The MiG-31IK cannot carry both the Kinzhal and its regular air-to-air missiles and must therefore be deployed alongside a protective air detail (TASS 2018h). The Kinzhal could potentially be used against targets on both land and sea and has reportedly been deployed on experimental combat duty in the Southern Military District since December 2017 (TASS 2018d). The Kinzhal was publicly demonstrated for the first time in an airshow in August 2019, although it is unclear if the missile was actually fired during the competition (TASS 2019e). In December 2021, Defense Minister Shoigu announced that in 2021 "a separate aviation regiment was formed, armed with MiG-31IK aircraft with the Dagger hypersonic missile" (Russian Federation 2021a), apparently in the North Fleet area on the Kola Peninsula. Plans reportedly are underway to equip the Western and Central Military Districts with Kinzhal missiles by 2024 (Izvestia 2021, TASS 2021m).
Additionally, the Russian Aerospace Force reportedly received its first batch of Su-57 (PAK-FA) fighter jets in late 2020 (TASS 2020j). Four more were scheduled for delivery in 2021—although given program delays and setbacks it is unclear whether any of these delivered took place—and the delivery of 22 aircraft are scheduled by the end of 2024 (Suciu 2021). The full contract is expected to comprise 76 planes for delivery by the end of 2028 (TASS 2020k). The US Defense Department says that the Su-57s are nuclear-capable (US Defense Department 2018). They will reportedly also be equipped with hypersonic "missiles with characteristics similar to that of the Kinzhal" (TASS 2018e).

Nonstrategic nuclear weapons in missile defense
The 2018 Nuclear Posture Review also asserted that Russia continues to use nuclear warheads in its air and missile defense forces; however, the document did not identify which systems have dual-capability or how many are assigned nuclear warheads. The US Defense Intelligence Agency said in its March 2018 Worldwide Threat Assessment that: "Russia may also have warheads for surface-to-air and other aerospace defense missile systems" (Ashley 2018). Russia currently operates several different kinds of missile defense complexes for use against different tiers of threats. The

mobile S-300 and S-400 systems are designed for theater air and missile defense, and US government sources privately indicate that both the S-300 (SA-20) and S-400 (SA-21) are dual-capable.
Russia is developing several next-generation air and missile defense systems to supplement—and in some cases—replace its older systems. It appears that several of these systems, including the S-550, Nudol, and Aerostat, are expected to utilize conventional warheads rather than nuclear ones; however, their improved ranges and speeds will also likely offer them the capabilities to target satellites in orbit (Hendrickx 2021; TASS 2021n).
The A-135 antiballistic missile defense system around Moscow is equipped with 68 nuclear-tipped 53T6 Gazelle interceptors. An upgrade of the A-135 is underway, and it will be known as A-235 (*Krasnaya Zvezda* 2017); however, it remains unclear whether the A-235 system will use either nuclear or conventional warheads, or perhaps instead rely on kinetic hit-to-kill technology.
Russian officials said over a decade ago that about 40 percent of the country's 1991 stockpile of air defense nuclear warheads remained. Alexei Arbatov, then a member of the Russian Federation State Duma defense committee, wrote in 1999 that the 1991 inventory included 3,000 air defense warheads (Arbatov 1999). Many of those were probably from systems that had been retired, and US intelligence officials estimated that the number had declined to around 2,500 by the late 1980s (Cochran et al. 1989), in which case the 1991 inventory might have been closer to 2,000 air defense warheads. In 1992, Russia promised to destroy half of its nuclear air defense warheads, but Russian officials said in 2007 that 60 percent had been destroyed (Pravda 2007).
If those officials were correct, the number of nuclear warheads for Russian air defense forces might have been 800 to 1,000 a decade ago. Assuming that the inventory has shrunk further since 2007 (due to the improving capabilities of conventional air-defense interceptors and continued retirement of excess warheads), we estimate that nearly 290 nuclear warheads remain for air defense forces today, plus an additional roughly 90 for the Moscow A-135 missile defense system and coastal defense units, for a total inventory of about 380 warheads. However, it must be emphasized that this estimate comes with considerable uncertainty.

Ground-based nonstrategic nuclear weapons
Russian Defense Minister Sergei Shoigu announced in December 2019 that the upgrade of all army missile brigades to the 350-kilometer (217 mile) range SS-26 (Iskander) short-range ballistic missile had been completed (Russian Federation 2019), but construction continues at several bases two years later and not all have missile depots. This includes at least 12 brigades: four in the Western Military District; two in the Southern Military District; two in the Central Military District, and at least four in the Eastern Military District. Each brigade has 12 launchers, each with two missiles for a total of 24 missiles (at least one reload is in storage). In 2019, Izvestia quoted unnamed defense ministry sources saying that each brigade would receive an additional battalion so that each brigade in the future would have 16 launchers with 32 missiles (Izvestia 2019). We estimate that there are roughly 70 warheads for short-range ballistic missiles. There are also unconfirmed rumors that the SSC-7 (9M728 or R-500) ground-launched cruise missile may have nuclear capability.
The US government also says that Russia has developed and deployed a dual-capable ground-launched cruise missile in violation of the now-defunct Intermediate-Range Nuclear Forces Treaty. The missile is identified as the 9M729 (SSC-8) (US State Department 2019a). In 2018, former Director of National Intelligence Dan Coats said Russia initially tested the 9M729 to prohibited ranges from a fixed launcher, then tested it to permitted ranges from a mobile launcher (Office of the Director National Intelligence 2018). US Gen. Paul Selva, former vice chairman of the Joint Chiefs of Staff, however, told Congress in 2017 that the 9M729 deployment at that time did not give Russia a military advantage: "Given the location of the specific missiles and deployment, they don't gain any advantage in Europe" (Brissett 2017). After having denied the existence of a 9M729 missile, the Russian military in January 2019 displayed what it said was a launcher, missile canisters, and schematics of a missile named 9M729, but claimed its range was less than 500 kilometers, or about 311 miles (TASS 2019g). However, a US intelligence report on the display subsequently concluded that the event was a hoax: Neither the missile, nor its launch vehicle, nor the schematics shown were what Russia claimed them to be (Panda 2019b). The Trump administration in February 2019 formally announced that the United States would withdraw from the Intermediate-Range Nuclear Forces Treaty effective in six months (US State Department 2019b). On August 2, 2019, the Intermediate-Range Nuclear Forces Treaty officially died.
The first two 9M729 battalions were deployed in late 2017 (Gordon 2017), and US intelligence sources indicated in December 2018 that Russia had deployed four battalions in the Western, Southern, Central, and Eastern Military Districts with nearly 100 missiles (including spares) (Gordon 2019). We estimate that these four battalions are co-located with the Iskander sites at Elanskiy, Kapustin Yar (possibly moved to a permanent base by now, possibly in the Far East), Mozdok, and Shuya.
It is unknown if Russia has added 9M729 battalions beyond the four reported in December 2018. There is no public confirmation that it has, but in February 2019, only a few weeks after Russia acknowledged the existence of the 9M729 but claimed its range was legal, the press service of Russia's Western Military District reported it had carried out "electronic launches" of the 9M279 in the Leningrad region (RIA Novosti 2019). This could indicate the 9M729 has been added to a fifth brigade: the 26th Missile Brigade outside Luga about 125 kilometers (about 78 miles) south of St.

Petersburg. And in December 2019, Izvestia reported that the Russian military planned to add a fourth battalion to each existing Iskander brigade, each of which previously comprised three battalions of four launchers each (each launcher carries two missiles and probably two reloads) (Izvestia 2019). It remains to be seen if this means that 9M729 launchers will be added to all of Russia's 12 Iskander brigades; however, in October 2020 Putin declared his willingness to impose a moratorium on future 9M729 deployments in European territory, "but only provided that NATO countries take reciprocal steps that preclude the deployment in Europe of the weapons earlier prohibited under the [Intermediate-Range Nuclear Forces] Treaty" (Russian Federation 2020b).

Notes

1. We estimate that Russia stores its nuclear weapons at approximately 40 permanent storage sites across the country, including about 10 national-level central storage sites (Kristensen and Norris 2014, 2–9). Essential references for following Russian strategic nuclear forces include the general New START aggregate data that the US and Russian governments release biannually; BBC Monitoring; Pavel Podvig's website on Russian strategic nuclear forces (Podvig n.d.); and the Russia profile maintained by the James Martin Center for Nonproliferation Studies (2018) on the Nuclear Threat Initiative website.
2. For examples of such analyses, see Sokov (2020); Oliker (2018); Tertrais (2018); Oliker and Baklitskiy (2018); Bruusgaard (2016, 2017).
3. Three Typhoon-class (Project 941) submarines also remain afloat. One has been converted to a missile test platform. None of these submarines carries nuclear weapons.
4. One normally well-informed source says there are no nuclear gravity bombs for the Tu-95MS and Tu-160 aircraft (Podvig 2005).
5. Russia is also adding conventional cruise missiles to its bomber fleet, a capability that was showcased in September 2015 when Tu-160 and Tu-95MS bombers launched several long-range conventional Kh-555 and Kh-101 cruise missiles against targets in Syria. New storage facilities have been added to Russia's bomber bases over the past few years that might be related to the introduction of conventional cruise missiles.
6. A US government telegram stated in September 2009 that Russia had "3,000–5,000 plus" nonstrategic nuclear weapons (Hedgehogs.net 2010), a number that comes close to our estimate at the time (Kristensen 2009). The US deputy undersecretary of defense for policy, James Miller, stated in 2011 that nongovernmental sources estimated Russia might have 2,000 to 4,000 nonstrategic nuclear weapons (Miller 2011). For a more in-depth overview of Russian and US nonstrategic nuclear weapons, see Kristensen (2012). Some analysts estimate that Russia has significantly fewer warheads assigned to nonstrategic forces (Sutyagin et al. 2012).

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

Hans M. 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 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, and a BA in European Studies from the University of Toronto.

Ukraine building a nuclear bomb? Dangerous nonsense.

By Mariana Budjeryn and Matthew Bunn
Source: https://thebulletin.org/2022/03/ukraine-building-a-nuclear-bomb-dangerous-nonsense/

Mar 09 – The Kremlin is claiming that Ukraine is developing nuclear weapons. Like most of Russia's other pretexts for invading Ukraine, this is dangerous nonsense.
In his February 21 war speech, Russian President Vladimir Putin stated that Ukraine possesses delivery systems and nuclear technologies inherited from the Soviet Union and that, with foreign support, "it is only a matter of time" before Ukraine creates nuclear

weapons. Echoing this concern, Russian Foreign Minister Sergei Lavrov in his address to the Conference on Disarmament on March 1, alleged that Ukraine "started dangerous games related to plans to acquire their own nuclear weapons."
It is true that Ukraine's President Volodymyr Zelensky, in his February 19 speech at the Munich Security Conference, questioned whether Ukraine was obligated to retain its non-nuclear status. He argued that Russia had grossly violated its security promises to Ukraine in the so-called Budapest Memorandum that set the terms for Ukraine eliminating the nuclear weapons it inherited from the collapsed Soviet Union. As a result, Zelensky argued, the whole "package of decisions" in that deal, including Ukraine's non-nuclear status, were "in doubt."

(Rusted) Missile silo of a SS-24 missile, Strategic Missile Forces Museum in Ukraine. Credit: Michael. CC BY 3.0. Accessed via Wikipedia.

Prior to President Zelenksy's recent remark, other Ukrainian politicians have also called for Ukraine's withdrawal from the Nuclear Non-Proliferation Treaty (NPT) and reconsideration of its non-nuclear status. These statements referred to Russia's 2014 seizure of Crimea and instigation of a war in Ukraine's Donbas region, which blatantly violated Russia's commitments to respect Ukraine's sovereignty and territorial integrity pledged in the Budapest Memorandum.
These calls, however, yielded nothing thus far and are highly unlikely to result in a change of Ukraine's nuclear policy in the future. There are good reasons for this. Today, despite the Kremlin's allegations, Ukraine lacks most of the crucial capabilities necessary for the development of a nuclear weapons program. While Western military assistance is pouring into Ukraine, no one is going to help Ukraine build nuclear weapons, especially as doing so would be a clear violation of the NPT.

Nuclear material

The first point is that Ukraine does not have the needed nuclear material for a bomb or the facilities to produce it. All of the highly enriched uranium (HEU) that used to exist at research and training facilities in Ukraine, including at the Kharkiv Institute of Physics and Technology which Russia recently shelled, was removed cooperatively during the Obama-era nuclear security summit process. Ukraine has uranium deposits, but no conversion facility for turning them into uranium hexafluoride gas used in enrichment plants. It also has no enrichment plants to separate out the uranium-

235 used in weapons from the more than 99 percent uranium-238 in natural uranium. Building that set of facilities would take years and great expense.

The alternative path to the bomb is based on plutonium. There's a good deal of plutonium in the spent fuel from Ukraine's nuclear power reactors, but it is about one percent by weight in massive, intensely radioactive fuel assemblies. To use it in a bomb, Ukraine would need a "reprocessing" plant to chemically separate the plutonium from all the rest. Once again, that is a facility Ukraine does not have and would take years to build. The plutonium from power reactors is "reactor-grade," with a variety of undesirable isotopes that make it less than ideal for nuclear weapons, though still usable.

Nuclear warhead production

Even if Ukraine had the needed nuclear material, it would not be easy to turn it into nuclear weapons. Designing nuclear weapons requires specialized expertise. Ukraine has many experts in civilian nuclear matters, but 30 years after Ukraine's participation in the Soviet military-industrial complex, many of the weapons experts left over are no longer available. Today, Ukraine has modest remaining expertise in the many specialized technologies involved in nuclear weapons design and manufacture.

Nor does it have any of the relevant facilities for those purposes. The enriched uranium or plutonium would have to be converted into metal and fabricated into metal bomb components. Specialty conventional explosives would be needed to set off the bomb, along with detonators with precision timing and a variety of other components. Ukraine does not have facilities for these purposes, and these, too, would be expensive and time-consuming to build.

Delivery vehicles

The nuclear missiles left on Ukraine's territory when the Soviet Union collapsed were destroyed decades ago. Nevertheless, as President Putin noted, Ukraine has legacy Soviet industries capable of designing and producing weapons delivery systems, both aircraft and missiles. The Antonov design bureau and aircraft manufacturer in Kyiv are known for their cargo aircraft, including the largest airplane ever made, the **AN-225 Mriya**, that was recently destroyed on the airfield by a Russian strike. The Ukrainian city of

Dnipro is home to the Pivdenne Design Bureau, Pivdenmash, once the largest missile factory in the world, capable of producing ballistic missiles. Kyiv's Luch is the designer and manufacturer of guided missile systems. Today, however, Ukraine has no missiles or aircraft designed to deliver nuclear weapons. Its missile building has been reoriented toward space projects. New missiles or planes would have to be designed and built or existing ones modified.

Treaties and inspections

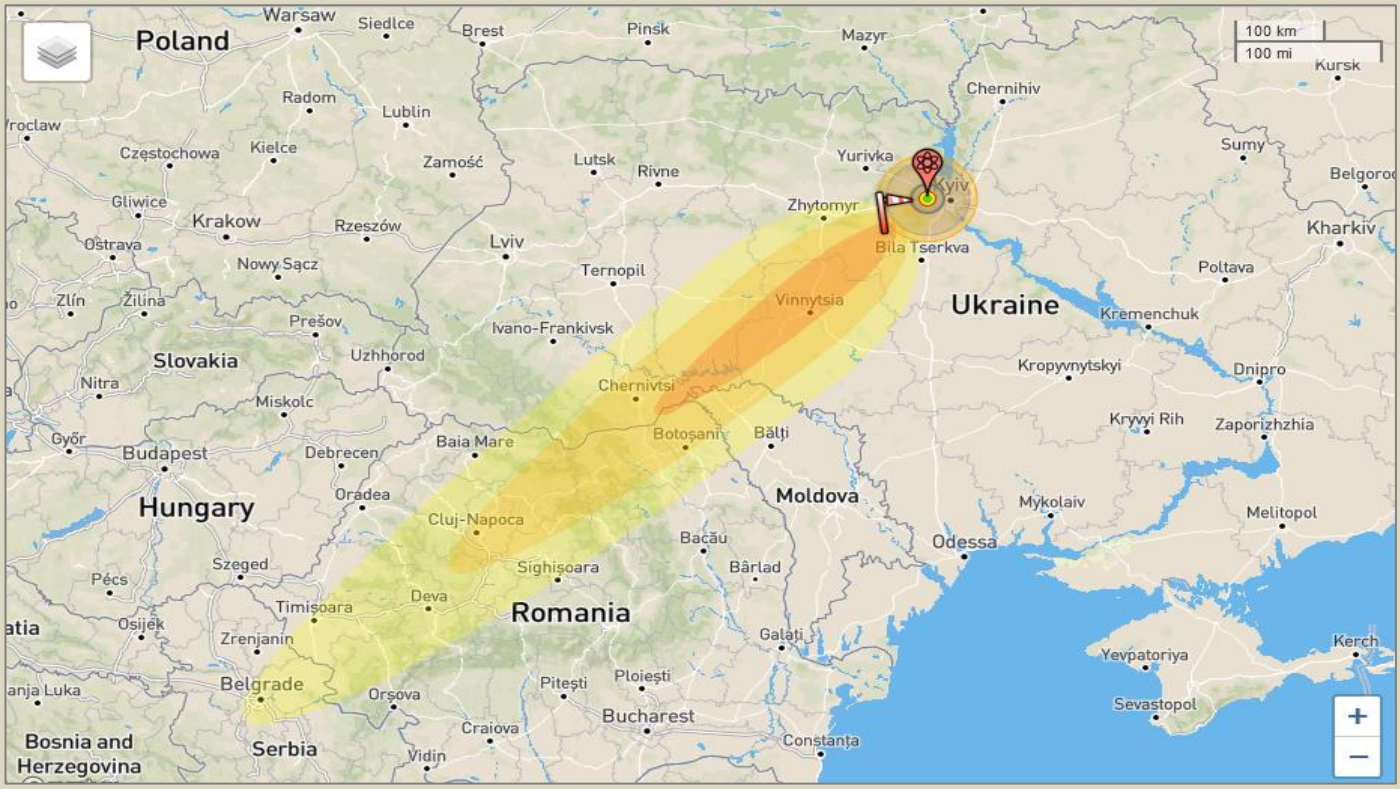
Beyond all that, Ukraine is committed by treaty not to build nuclear weapons, and all its nuclear facilities are under international inspection. To try to build nuclear weapons, Ukraine would have to either withdraw from the NPT and kick out the International Atomic Energy Agency (IAEA) inspectors or try to proceed in secret, evading the IAEA inspectors, a practice that ultimately proved unsustainable for other states. Either one of these paths would risk sanctions and international censure. Any Ukrainian attempt to launch a nuclear weapons program would lose it the critical support of its Western partners, including the United States, whose decades-long policy has been to thwart the spread of nuclear weapons around the world even by its allies, and on whose support Ukraine greatly relies in its defense against Russia.

With enough motivation, investment, time, and perseverance Ukraine could close the missing links and build a nuclear weapons program. But so could dozens of countries in the world. Even in the best of circumstances, such an undertaking would take years to bring to fruition—and would likely be found and stopped before succeeding. Now, with Russia's invasion, it's hard to imagine Ukraine being able to launch and sustain a nuclear weapons program. Today, as in the early 1990s when Ukraine was deliberating its nuclear choices, the costs of such an undertaking would far outweigh the benefits.

Mariana Budjeryn, PhD, is a research associate with the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science and International Affairs. Her forthcoming book *Inheriting the Bomb* explores the politics and history of Soviet nuclear collapse and Ukraine's nuclear disarmament.
Matthew Bunn is the James R. Schlesinger Professor of the Practice of Energy, National Security, and Foreign Policy at Harvard Kennedy School and the Co-Principal Investigator of the Project on Managing the Atom at Harvard Kennedy School's Belfer Center.

Tsar Bomba (50MT) dropped in Kiev – simulation

Source: https://nuclearsecrecy.com/nukemap/



Note: If you move the wind pole you can change the fallout

Effect distances for a 50 megaton surface burst:

● **Radiation radius** (500 rem): 5.05 km (80.2 km²)
500 rem ionizing radiation dose; likely fatal, in about 1 month; 15% of survivors will eventually die of cancer as a result of exposure.

● **Fireball radius:** 6.01 km (113 km²)
Maximum size of the nuclear fireball; relevance to damage on the ground depends on the height of detonation. If it touches the ground, the amount of radioactive fallout is significantly increased. Anything inside the fireball is effectively vaporized.

● **Heavy blast damage radius** (20 psi): 8.02 km (202 km²)
At 20 psi overpressure, heavily built concrete buildings are severely damaged or demolished; fatalities approach 100%. Often used as a benchmark for **heavy** damage in cities.

● **Moderate blast damage radius** (5 psi): 16.9 km (894 km²)
At 5 psi overpressure, most residential buildings collapse, injuries are universal, fatalities are widespread. The chances of a fire starting in commercial and residential damage are high, and buildings so damaged are at high risk of spreading fire. Often used as a benchmark for **moderate** damage in cities.

● **Light blast damage radius** (1 psi): 43.3 km (5,900 km²)

At a around 1 psi overpressure, glass windows can be expected to break. This can cause many injuries in a surrounding population who comes to a window after seeing the flash of a nuclear explosion (which travels faster than the pressure wave). Often used as a benchmark for **light** damage in cities.

● **Thermal radiation radius** (3rd degree burns): 51.4 km (8,290 km²)

Third degree burns extend throughout the layers of skin, and are often painless because they destroy the pain nerves. They can cause severe scarring or disablement, and can require amputation. 100% probability for 3rd degree burns at this yield is 13.6 cal/cm².

Estimated total-dose fallout contours for a 50 megaton surface burst (3% fission) with a 15 mph wind:

■ **Fallout contour for 1 rads per hour:**

- Maximum downwind cloud distance: 964 km
- Maximum width: 196 km
- Approximate area affected: 147,410 km²

■ **Fallout contour for 10 rads per hour:**

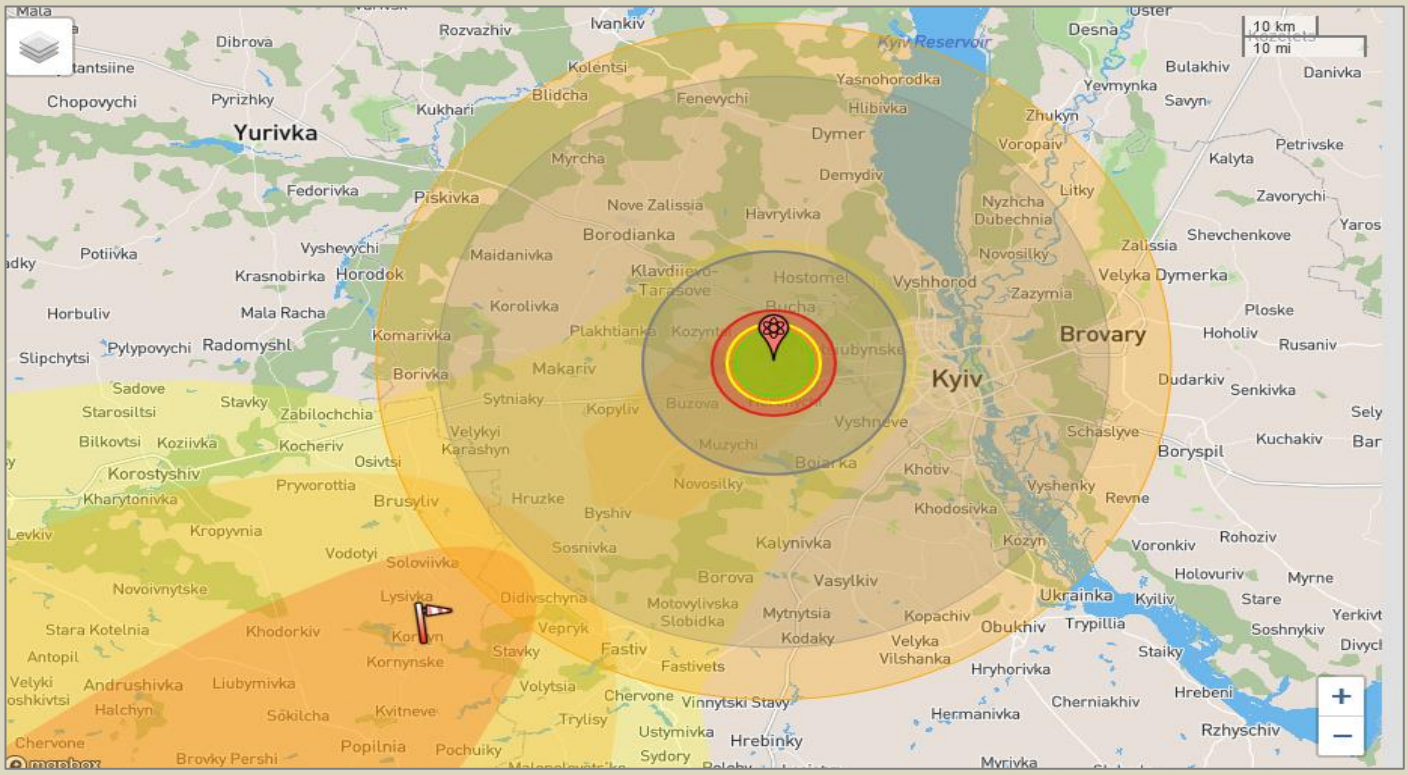
- Maximum downwind cloud distance: 675 km
- Maximum width: 126 km
- Approximate area affected: 66,380 km²

■ **Fallout contour for 100 rads per hour:**

- Maximum downwind cloud distance: 385 km
- Maximum width: 56.1 km
- Approximate area affected: 17,090 km²
- The selected radiation level is too high for stem fallout at this yield, and so this contour is not mapped. Maximum radiation contour for stem fallout that can be mapped for this yield is 56 r/hr.

■ **Fallout contour for 1,000 rads per hour:**

- The selected radiation level is too high for fallout at this yield, and so this contour is not mapped. Maximum radiation contour for cloud fallout that can be mapped for this yield is 634 r/hr; for stem fallout it is 56 r/hr.



Estimated fatalities: 483,580

Estimated injuries: 1,051,950

In any given 24-hour period, there are on average 2,905,669 people in the light (1 psi) blast range of the simulated detonation

This is how smaller atomic weapons could turn Ukraine into a nuclear war zone

Source: https://globalonlinemony.com/the-smaller-bombs-that-could-turn-ukraine-into-a-nuclear-war-zone/

A photo released by a Russian state-owned news agency showing an Iskander-M launch vehicle being loaded with a ballistic missile during military exercises at a Russian firing range in Ussuriysk in 2016. (Yuri Smityuk/TASS, via Getty Images)

Mar 22 – In damaging energy, the behemoths of the Chilly Warfare dwarfed the American atomic bomb that destroyed Hiroshima. Washington's largest take a look at blast was 1,000 instances as giant. Moscow's was 3,000 instances. On each side, the thought was to discourage strikes with threats of huge retaliation — with mutual assured destruction, or MAD. The psychological bar was so excessive that nuclear strikes got here to be seen as unthinkable.

At the moment, each Russia and america have nuclear arms which are a lot much less damaging — their energy simply fractions of the Hiroshima bomb's drive, their use maybe much less scary and extra thinkable.

Concern about these smaller arms has soared as Vladimir V. Putin, within the Ukraine battle, has warned of his nuclear may, has put his atomic forces on alert and has had his navy perform dangerous assaults on nuclear energy vegetation. The concern is that if Mr. Putin feels cornered within the battle, he may select to detonate one in every of his lesser nuclear arms — breaking the taboo set 76 years in the past after Hiroshima and Nagasaki.

Analysts observe that Russian troops have lengthy practiced the transition from typical to nuclear battle, particularly as a method to acquire the higher hand after battlefield losses. And the navy, they add, wielding the world's largest nuclear arsenal, has explored quite a lot of escalatory choices that Mr. Putin may select from.

"The possibilities are low however rising," stated Ulrich Kühn, a nuclear skilled on the College of Hamburg and the Carnegie Endowment for Worldwide Peace. "The battle shouldn't be going properly for the Russians," he noticed, "and the strain from the West is rising."

Mr. Putin may hearth a weapon at an uninhabited space as an alternative of at troops, Dr. Kühn stated. In a 2018 examine, he laid out a disaster situation during which Moscow detonated a bomb over a distant a part of the North Sea as a method to sign deadlier strikes to come back.

"It feels horrible to speak about these items," Dr. Kühn stated in an interview. "However we've got to contemplate that that is turning into a risk."

Washington expects extra atomic strikes from Mr. Putin within the days forward. Moscow is more likely to "more and more depend on its nuclear deterrent to sign the West and undertaking power" because the battle and its penalties weaken Russia, Lt. Gen. Scott D.

Berrier, director of the Protection Intelligence Company, informed the Home Armed Providers Committee on Thursday.
President Biden is touring to a NATO summit in Brussels this week to debate the Russian invasion of Ukraine. The agenda is predicted to incorporate how the alliance will reply if Russia employs chemical, organic, cyber or nuclear weapons.
James R. Clapper Jr., a retired Air Drive basic who served as President Barack Obama's director of nationwide intelligence, stated Moscow had lowered its bar for atomic use after the Chilly Warfare when the Russian military fell into disarray. At the moment, he added, Russia regards nuclear arms as utilitarian slightly than unthinkable.
"They didn't care," Mr. Clapper stated of Russian troops' risking a radiation launch earlier this month after they attacked the Zaporizhzhia nuclear reactor web site — the most important not solely in Ukraine however in Europe. "They went forward and fired on it. That's indicative of the Russian laissez-faire angle. They don't make the distinctions that we do on nuclear weapons."
Mr. Putin introduced final month that he was placing Russian nuclear forces into "particular fight readiness." Pavel Podvig, a longtime researcher of Russia's nuclear forces, stated the alert had most definitely primed the Russian command and management system for the potential of receiving a nuclear order.
It's unclear how Russia exerts management over its arsenal of much less damaging arms. However some U.S. politicians and specialists have denounced the smaller weapons on each side as threatening to upend the worldwide stability of nuclear terror.
For Russia, navy analysts observe, edgy shows of the much less damaging arms have let Mr. Putin polish his status for lethal brinkmanship and increase the zone of intimidation he must struggle a bloody typical battle.
"Putin is utilizing nuclear deterrence to have his method in Ukraine," stated Nina Tannenwald, a political scientist at Brown College who lately profiled the much less highly effective armaments. "His nuclear weapons preserve the West from intervening."
A worldwide race for the smaller arms is intensifying. Although such weapons are much less damaging by Chilly Warfare requirements, trendy estimates present that the equal of half a Hiroshima bomb, if detonated in Midtown Manhattan, would kill or injure half one million individuals.
The case towards these arms is that they undermine the nuclear taboo and make disaster conditions much more harmful. Their much less damaging nature, critics say, can feed the phantasm of atomic management when the truth is their use can immediately flare right into a full-blown nuclear battle. A simulation devised by specialists at Princeton College begins with Moscow firing a nuclear warning shot; NATO responds with a small strike, and the following battle yields greater than 90 million casualties in its first few hours.
No arms management treaties regulate the lesser warheads, identified typically as tactical or nonstrategic nuclear weapons, so the nuclear superpowers make and deploy as many as they need. Russia has maybe 2,000, in accordance with Hans M. Kristensen, director of the Nuclear Data Venture on the Federation of American Scientists, a personal group in Washington. And america has roughly 100, a quantity restricted by home coverage disputes and the political complexities of basing them in Europe amongst NATO allies, whose populations usually resist and protest the weapons' presence.
Russia's atomic battle doctrine got here to be referred to as "escalate to de-escalate" — that means routed troops would hearth a nuclear weapon to stun an aggressor into retreat or submission. Moscow repeatedly practiced the tactic in subject workouts. In 1999, as an example, a big drill simulated a NATO assault on Kaliningrad, the Russian enclave on the Baltic Sea. The train had Russian forces in disarray till Moscow fired nuclear arms at Poland and america.
Dr. Kühn of the College of Hamburg stated the defensive coaching drills of the Nineties had turned towards offense within the 2000s because the Russian military regained a few of its former power.
Concurrent with its new offensive technique, Russia launched into a modernization of its nuclear forces, together with its much less damaging arms. As within the West, a few of the warheads got variable explosive yields that may very well be dialed up or down relying on the navy state of affairs.
A centerpiece of the brand new arsenal was the Iskander-M, first deployed in 2005. The cell launcher can hearth two missiles that journey roughly 300 miles. The missiles can carry typical in addition to nuclear warheads. Russian figures put the smallest nuclear blast from these missiles at roughly a 3rd that of the Hiroshima bomb.
Earlier than the Russian military invaded Ukraine, satellite tv for pc pictures confirmed that Moscow had deployed Iskander missile batteries in Belarus and to its east in Russian territory. There's no public information on whether or not Russia has armed any of the Iskanders with nuclear warheads. Nikolai Sokov, a former Russian diplomat who negotiated arms management treaties in Soviet instances, stated that nuclear warheads may be positioned on cruise missiles. The low-flying weapons, launched from planes, ships or the bottom, hug the native terrain to keep away from detection by enemy radar.
From inside Russian territory, he stated, "they'll attain all of Europe," together with Britain.
Over time, america and its NATO allies have sought to rival Russia's arsenal of lesser nuclear arms. It began many years in the past as america started sending bombs for fighter jets to navy bases in Belgium, Germany, Italy, Turkey and the Netherlands. Dr. Kühn famous that the alliance, in distinction to Russia, doesn't conduct subject drills working towards a transition from typical to nuclear battle.

EU seeks to boost stockpile of iodine pills and nuclear protective gear

Source: https://www.ft.com/content/bb5e6fde-7b08-41d9-a983-61be53cf2917

Mar 20 – Brussels has accelerated plans designed to improve the EU's health response in case of a nuclear incident following Moscow's invasion of Ukraine, according to EU officials. The European commission is seeking to encourage EU members to stockpile iodine pills, protective suits and other medicine. It is also working on ways to deal with possible chemical and biological attacks after the US warned that Russia could use such weapons in Ukraine. A commission spokesman said: "The commission is working to ensure it enhances preparedness in the area of chemical, biological, radiological, nuclear threats (CRBN) generally, and this predates the war in Ukraine." The move comes as Vladimir Putin, Russian president, put his nuclear weapons forces on high alert. Earlier this month pharmacies in countries including Belgium, Bulgaria and the Czech Republic ran out of iodine pills after Russian forces targeted and damaged a Ukrainian atomic power station. The attack prompted warnings about the risks if a radioactive leak spreads across the continent. Such leaks release radioactive iodine, which concentrates in the thyroid gland when it is inhaled and can lead to cancer. Potassium iodine tablets saturate the gland with iodine, preventing the absorption of the radioactive material.

Brussels is applying the lessons learned from the Covid-19 pandemic, which caught Europe without sufficient supplies of personal protective equipment or a vaccine. Last September it established the European **Health Emergency Preparedness and Response Authority (HERA)** to identify possible future health emergencies and be ready for them. European parliamentarians say HERA needs to move faster to keep pace with developments in Ukraine. Véronique Trillet-Lenoir, an MEP for French president Emmanuel Macron's En Marche party, said: "We need to draw strong lessons from Covid. We require specific measures for nuclear sites. We are not ready. We do not have the stocks." "We have a nuclear threat from a mad guy in the Kremlin," she said. "We need a European stockpile and to have a system of alert and monitoring. We need to do simulations to be ready." National governments decide most health matters in the EU but the Covid crisis led to more joint action in Brussels, such as vaccine procurement. In case of an emergency HERA will be in charge of the response. It will activate funding and launch mechanisms for monitoring, targeted development, procurement and purchase of medical countermeasures and raw materials. It also has production facilities ready to fulfill the demand for drugs.

EDITOR'S COMMENT: Nuclear protective gear for whom? People in high places; the military; farmers? How many? 449.65 million (estimated EU population by the end of 2022) sets? What about training on how to use the PPE? Production facilities to fulfill the demand for iodine pills? When after 2-3 days; a week? Too late if you do not have a national stockpile. How to deliver the pills to the population? Distribution points? By mail? In advance? Let us hope that someone in the HERA would have already throught of these simple questions and propose viable solutions. Although I am not 100% sure about this … FT should choose more carefully the photos accompanying similar articles. Unless the plan is to distribute Level-A PPE to the people!

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

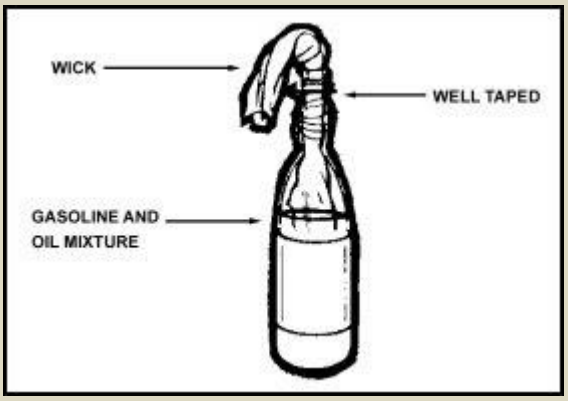
C2BRNE DIARY

EXPLOSIVE NEWS

Ukrainians urged to use Molotov cocktails to 'neutralise Russian troops'

Source: https://uk.news.yahoo.com/ukrainians-urged-to-use-molotov-cocktails-to-neutralise-russian-troops-100308035.html

Feb 25 – Ukraine has told its citizens to prepare Molotov cocktails to use against Russian soldiers as Vladimir Putin's forces close in on Kyiv.



Russian troops were feared to be on the verge of entering the capital on Friday morning after the city was hit by "horrific rocket strikes" overnight.

Ukraine has urged its citizens to take up arms against enemy troops, with President Volodymyr Velenskyy telling his people that anyone who wanted them would be supplied with weapons.

"We will give weapons to anyone who wants to defend the country. Be ready to support Ukraine in the squares of our cities," he said.

And on Friday, the Ukrainian Ministry of Defence's Facebook page posted: "We urge citizens to inform us of troop movements, to make Molotov cocktails, and neutralise the enemy."

What is a Molotov cocktail?

A Molotov cocktail is an improvised weapon that sees fabric stabbed into a bottle of flammable liquid that can be set alight and launched at a target.

They were first seen during the Spanish Civil War in the 1930s, but the name wasn't coined until the Winter War between the Soviet Union and Finland in 1939. The name was a reference to Soviet foreign minister Vyacheslav Molotov, one of the key architects of a peace treaty that brought the Winter War to an end.

EDITOR'S COMMENT: It may sound like a good idea and something that can be easily done. BUT this is war and not an urban demonstration where police will not shoot back. Soldiers will shoot to kill if spot someone throwing Molotov bombs!

Weapons manufacturing facility of ISIS found by Asayish in Syria's Raqqa

Source: https://npasyria.com/en/73076/

Some of items seized by Asayish at the facility - North Press

Feb 20 – The Internal Security Forces (Asayish) found on Sunday a weapons manufacturing facility containing a quantity of explosives and other military materials belonging to the Islamic State (ISIS), in Raqqa.

A weapons manufacturing facility of ISIS was found by Asayish near al-Rashid Park in the city of Raqqa, containing military materials, including a chemical mask device and a high-explosive TNT, the Asayish said on their Facebook page said.
The engineering team moved out those items present from the house where the facility is located after being cordoned off and evacuated. No damage was caused, they added.
The number of weapons was transferred by the Asayish from the facility amounted to about 48, in addition to one kilogram of high explosive (TNT) and a quarter of a kilogram of explosive paste.
"Our forces are calling on the citizens to take precautions and follow safety rules when seeing any suspicious object and to immediately report to the nearest center of our forces in order to preserve public safety," the Asayish said.

A low-cost dynamic pressure sensor that allows instantaneous measurements to be taken in multiple directions simultaneously

Source: https://ploughshare.co.uk/technology/dynamic-fluid-flow-sensor/

Calculating the forces during an explosion is a difficult task – especially when it occurs inside a building as the directional sensors may not be correctly positioned to account for the various reflections that take place. This new sensor can measure blast flow in any direction, making it much easier to position and in turn gives more accurate results.
The new sensor overcomes the positioning issues experienced with current devices by being able to measure fluid flow in several directions simultaneously. The sensor is also particularly suited to measurements in turbulent environments where rapid and often unpredictable changes in speed and direction of fluid flow can occur.

Benefits

- **Easy to Position** — avoids the need to accurately predict the blast flow due to its ability to measure fluid flow in several directions at once.
- **Range of Parameters** — many fluid flow parameters can be measured; both static and dynamic pressures can be easily derived.
- **Versatile** — the design can be optimised and scaled for different applications, e.g. to accommodate different measurement ranges.
- **Simple and Robust** — sensor has no moving parts and is suitable for harsh environments or where maintenance is difficult.

Applications

Although originally developed for improved blast flow measurement, the sensor has the potential to be used in other applications. It could, for example, also measure flow where traditional anemometers would not work. It is particularly suited for rapidly changing and short duration flow sensing where a fast response is required.

Thermobaric rockets: Russia's most fearsome weapon that could destroy a city block in a single shot

Source: https://www.euronews.com/next/2022/03/01/thermobaric-rockets-russia-s-most-fearsome-weapon-that-could-destroy-a-city-block-in-a-sin

Mar 01 – As the fighting in Ukraine intensifies in its largest cities, fears are rising that a war of attrition will mean an escalation of violence and the use of ever more deadly weapons.
On Saturday, a CNN correspondent captured footage of what appeared to be a TOS-1 heavy flamethrower system being transported to the Ukrainian border near the Russian city of Belgorod.
Nicknamed "Buratino" in reference to the Russian version of Pinnochio - because of its long, pointed nose - the TOS-1 is a 24-tube 220 mm multiple rocket launcher and one of the most fearsome weapons in Russia's arsenal.
What particularly raised eyebrows in CNN's footage was the weapon the TOS-1 is used to launch: vacuum bombs, also known as thermobaric rockets.

What is a thermobaric weapon?

The word thermobaric comes from the combination of the Greek words thermos, 'heat', and baros meaning 'pressure'. In practice, this weapon combines shockwaves and vacuums to produce a high-temperature explosion.

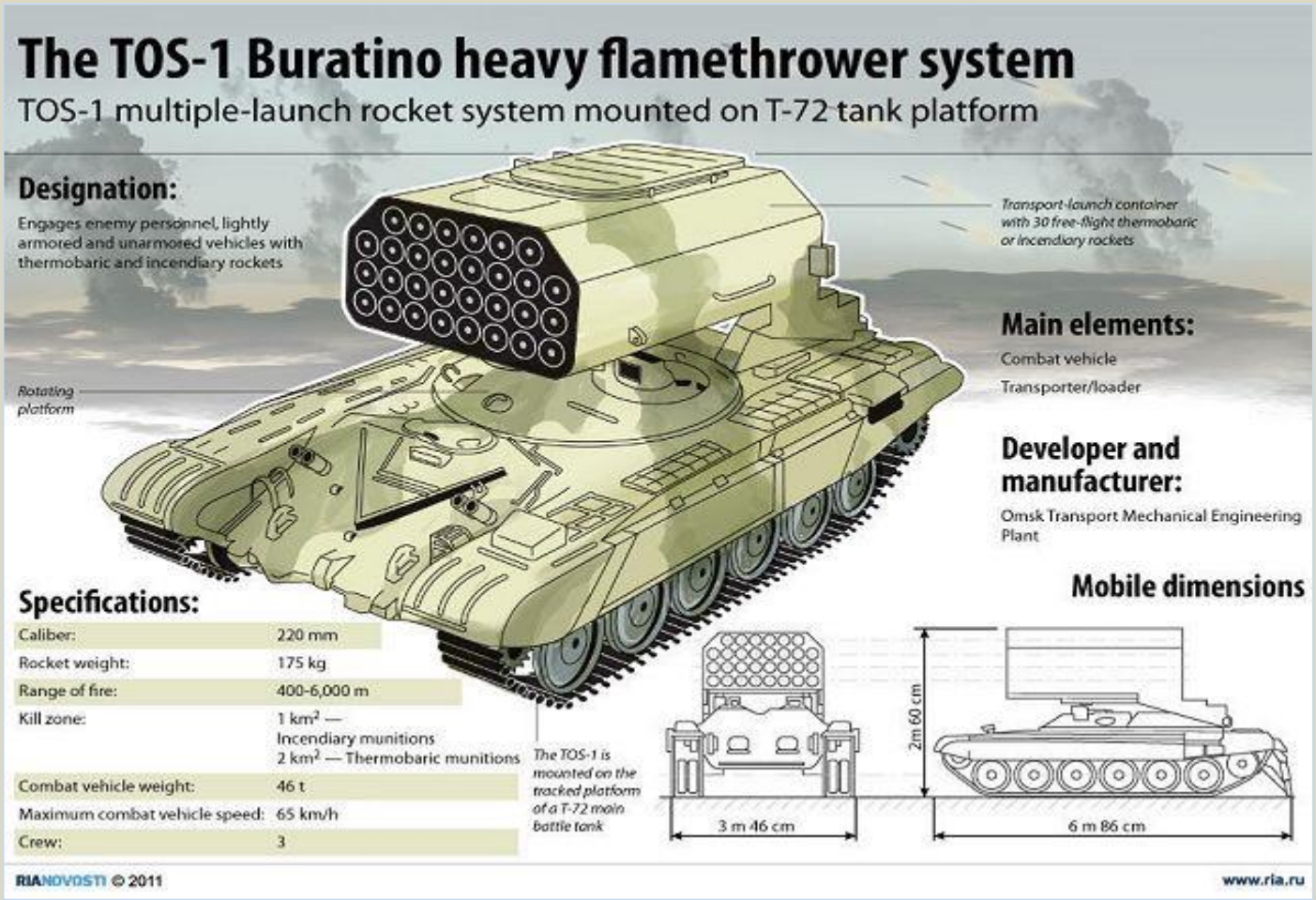
"It's a weapon that, when it explodes, will release its explosive - or its fuel - and will create an overpressure effect that's going to end up in a much greater detonation and be really devastating because of the shock wave," Jean-Marie Collin, expert and spokesperson for ICAN France, the French branch of the International Campaign to Abolish Nuclear weapons, told Euronews Next.

The need to use such a weapon is "this ability to create an overpressure that will create an extremely strong shock," he explained.

The TOS-1 was first deployed by Russia in Afghanistan in the 1980s and most recently in Chechnya and Syria, designed to take out infantry, bunkers, fortifications, and vehicles.

Collin traces them back further.

"The first uses go back to the Second World War. And it's also been used quite a bit in the wars, unfortunately, in Iraq or Afghanistan, most likely as well. So the use of a thermobaric weapon is something that, unfortunately, is used in different conflicts," he said.



While the US also makes these types of weapons, Russia is believed to have detonated the biggest yet in 2007, creating an explosion equivalent to 39.9 tons.

Back in 2015, Dave Majumdar, the Defence Editor for the website The National Interest, explained that "Buratino can obliterate a roughly 200 m by 400 m area with a single salvo. In other words, it can instantly turn several city blocks into smouldering rubble with a single shot".

How dangerous are they?

In February 2000, a report from Human Rights Watch sounded the alarm about the devastating effect of thermobaric weapons, quoting a study made by the US Defence Intelligence Agency.

"The [blast] kill mechanism against living targets is unique—and unpleasant. (...) What kills is the pressure wave, and more importantly, the subsequent rarefaction [vacuum], which ruptures the lungs. (...) If the fuel deflagrates but does not detonate, victims will be severely burned and will probably also inhale the burning fuel," the study said.
"Since the most common FAE fuels, ethylene oxide and propylene oxide, are highly toxic, undetonated FAE should prove as lethal to personnel caught within the cloud as with most chemical agents".
The study described that symptoms could be more dangerous in confined spaces.
"Those near the ignition point are obliterated" the study detailed. "Those at the fringe are likely to suffer many internal, thus invisible injuries, including burst eardrums and crushed inner ear organs, severe concussions, ruptured lungs, and internal organs, and possibly blindness".
For Collin, the impact is still very different from a nuclear bomb.
"A nuclear weapon is still a weapon of mass destruction whose use has long-lasting consequences, which is not the case with a thermobaric or conventional weapon system, even though this weapon system can obviously create a lot of injury and destruction," he told Euronews Next.
"A nuclear weapon is something that truly destroys all life in the place where it was used. We're talking about the power that is multiplied by several tens".

ICAN's response to nuclear threat
ICAN, the winner of the Nobel Prize in 2017, denounced the invasion of Ukraine on Sunday, describing it as Vladimir Putin's "dangerous game".
"President Putin is playing a dangerous game by placing nuclear weapons on combat alert. Our campaign strongly condemns this action and we call for an immediate ceasefire, as well as the withdrawal of Russian forces from Ukraine," Collin said in a statement sent to the AFP.
"The world is approaching a nuclear catastrophe, so we urge all nuclear-weapon states to remove their arsenals from alert status and refrain from threatening to use their arsenals," he added.
ICAN has stressed that "any use of nuclear weapons would cause catastrophic humanitarian suffering and the fallout - radioactive, economic, political, will be harming people for generations".

Is Russia Using Vacuum Bombs in Ukraine?

By Marcus Lütticke
Source: https://www.homelandsecuritynewswire.com/dr20220303-is-russia-using-vacuum-bombs-in-ukraine

Mar 03 – On Monday, the Ukrainian ambassador to the US accused Russia of using thermobaric weapons in Ukraine, but her claim has yet to be officially verified.
After meeting with US lawmakers in Washington, Oksana Markarova told reporters: "They used the vacuum bomb today, which is actually prohibited by the Geneva Convention."
What are vacuum bombs?
Also known as aerosol bombs or fuel-air bombs, vacuum bombs are thermobaric weapons. The name is derived from the Greek for heat and pressure.
Whereas most conventional weapons use a mixture of fuel and an oxidizing agent to cause an explosion, these bombs consist almost 100% of fuel and rely on oxygen in the air to explode. After the first explosion, the fuel is finely dispersed in the atmosphere like a cloud and then it is ignited, causing a massive blast.
After the detonation and the shock wave, there is a vacuum effect, when all oxygen is extracted from the air as the bomb does not have its own oxidizing agent.

What Damage Is Incurred?
Vacuum bombs have immense destructive power. In a report from February 2000, Human Rights Watch quotes a CIA study: "Those near the ignition point are obliterated. Those at the fringe are likely to suffer many internal, and thus invisible injuries, including burst eardrums and crushed inner ear organs, severe concussions, ruptured lungs and internal organs, and possibly blindness."
Have these weapons been deployed?
On February 26, Frederik Pleitgen, a reporter with the US network CNN, posted a video on Twitter with the title "Russian thermobaric 'vacuum bombs' launcher seen by CNN team in Ukraine"

Pleitgen wrote: "The Russian army has deployed the TOS-1 heavy flamethrower which shoots thermobaric rockets … South of Belgorod." Belgorod is a Russian city not far from the Ukrainian border.
"We know that the Russians have such weapons systems in the area," Frank Sauer from the Bundeswehr University in Munich confirmed.

Where Are They Alleged to Have Been Used?
Russia is accused of using the bomb in the Ukrainian city of Okhtyrka in Sumy Oblast. Photos and videos showing the alleged impact have been posted to social media channels.
Asked about this on Monday, White House spokesperson Jen Psaki said the US had not independently verified the reports. "I don't have any confirmation of that. […] We have seen the reports. If that were true, it would potentially be a war crime."
Two days later, Linda Thomas-Greenfield, the US ambassador to the UN, made a speech to the UN General Assembly in which she made similar allegations and told Russia to stop its war.
"We have seen videos of Russian forces moving exceptionally lethal weaponry into Ukraine, which has no place on the battlefield. That includes cluster munitions and vacuum bombs — which are banned under the Geneva Convention," she said.

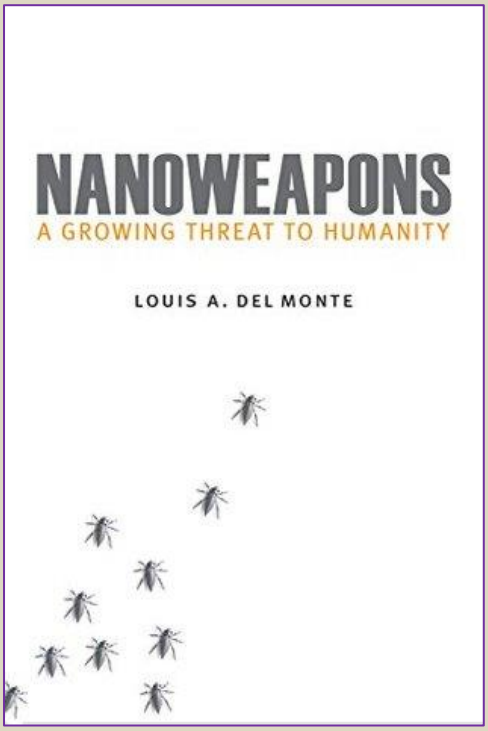
What Have Experts Said?
"Looking at the pictures from Ukraine, I think it is quite possible that aerosol bombs are being used there. However, it is not possible to confirm this with certainty from the video footage," said Sauer of the Bundeswehr University.
Military expert Gustav Gressel, who works at the European Council on Foreign Relations, a pan-European think tank, examined the footage for DW. He reasoned similarly: "In my opinion, no other weapon, apart from nuclear weapons, would have that strength."
But he added that it could not be ruled out that something explosive had been hit. "However, in that case we would be more likely to hear a series of detonations," he said. A report in the German *Frankfurter Allgemeine Zeitung* daily said there were doubts, even in Western intelligence circles, that the explosion analyzed had been caused by a vacuum bomb.
Should it turn out that Russia has used vacuum bombs in Ukraine, it would be considered a war crime and could be taken to court by Ukraine. "The possession of such weapons is not prohibited, but their use in populated areas is [outlawed] because they have an expansive effect," Sauer said.

Marcus Lütticke is a *DW* journalist.

Nanoweapons: A Growing Threat to Humanity

Author: Louis A. Del Monte.
Potomac Books, 2017, 244 pp.
Source: https://www.airuniversity.af.edu/AUPress/Book-Reviews/Display/Article/1731239/nanoweapons-a-growing-threat-to-humanity/

When new technologies cross from industry to the battlefield, calls arise to slow the process and consider international implications of using these weapons. Louis A. Del Monte's *Nanoweapons* is one of those calls. A physicist and former executive at IBM and Honeywell, Del Monte led advancements in microelectronics and sensors. His work is a serious attempt to use publicly available information to address the development and use of nanotechnology as weapons. The author brings together ideas normally relegated to science fiction (e.g., laser weapons, artificial intelligence, and self-replicating nanorobots) and uses his technical background to inform the reader as to what is science fact. While his most alarming predictions for humanity's survival project to the year 2050 and beyond, he argues that his concerns are timely. He indicates that while revolutionary military nanotechnologies (e.g., stealth aircraft) may take decades to field, they are nonetheless currently being developed. Now, according to the author, is the time to discuss the dangers of nanoweapons.



The author's main thesis is that nanoweapons are a danger to humanity that demand greater attention. Despite the secrecy surrounding the development of nanoweapons, Del Monte is confident of their threat. This fear is based in part on the ranking of nanotechnology weapons by the Global Catastrophic Risk Conference at the University of Oxford as the most probable means to cause human extinction by the end of this century. Examples of nanoweapons discussed in the book include nano-enhanced lasers, smaller munitions with increased explosive force, and self-replicating smart nanorobots (SSN). SSNs search for and destroy targets without human input and self-replicate with materials found in the environment. According to the author, SSNs are gravely dangerous nanoweapons that humanity should prohibit. Central to his concern for humanity's survival is what he sees as the inherent difficulty in mounting defenses to nanoweapons given their capability to avoid detection and the ability of those who use these arms to escape attribution. While considerable resources have been dedicated to countering nuclear weapons, little is publicly known about protection from nanoweapons. This is especially concerning to the author because some nanoweapons have characteristics similar to biological pathogens. Giving his readers reason to be apprehensive, Del Monte turns to explaining how today's nanotechnology can be used to create nanoweapons.

While nanotechnology is already improving our computers, sunscreens, and building materials, the first section of the book provides the nontechnical reader an easy-to-understand introduction to nanotechnology and how it may be used in arms development. The author organizes nanoweapons into five categories: offensive strategic, defensive strategic, offensive tactical, defensive tactical, and passive. Examples are provided for each category, along with an explanation of its offensive, defensive, or passive nature. For instance, the offensive strategic category includes artificially intelligent nanorobots that can target particular individuals, hypersonic glide missiles (whose development will rely on developing certain nanomaterials), nano-enhanced fuels, and nonelectric guidance systems. The other categories include additional guidance for organizing nanoweapons. While readers will find these categories helpful, a workable definition of nanoweapons is missing.

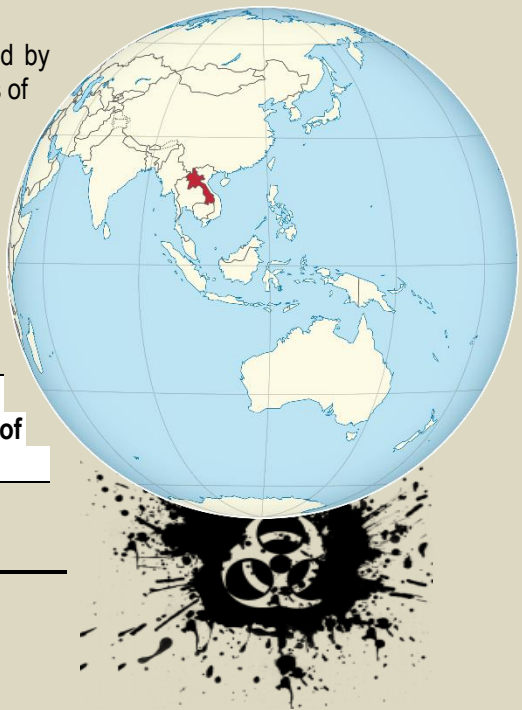
With this deep level of organization dedicated to understanding nanoweaponry, the reader would hope for a more useful definition of nanoweapons. *Nanoweapons* are defined in the book's glossary as "any military technology which exploits the use of nanotechnology (229)." Although this definition will capture all nanoweapons, it will also include many items that are not weapons. This definition would include a military finance office using a publicly available desktop computer with a nanomanufactured microchip. Is building a weapon with nanomanufactured components all that is required to make the weapon a nanoweapon? If a dry-docked ship is sprayed with anticorrosive nanocoating—increasing its hull strength tenfold (as an MIT study referenced in the book suggests)—is the ship now a nanoweapon? The book makes clear that nanotechnology is an enabling technology that will empower a wide range of civilian and military applications. But it does not wrestle with the problem that an SSN is fundamentally different than an anticorrosive nanocoating. This issue of defining nanotechnology is a common attribute of nascent scientific fields, but the reader is nevertheless left wanting more. Without addressing this definitional problem directly, Del

Monte instead uses other methods to discover what nations are emerging as nanoweapon leaders.
He categorizes the factors needed to facilitate nanoweaponry development and sorts nations by these factors into the Nanoweapons Offensive Capability of Nations (NOCON) list. The most powerful group, nanoweapon nations—such as the United States and China—has the ability to commercialize nanotechnology, possesses a national desire to strengthen its militaries, and demonstrates an ability to partner with other leading nanotechnology nations. Del Monte goes on to mention other nations on his NOCON list, all of which have varying interactions with nanotechnology. Giving the reader reason to be concerned for the international implications his NOCON suggests, he then highlights the events that may tip us into a nanoweapon-driven war.
He predicts two singularities that will spawn nanoweapon-related international disruptions. In addition to the creation of SSNs, the other singularity is the advent of artificial intelligence (AI) that will exceed human intellect. AI will solve many of humanity's greatest problems, the author posits, but it will also create better SSNs. If AI and SSNs are combined, alliances will form to maintain advantages in a new cold war around the development of AI-powered SSNs. Given their importance, international power will then be rebalanced around nanoweapon capabilities. Nuclear weapon use will increase since nanotechnology will empower their miniaturization and reduce their fallout. It is these disruptions, brought on by the AI and SSN singularities, that Del Monte claims will dramatically increase the chance of human extinction by 2100. Given this pessimistic prediction, *Nanoweapons* next discusses reasons for hope.
The author maintains some optimism for humanity. He notes that humanity has engaged in conflict since the beginning of our existence, but recent developments, such as the Treaty on the Non-Proliferation of Nuclear Weapons and the Biological Weapons Convention, show that humanity can act to prevent its extinction. Once humanity comes to know the existential threat that nanoweapons represent, humanity will act to limit their use and thus avert disaster. What we recognize when we use a new personal computer, he argues, is not the nanotechnology enabling its use but the impressive performance it achieves. The author states that humans understand technology by its function, not the technology itself. Thus, to forestall the need to demonstrate a nanoweapon's threat to humanity, he indicates that current treaties and conventions concerning weapons of mass destruction should also regulate strategic nanoweapons.
A workable and more precise definition of nanoweapons will improve this area of study by allowing policy makers to grapple with nanoweaponry development. It will empower leaders to specifically categorize an adversary's capabilities and document who is developing nanoweapons with greater specificity. Assuming that Del Monte's catastrophic predictions are accurate, more scenarios are needed to better inform technologists, military commands, and national leaders working on ways to prevent the negative implications of these technologies. This work is worth reading because it ties together the technical, political, economic, and practical challenges associated with nanoweapons. The initial portion of the book is especially worthwhile for those seeking an approachable introduction to nanotechnology and its use as weaponry. Suggestions for additional reading in this area of futurism are Peter W. Singer's *Wired for War* and Michio Kaku's *Physics of the Future*. Strategic leaders will appreciate the discussions on organizational problems associated with fielding nanoweapons and rebalancing international power. Tactical leaders will find themselves working through different ways to use and defend against nanoweapons. Finally, fans of science fiction will appreciate a technical introduction to many real concepts previously relegated to fantasy.

Maj Patrick M. Milott, USAF

Laos destroys 1.7M UXO devices during 1996-2021

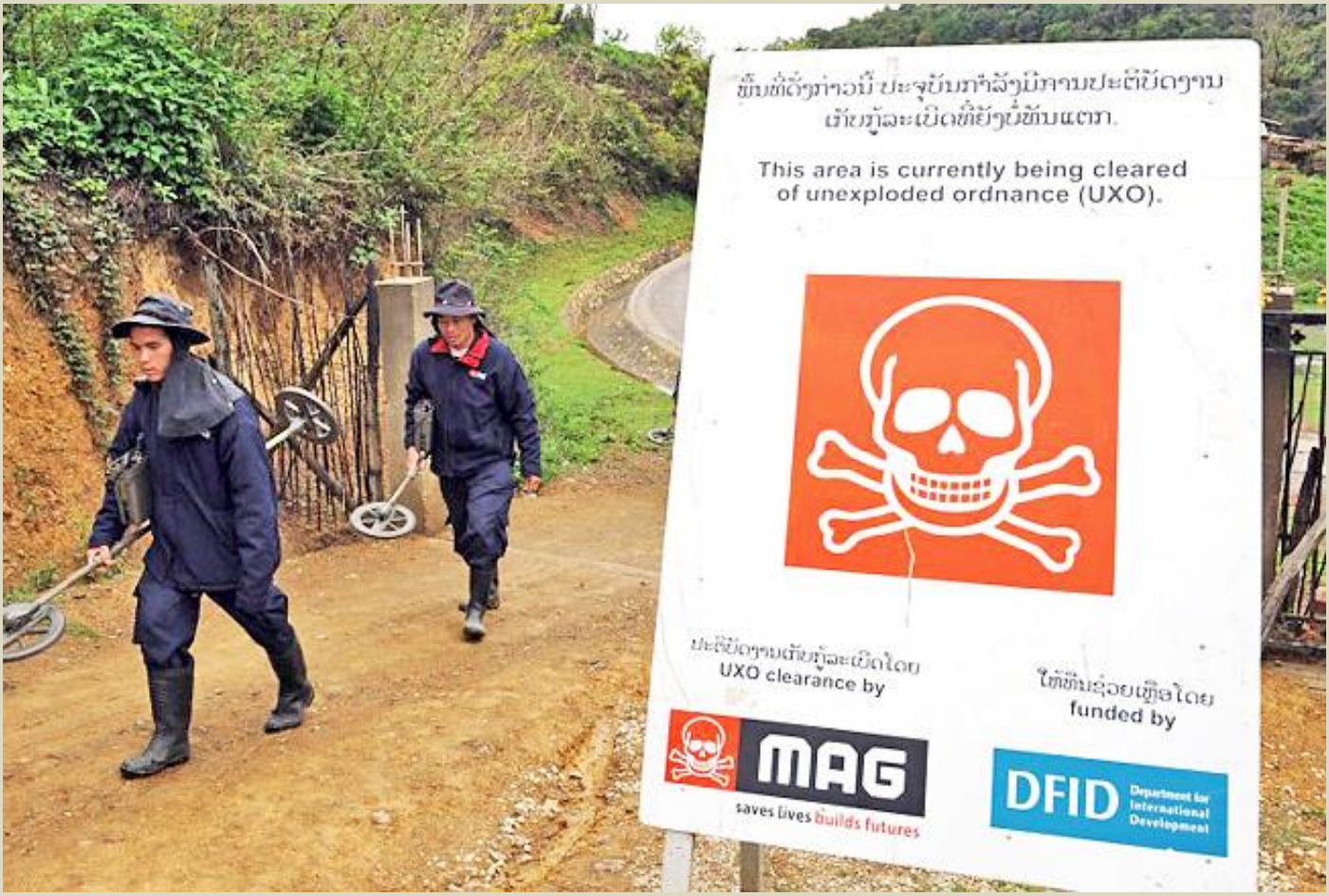
Source: https://borneobulletin.com.bn/laos-destroys-1-7m-uxo-devices-during-1996-2021-2/



Mar 03 – Nearly 1.7 million unexploded ordnance (UXO) items had been destroyed by clearance teams in Laos from 1996 to December 31, 2021, while over 71,000 hectares of land were cleared of munitions.
The figures were released at a consultation meeting on the Draft Unexploded Ordnance National Strategic Plan in Laos "Safe Path Forward III" for 2021-2030 in Lao capital Vientiane on Monday.
According to the national UXO database, from 1996 until December 16, 2021, 71,943 hectares of land in the country's all 18 provincial regions were cleared.
Of this, 55,286.3 hectares were agricultural land and 16,656.7 hectares were land targetted for development.

A total of 1,693,487 UXO items were destroyed, of which 4,288 were large bombs, 968,447 were bombies, 2,379 were landmines and 718,367 were other types of unexploded ordnance.

According to the National Regulatory Authority (NRA) for the UXO/Mine Action Sector, since 1996 the focus has been on UXO clearance in the nine most heavily impacted provinces of Laos, namely Huaphan, Xieng Khuang, Luang Prabang, Khammuan, Savannakhet, Champassak, Saravan, Xekong and Attapeu.
Over the past 10 years, the NRA has conducted 18,862 Mine Risk Education activities.



Workers of a UXO (unexploded ordnance) clearance team arrive at the Phuckae secondary school in the northern province of Xiangkhoang, Laos. PHOTO: AFP

'Exploiting Cadavers 'and 'Faked IEDs': Experts Debunk Staged Pre-War 'Provocation' in the Donbas

By Nick Waters
Source: https://www.bellingcat.com/news/2022/02/28/exploiting-cadavers-and-faked-ieds-experts-debunk-staged-pre-war-provocation-in-the-donbas/

Editor's note: This article contains and links to imagery that some readers may find disturbing

Feb 28 – With Russia's invasion of Ukraine ongoing, it's easy to forget the flurry of dubious provocations and staged events that appear to have been designed to implicate the Ukrainian armed forces and drum up military aggression in the days before the first shots were fired.
These included videos showing alleged border incursions by the Ukrainian military and footage of purported saboteurs attempting to blow up a chlorine facility at a sewage treatment plant – both of which showed nothing of the sort.
But one suspicious video, which showed a gruesome scene of charred bodies and human skulls that seemed to have been sliced open, appeared so serious and egregious that

Bellingcat decided to investigate further, speaking to an explosive weapons expert and a forensic pathologist in the process.

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

Nick Waters is an ex-British Army officer and open source analyst. He has a special interest in the conflicts in Syria, as well as social media, civil society, intelligence, and security.

Component in Iranian-made missiles used in attacks on Saudi Arabia traced back to a Turkish firm

Source: https://nordicmonitor.com/2022/03/iranian-made-missile-attacks/

Mar 09 – A barrage of cruise missile attacks against targets in Yemen and Saudi Arabia by missiles manufactured in Iran was made possible with parts procured in Turkey, according to findings submitted to the UN Security Council.

The revelations were made when UN investigators probed the chain of custody of several components recovered from the debris of missiles used in attacks on Saudi Arabia as well as those seized in the Gulf of Aden. The evidence led to the discovery that a key component used in the manufacturing of the missiles was imported from Germany by a Turkish company in 2016.

The component identified as 30.600 G OEM Pressure Transmitter was originally produced by German company BD Sensors and was used in the fuel-feed system of the missile. According to UN documents, the German company shipped the transmitter to the Istanbul-based Lonca Makina Sanayi Ticaret A.Ş., its only authorized distributer in Turkey.

The discovery is hardly surprising to observers of Turkey-Iran cooperation in sanctions busting techniques. Faced with US sanctions, Iran has extensively been using neighboring Turkey to procure critical components, especially for dual-use goods, to support its defense industry and produce arms and weapons, some of which it exported to fuel regional conflicts in the Middle East and Africa. Tehran has been significantly helped by Turkish President Recep Tayyip Erdoğan, who considers Iran his second home and actively works to facilitate Iran's operations in Turkey and other countries.

The UN documents highlight that the critical transmitters were found in the missiles seized from a dhow named Al-Raheeb in the Gulf of Aden by the US Navy on November 25, 2019. The dhow was transporting anti-tank guided missile launch containers, surface-to-air missiles, components for Quds-1 and C802 cruise missiles and uncrewed aerial vehicle and waterborne improvised explosive device parts. UN investigators examined the samples to trace the origin of the components used in the manufacture of these weapons.

The transmitters were part of the Quds-type cruise missiles used in 2019 and 2020 attacks on multiple targets in Saudi Arabia. The pressure transmitter that was used in one missile with serial number 10075204 was imported by Turkish company Lonca on July 14, 2016, although it is not clear how it ended up in an Iranian Quds missile. The Turkish company did not respond to a UN letter that asked about the delivery of the transmitters after it imported them from Germany.

The Islamist Erdoğan regime, filled with many pro-Iran Islamists in senior positions in the government, has openly declared its opposition to sanctions on Iran and pledged to beat the punitive measures in cooperation with the mullah regime in Tehran. The close engagement with Iran caused trouble for the Erdoğan regime with Turkey's long-time ally, the US. Two federal cases in the US have revealed how Turkish nationals of Iranian origin violated US laws using Turkish territory as an operations hub with full knowledge of Turkish government officials.

The most damning revelation was made when a corruption case involving Turkish-Iranian national Reza Zarrab, who bribed senior government officials including cabinet ministers and cultivated personal ties with Erdoğan, was made public on December 17, 2013. Dozens of suspects including Zarrab were detained and later arrested for violating several Turkish laws.

Erdoğan, who was incriminated in the probe, stepped in to derail the prosecution and helped release all the suspects after orchestrating the removal of the lead prosecutors and investigators in the case. All suspects including Zarrab were later acquitted by new judges who were brought in to hear the case by the Erdoğan government.

However, Zarrab was arrested by the FBI in Miami in 2016 and charged by the US Attorney for the Southern District of New York with engaging in hundreds of millions of dollars' worth of transactions on behalf of the Iranian government, money laundering and bank fraud. He cut a deal with prosecutors and decided to cooperate in a US federal case that exposed the role of Erdoğan, who had instructed Turkish state banks to participate in the multi-billion dollar scheme in exchange for kickbacks.

At the end of the trial, Mehmet Hakan Atilla, the deputy general manager of state lender Halkbank, was convicted and served time before returning to Turkey. The co-conspirators who were indicted by the US federal prosecutors including the former economy minister of Turkey in the Erdoğan cabinet remain beyond reach.

Another US federal case involved a Turkish national identified as Reşit Tavan, the owner of several shell companies in Turkey that acted on behalf of Iran in transporting goods from the US without declaring that the end destination was in fact Iran.

Tavan was indicted on June 27, 2017 by US federal prosecutors for conspiring to defraud the US and smuggle American-made products to Iran. The indictment alleged that marine goods such as outboard motors, generators and propulsion systems that were manufactured in Wisconsin were shipped first to Turkey and then to Iran without the knowledge of the manufacturers and without a license from the US government.

Tavan was arrested on June 8, 2017 when he was going through customs in Romania and unsuccessfully fought extradition. The Turkish Embassy in Bucharest lobbied to get him back to safety in Turkey, helped him hire a former justice minister of Romania as his defense attorney and even managed to get a ruling against extradition in the court of first instance. But the appeals court overruled the judgement and cleared the way for his extradition to the US. On December 11, 2017 he was formally arrested during his arraignment in federal court in Milwaukee after Romanian authorities turned him over to the US, balking at the Turkish government's request.

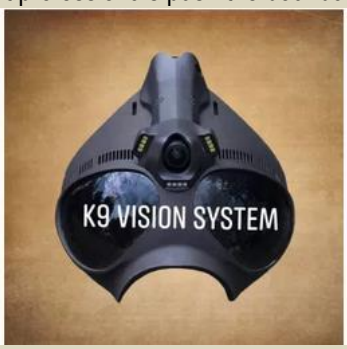
On April 2, 2019 faced with overwhelming evidence and the prospect of a long prison sentence, Tavan cut a deal with federal prosecutors and pleaded guilty to conspiracy to violate the US laws, saving himself from the lengthy sentence he would most likely receive

on the additional charges. The Federal District Court in Milwaukee sentenced him to 28 months' imprisonment on August 29, 2019. US District Judge Pamela Pepper ruled to release and deport him to Turkey given the fact that he had already spent 20 months in the Waukesha County Jail.

K9 Vision System

Source: https://devastratactical.com/spec-ops-dog-k9-vision-system/

The idea for the K9 Vision System arose from the need to solve a very real problem for us as military operatives. No matter how many breakthroughs we made in training K9s in laser-guided **explosive detection** or directionals for control at distance, we were limited by our visual field. Consequently, we set off on a different mission: to create a system that would allow us to see what our dogs could see, and give them commands when completely out of sight. Our goal was to develop a high quality, no-latency video and radio transmission system that would maximize our operational capabilities, but would also be comfortable and unrestrictive for the dogs. In cooperation with various innovators of drone technologies, the K9 Vision System came to life. Building on the system's success, we hope to continue helping military and law enforcement professionals push the boundaries of K9 operations.



Main Features

NO LATENCY
encrypted COFDM video and audio transmission.

UNMATCHED RANGE
in urban environment and dense vegetation: 350-800 meters.

NIGHT VISION
with remote control infra-red and white LEDs.

CUSTOM MOUNTS
and configurations

FIELD TESTED
and operational in 16 different countries.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Ukraine's Volunteer 'IT Army' Is Hacking in Uncharted Territory

Source: https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/

Feb 27 – Vladimir Putin's attack on Ukraine has been met with fierce resistance throughout the country's towns and cities. As Russian forces have moved closer to Kyiv, lawyers, students, and actors have taken up arms to defend their country from invasion. They are not the only ones: Volunteers have also flocked to join a Ukrainian volunteer "IT Army" that's fighting back online.

At around 9 pm local time on February 26, Ukraine's deputy prime minister and minister for digital transformation, Mykhailo Fedorov, announced the creation of the volunteer cyber army. "We have a lot of talented Ukrainians in the digital sphere: developers, cyber specialists, designers, copywriters, marketers," he said in a post on his official Telegram channel. "We continue to fight on the cyber front."

Ukraine has seen other volunteer-organized cyberdefense and attack efforts leading up to and early in the war effort. Separately hacktivists, including the hacking group Anonymous, have claimed DDoS attacks against Russian targets and taken data from Belarusian weapons manufacturer Tetraedr. But the development of the IT Army, a government-led volunteer unit that's designed to operate in the middle of a fast-moving war zone, is without precedent.

The IT Army's tasks are being assigned to volunteers through a separate Telegram channel, Fedorov said in his announcement. So far more than 175,000 people have subscribed—tapping Join on the public channel is all it takes—and multiple tasks have been dished out. The channel's administrators, for instance, asked subscribers to launch distributed denial of service attacks against more than 25 Russian websites. These included Russian infrastructure businesses, such as energy giant Gazprom, the country's banks, and official government websites. Websites belonging to the Russian Ministry of Defense, the Kremlin, and communications regulator Roskomnadzor were also listed as potential targets. Russian news websites followed.

Since then the IT Army channel has expanded its scope. On February 27, it asked volunteers to target websites registered in Belarus, one of Russia's key allies. The channel has also told subscribers to report YouTube channels that allegedly "openly lie about the war in Ukraine."

One former Ukrainian official who has knowledge of the IT Army's organization says it was formed as a way for Ukraine to hit back against Russian cyberattacks. Russia has significant hacking capabilities: Wiper attacks hit a Ukrainian bank in the buildup to the invasion, and government websites were knocked offline. "Our country didn't have any forces or intentions to attack anyone. Therefore, we made a call," the former Ukrainian official says. "We already know that they are quite good at cyberattacks. But now we will find out how good they are in cyberdefense," the former official says.

"For a country that's facing an existential threat, like Ukraine, it's really not surprising that this sort of call would go out and that some citizens would respond," says J. Michael Daniel, the head of the industry group Cyber Threat Alliance and former White House cyber coordinator for President Obama. "Part of it is also a signaling exercise. It's signaling a level of commitment across the country of Ukraine to resisting what the Russians are doing."

The impact of the IT Army is hard to gauge thus far. While thousands of members have joined the Telegram channel, there is no indication of who they are or their involvement in any response. The channel has shared screenshots of some Russian websites allegedly being taken offline, but it's unclear how successful these efforts have been or where they originated from.

While many nations around the world have offensive hacking capabilities, these are mostly shrouded in secrecy and run by intelligence agencies or military units. The IT Army will likely instead take on defensive tasks to free up Ukraine's government hackers. "It really is true that even in this age of automation and other things, additional bodies will make a big difference," says Daniel.

The challenge now will be to effectively corral those newfound resources. The former Ukrainian official says the IT Army is being coordinated through a Telegram channel as it is an easy way to broadcast messages to thousands of people at once. They say those working on the IT Army behind the scenes are doing so in more-secure messaging services, although they decline to say which ones. "We are trying to use any help to protect our country and people," they say.

"Managing the organization and logistics is a challenge in itself," says Lukasz Olejnik, an independent cybersecurity researcher and consultant who previously acted as a cyberwarfare adviser at the International Committee of the Red Cross. He says there are questions around how to vet volunteers, distribute targets, and avoid infiltration.

Who exactly Ukraine recruits will have the most bearing on what tasks the IT Army takes on. But it's likely to encompass the DDoS attacks that have been called for thus far, and potentially helping protect critical infrastructure. "The idea that you're going to grab this ragtag group of folk, even if they have an extensive pen testing background, that they're going to somehow hack into the Kremlin's networks and get valuable intelligence that's going to change the course, that's fantasy," says Jake Williams, an incident responder and former NSA hacker. "DDoS and defensive is probably more important for Ukraine right now than offensive."

It will also be important for the group to avoid any misfires. Launching more sophisticated cyberattacks—such as a worm, which can self-propagate from one system to the next—

would also risk spillover incidents, where the impact of a cyberattack goes well beyond its intended target. "You could take anything from emergency services, health care systems, or other things offline without meaning to. Which both has an immediate impact—you could hurt civilians inside Russia—and it could also inadvertently escalate things if the Russians perceive that as a direct order, the direct intent of the Ukrainian government, and they escalate and respond in kind," Daniel says. That caution applies as well, and perhaps even more so, to independent hacktivist groups like Anonymous, which has vocally joined the fray. Russia-based ransomware group Conti has said it would use its "full capacity" to retaliate if the West attempted to target critical infrastructure in Russian or "any Russian-speaking region of the world."

The government-backed IT Army builds on other Ukrainian hacking efforts. On February 25, Yegor Aushev, who has founded multiple cybersecurity companies in Ukraine, made the first call for volunteers. "The time has come to maximize the cyber protection of our country," Aushev wrote in a post on Facebook, which was first reported on by *Reuters*. Those wanting to offer their skills could sign up using a Google Form—they could be involved in defense or attack. Volunteers were asked how many years' experience they have in 12 specific areas, ranging from open source intelligence gathering and social engineering to malware development and DDoS operations. Those signing up were also asked to provide the name of a trusted reference who could vouch for their credibility.

Tim Stevens, a senior lecturer in global security at King's College London, says "the gloves are off" for both Russia and Ukraine. He warns that when it comes to cyberattacks there are a lot of unknown and hypothetical scenarios, but warns about the potential of escalation. "What concerns me is if there are non-Ukranians and Russians involved in this, because that is effectively an internationalization of the cyber aspect of this conflict and could be treated by either combatant as a de facto escalation of the conflict beyond Ukraine's borders."

But for the Ukrainians involved in the IT Army's efforts, it's all part of a broader push across the country to do whatever it takes to fend off an existential threat. "If Ukraine falls, and they didn't do everything possible to stop that," says Williams, "why would you leave anything on the table?"

Cyber Realism in a Time of War

By Ciaran Martin

Source: https://www.lawfareblog.com/cyber-realism-time-war

Mar 02 – It turns out that the next war was not fought in cyberspace after all. Or at least the start of it has not been.

There has been no shortage of predictions over the past two decades about the importance of the digital domain in conflict since John Arquilla and David Ronfeldt warned that "cyberwar is coming" in a Rand Corporation paper back in 1993. As recently as November 2021, British Prime Minister Boris Johnson remarked in a testy exchange with Tobias Ellwood, chairman of the committee of the House of Commons that oversees defense, that "the old concept of fighting big tank battles on the European land mass are over … there are other big things that we should be investing in … [like] cyber—this is how warfare of the future is going to be."

Ellwood, a strong critic of the British government's decision to cut Army personnel in favor of investment in cyber capabilities, replied, "You can't hold ground in cyber." And on military tactics, if nothing else, Russian President Vladimir Putin seems to have agreed with him. Despite being one of the world's foremost offensive cyber powers, the Russian invasion of Ukraine has, thus far, been utterly conventional in its brutality as the horrific pictures from Kyiv, Kharikiv and other cities show on an hourly basis. And Ukraine's heroic resistance is similarly centered on the traditional understanding of war.

Even those of us long skeptical about the mischaracterization of cyber operations and cyber risk as catastrophic weapons of destruction, rather than a still serious but quite different threat of chronic disruption and destabilization, have been surprised by just how little cyber operations have featured in the early part of the invasion. The Kremlin's handful of serious cyberattacks on Ukraine ahead of and around the beginning of the invasion represents its long-standing campaign of cyber harassment of the country over the past decade, rather than a serious escalation of it. There seems to have been little effort, for example, to strike the core of Ukraine's internet infrastructure. Instead, the missiles rain, and the soldiers and tanks roll in. Similarly, the actions of pro-Ukrainian actors in defacing and taking down Russian websites may embarrass the Kremlin but hardly merit the much misused term of "cyberwar." (As yet unverified reports of a massive data leak of the personal data of Russian soldiers would be much more impactful if true).

The reasons for this underuse of Russia's sophisticated cyber capabilities so far in the conflict are unclear. In an article for War on the Rocks, Lennart Maschmeyer and Nadiya Kostyuk make a very interesting case that for all the sophistication and intensity of the Russian cyber campaign against Ukraine since 2014—a period in which Ukraine has

become "Russia's cyber playground," with energy outages, the disruption of government and banking payments, and the harassment of Ukrainian business and civic society—it has been a failure. They argue that Russia's hacks have made no material impact on the Ukrainian leadership's decision-making and seemingly did nothing to undermine Ukrainians' confidence in that leadership. Alternatively, the Kremlin's calculation may have been more basic. As BBC security correspondent Gordon Corera put it on the day of the invasion, "For all the talk about 'cyber war', today shows that when conflict escalates to this point it is secondary. If you want to take out infrastructure then missiles are more straightforward than using computer code. Cyber's main role now is perhaps to sow confusion about events." It could be that Russia chose to leave the internet untouched because it needed it for its own communications. Or it could be that Russia's state hackers suffered from a similar lack of preparation as their conventional forces.

As the Putin regime continues to initiate further bloodshed, Western policymakers will have many more urgent matters to tend to than reflecting on what the conflict says so far about cyber power. But those within the national security communities charged with thinking about cyber as a national security risk—and a national security capability—still need to find the capacity to evaluate three things:

- What the risk of cyberattacks against the West are as the conflict continues.
- How to analyze the role of cyber in the potential escalation in this conflict, including the potential use of Western cyber capabilities.
- What all this means for the West's cyber posture and capabilities.

The Cyber Threat to Ukraine's Western Allies

Even though cyber operations have featured to an unexpectedly small extent in the conflict so far, the West still remains at higher risk of serious disruption—as distinct from catastrophic attack—via the cyber domain than it was before the invasion. To point out the misrepresentation of cyber capabilities, their limitations, and the lack of use of them so far in the conflict is to invite allegations of complacency. It should not; a nuanced understanding of the actual risks makes for better preparation for them.

There are two reasons why Western governments' advocacy for implementing a posture of heightened alert—or "shields up," in the catchy slogan of Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency (CISA)—is the right one. The first is accidental "crossfire" damage in cyber operations. There is still every chance that Russia will decide to mobilize its cyber capabilities against Ukraine to a greater extent than it has so far, particularly if cyber is seen to have a potential role in demoralizing and disrupting the Ukrainian population and the ability of Ukrainian society to function. The nature of the networked world means that those attacks may not be cauterized within Ukrainian systems.

In June 2017, the Russian military intelligence service, the GRU, launched one of its periodic cyber operations against a range of Ukrainian targets in the so-called NotPetya attack. The attack misfired, and spread globally, devastating the ability of multiple Western companies to function, causing around $10 billion in commercial damage. Maersk, the shipping giant, was heavily disrupted. Merck, the pharmaceutical company, just won its court case in January 2022 and was awarded an insurance payout topping $1.4 billion to cover its NotPetya losses. Many businesses, from the global law firm DLA Piper to Cadbury's chocolate production facilities in Hobart, off the south coast of Australia, were badly disrupted. The irony of the NotPetya case, as with the globally devastating WannaCry hack a month earlier by North Korea, was that had the hackers done their jobs better, the global impact would have been far less. Should there be an intensification of Russian cyber aggression against Ukraine, which there may well be, especially if the war drags on, the risk of such a repeat miscalculation increases.

The second risk is about the use of Russian cyber criminals as proxies for the Russian administration. The year 2021 was terrible for Western cybersecurity, and it had nothing to do with Ukraine. It did have quite a lot to do with Russia, but in a particular way. Russia is home to the world's largest concentration of cyber criminals. Chainanalysis calculated that nearly three-quarters of the exponentially rising revenue from ransomware last year went to cyber criminal groups in Russia. More importantly, the economic and social impacts of Russia-based ransomware attacks were beyond what had been experienced before and exposed a soft underbelly of vulnerability for disruption across the West. In the U.S., a criminal operation against the ordinary enterprise network of Colonial Pipeline caused the company to switch off the transportation of fuel to the eastern United States, causing major shortages at gas stations. The sophistication of this criminal attack was well below the capabilities of the Russian state, illustrating the disruption and damage that can be caused by even semicompetent hackers. Worse, an attack by the so-called Conti ransomware group shut down the administrative body in Ireland charged with managing the national health care system with hugely disruptive consequences for cancer, prenatal and other critical health treatments.

The Conti group published a statement threatening retaliation against countries that support Ukraine and pledging loyalty to Mother Russia (and, incidentally, suffered a serious internal security breach, seemingly from a pro-Ukrainian working with them). Their statement is an unusually obvious glimpse into the strange but largely symbiotic relationship between the Russian state and organized cyber-criminality. Last year, President Biden protested vocally to President Putin in Geneva about the "safe harbor" Russia provided for such activity. And since then there have been some

rather theatrical arrests of Russian cyber criminals. But such "gangster diplomacy," in the words of former CISA director Christopher Krebs, cuts both ways. A cornered Putin may not just ease up on the criminals but encourage them to wreak more havoc on the West. So for both of those reasons, organizations like CISA and the National Cyber Security Centre in the U.K. (which I used to lead) warned not of any specific threats, but of a more general higher level of risk.

What We're Learning about Cyber Capabilities and Escalation

Both of these risks—accidental and the use of proxies—have existed for years, so the current heightened threat level is just that: a possible intensification of what we already face. But will the circumstances of the war lead to a serious and unprecedented escalation of hostile cyber exchanges between Russia and Western states? This would be beyond anything undertaken before against a NATO state from Russia (excluding the high-intensity, medium-sophistication operation against Estonia in 2007 before the world really began talking about how to deal with cyber escalation). And will the West conduct cyber operations against Russia beyond the sort of espionage and influencing operations already expected and publicly articulated in general terms?

Plenty of experts seem to think so. And given the unpredictability of the Putin regime, the risk must not be discounted. CrowdStrike co-founder Dmitri Alperovitch, who has predicted with great precision how the conflict would begin, worries that the early underperformance of the Russian military and the strength of Western sanctions could provoke a cornered Kremlin with less to lose down this route. Perhaps more intriguingly, Washington and London abound with speculation that offensive cyber forms a part of the planned pushback against Putin. Alperovitch's concern is then of a "horribly escalatory … tit for tat between the U.S. and Russia to see who can destroy one another's critical infrastructure" with "potentially devastating impacts for our security."

Predicting how this aspect of the conflict turns out is extremely difficult. But preparing for it starts with grappling with what the cyber capabilities are, how they work and what impact they have. And not every American policymaker seems to have Alperovitch's expert understanding of the complexities. The day after the invasion began, NBC News reported that President Biden had been presented with a range of options for a cyber response against Moscow. Speculating that tampering with railroad switches could be part of the plan, one anonymous U.S. government source mused that "you could do everything from slow the trains down to have them fall off the track."

That one sentence encapsulated the many misunderstandings of cyber capabilities, which perhaps explains why the White House dismissed the whole NBC story in unusually strident terms. There is a hierarchy of cyber operations from the extremely basic to the most sophisticated. Difficulty rises in correlation. Anyone can have a go at taking down a Russian government website. Taking a medium-size—or, too often, even a large—company offline is well within the capabilities of low-sophistication criminals. Doing something like slowing the trains down by sabotaging the signaling is usually much harder. The sorts of capabilities to do that belong to a handful of nation-states. Forcing trains off tracks takes you into the realm of Hollywood cyber fantasy: Cyber operations are computer code, and any railway system worthy of the name does not have a computer that can be reprogrammed to drive trains off the tracks. A system on which people's lives depend, like air traffic control, must always have a fall-back mechanism. So, air traffic control will know how to land planes safely in the event of the total collapse of the network, whether by accidental or malicious means.

Way back in 2013, Thomas Rid, now at John Hopkins University, captured all of these nuances in his masterpiece "Cyber War Will Not Take Place." Of particular importance was his insight that cyber capabilities are not like missiles. They do not directly destroy anything. As such, cyberattacks rarely, if ever, kill or physically hurt anyone. They have an effect: It is usually gathering information by espionage, influencing outcomes through subversion, or disrupting through sabotage. But even cyber sabotage is an indirect outcome. In theaters of war, a cyber operation could have a battlefield impact, not by firing anything but by disrupting military logistics and capabilities (and these are often hard to do). In times of war or peace, sabotaging a railway signaling means the trains should stop, causing mass inconvenience and inflicting economic costs. It should not cause the trains to power ahead, crashing into each other, causing mass fatalities. Similarly, the many cyberattacks on health care so far have been mostly disruption of health care administration, which has serious indirect consequences but is fundamentally different from bombing a hospital.

This lesson of the limitation of cyber as a weapon of war is not always well enough understood. In February, a column in Britain's Daily Telegraph, where Prime Minister Boris Johnson spent most of his career and which is widely read by the governing party, called cyber "effectively a second-strike capability for NATO" and claimed that the West's "cyber divisions are worth more than aircraft carrier battle groups or nuclear weapons in the particular circumstances of the Ukraine crisis," equivalent to an alternative nuclear deterrent.

The reality is that cyber capabilities, as currently understood, can do everything from low-level harassment to serious disruption of everyday economic and social activity. But they can't do what missiles, fighter jets and soldiers do. So what should weigh on the minds of Western policymakers when evaluating (a) the risks of deliberate cyberattacks by the Russian state against the West and (b) the role Western offensive cyber capabilities might have in the campaign against Russia's aggression?

Broadly, four limitations apply and need to be considered.

Ease. Just as cyber capabilities don't have the impact of missiles or ground troops, they can't be directed like them either. While basic hacks are easy, at the higher end, where governments would be aiming to have a strategic effect, they can be complex operations that involve gaining entry to the network, remaining undetected, finding the right parts of the network, and configuring the operation to gain the desired outcome. For basic effects this is easy; for targeted attacks on critical infrastructure, it is harder. It takes time (sometimes lots of it), skill and luck. A leader cannot just order a "cyber strike" against an air defense, air traffic control or health care system and expect a successful operational report the next day. The feasibility of any cyber operation is the first hurdle to surmount.

Effectiveness. Some of the more difficult cyber operations could have an obvious and useful impact at a time of war, such as disrupting military logistics or undermining air defenses. Outside of war, extremely complex operations, such as that undertaken against the Iranian nuclear program in 2011 via the Stuxnet worm, can give real-world strategic gain to those carrying it out. But these are usually very difficult to do. Stuxnet took years. Easier operations could be mounted against privately owned civilian critical infrastructure. As with sanctions, the aim here is not to harm, but to influence. So what would influence Putin, or enough influential Russians, or the Russian population as a whole, to change course? Taking down the Kremlin website, as hacktivists somewhere seem to have done, causes embarrassment. So too does interrupting Russian media. But is it enough to have a decisive effect? That is highly doubtful.

Escalation. So what would have such an effect? Here is where the risks of escalation would come in. Both Russia and some of the major Western powers undoubtedly possess the capability for large-scale disruption of critical infrastructure. (Russia has shown that with the two disruptions of Kyiv's electricity in 2015 and 2016.) What needs to be understood here is that any such activity would be escalatory. If there was an attack of unprecedented sophistication on a British or American power grid, it would be blindingly obvious who had carried out it. The portrayal of cyber as a domain where there could be a decisive but secret intervention is one of the most dangerous mischaracterizations of the domain. Offensive cyber therefore needs the same calm evaluation of adversary response as any other form of escalation or deescalation. It is just another form of state capability.

Ethics. This is unlikely to be on Putin's decision tree, but it will and should be on the West's. Health care is the obvious example. If Putin were to be found to have ordered, or facilitated, a repeat in a Western country of the sort of attack seen by the Conti group on Ireland's health care in 2021, that would be seen as a highly escalatory act, completely outside the bounds of acceptable behavior, and an openly hostile act against countries that are not combatants in the war in Ukraine. So what does this mean for Western capabilities? Would the West do the same to Russian health care? Last June in Geneva, Biden handed Putin a list of some 16 sectors he said must not be the subject of malicious cyber activity. This presages a longer-term American, and wider Western, agenda to try to bring some sort of generally accepted understanding about where red lines are with respect to cyber activity. The world is a long way off from agreeing to such principles. But—even in this terrible conflict—Washington is likely to be wary of being seen to have trashed these principles and put noncombatant Russian civilians at risk of disruption of health care.

So there are practical, strategic, and, in the case of the West, ethical limitations on the potential for escalation in cyberspace. That is not to say it won't happen. A desperate Putin could launch whatever capabilities are at his disposal, and even with all these limits on the potency of cyber capabilities, repeated hostile attacks could cause major disruption (though most probably not death and destruction) in the West. And in any case, enough non-escalatory threats are already out there through spillover and the use of proxies to justify the current state of high alert.

What This Means for Western Cybersecurity Posture

At this early stage, the conflict so far tells us something about the limitations of cyber capabilities in both directions in this conflict. And the early stages of this war provide two important lessons of cyber realism for Western policymakers and their societies.

The first is realism about the limitations of cyber capabilities. For the reasons already explained, cyber capabilities give neither side a big red button to decisively alter the course of events. The war thus far has emphasized the limitations of cyber as a tool of war rather than its centrality to it. A more realistic consideration and public discussion of the role of cyber as a tool of statecraft—both the risks it poses and the capabilities it provides—is urgently needed. Cyber capabilities provide the potential to disrupt, delay, annoy, rob, steal from, spy on and influence an adversary. They therefore have a place in and outside of conflict, but they are not magic invisible weapons.

Furthermore, high-end technological capability is a must for all modern military systems. But, to return to the exchange between Ellwood and Johnson, no one should think that cyber operations, however defined, provide some sort of alternative capability to use computers to bring about military-style impact. Ellwood must be right about the limitations of cyber power, even if Johnson is surely right to overrule him on the question of no-fly zones. It's not just that you can't hold ground with cyber; you can't gain or reclaim it, either. That's not the way cyber capabilities work.

The second lesson, once the crisis has passed, brings to mind a famous speech by Winston Churchill a century ago, not long after another European land war. Referring to the pre-war reemergence of the age-old problem of Ireland in British politics, he said that "the whole map of Europe has been changed, but as the deluge subsides … we see the dreary steeples of Fermanagh and Tyrone emerging once again," citing the two Ulster counties most hotly contested as the island was divided. What he was saying was the world may have changed, but some problems were the same, and just as intractable as they were before the war.

The "dreary steeples" in Western cybersecurity are the problem, as old as the internet itself, of chronic digital insecurity. It is significant that the warnings coming from the likes of Washington and London to their own citizens are not about "cybergeddon." They are about the risks of overspill from Russian attacks and from Russian proxies, and the potential that the Putin regime may decide to take over from the proxies and do it better.

So a state can spend a fortune on high-end offensive capabilities and on securing its own most important military and other national security assets against cyber risks. But the reason people are scared about cyber in the context of this war is that they know that cyber defenses across their entire societies aren't strong enough yet (though they are better than they were). The strategic vulnerability to disruption and sabotage lies not so much in the military space but in the hospital booking system (Ireland), the logistics schedule (Maersk), the political party (as in the U.S. experience in the 2016 election), the electricity grid (Kyiv), and thousands of other mainstream, civilian, mostly privately owned networks.

However this horrendous war turns out, the West will be left with these strategic cybersecurity weaknesses to tackle. And in the meantime, the cyber domain may influence the war at the margins, but it will not decide it.

Ciaran Martin is Professor of Practice at the Blavatnik School of Government, University of Oxford. From 2014 to 2020 he set up and then led the National Cyber Security Centre of the United Kingdom, part of the intelligence agency GCHQ.

Anonymous vs. Russia: Hackers Say Space Agency Breached, More Than 1,500 Websites Hit

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/anonymous-vs-russia-hackers-say-space-agency-breached-more-than-1500-websites-hit/

Mar 01 – A hacking group affiliated with Anonymous claimed that it breached the control center of Russian State Space Corporation "Roscosmos" and cut off the agency's control over its spy satellites as part of the ongoing cyber-offensive against Russian government targets in protest of the invasion of Ukraine.

"The Russian Space Agency sure does love their satellite imaging," the group NB65 said in a post early today, posting accompanying screenshots. "Better yet they sure do love their Vehicle Monitoring System. The WSO2 was deleted, credentials were rotated and the server is shut down. Network Battalion isn't going to give you the IP, that would be too easy, now wouldn't it? Have a nice Monday fixing your spying tech. Glory to Ukraine."

"We wont stop until you stop dropping bombs, killing civilians and trying to invade," NB65 added. "Go the fuck back to Russia."

The same group did a data dump Sunday of more than 40,000 files that they said were swiped from the country's Nuclear Safety Institute (IBRAE). "We don't have the capacity to translate this many Russian documents, so enjoy and let us know what you find," the group said.

On Monday, one Anonymous account reported on Twitter that hackers associated with the collective had taken down more than 1,500 websites connected to the Russian and Belarusian governments, state media outlets, major banks and companies over the previous 72 hours.

Accounts reporting their hacks under the #OpRussia or #OpKremlin hashtags on Twitter also said the website of the Russian Ministry of Labour and Social Protection had been knocked offline (and was still down this evening).

Anonymous also leaked a database that hackers said came from breaching Russia's Ministry of Economic Development.

And hackers breached a maritime traffic tracking site to give Russian President Vladimir Putin's yacht "Graceful" a new call sign, ANONYMO, and a new destination, FCKPTN.

Anonymous accounts were encouraging those without hacking skills to join Russian social media sites and spread information to counter Russia's disinformation or lack of news about what is really happening in Ukraine.
They also countered disinformation that they said was being spread by Russian trolls using fake Anon accounts in order to discredit the Anonymous campaign by claiming that on March 3 the hackers would breach private Russian citizens' bank accounts and send the money to Ukraine. "This is false. Anonymous will not attack the people but the government. Fakes, expect us!" one Anonymous account responded.
And hackers also went after the pro-Russia Conti ransomware group, leaking internal chats and files from the group. The offensive action may have been what prompted this update on the Conti threat from DHS' Cybersecurity and Infrastructure Security Agency on Monday, warning stakeholders to not think the threat had abated: "Conti cyber threat actors remain active and reported Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike. While there are no specific or credible cyber threats to the U.S. homeland at this time, CISA, FBI, and NSA encourage organizations to review this advisory and apply the recommended mitigations."
A group called the Belarusian Cyber-Partisans said it hacked railway systems in Minsk, Orsha, and Osipovichi to obstruct Russian military movements toward Ukraine from the country. "The monitoring system of the Belarusian Railway's internal computer network," the group said, displaying a screenshot on Twitter. "An outdated piece of crapware that runs on Windows XP."
The Cyber-Partisans stressed that their railway hack would not endanger civilians: "Manual control mode is enabled, which will slow down the movement of trains but will NOT create emergency situations."
Hackers identifying with the Anonymous collective announced the launch of #OpRussia Thursday (Eastern time), saying that their cyber operations initially briefly took down some websites associated with the Russian government. The #OpRussia or #OpKremlin hashtags used to announce actions against Russian sites are similar to Anonymous' #OpISIS campaign that targeted the terror group's wave of online propaganda and the #OpKKK campaign that targets white supremacists.
Members of the collective posted a video press release Saturday that vowed "these actions will continue," as "activists will not sit idle as Russian forces kill and murder innocent people trying to defend their homeland."
The hackers acknowledged that "some of our actions may be considered illegal in the eyes of various governments," but they saw "no reason any western laws should be used against our actions in trying to protect and defend the people of Ukraine, and also to help educate the people of Russia."
DHS' Cybersecurity and Infrastructure Security Agency (CISA) and the FBI issued a joint Cybersecurity Advisory Saturday providing an overview of destructive malware that has been used to target organizations in Ukraine as well as guidance on how organizations can detect and protect their networks. On Wednesday, Russian cyber forces hit the websites of several Ukrainian banks and government departments with a wave of DDoS attacks.
An intelligence brief from the Department of Homeland Security in January warned stakeholders that Russia "would consider" launching a cyber attack against the United States if the U.S. or NATO respond to Russia's potential invasion of Ukraine in a way that the Kremlin perceived as threatening to Russian security.
The memo also noted that Russia's threshold for directly launching a destructive attack against U.S. critical infrastructure with its cyber arsenal "probably remains very high" though Moscow "continues to target and gain access to critical infrastructure in the United States."

Bridget Johnson is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Bridget is a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, New York Observer, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera, BBC and SiriusXM.

New Technology Will Make Cyber Attacks Easier to Detect

Source: https://i-hls.com/archives/113366

Mar 01 – Ransomware and malware, as well as cyberattacks, are a real threat to the systems of governments and local authorities, and the number of warnings regarding various attacks has increased in recent years. This is why the University of Waterloo have teamed up with Palitronica, a security company, and the Federal Government of Canada to develop a solution to enhance government IT infrastructure.

In an effort to guard against cyberattacks and security leaks, researchers at the **University of Waterloo** have created a technology that monitors increased energy consumption, which will help protect governments, businesses and other organizations.
Artificial intelligence (AI) software enables the technology to collect information with the assistance of hardware, so as to determine whether the use of electricity in the system conforms to known and expected patterns. When exceptional metrics are compiled, the artificial intelligence system sends an alert to the security officer in the organization, warning that the organization's infrastructure could be under attack by hackers or software attempting to steal or lock precious data.
In addition, when multiple machines show signs of increased power usage at the same time and in similar patterns, the suspicion increases that there might be crypto-ransomware distributed on the network. As reported by uwaterloo.ca, several authorities in Ontario, Canada, are undergoing extensive testing of the new technology. It is designed to complement existing control systems (such as network intrusion detection) and, eventually, will provide greater security for power-based systems.

Cyberspace: The New Battleground in Modern-Day Warfare

Source: https://www.homelandsecuritynewswire.com/dr20220303-cyberspace-the-new-battleground-in-modernday-warfare

Mar 03 – Bolstering cybersecurity is becoming ever more important as nation states wage war in new and complex arenas.
That is the view of two UNSW academics in the wake of a wave of online attacks linked to Russia's military invasion of Ukraine.
As well as the use of tanks and bombs and soldiers on the battlefield, countries are now also waging war in cyberspace in order to weaken their enemies, most notably by targeting crucial infrastructure such as power and communications systems.
For example, in recent days and weeks Ukraine has accused Russian hackers of launching massive denial of service attacks on their government agencies, banks and the defense sector.
The United States government also claims Russia breached the networks of multiple defense contractors and gained sensitive information about weapons-development communications infrastructure.
And back in 2015, a series of power outages across Ukraine were allegedly caused by military hackers in the Russian GRU (Intelligence Agency) Main Center for Special Technologies.

CIA Triad

"Cyber warfare has become a tool by nation states to attack other countries," says Professor Sanjay Jha, deputy director of the UNSW Institute for Cybersecurity (IFCYBER).
"In the modern digital world, by attacking a computer server in the network of some critical piece of infrastructure, you can potentially take down an entire power system and with that, you could paralyze large parts of the economy.
"Other targets might be the banking system or a server that deals with communications systems so these system become unavailable to legitimate users.
"In cybersecurity any system needs to maintain confidentiality, integrity and availability, aka the 'CIA Triad'.
"Availability is actually very important, and attackers can affect that by launching what is known as a distributed denial-of-service (DDoS) attack where they just bog down a system with junk data that it has to process.
"Nowadays attackers can draft 20, 30, 50 or 100s of servers all over the world sending packets of information and maybe wasting 99 per cent of the server's time dealing with it.
"Just like in conventional conflict, each party wants to maximize the amount of damage and discomfort to the target."
Professor Salil Kanhere, another cybersecurity expert from UNSW's School of Computer Science and Engineering, says finding and then fixing vulnerabilities in computer programs or software is one of the most crucial ways to defend against attacks by state-sponsored hackers and others.
In December 2021, for example, news started to spread of an exploitation in Log4j, a software library that records a wide variety of otherwise mundane information in a vast number of computer systems.
It became clear that attacks on Log4j could allow hackers to submit their own code into the targeted computer and potentially steal information or even take control of the affected system.
"This particular vulnerability was really bad because Log4j software is used in a wide variety of consumer and enterprise services, websites, and applications," says Professor Kanhere.
"The question then becomes, do organizations have the resources to quickly act on the attacks and fix the vulnerability. The big players, and government agencies, will be able to but small-medium enterprises possibly can't react very fast, which means those systems are still vulnerable to attacks.
"What attackers then do is scan the internet, trying to find a system that still has this weakness and then exploit it.

"The major problem is that computer systems nowadays are so complex and intertwined that if attackers find one weak link somewhere, that is enough to gain access into critical systems and steal data or launch further attacks."

Social Engineering

On top of all that, cyber attacks can also be cleverly targeted not only at computers themselves but also by the humans who use them. Phishing attacks can trick users into giving out sensitive information that then compromises security and allows nefarious access into systems.

"Some of the phishing nowadays is so sophisticated," says Prof. Jha. "So much so that even a fairly educated cybersecurity person may be tricked.

"There are also social engineering tactics where people are manipulated into clicking something that then allows an attacker to install malware, or ransomware, or steal information."

In times of war, such as the current Russian invasion of Ukraine, Prof. Kanhere says gaining access to information has the potential to have a huge impact on the success or failure of actual military attacks.

Discovering battle plans, potential maneuvers of troops and equipment, or hacking into secure communications systems used by soldiers and their command could help win wars in the modern age.

"In the past a lot of that information would have been on paper, but now it is all digitized and therefore may be vulnerable," Prof. Kanhere says.

"If you can extract that information then it could certainly give you the upper hand militarily. Traditional wars were fought on land, air, and sea. But now we also have space and cyberspace as the fourth and fifth battlegrounds that are emerging."

And that means that all major governments around the world, not just the Russians, are likely to have cyber experts on hand to play their part in the way 21st-century conflicts are now fought.

"The specific details about that are bordering on national intelligence which I'm not an expert on, but it's not surprising to think that given the importance of information technology and the potential to disrupt networks, that would be a very obvious choice for militaristic efforts," Prof. Jha says.

"It would be reasonable to conclude that all governments, not just Russia, have some sort of cyber units placed in different organizations with the capability of launching offensives if needed."

In terms of bolstering cybersecurity, the UNSW academics say it is a constant game of cat-and-mouse as countries try to secure their systems and fix vulnerabilities faster than the hackers can exploit them.

Artificial Intelligence

Prof. Jha is currently conducting research, funded by Cybersecurity CRC, that aims to help develop tools to identify potential security issues in Australia's Distributed Energy Resource Management System (DERMS) that links a range of electrical power industries.

He is also involved in work to improve artificial intelligence models that can identify patterns of cyber attacks and predict future risks using a range of internal and external intelligence.

Prof. Kanhere, meanwhile, is researching the use of machine learning to design network protocol fuzzing tools, which can automatically find vulnerabilities and attack strategies in network routing protocols that are critical to the functioning of the internet.

"The general advice is for systems to be patched to make sure they are secure and for networks to be configured so they can handle any denial-of-service attacks by doing some early detection," says Prof. Jha.

"There is a lot of development in artificial intelligence and machine learning, plus software looking at vulnerability detection.

"But as our dependency on computers keeps increasing, these problems and these attacks are not going to go away. As quickly as we come up with a solution, the bad guys are thinking of another way to attack.

"Now that these vulnerabilities can be exploited during warfare, it's becoming absolutely important that we pay a lot attention to cybersecurity going forward."

A War Within a War: Cyberattacks Signal a New Approach to Combat

Source: https://www.homelandsecuritynewswire.com/dr20220303-a-war-within-a-war-cyberattacks-signal-a-new-approach-to-combat

Mar 03 – Over the past few days, the Russian invasion of Ukraine has captivated the attention of the world. But in addition to fighting with troops on the ground, the nation is also defending itself on another front, from cyberattack.

This 'war within a war' is another strategy used by Russia to disrupt and disable life in Ukraine and increase that nation's vulnerability. But the attacks aren't confined just to two

nations. The ripple effects can be seen around the world. In fact, Ukrainian leaders have asked international cyber experts to help them create an "IT Army" to protect it from harm.

Professor Stephen Fitzgerald of the Operations and Information Management Department at the University of Connecticut School of Business has closely monitored the cyber threats in Ukraine. In a conversation with *UConn Today*'s Claire Hall, he says the attacks and counterattacks are something the U.S., too, should follow closely.

Claire Hall: How will this online war impact the United States?

***Stephen Fitzgerald*:** This is a tough question to answer because there is currently so much uncertainty. While the U.S. is physically distant from the fighting, cyberwarfare is not constrained by distance. Some say President Biden has been pressured to take action on Russia, many of which include cyber attacks of our own to disrupt Russian internet connectivity, electrical power, and transportation. Of course, this invites a retaliatory effort from our historic adversary which should give officials appropriate pause. It is completely reasonable to expect that whatever we can do to Russia, they can do to us. The U.S. does not want open cyber conflict with Russia and an actual cyber attack from the U.S. is almost completely off the table from what is being discussed, according to the White House.

This back and forth highlights just how tricky the situation is and how hard it is to pin down reliable information. One concern that we can cite for certain is the idea that the software programs used in these attacks could spill over or cause collateral damage based on their design.

Hall: How vulnerable is the U.S. to similar attacks?

***Fitzgerald*:** It is unlikely that individual Americans will be targeted by attacks, but if we were to see conflict we would likely see attacks that target valuable infrastructure or specific corporations.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has made a point to warn Americans about some of the malware we have seen coming out of the conflict, and has taken on the mantra "Shields Up" to describe our nation's cyber defense posture.

"While there are no specific or credible cyber threats to the U.S. homeland at this time, Russia's unprovoked attack on Ukraine, which has involved cyber-attacks on the Ukrainian government and critical infrastructure organizations, may impact organizations both within and beyond the region, particularly in the wake of sanctions imposed by the United States and our Allies. Every organization—large and small—must be prepared to respond to disruptive cyber activity," CISA said in a statement.

In the meantime, CISA has published a page describing some of the steps and resources individuals and companies can use to protect themselves from any sort of online shrapnel. As with all cybersecurity risks, the best thing we can do is to proactively prepare and have a plan if we are to be attacked.

Hall: How might the international community address these aggressions?

***Fitzgerald*:** Microsoft, which has for some time called for the creation of a new Geneva Convention pact governing cyberspace, is now suggesting that some cyberattacks on Ukraine could be considered war crimes under existing international laws. This is certainly something the international community will need to address at some point in the near future. Although international cyberlaw is in its infancy, it will need to quickly mature as the international community deals with the ongoing wartime cyberattacks.

High Above Ukraine, Satellites Get Embroiled in the War

Source: https://www.wired.com/story/ukraine-russia-satellites/

Mar 03 – The traffic jam stretched from the Russian city of Belgorod to the Ukrainian border. Google Maps marked the congestion with red and orange, just as it does in all countries where the app is used to track traffic. But the GPS satellites sending these vehicles' positions to Google were not picking up an ordinary traffic jam. This was 40 kilometers of traffic caused by Russian troops. That convoy turned out to be an early warning that the Russian troops amassed on Ukraine's borders were on the move. It was first noticed at 3:15 am on Thursday of last week by Jeffrey Lewis, a professor at the Middlebury Institute of International Studies (MIIS), a graduate school in California—hours before reports of Ukraine's first explosions filtered into the news. But he did not stumble on it by accident. Lewis had a tip-off from a radar image taken by a commercial satellite company called Capella Space, which showed Russian troops lined up along the road in columns near Belgorod. "When the Russians are camping for a long time they park their tanks in a square and they put up tents," says Lewis.

But this satellite image showed troops in a very different formation. There were no tents; they were ready to move. When one of Lewis' colleagues started searching for the routes this column might take to move toward Ukraine, he found the traffic jam. "It's really a story about fusing different kinds of data," says Lewis.

Then, on February 28, Google said it would temporarily turn off live traffic updates in Ukraine "after consulting with multiple sources on the ground, including local authorities." Google did not elaborate on why it was worried about the feature. But researchers speculate the company is concerned that traffic data revealing the location of troops or refugees could be

used to inform military strikes. “You can understand why Google would not want to be a party to providing targeting data in an international conflict,” says Lewis.

Courtesy of Capella Space

In the sky above Ukraine right now are around 50 working satellites, estimates Todd Humphreys, a professor at the University of Texas. Those satellites have become a key part of Ukraine’s efforts to fend off a Russian invasion. The government there has been pleading for satellite images for clues of where Russian troops might move next.

US authorities gave Ukrainian president Volodymyr Zelensky a satellite phone so they could stay in touch, according to CNN. And Ukraine is also flying drones made by a Turkish company, Bayraktar, which allows some of its models to be controlled remotely via satellite link. But the reliance on commercial satellites in Ukraine is raising concerns about the power they give to the companies that control them, and also the risk of satellite companies being dragged into the conflict.

This is not the “world’s first satellite war.” That title was given to the Gulf War, three decades ago. Since then, space has become a normal part of modern conflict, says Almudena Azcárate Ortega, associate researcher at the United Nations Institute for Disarmament Research (UNIDIR). “In recent years, there's been a tendency to outsource a lot of this work due to the fact that private companies have specialized knowledge and they are often better able to develop and deploy certain types of space of technology,” says Ortega, adding that many space objects are now called “dual-use.” “That means that one satellite can be used at the same time for military purposes, but also for civilian everyday things,” she says.

At this time of year, Ukraine’s skies are carpeted with clouds. Companies are now in high demand if they can produce a type of data called radar, which works at night and can see through clouds. Radar images are generated by Synthetic Aperture Radar (SAR) satellites, which map the world in a way that’s similar to how bats navigate in the dark—by sending out radio waves and measuring how their signals are reflected back. To carry out their work, open-source researchers like Lewis buy radar data from companies like Capella and Planet, both based in San Francisco. They also have to pay for a software, such as ENVI, to interpret that radar data and turn it into images. His team’s ability to use this software is a result of years of training, he adds. “Three years ago we would not have been able to do this.”

Open-source researchers are not the only ones demanding this data. Militaries want it too. "We badly need the opportunity to watch the movement of Russian troops, especially at night when our technologies are blind,” Ukraine’s vice prime minister Mykhailo Fedorov said on March 1. In a letter posted on Twitter, Fedorov called on eight commercial satellite companies to send SAR satellite data to help Ukraine’s Armed Forces see Russian troop movements through clouds. One of the companies to respond

was Capella. Its founder and CEO, Payam Banazadeh, says the company is providing satellite imagery of Ukraine to both the Ukrainian and US governments.
"We have capabilities that governments don't have," says Banazadeh. He shrugs off questions about staying neutral in a conflict. "We're a private commercial company and anyone can—as long as we have imagery available—purchase imagery from us," he says. "But beyond that, we're an American company and we're not playing politics or policy. We've built a commercial capability that really anyone in the world can have access to."
But some researchers are worried that the reliance on satellite imagery has given too much power to the companies that control this technology. "There's companies like Maxar and Planet that are privately owned and they have the final say on whether or not they want to share the information," says Anuradha Damale, policy fellow at the British American Security Information Council think tank. "Do we trust these organizations to act like this in every conflict, given that they may have military contracts with specific countries?"
The role of private companies in conflicts such as Ukraine means commercial satellites could become targets. In the days before Russia invaded, US space officials warned satellite companies that the conflict could extend into space. "Ensure that your systems are secure and that you're watching them very closely because we know that the Russians are effective cyber actors," said National Reconnaissance Office director Chris Scolese at a National Security Space Association conference on February 23. "It's hard to say how far their reach is going to go in order to achieve their objectives, but it's better to be prepared than surprised."
Those attacks could take the form of cyber-attacks or spoofing, when a radio transmitter is used to fake a GPS signal. Russia has been one of the few countries to demonstrate its spoofing capabilities in the open, says Humphreys, of the University of Texas. "They are causing all sorts of trouble in the Mediterranean because of spoofing they're doing in Syria," he says, adding this has been causing problems for Israeli planes flying into Tel Aviv. Humphreys says Russia is not trying to disrupt Israeli planes but trying to prevent a repeat of the drone swarm that attacked its Hmeimim air base in Syrian in 2018. "So they are sending out jamming and spoofing signals to confuse the drones' GPS receivers," says Humphreys.
But Russia has not only been tricking satellites to bolster its defenses, it has also practiced blowing them up. In November, the country carried out a missile test on one of its own satellites, raising the possibility that satellites could eventually become physical targets. Capella's Banazadeh does not believe his company is facing an imminent threat as a result of its involvement in Ukraine. "Is it something that is keeping us up at night? No," he says. "Is it something that we're aware of and we've made sure that the company and the satellites are protected? Yes."
Another company that could become a target for attacks is Elon Musk's Starlink, which delivered terminals to Ukraine with the idea that they can provide a backup internet connection if the country's network infrastructure is damaged by fighting. However, businesses are unlikely to announce publicly if their satellites have been spoofed or jammed, says Rainer Horn, managing partner of German consultancy SpaceTec Partners, adding that he has not heard about any recent attacks.
But with violence intensifying in Ukraine, researchers suspect satellites have already been targeted—we just don't know about it yet. "The way Putin is moving right now, I wouldn't be surprised if that was something he would consider or has already done," says Damale.

Why the undersea cables that connect the world are a subject of concern

Source: https://www.theweek.co.uk/news/technology/955812/undersea-cables-connect-world-subject-concern

Feb 18 – The "backbone" of the internet, the data superhighway that connects the world's online computer networks, is a web of fiber-optic cables. Between continents and land masses, the internet relies on cables crossing the sea floor.

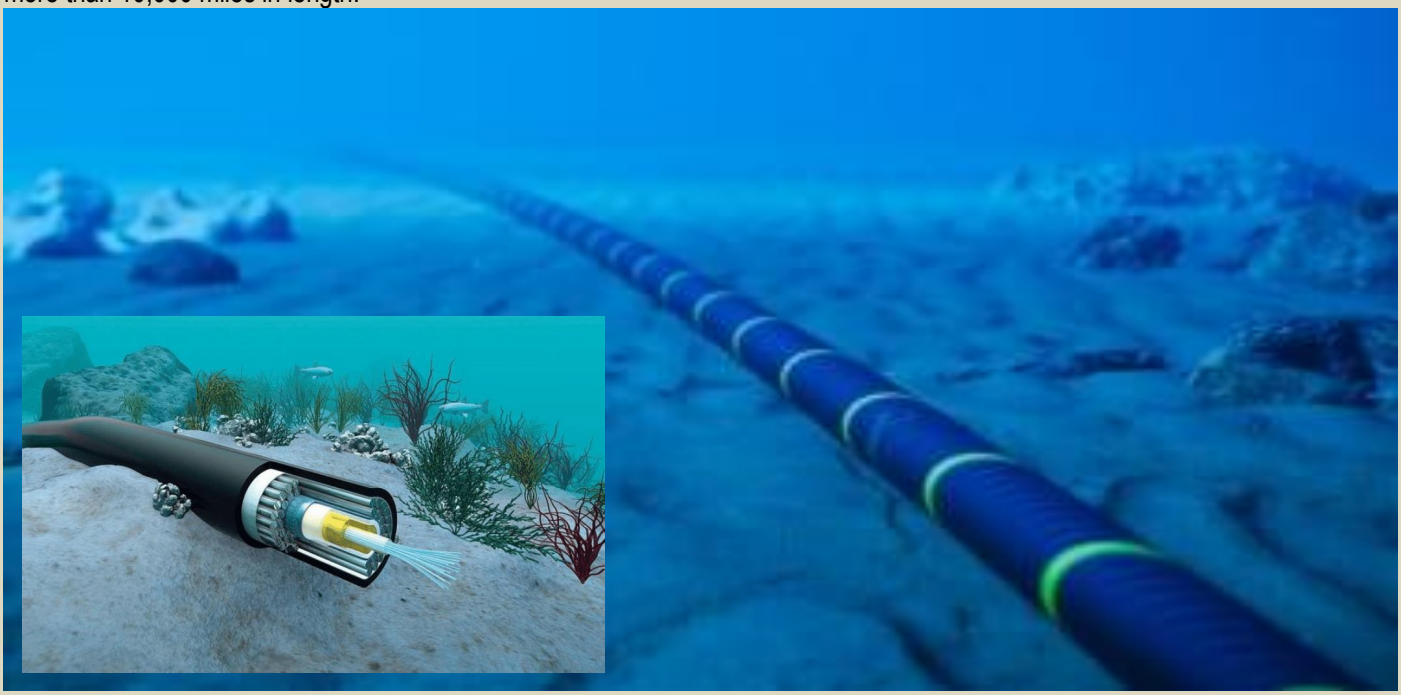
Internet network, which is over half a million miles in length, and comprised of over 200 independent systems of interconnected cables, carries over 95% of global communications (the rest is carried by satellite). If you open a foreign webpage, the data you're accessing will have been propelled by lasers down fiber-optic threads under the sea, at almost the speed of light. In a single day, this network also processes some $10trn in financial transfers via the SWIFT system, which manages global bank transactions.

The recent explosive growth of cloud computing has vastly increased the volume and sensitivity of data – from military documents to scientific research – crossing these cables.

How do the cables work?

Undersea cables have been used since the 1850s. Today, they've evolved into technological marvels. Laid by slow-moving ships, they are typically between two and seven inches thick and have a lifespan of approximately 25 years. Each cable contains fibre threads capable of transmitting data at 180,000 miles per second, wrapped in steel armour, insulation and a plastic coat.

These fibres have the capacity to transmit up to 400GB of data per second (about enough for 375 million phone calls); a single undersea cable contains anywhere up to 200 such fibres. By way of context, eight fibre-optic strands could transfer the entire contents of the Bodleian Library across the Atlantic in about 40 minutes.
Some new cables, such as the Asia-America Gateway cable, which links California to the Philippines and Southeast Asia, stretch to more than 10,000 miles in length.



Why are they a subject of concern?

Because of their vulnerability. To take an extreme recent example: in January, a volcanic eruption severed the single cable to Tonga, cutting off all communications to the Pacific island for five days. Phone contact has now been restored, via satellite, but normal internet service has still not been reinstated.
Damage occurs fairly regularly: an estimated 100 to 150 cables are severed every year, the vast majority due to fishing equipment or anchors. Usually, the system has enough slack in it to deal with such damage: most nations are connected by scores of fibre-optic cables, so if one or two are damaged, data can be rerouted without disruption. But problems do occur. In 2008, three cables linking Italy and Egypt were accidentally cut, causing data connectivity between Europe and the Middle East to plummet, with knock-on effects for American military operations in Iraq.

How could this affect the UK?

Britain, unlike Tonga, is connected to the rest of the world by around 60 cables, not just one: from the 80-mile CeltixConnect cable to Ireland; to the Tangerine, which runs 81 miles from Kent to Belgium; to the Tata TGN-Atlantic, stretching 8,000 miles from Somerset to New Jersey.
Yet the UK is far more reliant than Tonga on digital services. “Even more significantly, unlike Tonga, we have powerful enemies,” said Harry de Quetteville in The Daily Telegraph. Sabotaged cables could pose “an existential threat” to British security, warned the now-Chancellor Rishi Sunak in a 2017 report for the Policy Exchange think tank. “The most severe scenario… of connectivity loss is potentially catastrophic,” he added – and even relatively limited damage could “cause significant economic disruption and damage military communications.”

How might they be sabotaged?

“Disrupting cables is not only possible,” wrote Sunak, it’s “surprisingly easy.” There is a long history of countries hostile to one another sabotaging cables. Britain cut five German cables in the First World War; in the Cold War, the US placed wiretaps on Soviet subsea cables.
When Russia annexed Crimea in 2014, one of its first moves was to sever its cable connection. The cables are generally owned and installed by consortia of internet and telecoms companies, without much government oversight. Their locations are usually both isolated and publicly known, making them vulnerable to sabotage. There are also several

"choke points" potentially vulnerable to attack, such as Wall Township, a small town in New Jersey where five major cables come ashore.

Have any cables been threatened?

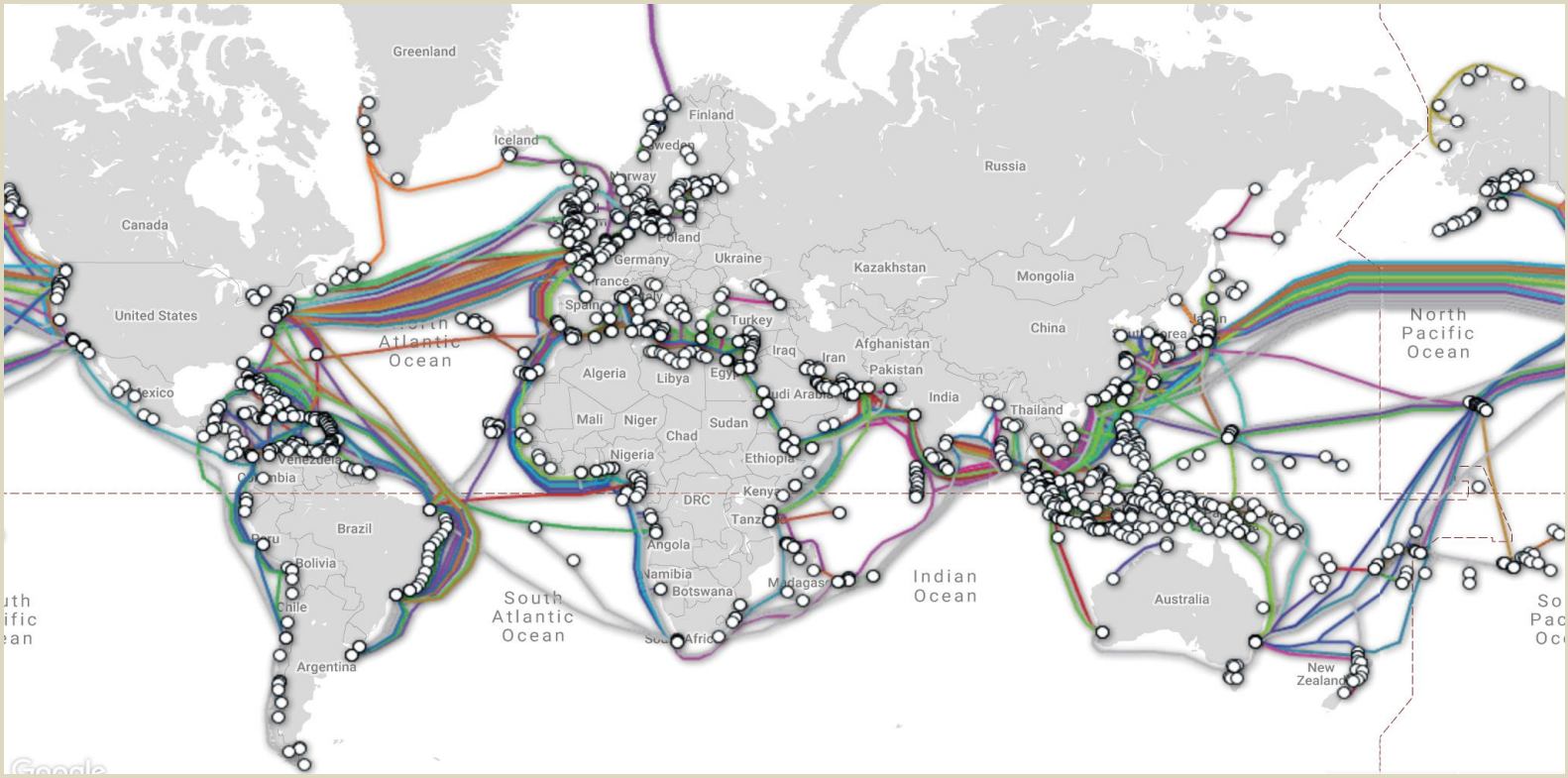
Just last month, the head of the UK's Armed Forces, Admiral Tony Radakin, warned that Russian submarine activity is threatening underwater cables and that the Kremlin has "grown the capability" to exploit them.

Russia, through its Main Directorate of Undersea Research, probes cables using vessels such as the research ship Yantar, equipped with submarines and undersea drones thought to be capable of cutting or tapping cables. Last summer, it was tracked in a position around transatlantic cables off the coast of Ireland; a month later, it was in the English Channel.

What can be done about this?

A number of concrete proposals have been put forward. One option is to establish "cable protection zones", which would ban certain types of anchoring and fishing, and require greater disclosure by vessels inside them. Other solutions include updating international law around cables, and establishing treaties that would criminalise foreign interference.

Nato has held exercises to hone potential responses to an attack on infrastructure. So-called "dark cables" – or backup systems – could also be built to increase resilience in the global network. But it's clear that much more needs to be done to protect a critical part of the infrastructure of modern life.



TeleGeography's Submarine Cable Map (March 2019).

Invisible and Vital: Undersea Cables and Transatlantic Security

By Pierre Morcos and Coli Wall

Source: https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

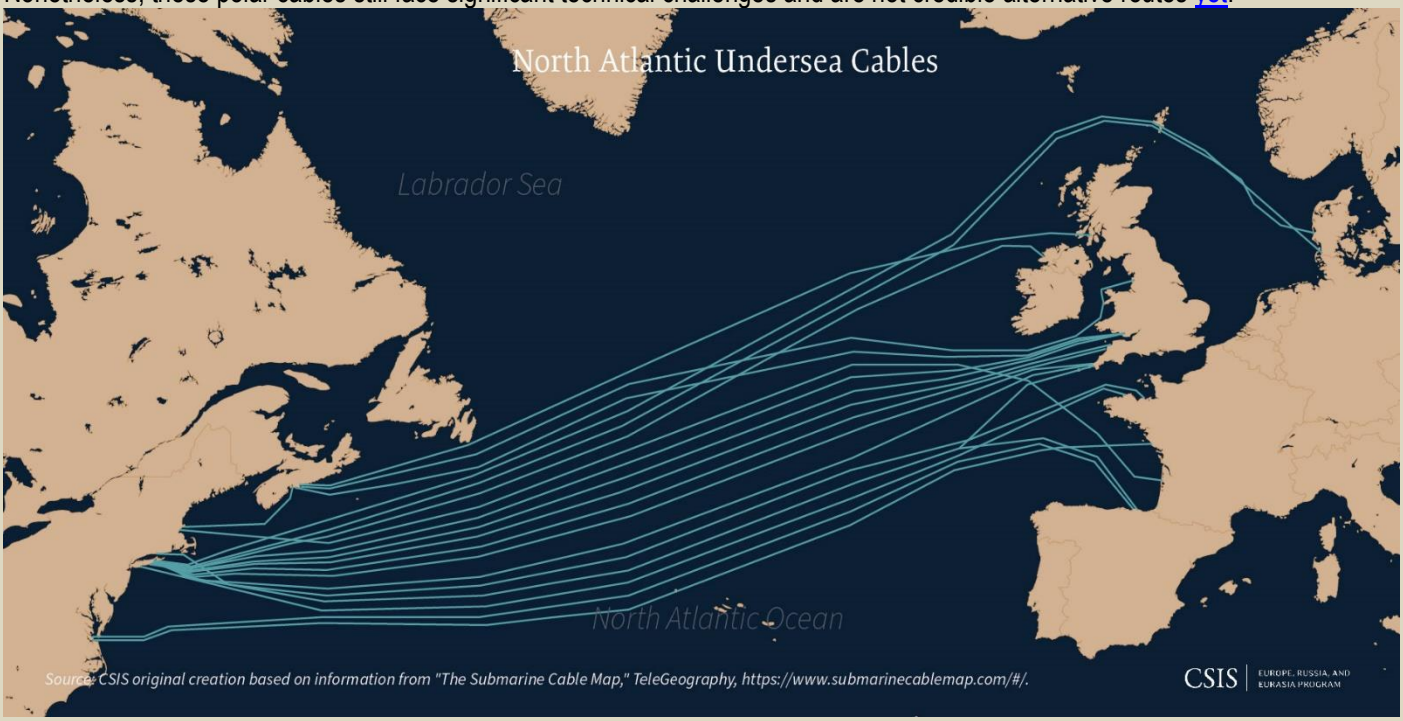
In October 2020, allied defense ministers received a confidential report on a pressing challenge that often receives less attention than it is due: the vulnerability of transatlantic undersea cables. Sometimes described as the "world's information super-highways," undersea cables carry over 95 percent of international data. In comparison with satellites, subsea cables provide high capacity, cost-effective, and reliable connections that are critical for our daily lives. There are approximately more than 400 active cables worldwide covering 1.3 million kilometers (half a million miles).

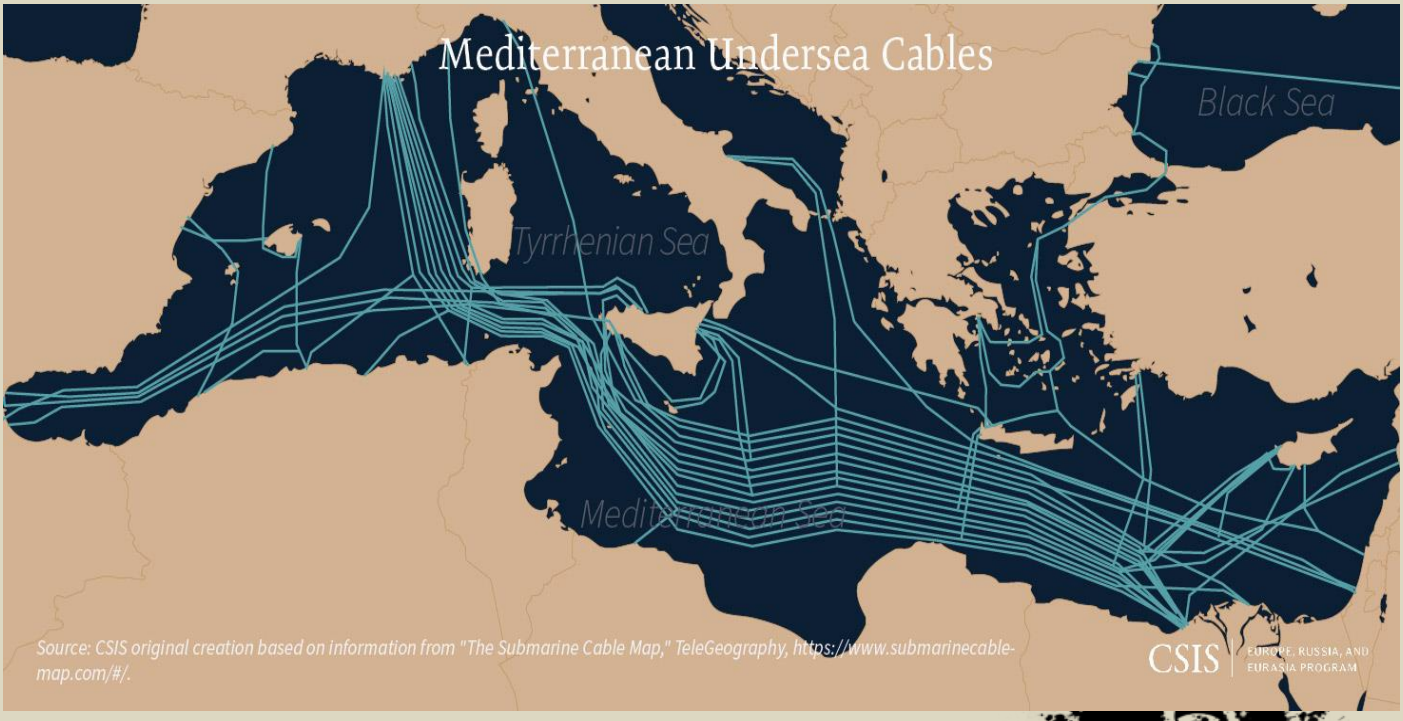
After the October meeting of allied defense ministers, and in the months since, Secretary General Jens Stoltenberg of the North Atlantic Treaty Organization (NATO) underscored the need for the alliance to monitor and protect this critical infrastructure. However, despite the proliferation of public statements underlining the importance of protecting them, collective

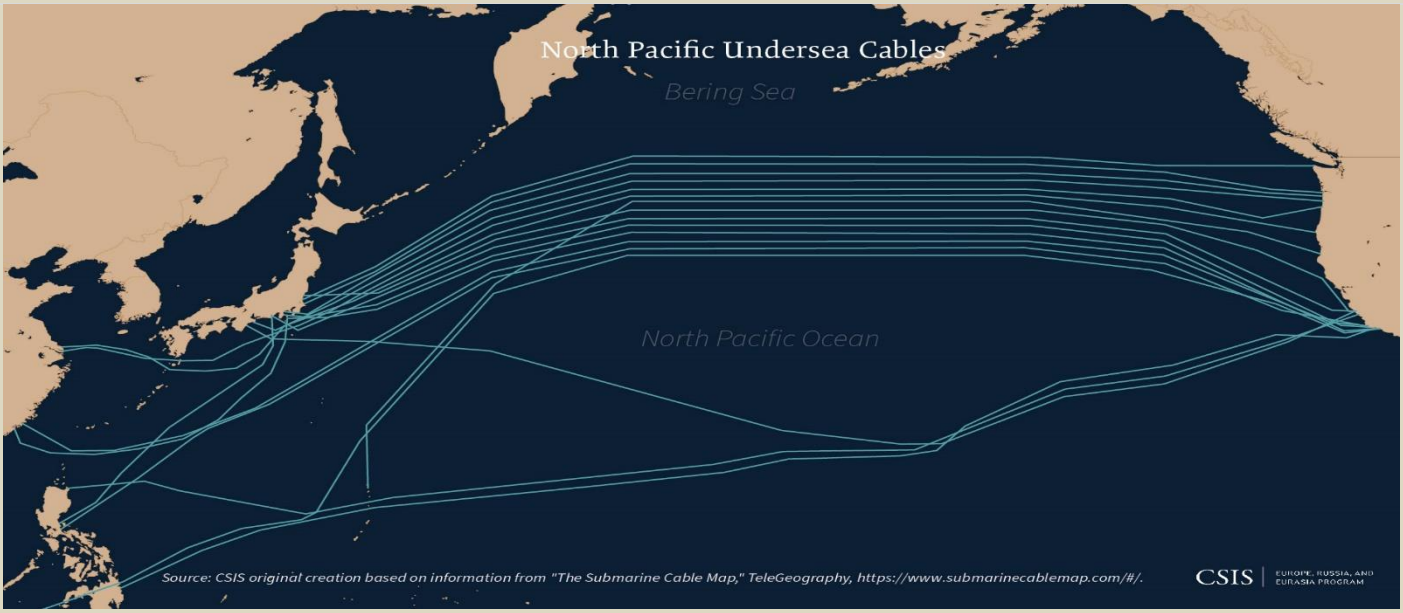
action to enhance their security has so far been lacking. A number of measures could be taken by allies to effectively protect subsea cables harnessing the full potential of their bilateral cooperations, NATO, and the European Union, in close coordination with the private sector.

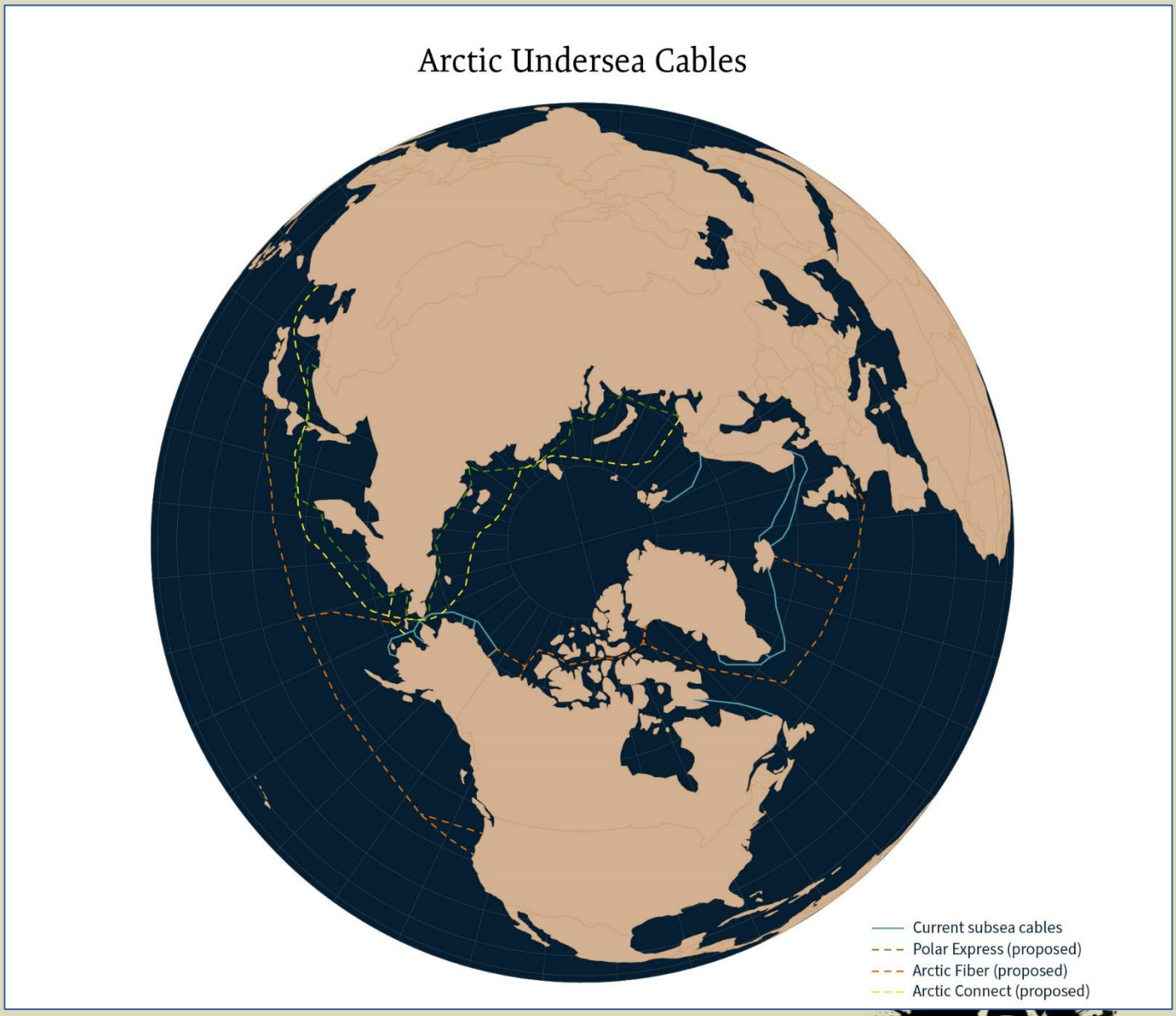
Critical Communications Infrastructure

The Euro-Atlantic area is the oldest undersea cable route and carries traffic between the two biggest economic hubs with dozens of cables, the majority of which are between the United States, the United Kingdom, and France. Europe relies heavily on these cables as a majority of its data is stored in data centers located in the United States. Other major routes are those connecting Europe to Asia (through the Mediterranean Sea and the Suez Canal) as well as Asia with the United States (through the Pacific Ocean). From a more forward-looking perspective, Europe to Asia Arctic routes are increasingly explored as they offer dramatically shorter routes. Nonetheless, these polar cables still face significant technical challenges and are not credible alternative routes yet.






North Pacific Undersea Cables
Bering Sea
North Pacific Ocean
Source: CSIS original creation based on information from "The Submarine Cable Map," TeleGeography, https://www.submarinecablemap.com/#/.
CSIS
EUROPE, RUSSIA, AND EURASIA PROGRAM


Arctic Undersea Cables
Current subsea cables
Polar Express (proposed)
Arctic Fiber (proposed)
Arctic Connect (proposed)

The planning, production, deployment, and maintenance of subsea cables are almost entirely in the hands of the private sector. Currently, the four largest suppliers are Alcatel Submarine Networks (France), SubCom (United States), NEC (Japan), and newcomer Huawei Marine Networks (China), whose market share has progressively risen to 10 percent. If network operators have traditionally been the main investors in undersea cables, content providers (Google, Amazon, Microsoft, Facebook) are also expanding their investments in this sector to ensure the interconnection of their data centers.

This global network of undersea cables provides the high-bandwidth connections needed for a wide range of activities vital for our modern society, from financial transactions to global communications or international scientific cooperation. In the financial sector alone, undersea cables carry some $10 trillion of financial transfers daily. Reliance on submarine cables will continue to increase as demand for data is expected to grow: driven by a shift toward cloud services and the spread of 5G networks, bandwidth demand will almost double every two years in the near future.

Submarine cables are also critical for transatlantic security as governments rely heavily on this infrastructure for their own communications. Diplomatic cables and military orders largely pass through these privately owned cables as military operated, and classified cables remain marginal. Undersea cable breaks between Egypt and Italy in 2008 led U.S. drone flights in Iraq to decrease sharply from hundreds to tens a day. This reliance on subsea cables to project and sustain power will increase in the future as the military applications of 5G are many in terms of intelligence, command and control, or unmanned and autonomous vehicles.

The Nature of the Threat

Undersea cables have two types of vulnerabilities: physical and digital. However, it should be noted that the most common threat today—responsible for roughly 150 to 200 subsea cable faults every year—is accidental physical damage from commercial fishing and shipping, or even from underwater earthquakes. Industry actors have the prime responsibility for accounting for and mitigating these incidents. Of greater concern are more malicious threats. Regarding physical challenges, the two primary concerns are that the cables might be destroyed or tapped—by either a non-state actor, as per some recent isolated incidents of piracy, or, more likely, by a state adversary like Russia.

Indeed, in recent years, Russian attention to transatlantic undersea cables, particularly in the North Atlantic Ocean, has increased commensurately with NATO's perception of undersea cables' importance and vulnerability. Moscow has two primary means by which it could directly threaten the cables: submarines and surface vessels that can deploy autonomous or manned submersibles. An example of the former was the *Losharik* spy submarine, which—before a tragic fire in 2019 decommissioned it—likely had the deep-sea capability necessary to map or destroy undersea cables. While the *Losharik* is being repaired, the Russian Navy has other such submarines and is developing unmanned undersea drones, such as the nuclear-powered *Poseidon*. As for surface ships, the most famous is the *Yantar*, which is ostensibly a research vessel but is understood to act as a spy ship that could deploy underwater submersibles to attack and destroy sections of cables.

There are several conceivable objectives severing a cable might achieve: cutting off military or government communications in the early stages of a conflict, eliminating internet access for a targeted population, sabotaging an economic competitor, or causing economic disruption for geopolitical purposes. Actors could also pursue several or all of these objectives simultaneously.

More difficult and subtle than destroying the cables is tapping them to record, copy, and steal data, which would be later collected and analyzed for espionage. It is believed this could be done in one of three ways: inserting backdoors during the cable manufacturing process, targeting onshore landing stations and facilities linking cables to networks on land, or tapping the cables at sea. Each is more difficult than the one before, and the last—tapping the cables at sea— is believed to be so technically challenging that it is not publicly known whether any country is even capable of it.

The final type of threat is cyber or network attacks. By hacking into the network management systems that private companies use to manage data traffic passing through the cables, malicious actors could disrupt data flows. A "nightmare scenario" would involve a hacker gaining control, or administrative rights, of a network management system. At that point, they could discover physical vulnerabilities, disrupt or divert data traffic, or even execute a "kill click" deleting the wavelengths used to transmit data. The potential for sabotage or espionage is quite clear—and according to Lawfare, the security of many of the network management systems is not up to date. The recent SolarWinds and Colonial Pipeline cyberattacks also exposed the cyber vulnerabilities of the U.S. private sector with dramatic implications for national security.

At the time of this writing, there is no publicly available information indicating that any actor, be it Russia, China, or a non-state group, is entertaining such a cyberattack. But one could imagine feasible motives for all of them: for Russia, the same reasons that it might consider a physical attack would apply; for China, its emergence as a leading global competitor in providing undersea cables could make the prospects of discrete espionage or even industrial sabotage alluring; and for a terrorist group, the prospect of holding transatlantic financial commerce hostage or destroying it could be enticing. At the moment, however, assigning these motives is a speculative exercise.

Strengthening Undersea Cables Resilience

Given the critical importance of subsea cables for transatlantic security, ensuring their full resiliency should be a collective priority for the United States and its European allies and partners—and while some have already adopted measures at the national level, multilateral action remains limited. Given the multi-faceted nature of the use, private ownership, and vulnerabilities of subsea cables, international action would necessarily need to leverage different formats to be effective. The following steps could be taken:

Increase intelligence sharing among allies: The U.S. administration should conduct bilateral confidential dialogues with its main European partners, in particular, the United Kingdom and France, to exchange information on their threat perspective and analysis, their respective cable projects, and the national measures implemented to protect them. At NATO, allies should work on a collective assessment of both the potential vulnerabilities to undersea cables in the Euro-Atlantic region and the implications of disruptions for allied operations. The upcoming NATO summit on June 14 may provide an opportunity to begin that conversation.

Promote national risk assessments of cable projects: Even though cables are privately managed, maintained, and secured, governments have a responsibility to make sure that any project is closely scrutinized beforehand to avoid security breaches. National authorities also have a responsibility to ensure that cable routes are redundant and diverse enough to guarantee their overall resilience. Individual allies have already put in place such procedures, starting with the United States where an interagency group known as "Team Telecom" reviews the national security implications of all potential subsea cables landing on U.S. shores. In Europe, the European Union should use its regulatory power to likewise promote high security standards for all member states, building on its 2008 critical infrastructures directive and its growing efforts in the field of cybersecurity. Security at landing stations, which is often limited, should be a priority in this regard.

Ensure private sector commitment to security: In addition to reviewing projects in advance, national governments should also ensure that operating companies implement the highest standards. As a first step, allies should encourage operators to adhere to voluntary guidelines, most notably those provided by the International Cable Protection Committee (ICPC), an industry forum for cable owners and some governments that develops standard procedures. Allied governments, which are not members, should also consider joining, as this would enhance the legitimacy of the organization. If voluntary standards fail to incentivize companies to invest adequately in cybersecurity, allies should consider defining mandatory requirements, as recently decided in the United States for oil and gas pipelines following the ransomware attack against Colonial Pipeline.

Develop national monitoring and repair capabilities: Allied governments should also step up their efforts to protect this critical infrastructure from malicious activity. Once allies agree on a shared assessment of vulnerabilities, NATO defense planners could consider setting capability targets to encourage allies to develop appropriate assets, such as surveillance ships or autonomous undersea drones. The United Kingdom has already announced the

acquisition of a vessel specifically designed to protect underwater infrastructure. It will be equipped with advanced sensors and underwater drones and is expected to come into service by 2024. In addition to monitoring capabilities, allies could also consider policies to bolster the global fleet of cable repair vessels, which as of now is both overstretched and informally organized. The Fiscal Year 2020 U.S. National Defense Authorization Act (NDAA), for example, allocated a small stipend for a program to incorporate two privately owned vessels into a "fleet" the government can activate in a crisis.

Adopt contingency planning in case of major breaks: The United States and its European allies and partners should also develop, in close coordination with the private sector, contingency planning to prepare for the consequences of intended or unintended significant cuts. A focus should be on scenarios where many cables are severed in a short time period, overwhelming the redundancy features that the private sector builds into account for more common, isolated failures. This planning process could help governments and cable owners to identify national points of contact, conduct regular exercises, and determine ways to improve the resiliency of the networks. This effort could be undertaken at the national level or collectively as appropriate. This could be an area of cooperation between the European Union and NATO, harnessing the strengths of both organizations (the European Union's financial and regulatory competence and NATO's experience in military planning).

Complete international legal framework:Finally, the United States and its European partners should explore ways of better protecting undersea cables from a legal point of view. As of now, the legal regime is a patchwork of international conventions and customary law, in particular, the United Nations Convention on the Law of the Sea (UNCLOS), which does not fully protect cables. Significant gaps remain: this regime does not explicitly prohibit, for instance, states from treating undersea cables as legitimate military targets during wartime. The U.S. administration, together with Europeans, should therefore promote a more comprehensive and holistic legal regime that would apply to all states.

While there is certainly much more that can be done, these recommendations are intended to serve as a useful starting point as the United States and its European allies and partners begin to consider how to collectively ensure that the protection of this critical infrastructure is commensurate with their immense importance for transatlantic security, societies, and economies.

Pierre Morcos is a visiting fellow with Europe, Russia, and Eurasia Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.
Colin Wall is a research associate with the CSIS Europe, Russia, and Eurasia Program.

More Than 5 Million Anti-Propaganda Text Messages Sent to Russians in Anonymous Information Warfare

By Bridget Johnson

Source: https://www.hstoday.us/featured/more-than-5-million-anti-propaganda-text-messages-sent-to-russians-in-anonymous-information-warfare/

Mar 09 – A digital army from around the globe laboring to counter Russia's disinformation ops has sent more than 5 million text messages to Russian cell phone numbers relaying information about what's really happening in Ukraine.

"We have a message for the citizens of the free world: the legion is calling you. Ukraine needs you. You are the largest army in the history of the world," Squad303, which created the tool enabling digital warriors to reach past the Russian regime's information wall, said in a video today. "You don't need any weapons or ammunition. Your weapons are smartphone and your ammo is messages sent to Russian citizens."

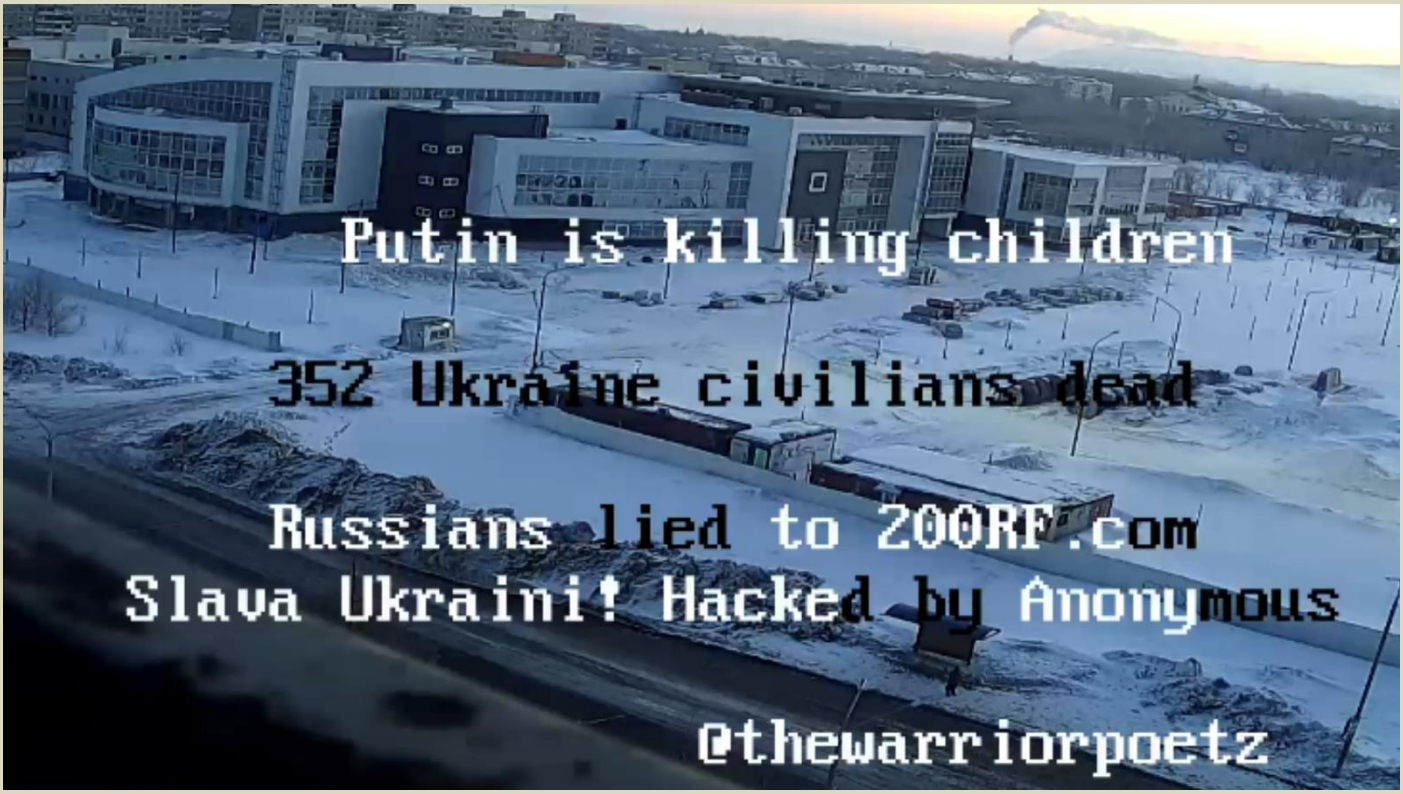
The hacking collective Anonymous launched the #OpRussia cyber offensive nearly two weeks ago in response to the Ukraine invasion, resulting in hacks and takedowns of Russian government websites along with leaks of seized data. Hackers have used their access to broadcast the truth about Putin's war to the citizenry and call on Russians to oppose the attack on their neighbor.

Anonymous programmers Squad303 created a tool that allows non-hackers to make a positive contribution to "the largest and most successful cyber operation in the history of the world." Within 48 hours of releasing the 1920.in tool, the group reported on Twitter that "the people of the free world sent the Russians 2 million text messages" warning that the people of Russia would suffer as a result of nations' response to Vladimir Putin's aggression and that they need to know the truth about his unprovoked war. By Tuesday, that volume had hit 5 million and still climbing.

The group also posted on its Telegram channel a list of Russian Duma members' mobile phone numbers, encouraging the digital army to "have a nice chat" with the lawmakers.

Another Anonymous group said it seized control of more than 400 Russian camera feeds including government facilities, offices, schools and businesses, and posted some on a

website with a message overlaying the feeds that includes the latest civilian death toll in Ukraine and begins with, "Putin is killing children."



A hacked camera feed in Russia (Anonymous image)

"This is anti-propaganda to open the eyes of Russian civilians," the Anon account tweeted Monday. "We have already been working on our next camera dump which will contain cameras from Belarus and Ukraine, mostly combat zones which will be more useful for recon than these. This is strictly anti-propaganda for the Russian people."

In a mission statement on their behindenemylines.live camera dump site, the Anonymous hackers noted, "If you are Russian, we just want you to know that you are being brainwashed by state propaganda, and the Kremlin and Putin are lying to you. Ukraine is not controlled by Nazis, they do not need you to 'free' them. You need to fight back and free yourself from your Dictator. We realize this is scary, and easier said than done, but you will have the entire world behind you, supporting you and watching you."

A table tweeted by one Anonymous account estimated that as of March 3 about a third of prominent hacker groups were involved in "the largest cyber war ever right now," with just 12 of the 49 groups siding with Russia, three whose support was unknown, and the rest supporting Ukraine.

NB65, a hacking group affiliated with Anonymous that earlier said it breached the control center of Roscosmos and cut off the agency's control over its spy satellites as part of the ongoing cyber-offensive, promised Tuesday that a Kaspersky source code leak is forthcoming. "I'm sure you'll find interesting relationships in this code," the group tweeted. "Glory to Ukraine."

In a message posted Sunday, NB65 declared that "we really enjoyed Kaspersky's endpoint security, it's a great foothold!"

More than 2,500 websites linked to the Russian and Belarusian governments along with state-run media, banks, hospitals, airports, and companies were hacked in the first week after the Anonymous collective declared that they launched cyber operations, a prominent Anonymous account reported last week. The antiwar hackers have also gone after pro-Russian hackers, swiping and leaking thousands of internal chats from the Conti ransomware group, as well as military communications and more.

Hackers announced Sunday that they had breached Russian streaming services Wink and Ivi and live broadcasts on TV stations Russia 24, Channel One, and Moscow 24 to broadcast war footage from Ukraine.

The hack included a text message on the screen calling on Russians to stand up against Putin's war: "We are ordinary citizens of Russia. We oppose the war on the territory of Ukraine. Russia and the Russians against the war! This war was waged by Putin's criminal, authoritarian regime on behalf of ordinary Russian citizens. Russians, oppose the genocide in Ukraine."

On Friday, state communications watchdog Roskomnadzor said it blocked Facebook and Twitter as the Putin regime has tried to stifle the free flow of information on social media.

Putin also signed a bill that was jammed through by pro-Kremlin lawmakers to penalize with up to 15 years in prison those disseminating information about the war that doesn't fit the Kremlin's disinformation narrative. Russia is also requiring all servers and domains to be transferred to a Russian intranet by March 11.
On Tuesday, Twitter launched a Tor onion service domain to let users access the site through the dark web and get around the Russian government block.
Cybersecurity expert Alec Muffett, who assisted Twitter with the project, announced the launch on Twitter, noting the move will be "providing greater privacy, integrity, trust, & 'unblockability' for people all around the world."
"So why am I first(-ish?) to tweet about it?" Muffett added. "From past experience with the Facebook and BBC Onion sites, any sufficiently large announcement leads to a load-spike, and given that @TwitterSafety has 3.6 million followers it would not be wise in a time of global crisis."

Bridget Johnson is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill. Bridget is a senior fellow specializing in terrorism analysis at the Haym Salomon Center. She is an NPR on-air contributor and has contributed to USA Today, The Wall Street Journal, New York Observer, National Review Online, Politico, New York Daily News, The Jerusalem Post, The Hill, Washington Times, RealClearWorld and more, and has myriad television and radio credits including Al-Jazeera, BBC and SiriusXM.

Smart Devices Are Spying on You Everywhere, And That's a Problem

By Roberto Yus and Primal Pappachan
Source: https://www.sciencealert.com/the-internet-of-things-is-probably-violating-your-privacy-here-s-how

Mar 15 – Have you ever felt a creeping sensation that someone's watching you? Then you turn around and you don't see anything out of the ordinary. Depending on where you were, though, you might not have been completely imagining it. There are billions of things sensing you every day. They are everywhere, hidden in plain sight – inside your TV, fridge, car and office. These things know more about you than you might imagine, and many of them communicate that information over the internet.
Back in 2007, it would have been hard to imagine the revolution of useful apps and services that smartphones ushered in. But they came with a cost in terms of intrusiveness and loss of privacy.
As computer scientists who study data management and privacy, we find that with internet connectivity extended to devices in homes, offices and cities, privacy is in more danger than ever.

Internet of Things
Your appliances, car and home are designed to make your life easier and automate tasks you perform daily: switch lights on and off when you enter and exit a room, remind you that

your tomatoes are about to go bad, personalize the temperature of the house depending on the weather and preferences of each person in the household.
To do their magic, they need the internet to reach out for help and correlate data. Without internet access, your smart thermostat can collect data about you, but it doesn't know what the weather forecast is, and it isn't powerful enough to process all of the information to decide what to do.
But it's not just the things in your home that are communicating over the internet. Workplaces, malls and cities are also becoming smarter, and the smart devices in those places have similar requirements.
In fact, the Internet of Things (IoT) is already widely used in transport and logistics, agriculture and farming, and industry automation. There were around 22 billion internet-connected devices in use around the world in 2018, and the number is projected to grow to over 50 billion by 2030.

What these things know about you
Smart devices collect a wide range of data about their users. Smart security cameras and smart assistants are, in the end, cameras and microphones in your home that collect video and audio information about your presence and activities.
On the less obvious end of the spectrum, things like smart TVs use cameras and microphones to spy on users, smart lightbulbs track your sleep and heart rate, and smart vacuum cleaners recognize objects in your home and map every inch of it.
Sometimes, this surveillance is marketed as a feature. For example, some Wi-Fi routers can collect information about users' whereabouts in the home and even coordinate with other smart devices to sense motion.
Manufacturers typically promise that only automated decision-making systems and not humans see your data. But this isn't always the case. For example, Amazon workers listen to some conversations with Alexa, transcribe them and annotate them, before feeding them into automated decision-making systems.
But even limiting access to personal data to automated decision making systems can have unwanted consequences. Any private data that is shared over the internet could be vulnerable to hackers anywhere in the world, and few consumer internet-connected devices are very secure.

Understand your vulnerabilities
With some devices, like smart speakers or cameras, users can occasionally turn them off for privacy. However, even when this is an option, disconnecting the devices from the internet can severely limit their usefulness.
You also don't have that option when you're in workspaces, malls or smart cities, so you could be vulnerable even if you don't own smart devices.
Therefore, as a user, it is important to make an informed decision by understanding the trade-offs between privacy and comfort when buying, installing and using an internet-connected device.
This is not always easy. Studies have shown that, for example, owners of smart home personal assistants have an incomplete understanding of what data the devices collect, where the data is stored and who can access it.
Governments all over the world have introduced laws to protect privacy and give people more control over their data. Some examples are the European General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA).
Thanks to this, for instance, you can submit a Data Subject Access Request (DSAR) to the organization that collects your data from an internet-connected device. The organizations are required to respond to requests within those jurisdictions within a month explaining what data is collected, how it is used within the organization and whether it is shared with any third parties.

Limit the privacy damage
Regulations are an important step; however, their enforcement is likely to take a while to catch up with the ever-increasing population of internet-connected devices. In the meantime, there are things you can do to take advantage of some of the benefits of internet-connected without giving away an inordinate amount of personal data.
If you own a smart device, you can take steps to secure it and minimize risks to your privacy.
The Federal Trade Commission offers suggestions on how to secure your internet-connected devices. Two key steps are updating the device's firmware regularly and going through its settings and disabling any data collection that is not related to what you want the device to do. The Online Trust Alliance provides additional tips and a checklist for consumers to ensure safe and private use of consumer internet-connected devices.
If you are on the fence about purchasing an internet-connected device, find out what data it captures and what the manufacturer's data management policies are from independent sources such as Mozilla's Privacy Not Included. By using this information, you can opt for a version of the smart device you want from a manufacturer that takes the privacy of its users seriously.

Last but not least, you can pause and reflect on whether you really need all your devices to be smart. For example, are you willing to give away information about yourself to be able to verbally command your coffee machine to make you a coffee?

Roberto Yus is Assistant Professor of Computer Science @ University of Maryland, Baltimore County.
Primal Pappachan is Postdoctoral Scholar in Computer Science @ Penn State.

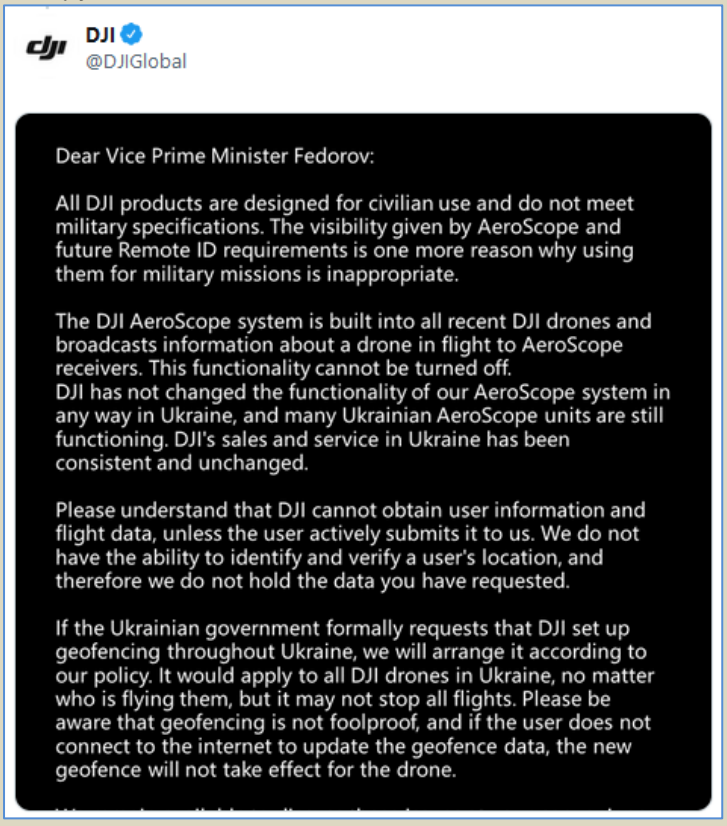
Tinder traps & TikTok: How technology has transformed warfare in Ukraine

Source: https://newatlas.com/technology/ukraine-russia-technology-modern-warfare-drone-airbnb-tiktok-deepfake/

Mar 20 – Commercial drones, Airbnb donations, TikTok chronicles, deepfake propaganda, and trolling Russian soldiers through Tinder. The conflict in the Ukraine has precipitated new ways in which modern technology can influence war in the 21st century.
The Russian invasion of Ukraine is the biggest military assault on a European state since World War II. While there certainly is nothing unique about human beings fighting one another, the nature of war is always profoundly affected by current technology, and this war is no exception.
Here are five recent stories of technology changing the face of modern warfare – for good and bad …

Domestic drones

Over the last decade a multi-billion dollar commercial drone market has emerged allowing people cheap access to a technology previously only really available for military purposes. For a few hundred dollars anyone can buy a small drone, and when Russia began their invasion in February the Ukraine drone community quickly jumped into action.



The Ukrainian military reportedly posted a call out on Facebook for citizens to donate their drones to help with surveillance operations. "Kyiv needs you and your drone at this moment of fury!" read the post.
A commercial drone retailer in Kyiv dispensed around 300 DJI drones to the military. However, concerns have already been raised over what responsibility DJI as a company has in regulating the uses of its products in a time of war.
A recent open letter from Ukraine's Vice Prime Minister to DJI called on the company to block access to its products registered in Russia. The letter also claimed the Russian military was using a DJI product called AeroScope to target missiles at Ukrainian citizens.
AeroScope is a surveillance system that geolocates DJI drones and their pilots in real time. Unverified reports out of Ukraine allege Russian forces are using AeroScope technology to locate and target civilians who are assisting the military with their domestic drones.

DJI has responded to the Ukrainian letter claiming it has no control over the use of AeroScope technology and cannot disable those systems. The company did suggest it was open to geofencing DJI products in Ukraine's airspace, essentially disabling use of its drones in the country.

Airbnb Humanitarians

As billions of people watch the devastation in Ukraine from afar it is a natural response to want to help. In times of crisis non-government organizations and charities quickly step up to offer aid to victims of war, and donating to those organizations is often the first port of call for someone looking to help.

However, in today's hyper-connected world new ways of offering aid in times of crisis have emerged. Within days of Russian forces invading Ukraine people around the world started booking out Airbnb stays in the country as a way of sending money to those directly in need.

The idea quickly went viral and within two days more than 61,000 nights in Ukrainian Airbnb stays were purchased, totaling nearly US$2 million dollars. Airbnb immediately suspended its own fees on Ukraine stays so all the money went directly to the hosts.

Of course, you can probably guess what happened next. As soon as the trend picked up pace scammers appeared posting fake listings to skim cash from unsuspecting humanitarians.

In a recent statement Airbnb claims to have suspended a small number of fake accounts. The company also reports around $15 million dollars has been sent to Ukraine through international donation bookings.

Besides scammers, some commentators have questioned whether "donating" money through Airbnb listings sends cash to the people who really need it. Anit Mukherjee, from the Center for Global Development, recently made the point to Vox News that those in Ukraine who own Airbnb listings are likely among the wealthiest one percent in the country. So despite good intentions this is probably not the most effectively targeted way to deliver support to those in need.

TikTik Correspondents

New media has always profoundly changed the way the general public relate to war. Perhaps the most studied example is how television in the 1960s brought the Vietnam war into the lounge rooms of millions of Americans, with some experts arguing this ultimately bolstered the anti-war movement. Smartphones and social media have already made their mark on international politics. Most prominently, around a decade ago Twitter was widely used to mobilize protests during the Arab Spring wave of revolutions in the Middle East and North Africa. In 2022 the invasion of Ukraine has ushered in a new type of war correspondence: young people using the social media app TikTok, a platform with over one billion active users. TikTok is characterized by users posting short pithy videos, often with backing music. And it has been this form that young Ukrainian influencers have been using to communicate their experiences within a modern war zone. So far TikTok posts from the frontline have spanned everything from traditional vlog-style reports from young people huddling in bunkers while their cities are bombed, to more surreal posts in classic TikTok-style showing explosions in the sky over Kyiv while pop music plays on the soundtrack.

And of course, as with any new medium of communication, misinformation has quickly become a major problem. As Russia worked hard to control the narrative of the war within its borders, TikTok swiftly banned user uploads from inside the country.

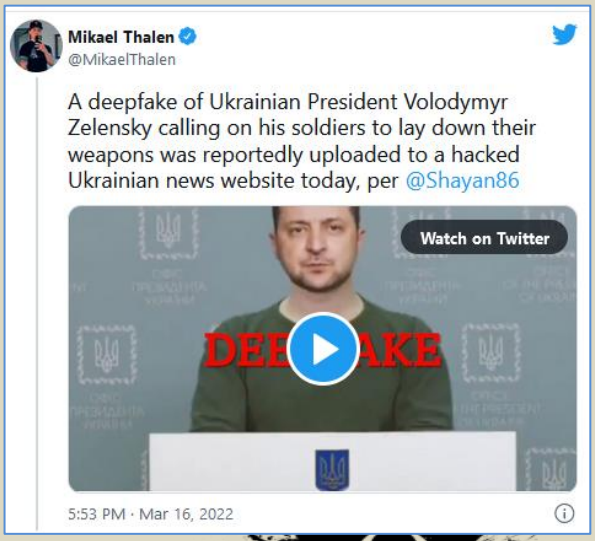
An investigation by Vice News recently revealed pro-Russia disinformation is still spreading on TikTok. The Kremlin is allegedly paying Russian social media influencers to post propagandic messages on the platform.

Deep Fake Propaganda

For the last few years researchers have warned us about the dangers of deepfakes, and now we have seen one of the first wartime deployments of the technology. This video of Ukrainian president Volodymyr Zelenskyy calling for his solders to lay down their weapons and surrender to the Russians recently appeared on a tabloid news site.

The editor of the Ukraine-based Russian-language news site where the video appeared claims the website was hacked by Russians, but the true source of the deepfake has yet to be revealed. Although Russian media has been promoting the video, some experts suggest the the poor quality deepfake may not necessarily be Kremlin-sourced propaganda.

Regardless of the video's ultimate source the appearance of a fake video such as this is a strong example of how modern technology offers new and perfidious methods to build on traditional modes of wartime propaganda. In World War II, for example, an infamous fake radio show was created in the UK and broadcast across radio stations in Germany.



The short profane rants from a German character known as The Chief told the story of rebel Nazis conspiring against the corrupt state. The Chief's broadcasts were reportedly so convincing that US officials in Berlin passed the fake news onto Franklin D. Roosevelt who was ultimately amused to find out the project was fake.

The Tinder Trap

Dating apps are a global phenomenon and they work because of the precise ability for smartphones to geolocate a user and match them with other users in a nearby vicinity. So what happens when a bunch of Tinder-linked young, single, Russian, male soldiers invade a neighboring country?

Early in the invasion an extraordinary report from The Sun described a number of experiences where Ukrainian women suddenly had their phones light up with automated Tinder matches from nearby Russian soldiers waiting across the border to invade. The surreal story recounts Ukrainian women dealing with flirty Russian soldiers just miles away.

As word of the Tinder situation spread, users around the world quickly started to change their locations to spots in Ukraine or Russia in order to either troll Russian soldiers or attempt to counter propaganda spread within Russia. A group of Slovakian creatives started a movement called Special Love Operation designed to connect with Tinder users inside Russia and help spread genuine news about the war.

While there is no evidence Tinder has been used in any spy or surveillance capacity so far, the involvement of the technology does allude to a long history of women as resistance fighters seducing enemy soldiers in war and luring them to their death.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

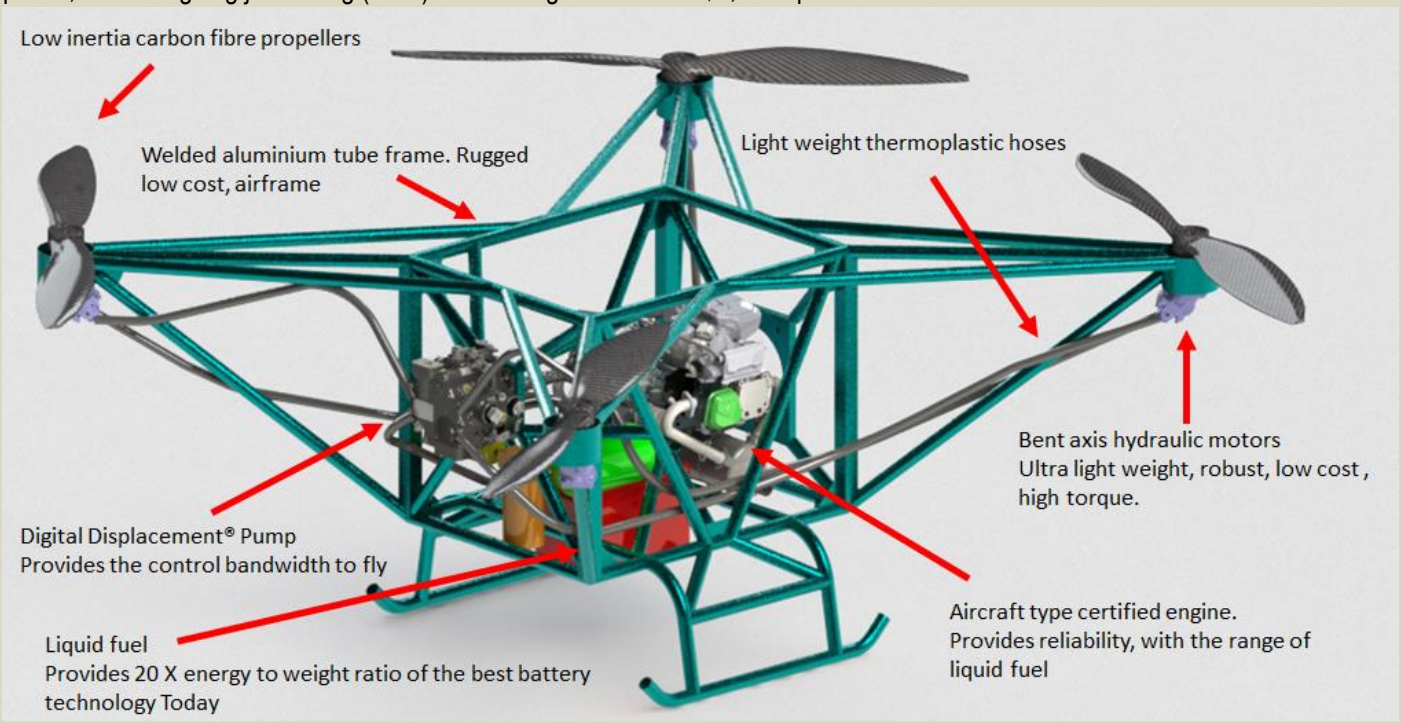
DRONE NEWS

Flowcopter begins testing the world's first hydraulic multicopter

Source: https://newatlas.com/aircraft/flowcopter-hydraulic-drone/

Flowcopter is beginning to flight-test the world's first hydraulically propelled drone (Flowcopter)

Feb 24 – Multicopters would be able to lift heavier loads and stay in the air longer if they could use a high-density power source like gasoline instead of low-density lithium batteries. But gasoline engines, with their weird, peaky torque curves, aren't nearly responsive enough to keep a multicopter balanced against rapidly changing winds. We've seen a number of different ways of addressing this – one memorable idea that springs to mind from many years ago proposed running both electric and combustion motors together, directly on each propeller shaft, with the gas engine supplying more or less constant torque, and the electric motors kicking in when high-speed adjustments were needed. Edinburgh's Flowcopter has a different solution entirely. Its heavy-lift cargo drones will run aviation-certified combustion engines, and these engines will drive Digital Displacement pumps repurposed from the off-road and industrial vehicle markets, to run hydraulic motors at the props. These pumps are able to distribute and regulate hydraulic flow between a number of different outputs, under digital control, with the kinds of near-instant response times you need to balance a drone in flight. Each hydraulic motor will deliver up to an enormous 96 kW (129 hp) of power, while weighing just 5.5 kg (12 lb) and costing less than US$1,000 apiece.



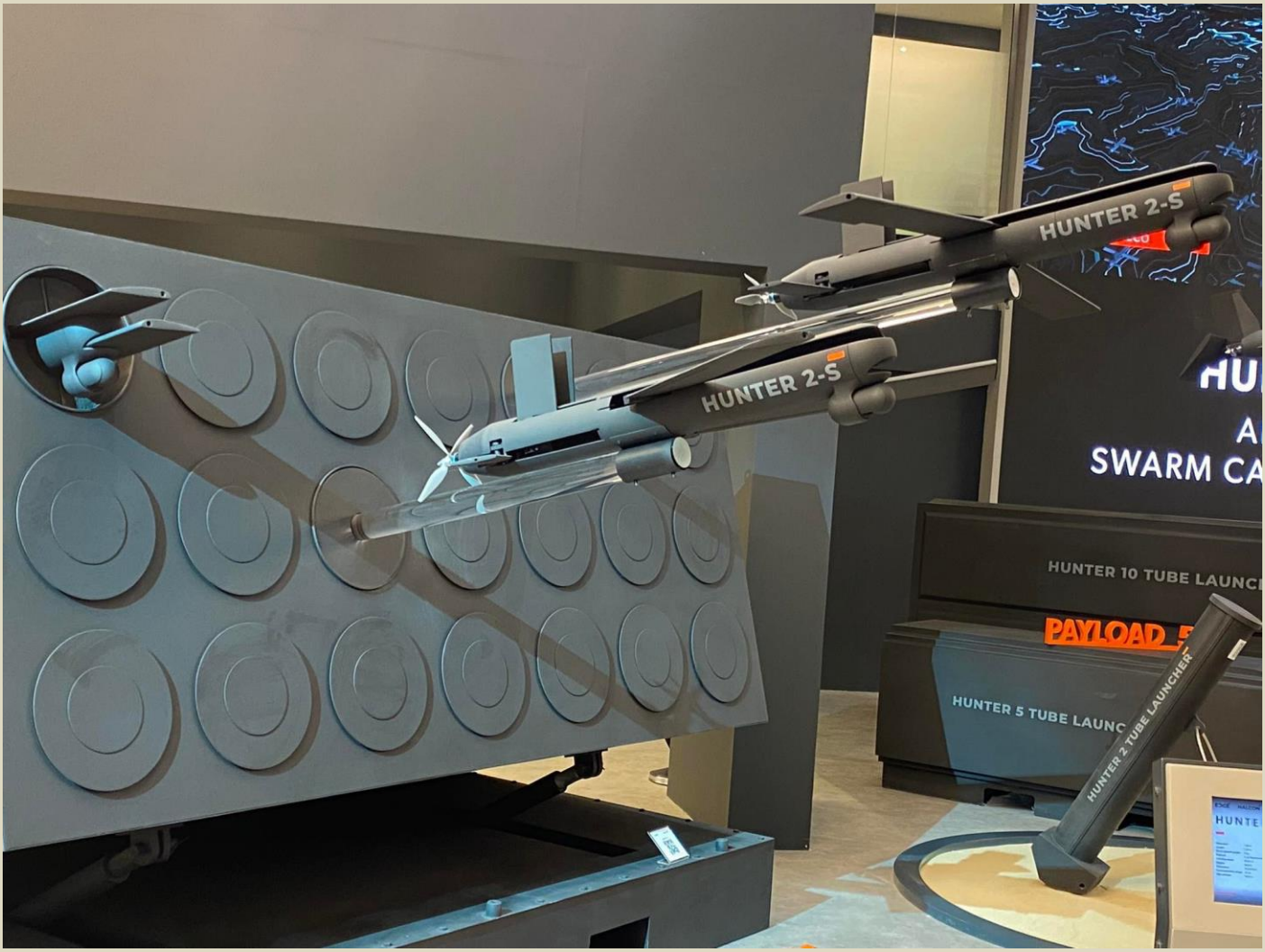
A combustion engine and digital displacement pump allow near-instant torque control, huge power and exceptional range (Flowcopter)

Flowcopter says "nothing electric comes even close." The weight of the Digital Displacement pump, combustion engine and fuel system might be significant, but gasoline offers so much more usable energy per kilogram than lithium that the benefits will more than outweigh the

drawbacks in Flowcopter's estimations. The company promises endurance up to 6 hours on a tank of gas, and range figures up to 900 km (560 miles), from a straight-up multicopter with no efficient winged flight mode. It'll be holding itself up on propeller power alone for all six of those hours. Payloads will be up to 150 kg for shorter missions.
Flowcopter has built a fairly raw-looking prototype – none of your fancy carbon fiber here, folks, it's a welded metal frame – and has been doing some tethered flight testing. It's a little on the wobbly side, as you'll see below, but it flies, and as the world's first hydraulic hybrid multicopter, that's an impressive achievement. It'll be interesting to see if this technology pans out into widespread use.

ABU Dhabi Reveals New AI-based UAVs

Source [+video]: https://i-hls.com/archives/113293



Hunter 2-S uses 3D printed parts, specifically aerospace-grade thermoplastic materials

Feb 25 – UAE unveils new aircraft from HALCON Unmanned Aircraft Series, a regional leader in the production and supply of guided weapons and unmanned aerial vehicles (UAVs) during the Abu Dhabi UMEX Innovation Conference. HALCON is a member of the EDGE Group, UAE's leading security technology company.
HALCON CEO Al Mansoori told breakingdefense.com the new UAVs, based on the Emirates' Hunter 2 series, uses artificial intelligence technology to share information as they fly in coordination and in a stable formation towards the target.
"Once the target has been identified, a group decision is taken, and based on the size, shape, and category of the target, a decision is made as to how many UAVs are needed to complete the mission," Al Mansoori explained. UAVs in this group can assemble into a swarm system, can hit moving targets as well as static ones, and execute complex missions. UAVs with

wings can be deployed in just a few seconds, resulting in wings 1.4m long and a vessel of 1.25m in length.
Al Mansoori also added that while unmanned aerial vehicles are the most innovative and leading in unmanned systems, land-based autonomous systems are gaining in popularity. In consequence, land-based technologies are catching up with the accomplishments of aerial technologies.

A New Study By Cranfield University Analyzes The Sound Impact Of Drones

Source: https://i-hls.com/archives/113253

Feb 23 – At Cranfield University, unmanned aerial vehicles (UAVs) were submitted to a sound measurement test in order to better understand their potential and environmental impact in urban contexts.
Because of the volume and frequency of noise produced by unmanned aerial vehicles, they are often an annoyance, especially when flying over metropolitan areas.
According to recent research by the UK Regulatory Horizons Council, UAVs are becoming less popular in and around residential areas as a result of the noise they produce, which is becoming a significant problem as their usage for examinations and shipments grows. This study might help with the development of measuring tools as well as a better understanding of the noise produced by unmanned aircraft.
A series of tests conducted in collaboration with noise experts from the Envirosuite Group and the ARPAS-UK Skimmer Industry Group, as well as environmental noise experts from Cranfield University and CAA, found that microphones can effectively capture different levels of UAV noise at different heights and that the spectrum can be used to identify different types of UAVs based on their unique noise.
As part of the measurement investigations, a large number of small to medium-sized multi-rotor drones flew in a variety of pre-defined flight patterns at Carnfield Research Airport. Noise levels from many drones flying above 100 feet were frequently in the 50-60 decibel (dBA) range, which is equivalent to noise levels in a packed restaurant.
Dr. Simon Jude, a senior lecturer at Cranfield University's Environmental Center, told uasvision.com that the study highlights the need for greater research as well as public knowledge, involvement, and acceptability of noise from unmanned aerial vehicles. It claims that perceptions and attitudes toward unmanned aerial vehicles vary by culture, and that public concerns might be a significant barrier to effective adaptation and use of this technology.
The knowledge gained from these trials will hopefully educate the approaches needed to accurately quantify and comprehend UAV noise.

The Role of Drones in Ukraine's Military Defense
By Lauren A. Kahn
Source: https://www.homelandsecuritynewswire.com/dr20220303-the-role-of-drones-in-ukraine-s-military-defense

Mar 03 – Drones are playing a critical role in Ukraine's military defense against the Russian invasion, but they will likely become more vulnerable as the war expands.

What Are Ukraine's Drone Capabilities?
Ukraine possesses at least twelve Turkish Bayraktar TB2 drones, and reports suggest that it might have as many as thirty-six additional units. These are the same drones that Azerbaijan used effectively against Armenia in the 2020 Nagorno-Karabakh conflict. Ukraine first purchased six of these medium-altitude, tactical uninhabited aerial vehicles (UAV) from Turkey in a $69 million deal in 2019. Each Bayraktar TB2 system consists of six aerial vehicles (or drones), two ground control stations, and related support equipment, so the initial purchase was for one complete system. The UAVs, which are Ukraine's only armed UAV capability, have a range of up to three hundred kilometers, last up to twenty-seven hours, and can carry up to four laser-guided munitions.
At the start of the Russian invasion, Lieutenant Colonel Yuri Ignat, spokesperson for the Ukrainian Air Force, said Ukraine had approximately twenty Bayraktar drones. Baykar (the drone manufacturer), Turkey, and Ukraine have all declined to confirm the number of drones that have been delivered to Ukraine to date.
The Bayraktar TB2 initially proved itself when Turkey used them against Russian-made vehicles in Libya and Syria; it solidified this reputation in the Armenia-Azerbaijan conflict. In these conflicts, the drones successfully destroyed armored vehicles and mobile air defense systems.

How Has Ukraine Used These Drones against Russian Forces?
The first reports of Ukraine using the Bayraktar TB2s against Russian forces since the invasion came on February 27, 2022. Ukrainian General Serhiy Shaptala shared video footage on Twitter of a TB2 hitting a Russian Buk surface-to-air missile system near a town around one hundred kilometers northwest of Kyiv. Ukraine's air force has since confirmed two drone strikes on Russian targets. Many more have been shared on social media, but they have not been verified.
Ukraine's use of the TB2 builds on operational experience it gained last year during the conflict in the country's east. In October 2021, Ukrainian armed forces confirmed the use of the TB2 in the Donbas region during a counter-battery mission in a separatist-controlled area. The attack was reportedly successful, despite the presence of Russian electronic warfare and air defense assets. After the attack, Moscow accused Kyiv of "provocative activity." Ukrainian Defense Minister Oleksii Reznikov responded that Ukraine used the drone "for one tidy shot"

and that, since then, enemy soldiers had not challenged the drone systems further. Prior to that point, Ukraine is understood to have been using at least a dozen TB2s in reconnaissance missions.
After the strike in Donbas, Ukraine issued a formal statement that it would "continue to increase tactics and methods of combat use of Bayraktars to deter Russian aggression and protect Ukraine's interests."

How Vulnerable Are They?
Current-generation drones such as the Bayraktar TB2 are vulnerable to air defense systems, air attacks, and electronic warfare. Bayraktar TB2s are slow, large, low-flying, and radio-controlled, making them comparatively easy targets for more sophisticated, layered air defense systems and electronic warfare capabilities. Moreover, the earlier successes of the TB2 in Nagorno-Karabakh and Libya were in part due to their use against uncamouflaged, undispersed targets and older air defense systems. Until now, there was little evidence that the Bayraktar TB2 or any current-generation drone could operate effectively against the updated, integrated air defenses that Russia possesses (though how extensively they have deployed those defenses in the invasion of Ukraine is unclear).
In addition to having prior direct (and indirect) exposure to Bayraktar TB2s, the Russian military has the capacity to identify and target them more quickly than forces previously targeted by such drones. Furthermore, Russia can use missile strikes and ground assaults to capture and destroy airfields where the UAVs operate or the ground stations used to control them. Russian state media has already asserted as much, saying Russian forces have destroyed "74 ground facilities of Ukraine's military infrastructure," including eleven airfields, three command points, a naval base, eighteen radar stations of S-300 and Buk-M1 missile systems, and four TB2s. Russia has so far been unable to achieve air superiority over all of Ukraine, including its drones. Why Russia has been unable (or hesitant) to ground Ukraine's Bayraktar TB2 force—despite having the capability, the opportunity at the start of the war, and familiarity with the UAVs—remains unclear. It is possible that Russia was surprised by the level of resistance from Ukrainian forces.
Ukraine will likely continue to deploy its Bayraktar TB2s, along with other air assets, to attack Russian tanks, other armor, and mobile anti-aircraft systems as long as it has these capabilities.

Lauren A. Kahn is Research Fellow at *CFR*.

Five Innovative Technologies in Security Robotics

Source: https://i-hls.com/archives/113387

Mar 02 – Robots help secure remote facilities and wide-area perimeters. Security robotics is a relatively new field, but it's already shown impressive innovation featuring new technologies. Roboticstomorrow.com elaborates on recent developments that show potential in security robotics:

- **Real-Time Video Analytics** – While early security robots either sent live video feeds to remote operators or recorded video data for future use, advances in machine learning let robots recognize objects and movements in real-time, letting them react independently to their situation. Capabilities include the recognition and scanning of license plates in order to detect suspects' vehicles or stolen cars, for example.
- **Unique Media Access Control (MAC) Address Recognition** – New tools let security robots scan local networks to check devices' MAC addresses, which are unique digital signatures that identify phones and computers.
- **Power Source** – Standard Lithium-ion batteries have limited operation times, especially in robots and drones, due to their small size. Graphene batteries can help security robots operate for far longer between charges, making them more useful. These batteries can retain 80% of their capacity through 1,400 charging cycles, charge faster than traditional alternatives, last longer, and operate at extreme temperatures.
- **Hyper-Spectral Cameras** – Machine vision is at the heart of many security robots. But it can only be as effective as the cameras that provide data. Hyper-spectral (HS) cameras can collect the full-color spectrum of a scene, making it easier for machine vision to work.
- **Sound Recognition** – Machine learning-powered sound recognition works like machine vision but helps robots detect and recognize audio signals like gunshots, breaking glass, alarms, or screams. New sound recognition algorithms use a library of more than six million audio files, with similar sounds clustered into groups. This organization enables robots to register what type of sound they've heard, then narrow it down to possible sources. They can then provide a more accurate alert to security personnel and other people in the area.

China Unveils Giant Yak-Robot

Source: https://i-hls.com/archives/113483

Mar 07 – Many people have heard of Boston Dynamics, the robotics giant who became famous a decade ago with the robotic dog, **BigDog** (right photo), which had no head. It seems China is now following suit in its own way.

In an official video released last month, China revealed a new robot to carry twice the weight of yaks native to the Himalayas. It is possible, however, that the claims regarding the capabilities of the **robotic yak** are exaggerated based on a video published in a newsletter associated with the Chinese Communist Party.

According to techeblog.com, China's official releases characterize the robotic yak as the world's largest and heaviest robot, capable of speeding to 10 km/h, understanding voice orders, and utilizing face recognition. However, despite the success that the Chinese ruling party is proud of, several sites, like popularmechanics.com, claim that the video portrays an image that exaggerates the robot's capabilities. One example is that a robot includes a system that allows it to leap or skip over different locations, a technology based on lidar sensors that is also used in commercial marketing items such as a robotic vacuum cleaner. Watch the video and decide for yourself.

Israeli System Downs ISIS Drones In Mozambique

Source: https://www.thedefensepost.com/2022/03/10/israeli-counterdrone-mozambique/

Mar 10 – The Mozambique Army downed three ISIS drones using an Israeli counter-drone system in the country's north, *Israel Defense* reported, citing the army. The MC-Horizon 360D V3 counter-drone system reportedly jammed the drones that were likely sent to gather

information on troops. According to *The Jerusalem Post*, the drones were also going to be used to bomb the soldiers.
The downing happened within a year of the Kfar Saba-based MCTECH RF Technologies craft being sold to the East African country.

Features
The system provides 360-degree coverage and detects drones through a "signaling channel and radio transmission (both the uplink and downlink)," at a radius of 1.5 kilometers (0.93 miles), triggering a "neutralization system which deactivates the drone/quadcopter from any operation," the manufacturer wrote. The 20 kilograms (44 pounds) modular system can be carried in a backpack and attached to a vehicle or vessel.

MC-HORIZON D360 v3 counter-drone system. Image: MCTECH Technologies

Citing the CEO of Israeli private security company Orad, *The Jerusalem Post* reported that MCTECH RF Technologies has sold the system to many militaries worldwide since 2014 and that the downing was the first by a foreign military.

"In Mozambique, ISIS is attacking troops with drones. They use drones to identify troops, to bomb troops, and even to identify troops and then navigate artillery to hit forces. This is exactly the same thing that happened with ISIS in Iraq," Orad CEO Yossi Goferwa said.

Underlining the significance of the kill, Gofera added that the drones used by the terrorist group are "so small and they fly very fast and very low to the ground so that it's hard to identify them. You need a very good radar."

Northern Mozambique has faced waves of ISIS-linked jihadist groups for the last four years, claiming at least 3,340 lives and displacing more than 800,000 people.

Science & Tech Spotlight: Counter-Drone Technologies

GAO-22-105705
Source: https://www.gao.gov/products/gao-22-105705

Mar 15 – Uncrewed aircraft systems, or "drones," can pose safety and security risks to critical U.S. sites and may be used for smuggling or other criminal activity. With over 2 million drones projected in the U.S. by 2024, these risks are likely to grow. Detection and mitigation technologies could counter these risks, but may face challenges around effectiveness and unintended impacts.

The Technology
What is it? Uncrewed aircraft systems (UAS), or "drones," have a variety of uses, such as photography, delivering packages, and monitoring crops. However, UAS can also pose significant safety and security risks if they enter airspace around critical U.S. sites without

authorization or if used for illegal activities. To reduce these risks, counter-UAS technology can detect such unauthorized or unsafe UAS and, when needed, jam, capture, or disable them.
Several UAS incidents have been reported in the U.S. For example, in January 2019, Newark Liberty International Airport halted all landings and diverted planes for over an hour after a potential UAS sighting nearby. Furthermore, smugglers have used UAS to deliver illegal drugs into the country (see fig. 1).

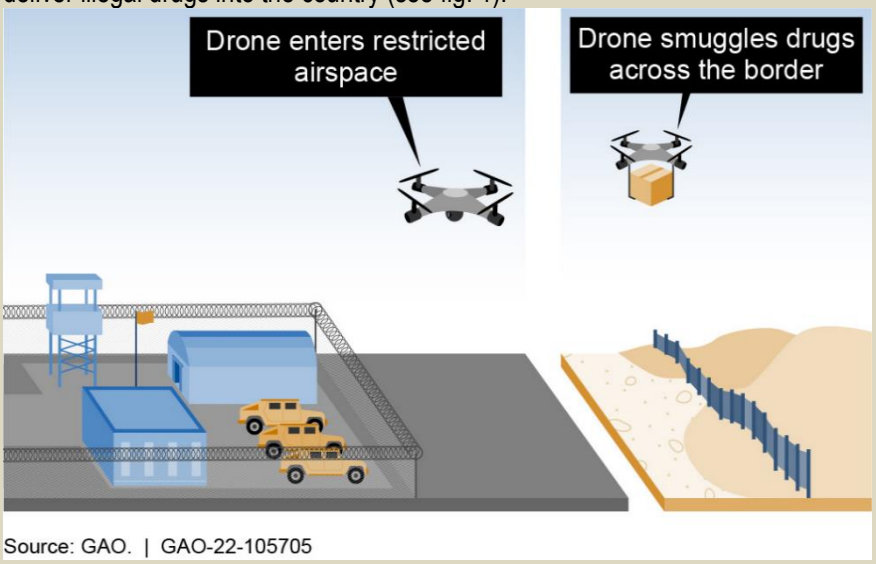


Figure 1. Some of the risks posed by uncrewed aircraft systems.

Reported incidents like these may increase as the use of UAS increases. The Federal Aviation Administration (FAA) has forecast that by 2024, the commercial UAS fleet will reach around 828,000, and the recreational fleet will number around 1.48 million.
Domestically, counter-UAS activities may be restricted or prohibited by existing federal laws such as the Aircraft Sabotage Act or the Computer Fraud and Abuse Act. However, four federal agencies—the Departments of Defense, Energy, Justice, and Homeland Security—have been authorized to deploy counter-UAS technologies under certain circumstances, such as to protect sensitive government facilities, including domestic military bases and prisons, or to provide security during sports championships.

How does it work? Counter-UAS technologies generally fall into two categories: detection and mitigation. Detection technologies include infrared devices to track heat signatures, radio frequency systems to scan for control signals, and acoustic methods to recognize the unique sounds produced by UAS motors. According to a 2019 Bard College report, radio frequency and radar systems are the most common detection technologies (see fig. 2).

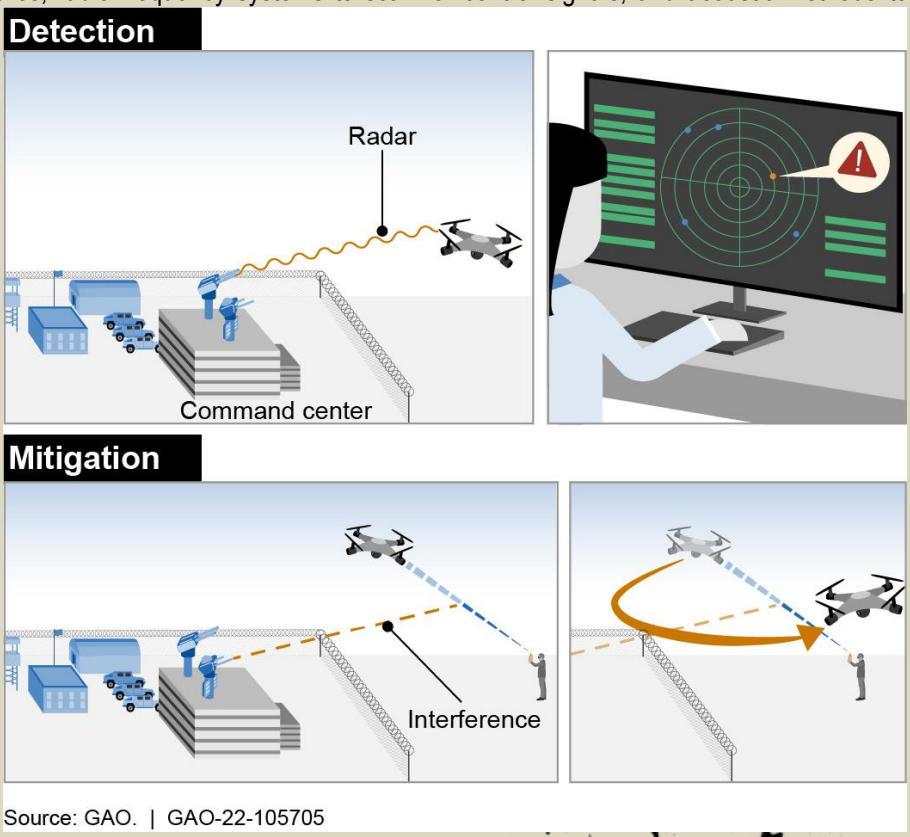


Figure 2. In this example, a critical site detects an unauthorized UAS nearby. An interference signal jams the connection between the UAS and its operator to reroute the UAS away from the site.

Mitigation technologies can repel or intercept an unauthorized UAS. For example, interference signals can jam or break the communications connection between the UAS and its operator, which can trigger the UAS to land or return to its operator. According to the Bard College report, jamming is the most common mitigation technology. Other mitigation technologies can use a net or kinetic force (such as lasers or projectiles) to disable or destroy the UAS. However, kinetic methods can be problematic because a falling or exploding UAS may cause unintended damage.

How mature is it? Although the Department of Defense has used counter-UAS technology abroad since at least 2014, domestic use has been limited. Over the last 4 years, the

authorized agencies have deployed some counter-UAS technologies domestically. However, some of these technologies have limited ability to detect and track small UAS (less than 55 pounds). Furthermore, few can successfully jam or disable a UAS, and many of those that can are only effective at around 1,000 feet or less.

To counter UAS risks, the FAA (which has been authorized to conduct limited testing activities) and the authorized agencies are continuing to test, evaluate, and develop integrated counter-UAS platforms. These platforms' capabilities are designed to address specific risk environments. For example, a powerful long-range signal jammer may be effective at mitigating UAS in rural locations, like near some domestic military bases, but this same technology could also disrupt legitimate and vital communications if used in a city or near an airport.

UAS technology continues to advance and become more accessible to the public. For example, UAS have become smaller and more maneuverable, making detection and mitigation more challenging. To stay effective, counter-UAS technology will need to adapt to such changes.

Opportunities

- **Enhanced security.** UAS have interfered with military and commercial aircraft operations, entered airspace over large sporting events, illegally accessed wireless networks, and been sighted over sensitive national security facilities. Counter-UAS technologies could address such threats to critical sites and assets.
- **Better situational awareness.** Counter-UAS platforms could allow tracking of UAS activity near critical sites and allow data analysis over time or locations to better understand the threat.

Challenges

- **Effectiveness**. Electromagnetic interference (e.g., power lines and LEDs) and small airborne objects (e.g., birds) can decrease detection capabilities or generate false detections. Mitigation systems may have a limited effective range or have difficulty against UAS that are quick or move in unpredictable patterns.
- **Unintended effects**. Counter-UAS platforms may pose safety hazards by interfering with nearby communications, such as devices that use navigation systems. For kinetic mitigation, errant projectiles or falling UAS could damage property or injure people on the ground.
- **Limited number of authorized agencies**. As of March 2022, only four federal agencies are authorized to conduct counter-UAS operations under certain circumstances, and no state or local agencies (or individuals) have such specific federal authorization. According to the Bard College report, local agencies generally rely on a small number of federal counter-UAS units to respond to and protect against UAS threats in their area.

- **Privacy concerns**. Counter-UAS detection methods could collect personally identifiable information, such as information about the operators or camera images of bystanders.

Policy Context & Questions

With increased use of UAS and, along with it, increased demand for counter-UAS technologies, key questions for policymakers include:

- What research and development might lead to innovative counter-UAS solutions that can more effectively address UAS safety and security risks while minimizing unintended effects on airspace or the public?
- What are the potential trade-offs if policymakers consider authorizing the use of counter-UAS by others, including state and local law enforcement agencies, and expanding the use of these technologies?
- If policymakers consider expanding authorization, what is the appropriate level of jurisdictional coordination and regulatory oversight for the use of these technologies among federal agencies and others?

●▶ Read also:

- GAO's "Uncrewed Aircraft Systems" issue area website for additional information and products, Washington, D.C., 2022.
- Unmanned Aircraft Systems: Current Jurisdictional, Property, and Privacy Legal Issues Regarding the Commercial and Recreational Use of Drones, B-330570, Washington, D.C., 2020.

Russia may have used a killer robot in Ukraine. Now what?

By Zachary Kallenborn

Source: https://thebulletin.org/2022/03/russia-may-have-used-a-killer-robot-in-ukraine-now-what/

A screenshot of the loitering munition known as the KUB-BLA in English. Credit: Kalashnikov Group.

Mar 15 – Using pictures out of Ukraine showing a crumpled metallic airframe, open-source analysts of the conflict there say they have identified images of a new sort of Russian-made drone, one that the manufacturer says can select and strike targets through inputted coordinates or autonomously. When soldiers give the Kalashnikov ZALA Aero KUB-BLA loitering munition an uploaded image, the system is capable of "real-time recognition and classification of detected objects" using artificial intelligence (AI), according to the Netherlands-based organization Pax for Peace (citing *Jane's International Defence Review*). In other words, analysts appear to have spotted a killer robot on the battlefield.

The images of the weapon, apparently taken in the Podil neighborhood of Kyiv and uploaded to Telegram on March 12, do not indicate whether the KUB-BLA, manufactured by Kalashnikov Group of AK-47 fame, was used in its autonomous mode. The drone appears intact enough that digital forensics might be possible, but the challenges of verifying

autonomous weapons use mean we may never know whether it was operating entirely autonomously. Likewise, whether this is Russia's first use of AI-based autonomous weapons in conflict is also unclear: Some published analyses suggests the remains of a mystery drone found in 2019 Syria was from a KUB-BLA (though, again, the drone may not have used the autonomous function).
Nonetheless, assuming open-source analysts are right, the event illustrates well that autonomous weapons using artificial intelligence are here. And what's more, the technology is proliferating fast. The KUB-BLA is not the first AI-based autonomous weapon to be used in combat. In 2020, during the conflict in Libya, a United Nations report said the Turkish Kargu-2 "hunted down and remotely engaged" logistics convoys and retreating forces. The Turkish government denied the Kargu-2 was used autonomously (and, again, it's quite tough to know either way), but the Turkish Undersecretary for Defense and Industry acknowledged Turkey can field that capability.
Autonomous weapons have generated significant global concern. A January 22, 2019 Ipsos poll found that 61 percent of respondents across 26 countries oppose the use of lethal autonomous weapons. Thousands of artificial intelligence researchers have also signed a pledge by the Future of Life Institute against allowing machines to take human life. These concerns are well-justified. Current artificial intelligence is particularly brittle; it can be easily fooled or make mistakes. For example, a single pixel can convince an artificial intelligence that a stealth bomber is a dog. A complex, dynamic battlefield filled with smoke and debris makes correct target identification even harder, posing risk to both civilians and friendly soldiers. Even if no one is harmed, errors may simply prevent the system from achieving the military objective.

The open questions are: What will the global community do about autonomous weapons? What should it do?

In the first case the answer is pretty clear: Almost certainly nothing. International norms around autonomous weapons are quite nascent, and large, powerful countries, including the United States, have pushed back against them. Even if there were broadly accepted norms, it's not clear how much more could be done. Russia is already under harsh, punishing sanctions for its actions in Ukraine. The US Congress just approved a $13.6 billion Ukraine aid bill, which includes providing Javelin anti-tank and Stinger anti-aircraft missiles. The United States and its allies have also been clear they have little appetite for direct military intervention in the conflict. Plus, how much can the global community really do without knowing for sure what happened? But Russia's apparent use of the KUB-BLA does lend greater urgency to broader international discussions around autonomous weapons.

The state of autonomous weapons discussions

Last week, global governments met in Geneva under the auspices of the United Nations Convention on Certain Conventional Weapons to discuss questions raised by autonomous weapons, including whether new binding treaties are needed. Arms control advocates have not been successful in winning support for a binding treaty banning autonomous weapons so far. The convention's process requires member states to reach consensus on any changes to the treaty. The United States, Russia, and Israel have significant concerns, and various others do not support a ban. The Convention on Certain Conventional Weapons process just is not going anywhere.
Nonetheless, the discussions at the convention have had great value in clarifying options and positions. Delegates to the convention have previously identified four general approaches for addressing autonomous weapons: a legally-binding instrument; a political declaration; strengthening the application of existing international humanitarian laws; and the option of doing nothing. In addition, there's likely a fifth possibility: Countries could, where applicable, raise the issue of autonomous weapons in discussions on other weapons treaties, like those addressing nuclear or chemical weapons.
A legally-binding comprehensive ban on autonomous weapons would represent the strongest possible measure. But the reality is that major military powers would never support this tack. The active protection and close-in weapon systems they use to defend military platforms from incoming missiles and other attacks are simply too valuable.
Advocates might have some greater success if they rally around the position of the International Committee of the Red Cross, which offers an option for common ground. The organization's position on autonomous weapons focuses on their risky aspects. It recommends a ban on unpredictable autonomous weapons, autonomous weapons that target human beings, and various regulations on other sorts of "non prohibited" autonomous weapons. The committee's position also would likely remove the autonomous weapons militaries depend on, like active protection systems and close-in weapon systems, from a potential ban.
Alternatively, governments could focus on better implementing existing international humanitarian law. They could develop a set best practices, practical measures, and general information sharing to improve compliance with international humanitarian law for autonomous weapons. Developing best practices might include ensuring weapons undergo rigorous testing; developing military doctrine, training practices, and procedures to increase the accuracy of any weapons; or undertaking a legal review of weapons use.
However, there is an underlying question of how well autonomous weapons can comply with existing humanitarian law. If failure is rampant and occurs even with best practices in place, then those measures are not enough. Conversely, if those measures do effectively—or even drastically—reduce the risk, then perhaps this approach is useful. Of course, error rates may

vary between weapon systems: perhaps risk can be reduced reliably in some types of weapons, but not others. This may lead to future discussions about narrow bans, better informed by battlefield experiences.
Or countries could just issue a political declaration about the necessity of human control. This might be the easiest approach because no one would be required to give up or alter their weapon systems. But that may also place countries in an awkward position: If human control is necessary, why have autonomous weapons? At the same time, advocates for a ban on the weapons might oppose a declaration with minimal effects on military activity. So, ironically, the seemingly easiest compromise actually might be the least likely.
Last, countries could simply ignore the growing tide of public opinion against autonomous weapons. This would let militaries keep, without apology, whatever autonomous systems they like, but also could be a challenge in democratic societies where public opinion has at least some effect.

Autonomous weapons and weapons of mass destruction treaties
Another possibility for placing some sort of guidelines around autonomous weapons, one that has garnered minimal attention in Geneva, would be to expand the debate to other international treaty discussions. Treaties around chemical, biological, radiological, and nuclear weapons might have applicability to autonomous weapons in certain contexts.
The Nuclear Non-Proliferation Treaty does not require states to maintain human control over decisions to use nuclear weapons. Incorporating the requirement for human control in some manner might actually get great power support. And that is quite significant, because autonomous nuclear weapons are perhaps the riskiest autonomous weapons. An error could wipe out humanity. (Large autonomous drone swarms are another significant risk.) The congressionally authorized National Security Commission on Artificial Intelligence recommended the United States not allow AI to make decisions on firing nuclear weapons. Notably, TopWar, a Russian defense outlet, wrote in support of arms control negotiation on autonomous nuclear weapons on March 8, shortly after the current conflict started.
Advocates could also raise the topic in Chemical Weapons Convention or the Biological Weapons Convention discussions that consider how potential risks might be limited. The more precise targeting that autonomous weapons offer is quite significant for chemical and biological weapons delivery. Part of why most countries have given up chemical and biological weapons is because delivery is unreliable, making them militarily less useful. An errant wind might blow the agent away from the intended target and towards a friendly or neutral population. But artificial intelligence-aided delivery could change that, and may weaken the existing norms around those weapons further.
At minimum, states might consider whether and how to adopt export control measures to reduce the risk of algorithms and software designed for dispersal of pesticides or other chemicals falling into the hands of governments that have chemical and biological weapons. Other treaties may also be options for regulating autonomous technologies in some fashion.
Of course, establishing treaties and norms is only the first step. The next is figuring out an enforcement mechanism: Well, what does the global community do if those treaties and norms are violated? The nature of the response will depend in large part on which option countries can settle on, and how they do so. Arms control advocates might conclude that countries with large, powerful militaries will never be supportive of regulations on autonomous weapons and therefore could attempt to establish a comprehensive ban among whichever states are willing to sign on.
But if great powers do not support the norm, potential punishments like economic sanctions or military intervention won't be meaningful. Certain punishments like robust military intervention might require a specific country like the United States to carry it out and accept whatever risks may come. Conversely, if countries settle on a public declaration advocating for human control or strengthening the applicability of existing international law, nothing may happen until after a conflict and the global community considers what, if any, war crimes may have been committed.
Once again, a potential AI-based autonomous weapon was used in combat. Once again, the details are murky. Once again, the question remains: What do we do now?

Zachary Kallenborn is a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), a policy fellow at the Schar School of Policy and Government, a US Army Training and Doctrine Command "Mad Scientist," and national security consultant. His work has been published in a wide range of peer-reviewed, trade, and popular outlets, including Foreign Policy, Slate, War on the Rocks, and the Nonproliferation Review. Journalists have written about and shared that research in outlets including Forbes, Popular Mechanics, Wired, The Federalist, Yahoo News!, and the National Interest.

EDITOR'S COMMENT: No big news! There was another "killer drone" used in the Libya conflict (Turkish Kargu-2). The future is already here …

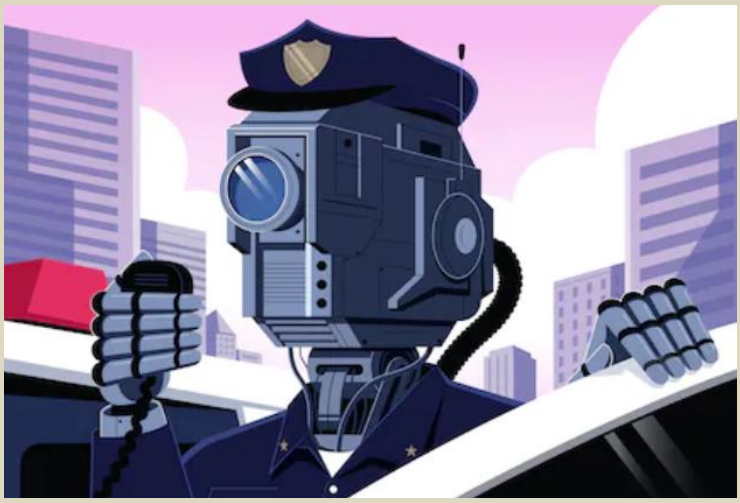
Drones, robots, license plate readers: Police grapple with community concerns as they turn to tech for their jobs

By Danielle Abril

Source: https://www.washingtonpost.com/technology/2022/03/09/police-technologies-future-of-work-drones-ai-robots/

Mar 09 – Last year, police in Mountain View, Calif., knew they had a potentially dangerous situation on their hands when a man barricaded himself inside an unlocked three-story townhouse along with the homeowners.

Police received a call from the homeowners, who said the man was armed with a knife. They didn't know whether they could safely enter the home or where to post up inside. And they didn't know the man's intentions. So instead of taking any risk, police called in their trusty sidekick: A camera-equipped drone.



Officers on the ground used the drone to live stream video from the second- and third-floor windows, giving them the opportunity to assess the gravity of the situation and the location of the suspect. They quickly learned the man did not have any visible weapons on him.

"There was no risk to life, so we let him sit in there and did our best to communicate with him," said Lt. Scott Nelson of the Mountain View Police Department. "No use of force was needed."

The situation ended peacefully when after four hours, the man, who was experiencing delusions, exited the home voluntarily, police said.

Police across the United States are increasingly relying on emerging technologies to make their jobs more efficient. In their daily work, they are using drones, license plate readers, body cameras and gunshot detection systems to reduce injury and bodily harm. The move comes as some law enforcement agencies are struggling with retention and hiring during the pandemic, when hundreds of cops in cities including Los Angeles and New York were sidelined because of the spread of the coronavirus. As police departments determine which technologies to adopt, they are also grappling with growing concerns about privacy that these technologies bring and potential complications they could create for officers on the job.

"Tech can be a great tool for law enforcement to use," said Sgt. James Smallwood, Nashville-based treasurer of the national Fraternal Order of Police. But "as with anything else, we have to balance the line of privacy and meeting the expectation to promote public safety."

Enter the two drones that Mountain View police say cost $16,000 to begin operating and that they've used about a dozen times in the past two years. They've helped in potentially dangerous situations, search efforts and finding weapons. As a result, the department is looking to expand the program to include more drones with more features such as longer flight time, higher video quality and infrared capabilities, which help detect body heat.

DJI, the Chinese tech company that makes many of the drones adopted by police departments, said more than 1,000 police departments across the country use some type of drone. But most departments that purchase DJI's drones do so through American suppliers, DJI's North American spokesman Adam Lisberg said. Drones are proving to be a police force multiplier across the nation, aiding with everything from lost children to dangerous suspects to crash reconstruction. But Lisberg doesn't think they'll ever replace police officers.

"You need a sense of humanity at work in policing," he said. "A drone is a tool that helps accomplish the goals [police] already have. [To] do it better, safely and more efficiently."

In terms of privacy, Lisberg says DJI advises departments to be upfront with the community on how and when the tech will and won't be used.

Drones aren't the only tech tools that police say have made them more efficient. More than 120 cities are using gunshot detection systems, which alert police to gunfire within the devices' coverage area. The tech is provided by Fremont, Calif.-based ShotSpotter, which has been partnering with cities and police for 25 years.

The systems use sensors and algorithms that can identify and determine which loud bangs are probably gunshots. Within about 60 seconds, they can alert police to the precise location in which the gunshots were heard. That allows police to better deploy their resources,

especially in cases where they may have had to cut back on neighborhood patrols, said Ron Teachman, ShotSpotter director of public safety solutions.

"Police chiefs are looking for innovative ways to deal with the responsibilities they have," he said. "They're finding ways to provide them even in areas where budgets are tight."

Douglas Griffith, president of the Houston Police Officers' Union, said ShotSpotter has helped the Houston Police Department make more than 70 arrests as well as respond to gunshot victims faster. The department has 400 fewer officers than it did 24 years ago, yet they are still responsible for covering 671 square miles.

"We have to rely on tech because we don't have the manpower sometimes," Griffith said.

Police also have to consider what tech might be helpful to carry with them. Over the years that has evolved to include body cameras — which not only provide a video record of altercations but in some cases can provide automated reporting — license plate readers and laptops that help them document from the field, and less-lethal restraining devices.

The BolaWrap is a handheld remote restraint device. (Marvin Joseph/The Washington Post)

Nelson said Mountain View is one of the first police departments in the Bay Area to start using a restraining device called the BolaWrap. The device, which discharges two lasso-like tethers to temporarily wrap up a person's arms or legs, is expected to be a less harmful restraining device than a Taser. The department has about 25 of the devices, which have aided in situations like mental health crises when people may harm themselves, Nelson said.

And in some cases, tech that police adopt has the ability to integrate with personal technology that residents own. The Seattle Police Department, for example, uses tech and body cameras from Scottsdale, Ariz.-based Axon. Through Axon's Citizen app, officers can send a resident a link to upload their own video or pictures, which then get tagged with the case number.

Similarly, some departments have turned to Coplogic, incident-reporting software developed by New York-based LexisNexis. Coplogic allows community members to submit their own crime reports for minor incidents, which helps free up police officers' time. Seattle police Sgt. Randy Huserik says it helps officers "streamline the process" of creating incident reports.

"We have to do the same amount of work with less bodies," he said. "So obviously the integration of technology has the potential to enhance that."

To be sure, not all of the technology is proving to be positive, says Griffith of Houston's police union. He noted that while tech can add a level of efficiency, it also can increase stress levels for officers, who have been experiencing increased scrutiny for excessive use of force and discriminatory practices in recent years. Body cameras, for example, can help police and the community better understand the details around an incident in which an officer resorted to use of force. But the cameras also can catch small, sometimes minor policy violations from police that don't affect the overall outcome of any situation, such as whether a police officer buckled his seat belt before pressing the gas, Griffith said.

Acting Lt. Joseph O'Neal demonstrates the Honolulu Police Department's robotic dog in May 2021. Police officials experimenting with the four-legged machines say they're just another tool, like drones or simpler wheeled robots, to keep emergency responders out of harm's way. (Jennifer Sinco Kelleher/AP)

"We know that there will be more tech coming," he said. "But we pray it's something that will help [officers] and not make it to where they have to be perfect every minute of every day."

Police also have to walk a fine line when it comes to implementing new technology, taking into account the community's comfort level and privacy concerns, they say.

The New York Police Department learned that very quickly when it started using a robotic dog to help with surveillance and dangerous situations at the end of 2020. The 70-pound robot named Spot can climb stairs, traverse loose gravel and carry up to 30 pounds of equipment while using its built-in cameras to survey the area. After backlash over additional surveillance and use of police funds, the department ultimately moved to scrap its $94,000 contract with the device maker Boston Dynamics just a few months later.
Boston Dynamics said the cancellation of the program in New York "reinforced the importance of education and dialogue when introducing new technologies" and that the company continues to work on explaining Spot's capabilities. Spot most recently has been adopted by the St. Petersburg Police Department in Florida, which last month said it plans to use the robot dog for de-escalation efforts, to avoid the use of force, or in dangerous situations. The department also said the dog will only be deployed under the supervision of the Special Weapons and Tactics team or for fire rescue efforts.
Bernie Escalante, interim chief of the Santa Cruz Police Department in California, said that in communities like his, a human police officer will provide help when needed — a consideration the department takes into account when considering adopting tech.
"There's definitely a role for [tech], but I also believe the community wants interaction and engagement with someone in uniform," he said.
Some communities are actively trying to find the right balance. After first adopting the technology, Santa Cruz banned the use of predictive policing software, which uses algorithms to predict where crimes will most likely occur. Lawmakers in Boston, Alameda, Calif., and the state of Virginia are among those who took steps to limit the use of facial recognition by law enforcement agencies. Several California cities including Pasadena and San Jose have opted for more license plate readers to curb crime even amid pushback from organizations like the American Civil Liberties Union. And San Francisco is considering broadening government access to private cameras, which it curtailed in 2019.
Farhang Heydari, executive director of the nonprofit Policing Project at New York University School of Law, said he's mostly concerned with increasing access to private cameras and third-party databases and the ability to tie them together, which could create a new kind of surveillance, he said.
That has the potential to magnify some of the harms of policing, like the overenforcement of low-level crime or the exacerbation of racial disparities. Ultimately, Heydari says, police shouldn't be charged with deciding on their own what technology to use. Regulators and communities should, he said.
But as it stands, police departments are navigating tech through research, community input and via discussions with the cities they serve. Mountain View police say that in some respects, their location in the heart of Silicon Valley serves as an advantage to evaluating tech for the department.
"We have a sworn staff here with high-tech backgrounds," said Sgt. Fernando Maldonado. "Just because someone comes in with tech doesn't mean it applies to us or that it's going to work. But we have that background [to understand it]."

Dubai Police's drone-deploying driverless road patrols

Source: https://www.thenationalnews.com/uae/2022/03/14/dubai-polices-drone-deploying-driverless-road-patrols/

Mar 14 – Dubai Police have unveiled a futuristic fleet of driverless vehicles aimed at keeping the force one step ahead of criminals. The autonomous cars can deploy drones and use artificial intelligence to predict potential criminal activity.

The machine-learning patrols will be able to "communicate" directly with police operation rooms to boost the fight against crime.
The cutting-edge patrols were on display on the opening day of the inaugural World Police Summit at Expo 2020 Dubai on Monday.
"There are two versions, the M01, which will be able to access all roads, and the buggy-like M02, which is dedicated for narrow roads and dense residential neighbourhoods," said Col Mansoor Al Gargawi, director of Administration Affairs Department at Dubai Police.

The M01 at the World Police Summit, which brings together law enforcement officers, police departments and organisations from more than 50 countries.

"It has been equipped with smart technology.
"The electric motor has a machine-learning feature which means it can detect patterns of criminal activities or accidents that happen around it."

The M02 is buggy-like and can drive on narrow roads.

"It learns on its own. For example, an area that has been very quiet and begins to witness more traffic, the car will notice that and add the new details to its database," said Col Al Gargawi.
The cutting-edge vehicles are equipped with cameras, 4D imagine radars, data analysis and face recognition features.
Police have been working on the M01 and M02 since 2018, with an official launch date still to be confirmed.

Drone Warfare Is Increasingly Sophisticated, Deadly

By Jim Hanchett
Source: https://www.homelandsecuritynewswire.com/dr20220322-drone-warfare-is-increasingly-sophisticated-deadly

Mar 22 – Policymakers, legislators and military strategists must prepare for the consequences of other countries and actors such as the Islamic State using unmanned aerial vehicles, or drones, in the Ukraine-Russia conflict and others, according to panelists in a Cornell discussion on March 14.
"We're here to make sense of this evolving technology," said panel moderator Sarah Kreps, the John L. Wetherill Professor of Government in the College of Arts and Sciences and a member of the faculty in the Cornell Jeb E. Brooks School of Public Policy.
While the U.S. has used drones for the targeted killing of terrorists, their use by other entities around the world is on the rise.
"Drones can aid, they can watch, and they can kill," said U.S. Army Lt. Col. Paul Lushenko, a General Andrew Jackson Goodpaster Scholar at Cornell and a doctoral student in the field of international relations.
Former CIA Director John Brennan said drones were used during his time in office to target terrorist targets where the challenge was preventing the deaths of civilians living or working along terrorists. "If you're going against conventional military, you're hitting anyone from the

opposing side, so they have wide applications in conventional conflicts as we're seeing right now in Ukraine," Brennan said.
Brennan said the military use of drones spares the lives of pilots and makes them especially valuable for smaller militaries. But Lushenko said there is increasing evidence that military drone operators are susceptible to post-traumatic stress disorder.
"Warfare is intensely human, a battle of wills," Lushenko said. "Drone operators feel that more intimately because they are staring at their targets for so long."
Asfandyar Mir, a senior expert at the United States Institute of Peace, said an emerging discussion in the field is over escalation risk. If an unmanned drone is shot down, there is less likely to be political pressure to escalate a conflict, Mir said. But the improvements in technology could change that equation.
The panelists also pointed out that the low cost of drones makes them attractive to so-called "non-state" actors who can cause mayhem with minimal personal risk. Lushenko said drones aren't just a platform for weaponry that enters a target zone, fires, and then returns to the operator. They can also be rigged to explode on contact, a sort of flying car bomb.
"This brings a new dimension to lethal strikes," he said.
The character of war is shifting in other ways. Using widely seen video of the Russian convoy in Ukraine as an example, Kreps pointed out the abundance of what is called open-source intelligence – easily accessed social media, satellite imagery and drone video and photography.
"The challenge is not the dearth of information, the challenge is the overwhelming volume of information," Brennan said. There is a tremendous need, he said, for analysts able to sort through that abundance, separate information from misinformation, and develop an accurate picture of reality.
This virtual discussion hosted by eCornell was a collaboration between the Cornell Brooks School, Cornell Tech Policy Lab, the Cornell Institute of Politics and Global Affairs, and the Judith Reppy Institute for Peace and Conflict Studies.

Jim Hanchett is assistant dean for communications in the Cornell Jeb E. Brooks School of Public Policy.

Meet the Golden Eagle Unmanned Helicopter

Source: https://i-hls.com/archives/113805

Mar 22 – The Golden Eagle, the first unmanned helicopter of its kind, employs **robotic weapons for precision strikes**, and is the result of a joint project between Israeli technology firms Steadicopter and Smart Shooter.
The new helicopter uses Black Eagle 50E combat platform technology as well as SMASH Dragon and artificial intelligence. AI enables a high level of awareness of a wide range of

situations, along with classification, scanning, and autonomy detection capabilities. The SMASH Dragon system allows the helicopter to shoot and hit stationary or mobile targets with the greatest accuracy, while being controlled remotely. In addition, the helicopter is capable of vertical takeoff and landing.

According to uasvision.com, a unique stabilisation concept is also incorporated into the SMASH Dragon platform, as well as proprietary target acquisition, tracking algorithms, and an advanced computer vision system. With these, target hitting can be done with various types of weapons, such as assault rifles, sniper rifles, 40mm and more.

Through advanced data processing, the AI system detects, classifies, and distinguishes between different kinds of targets (such as people in vehicles, moving or in a static position). As a result of the helicopter's lightweight, it is durable and can perform various tasks for a prolonged period of time.


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

Domestic Preparedness in a Post-COVID-19 World

By Nathan DiPillo

Traditional definitions of domestic preparedness have been influenced by the Cold War and international terrorism. As the 20-year milestone of the 9/11 attack on the United States passed, domestic terrorism also has made its mark on the interpretation of domestic preparedness. It is time for a fresh look, considering pandemics, local human-caused and natural catastrophes, reoccurring threats (like wildfires, earthquakes, and cyberattacks), and crumbling domestic infrastructure. The landscape of emergency response actions and readiness of public and private agencies in a globally interconnected world has left a deep scar on domestic preparedness and how risk is evaluated both nationally and internationally.

A Major UN Climate Change Report Was Just Approved by Nearly 200 Nations

Source: https://www.sciencealert.com/nations-approve-major-ipcc-report-for-policymakers

Feb 27 – Nearly 200 nations approved a major UN climate change report detailing the accelerating impacts of global warming on Sunday, at the end of a sometimes fraught two-week meeting overshadowed by Russia's invasion of Ukraine.
The Intergovernmental Panel on Climate Change (IPCC) confirmed that debates had concluded over the report's crucial "Summary for Policymakers", a 40-page overview distilling the thousands of pages of scientific research, which has been reviewed line-by-line and will be made public on February 28.
Species extinction, ecosystem collapse, mosquito-borne disease, deadly heat, water shortages, and reduced crop yields are already measurably worse due to global heating.
Just in the last year, the world has seen a cascade of unprecedented floods, heatwaves and wildfires across four continents.
All these impacts will accelerate in the coming decades even if the carbon pollution driving climate change is rapidly brought to heel, the report is expected to warn, according to an early draft seen by AFP in 2021.
It will also underscore the urgent need for "adaptation" – a term that refers to preparations for devastating consequences that can no longer be avoided.
In some cases this means that adapting to intolerably hot days, flash flooding and storm surges has become a matter of life and death.
The 2015 Paris deal calls for capping global warming at "well below" 2 °C, and ideally 1.5 degrees Celsius (2.7 degrees Fahrenheit).
In August 2021, another IPCC report on the physical science of human-caused climate change found that global heating is virtually certain to pass 1.5 °C, probably within a decade.
Earth's surface has warmed 1.1 degrees Celsius since the 19th century.
"We cannot escape the climate crisis," said Mohamed Adow, the head of think tank Power Shift Africa.
He said the IPCC report would be useful for people to understand "the scale of the suffering we will endure" if humanity does not drastically cut greenhouse gas pollution – as well as adapting to the challenges to come.
"The backbone of climate action is science and the science is clear. It's telling us how dire our situation is. What is lacking is action from governments," he told AFP.

A New Model for Proactive Prevention

By Rick Shaw

Source: https://www.domesticpreparedness.com/preparedness/a-new-model-for-proactive-prevention/

Mar 02 – Shootings, acts of violence, crimes, abuse, suicides, overdoses, and other incidents and tragedies are increasing nationwide. Cities across the nation saw a surge of homicides in 2020 and many cities were at or near record levels for homicides in 2021. Cities also saw spikes in 2020 and 2021 with crimes, abuse, suicides, overdoses, and other incidents. Organizations, schools, and communities have continued to add more security

solutions as well as more hotlines, safety/threat assessment teams, policies, trainings, and laws. However, violence and crime statistics do not reflect better safety.

Decades of post-incident reports from the U.S. Secret Service, Federal Bureau of Investigation (FBI), and other federal agencies have researched numerous incidents and tragedies and issued various documents regarding mass shootings and other acts of violence. Most post-incident reports routinely identify the presence of more than enough pre-incident indicators existing before a mass shooting occurred and a pathway to violence also existed for most attackers and shooters as they escalated and then executed their plans. But even with more than enough pre-incident indicators, proactive prevention actions still failed.

A Shift in Focus – Asking the Right Questions

Most after-action reports focus on how and why an incident occurred – the pathway that led to the violence and a profile of the attacker – in hopes of finding ways to prevent future attacks. However, when the focus of the research is shifted from the violence aspect to the prevention aspect, the research provides community leaders with new ways and new models to prepare for and prevent future threats. Shifting from validating a pathway to violence to identifying a profile of failed preventions is proving to be a game-changer, but this shift is only possible when leaders of communities and organizations start asking the right questions – and different questions – such as:

- Were pre-incident indicators observed and known by others before the attack?
- Were multiple incident reporting options available?
- Were resources/safety/threat teams available?
- Were trainings and policies provided?
- Were security solutions in place?
- Were laws and standards available?
- Were social workers and mental health resources available?
- Were law enforcement resources available?

Asking questions, especially different questions, is a good way to uncover what might be commonly overlooked or missing. The answers to the questions above can help to reveal additional questions that need to be asked and answered. For example, when asking the above questions after incidents or tragedies occurred over the past several years, the answer to each of these questions is often "yes."

Because of the "yes" answers, follow-on questions are needed to better understand why prevention efforts still failed. For example, if pre-incident indicators were exhibited, observed, and even reported before an incident occurred, then:

- Where were they?
- Who were they reported to?
- Why were the pre-incident indicators not shared with the right people?

Research from hundreds of past incidents reveals that pre-incident indicators almost always exist. However, when the indicators were reported, numerous incident reporting options are being used. This causes the indicators to be scattered across multiple incident reporting options, across multiple entities, across multiple systems, and across multiple people and departments. Some of the incident reporting options include:

- *Hotlines* – including organizational, community, local law enforcement, state agency, federal (like See Something Say Something, Crime Stoppers, 9-11, etc.), nonprofit, or other specific hotlines such those established for bullying, weapons, suicide, gangs, domestic violence, workplace violence, fraud, ethics, or numerous others
- *Electronic communications* – including text lines, mobile apps, emails, websites, or social media

- *Personal contacts* – including trusted adults (such as teachers), supervisors, human resources, security, teams (threat, safety, risk, behavior, workplace violence, etc.), counselors, mental health workers, employee assistance, legal advisors, friends, or family

Closing Prevention Gaps – A New Model

There are many reasons why pre-incident indicators are not collected and not shared with the right people who have authority to take proactive intervention actions. In addition to incident reporting silos mentioned above, there are numerous other issues related to trust, confidentiality, and sensitivity that can create gaps in information sharing. For example, misunderstandings regarding the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and other privacy guidelines are common. Personality traits and egos, departmental turf wars, and information not being shared and not assessed because those receiving the information do not believe it is their job are also common. Numerous other issues are also contributing factors, such as not knowing who the right team members are to share the information with or which other internal and external resources need to know about the information, especially as entities experience employee turnover or attrition.

Pulling together disparate information sources reveals the bigger picture surrounding individuals and situations of concern, which is vital for prevention.

When asking different questions, the different research path reveals numerous and dangerous gaps, silos, and disconnects that are making prevention difficult, if not impossible. Smart funneling and secure information sharing is critical to ensuring the right team members and resources are seeing the bigger picture surrounding individuals and situations of concern. Sadly, scattered pre-incident indicators, scattered team members, scattered community resources, and other scattered expertise are common reasons why proactive prevention efforts continue to fail.

Collecting and sharing indicators are just part of a comprehensive six-stage prevention model. Community leaders need to know what they do not know and know what others know on how to replace old and outdated models with the new research-based prevention model. Community leaders must understand:

- New strategies to build awareness of key indicators
- New ways to collect and funnel the warning signs into a central and secure platform
- How to share information with the right people
- How to empower the right people to assess the indicators/information
- How to connect the dots – connect at-risk individual(s) with community resources for intervention and monitoring, and ultimately how to proactively intervene, disrupt, and prevent escalation of at-risk behaviors

Preventing more incidents and tragedies is possible using the new First Preventers model to complement and help their first responders. The new model consists of innovative, research-based, and real-world proven strategies, templates, and tools that were created by asking the right questions, so the right people are seeing the bigger picture, connecting the dots, and proactively preventing more incidents and tragedies before they occur. Everyone can and must do better.

Rick Shaw founded Awareity in 2004 and founded First Preventers in 2019 and is a prevention expert, author, and prevention coach to organizations and communities. For the past 20+ years, he has been researching post-incident reports, lawsuits, and lessons learned to identify the profile of failed preventions involving terrorism, violence, shootings, suicides, sex abuse, human trafficking, and numerous other incidents. His unique research exposed a profile of failed preventions due to dangerous gaps, silos, and disconnects that conventional and old playbook practices have created. He utilized the research to develop the First Preventers Model.

Space Aliens – Emergency Management Roles & Responsibilities

By Michael Prasad

Source: https://www.domesticpreparedness.com/preparedness/space-aliens-emergency-management-roles-responsibilities/

Oct 2021 – Planning for the emergency management needs of space aliens on Earth, in terms of their well-being before, during, and after disasters could be the plot of a science fiction movie script. The movie District 9 has a similar premise: the aliens that arrived on Planet Earth were not warriors, but rather sentient beings totally reliant on help instead. The reality is there are beings like this in every community. They are called "children."

Like the aliens in movies, children eat different foods (and in different ways than adults), have different sleep patterns, and have more energy on average than most adults (but they generally lack the same level of strength). They also grow in physical size almost exponentially. They have a great need for education. They have an uncanny ability to

communicate with each other very easily, especially with nonverbal cues and signals. Many times, adults have a difficult time communicating with them. Governments at all levels have already made the decisions and commitments to completely integrate children into society, helping them to learn skills and to educate them. Families are recognized (or are established) to help them fully fit into society with everyone else. Children are vastly different from adults: laws are made, as are procedures, facilities, systems, etc. to support them in their uniqueness – yet generally those differences between adults and children are ignored during disasters. During past emergencies and disasters, children's issues sometimes would become a temporary priority to local and even state governments. However, during this worldwide pandemic, the specific disaster needs of all children – and their families – became a national concern. These types of disaster needs were and continue to be very different from those of adults. Emergency managers must consider the threats and hazards associated with children before, during, and after any disaster through the same planning, organization, equipping, training, and exercising – just as would be done for any other concern. These are some of the *specific* children-in-disaster related impacts, along the lines of the U.S. National Emergency Support Functions (ESF) and the Recovery Support Functions (RSF) – with a bit of Preparedness/Protection/Prevention and Mitigation aspects as well.

Emergency Support Functions

ESF#1 – Transportation. Specialized transportation vehicles are used for children. Transportation accidents involving these specialized vehicles are more complex than for other vehicles. There are also transportation regulations and laws related to the movement of children. For example, emergency managers may have to decide whether they would recommend the suspension of car seat and seat belt laws during an evacuation. Evacuation routes from schools and childcare facilities must be considered in reverse-lane planning – including the possibility of using those facilities as endpoint reception centers/shelters.

ESF#2 – Communications. Although there are currently no interoperability communications missions for responders to directly communicate with children (children under 18 are not generally thought of as emergency responders themselves – there are no interoperable communications concerns with children per se), one of the mass care missions is *Family Reunifications Services*. This can be used to reconnect children with their host families and requires dedicated communications channels to prioritize the message traffic for this mission.

ESF#3 – Public Works and Engineering. In many communities, the public-owned schools and other educational/childcare facilities are used for other non-disaster activities (e.g., voting, community meetings) and many have been designated (purpose-built, in many

cases) for major disaster use since the cold-war days more than 50 years ago. K-12 schools and college/university facilities should be considered critical infrastructure/key resources (CI/KR) and designed in ways to support incident response and recovery. Public-private partnerships should be established to also utilize (and support) private schools for these same purposes. In many states, mitigation grants have already been utilized to build safer rooms within schools to protect the community from tornadoes and other weather hazards.

ESF#4 – Firefighting. Part of the skills taught to children includes fire prevention and protection. Firefighters also need training on the differences in size, cognitive skills, and language ability of children, which makes search and rescue aspects different from adults. Also, children may have a fear of firefighters and hide from rescue efforts.

ESF#5 – Information and Planning. As described here, there are many informational and incident planning differences between adults and children. Several children-specific Essential Elements of Information are noted here. TEEX has a course (MGT-439) that covers many of the medical disaster response and emergency preparedness concerns for children. Also, FEMA currently is building a five-hour needs integration course.

ESF#6 – Mass Care. Sheltering for children and their families may require special services (e.g., beds/cots, dietary needs, consumer medical supplies, durable medical equipment, personal assistance). Extra supervision is needed to protect unaccompanied children. Feeding – including mobile feeding – will also have dietary concerns for children, but probably not too different from the variants adults would need (e.g., allergies, vegetarian, kosher/halal). Distribution of emergency supplies must include special items unique to children. Family reunification services, as noted under ESF#2 is critical, especially for unaccompanied children who have been separated from their host families.

They eat different foods, have different sleep patterns, have more energy, grow exponentially, require education, and communicate using nonverbal cues and signals.

ESF#7 – Logistics. As noted under ESF#3, childcare and educational facilities and their staff may be resources available for operations. For example, many of these facilities have food service capabilities that could be used for everyone. Also, getting resources to childcare and educational facilities should be a mission priority (at the same level as restoring any other ESF or establishing a Recovery Support Function [RSF]) as the restoration of educational, health, and mental health services for children and young adults should be a federal Primary Mission Essential Function (it is not currently designated as such).

ESF#8 – Public Health. Although a child's physiology may appear like an adult's, it is not simply scaled by size. Medical treatments, consumable medical supplies, durable medical equipment, etc. are very different for children – and surge capacity issues during mass casualty incidents require extra/different planning, staff organization, equipment, and responder training as well as being exercised regularly. Children have physical, mental, cognitive, emotional, and other health issues that are more critical in their age bands than in adults. Operational sites such as points of distribution for mass prophylaxis and community reception centers for decontamination need to be configured for both unaccompanied children (who may need assistance from responders), as well as children with their host families.

ESF#9 – Search and Rescue. As noted under ESF#4, children may be reluctant to be rescued. They may hide or stay behind with pets. Special protective seating and carrying devices for transporting/evacuating children, are necessary for infants, toddlers, and smaller children.

ESF#10 – Oil and Hazardous Materials Response. Some high school, college, and university facilities have chemicals and other hazardous materials stored onsite for education and research purposes. Some college campuses have their own cogeneration electrical plants, others even have nuclear acceleration laboratories. Proper resource surveys need to be conducted as part of the CI/KR research and review. Grid-mapping of hazard areas, during the preparedness phase will help first responders at these facilities and complexes.

ESF#11 – Agriculture. As noted previously, the amounts and types of foods children eat can be very different from adults. Children have a strong connection with pets. There are no additional biohazard concerns for children related to the food supply, but some foodborne illnesses (e.g., listeria, salmonella) affect children more seriously.

ESF#12 – Energy. In general, there is no difference in energy usage by children. However, their facilities should be prioritized for utility restoration as any other CI/KR site. This will help continue children-in-disaster support missions, as well as provide logistics capabilities from childcare and educational facilities for other ESF use, if needed.

ESF#13 – Public Safety. The legal system treats most children under 18 years old with different laws and issues as to criminal activity. For example, during incidents, curfews may be established for children only. There are also special protection laws for children against harm or abuse, especially those who have been separated from their host families. Searching for missing children is a dedicated task force within operations and has multiple public-private partnerships involved during non-disaster times as well.

ESF#14 – Cross-Sector Business and Infrastructure. There are many people who work at childcare and educational facilities (both public and private) – many can be cross trained for disaster roles. There are also numerous support businesses associated with

children. Childcare and educational facilities (both public and private-owned) should be part of the Building Resilient infrastructure and Communities (BRIC) Mitigation Planning, as their cross-functional use for supporting other ESFs can be a community asset.
ESF#15 – External Affairs. How emergency management is supporting children, their host families, facilities, etc. is no different than any other ESF or RSF. It certainly requires leadership and subject-matter expertise (SMEs) for this specific field. Public information officers (PIOs) would be strongly encouraged to understand the basics of supporting children during disasters but should also have PIO support by childcare and educational SMEs at the ready (e.g., press conferences, joint information centers).

Recovery Support Functions
Housing RSF. Children need to be considered in housing capacity, both as part of host-family sizing calculations and as collective units within any residential child support site(s) for children without host-families (e.g., group homes, orphanages). Children with disabilities also may need separate residential support sites.
Health & Social Services RSF. As a continuation beyond the response from ESFs# 6 and 8, the health and social service needs of children has been noted previously. The skills learning and education by children is a greater need than what this RSF currently is designed to support.
Community Planning and Capacity Building RSF. Childcare and educational facilities, when damaged or destroyed by a disaster – or are in insufficient quantities and capacities for post-recovery growth of a community – need to be included in the community planning process. The same is true for the support services needed, which are child-specific (e.g., medical/mental health treatment facilities, libraries).
Economic RSF. Prioritized restoration of childcare and educational facilities and support services provides three major economic benefits:

- Without these facilities, most host-families (and many emergency responders) may not be able to fully return to work since they must provide full-time care for their children.
- There are many jobs and financial support systems associated with these childcare and educational facilities. Restoring these facilities greatly supports the local economy.
- In the long run, properly educated and trained children contribute to society.

Infrastructure Systems RSF. As a continuation of ESF#3, the interagency and interjurisdictional support of both public and private childcare and educational facilities leverage innovative and green technologies and support renewed economic activity.
Natural and Cultural Resources RSF. Children and their host families benefit from restored natural and cultural resources as adults do. The significance and importance of these resources is something to share with children for long-term community well-being.
FEMA is already starting to recognize the complex aspects of supporting children in disasters. Also, the new IS-237 course introducing Deliberate Planning specifically notes that whole community planning needs to include restoring childcare and educational facilities as a community need. The points made about restoring those facilities alone, for first and emergency responders, should be a priority to sufficiently have the workforce needed to support the response and recovery from any disaster. The International Association of Emergency Managers – Children and Disasters Caucus is also working on a long-term project to amplify the disaster needs of infants, children, and young adults (from pre-K through college) to the same levels of Community Lifelines, Emergency Support Functions and/or Recovery Support Functions. Emergency managers need to consider their community's children as unique and vital in many ways.

Michael Prasad is a Certified Emergency Manager and is the senior research analyst for Barton Dunant Emergency Management Consulting and a regional product and services representative for The Blue Cell. He is also a member of the International Association of Emergency Manager's Children and Disasters Caucus and the vice president for the IAEM-USA's Region 2. He holds a Bachelor of Business Administration degree from Ohio University and is a Master of Arts candidate in Emergency and Disaster Management from American Public University.

EU MEDEA project

Source: https://www.medea-project.eu/

MEDEA is an EU-funded Coordination and Support Action project the scope of which is to establish and further develop a regional network of practitioners and other security-related actors in the Mediterranean and the Black Sea region. MEDEA project groups the practitioners into 4 thematic communities: Managing migration flows and asylum seekers; Border management and surveillance; Fighting against cross-border crime and terrorism; Managing natural hazards and technological accidents. MEDEA aims to engage a critical

mass of security practitioners, and actors including first-aid responders, border guards, national police, civil protection teams, humanitarian workers, defense entities, and other interested stakeholders in efficient cooperation with cross-discipline entities from other countries. The expected result would be an effective response to all security threats common to the Mediterranean and the Black Sea region. The requirements from all four communities will be featured as inputs (regional operational needs) in the Mediterranean and Black Sea Security Research and Innovation Agenda (MSRIA).

▶**Project Coordinator:** Center for Security Studies (KEMEA – Greece)

ICI International

CBRNE INSTITUTE

Because international CBRNE First Responders need a common roof!

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