

05\22

I
C
I

2 CBRNE

*Dedicated to Global
First Responders*

DIARY

May 2022



PART B

**New
CWA
nasal
spray**



An International CBRNE Institute publication

IOI
International
CBRNE
INSTITUTE

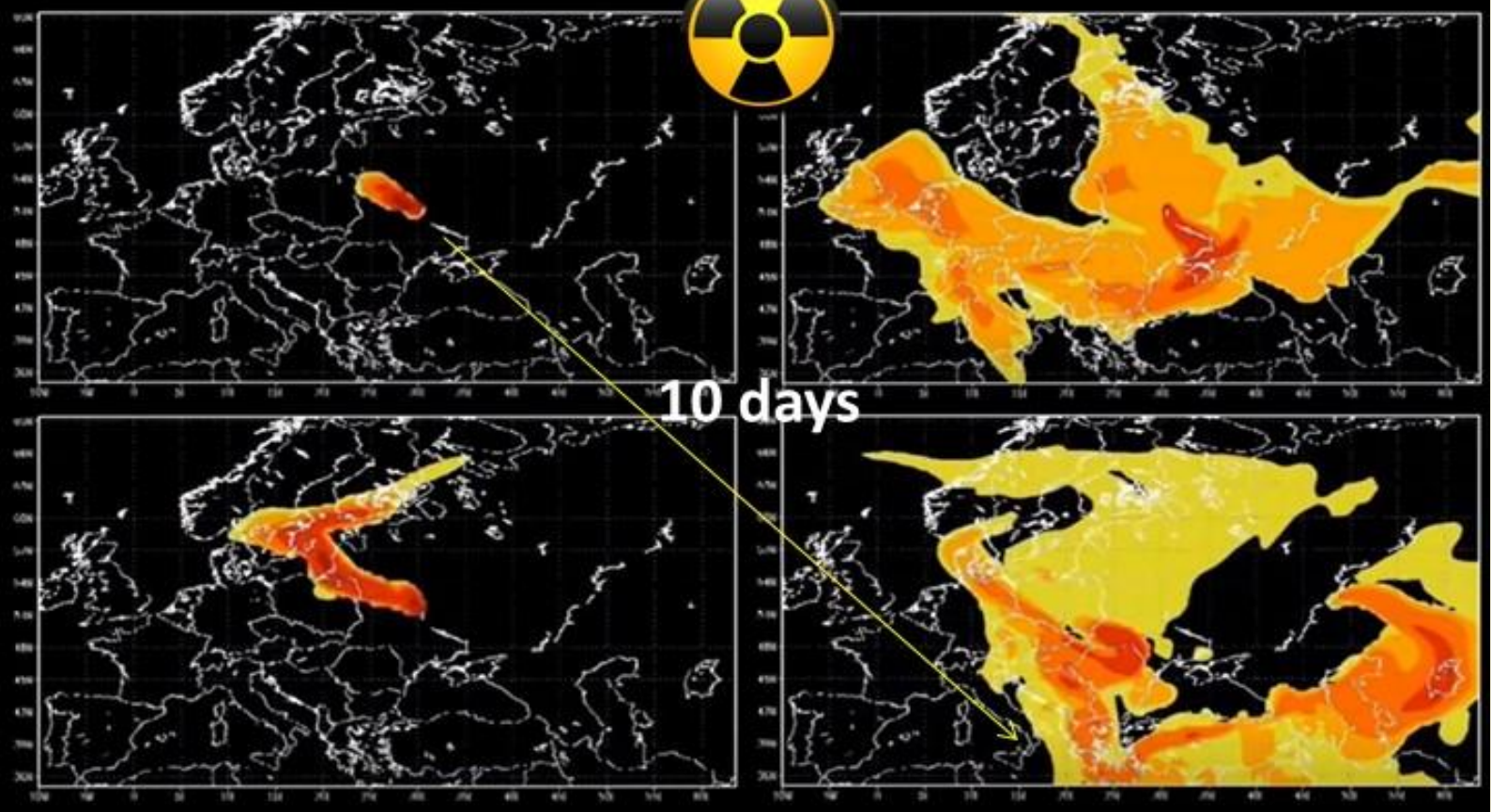


C²BRNE
DIARY

DIRTY R-NEWS



26 April 1986
CHERNOBYL *disaster*
26 April 2022



Siegfried Hecker: Putin has destroyed the world nuclear order. How should the democracies respond?

By John Mecklin

Source: <https://thebulletin.org/2022/04/siegfried-hecker-putin-has-destroyed-the-world-nuclear-order-how-should-the-democracies-respond/>



Siegfried Hecker (second from right) visits the secret Russian nuclear city of Sarov in February 1992. Credit: screen grab from Stanford University "Doomed to Cooperate" video, available on YouTube at: <https://www.youtube.com/watch?v=81ZpFLO4hmE&t=1s>

Apr 21 – One of the world's foremost nuclear security and policy experts, Sig Hecker has spent much of an illustrious career working to enhance cooperation among US and Russian scientists and their governments in hopes of reducing nuclear risk. In fact, Hecker has literally edited the book on the subject, [Doomed to Cooperate](#): *How American and Russian scientists joined forces to avert some of the greatest post-Cold War nuclear dangers*.

Clearly, Russia's brutal invasion of [Ukraine](#) has changed international relations in profound and potentially lasting ways and brought the real possibility of nuclear weapons use to the forefront of public consciousness. An emeritus fellow at Stanford's Freeman Spogli Institute for International Studies, a former director of Los Alamos National Laboratory, and a longtime contributor to the *Bulletin*, Hecker took time last week to speak with *Bulletin* editor in chief John Mecklin about the enormous damage that Russian President Vladimir Putin has done to the world nuclear order via his decision to invade Ukraine. That decision marks, Hecker contends, a turning point in world nuclear affairs as momentous as the dissolution of the Soviet Union.

John Mecklin: In a [talk](#) earlier this week to the American Physical Society, you said that Putin has essentially turned the whole nuclear order upside down by invading Ukraine. Why don't you, in summarized form, explain what you meant by that.

Siegfried Hecker: What I said is that the major question right now that seemed to be on people's mind is whether Russia, meaning Putin, is going to use nuclear weapons in Ukraine.



I said, I don't really know, although the chances are certainly non-zero, and I can get back to that.

But what I do know is that he's blown up the global nuclear order that has been developed over the last 70 years, for the most part by the United States and Russia. That order has helped to allow the world to take advantage of the benefits of nuclear energy—such as nuclear electricity and nuclear medicine—while avoiding the worst potential consequences, everything from nuclear weapons use, to lots of countries seeking nuclear weapons (we have fewer than 10 today), to nuclear terrorism, and nuclear accidents. The global order has allowed us to have the benefits outweigh the risks of nuclear energy.

And I see that order being destroyed by what Putin has done in Ukraine, every facet—from nuclear deterrence, to nonproliferation, to the prevention of nuclear terrorism, and the future of nuclear power.

Mecklin: Do you think he meant to? Do you think Putin was trying to upend the whole appletart or just screwed up?

Hecker: Oh, absolutely not. Destroying the nuclear order was not by design. There are bits and pieces of the of the nuclear order that he's objected to for quite some time, and I've been watching that over the past 20 years or so. But for example, on the issue of nuclear power, what he's really done is he's shot himself in the foot. That was one of the biggest high-tech exports that Russia had. It was the leader in foreign nuclear power plant construction and nuclear fuel services. I can't imagine that Putin would have thought that the invasion of Ukraine is going to have any effect on that.

From the best that we can put the pieces together, he thought Ukraine was going to be real quick and simple, something like the annexation of Crimea. He was going to go in, take things over. I don't think all of these things that I'm really concerned about were at the forefront of his thinking.

Mecklin: You touched on the nuclear power industry; the war is kind of a disaster for the Russian nuclear industry. What does it mean, internationally? Because there are lots of other countries that are involved in commercial nuclear power.

Hecker: Indeed, the question is going to be—since Russia has played such a large and prominent part, especially in fuel cycle services, like enrichment of uranium for nuclear power plants; Russia supplies about 35 percent of the world's enrichment capacity today—where is nuclear fuel going to come from? Where's the enrichment going to come from? And, of course, what about nuclear power plants?

Now that Russia has shelled the Zaporizhzhia operating nuclear plant in Ukraine and had its soldiers overrun the Chernobyl radioactive exclusion area, what country is going to have Russia build it a new nuclear power plant? Will anyone else be able to step in? I think the one best prepared to step in is China. However, along the way, there are going to be all these different bits and pieces [of the global nuclear industry] that are missing, that will have to be rebuilt.

The nuclear nonproliferation regime was built around the Nuclear Non-Proliferation Treaty as its central element. However, it is embedded in a fabric of other agreements, practices, and norms that require international cooperation—and leadership from the big nuclear powers. Russia has played a central role in the nonproliferation regime and with the International Atomic Energy Agency. It's going to be difficult to see how we're going to live with an international system, where we have a formerly responsible nuclear state that's now become a pariah state—a country we can no longer count on to be responsible in nuclear matters—but is still so actively involved in the nuclear arena, even though it might have shot itself in the foot.

I should add that in addition to upending the global nonproliferation regime, Russia may have also delivered the death knell to arms control, which has already been on the ropes over the past 20 year—being diminished by both Russian and American governments.

Mecklin: You also mentioned nuclear terrorism. How has the invasion changed your concerns?

Hecker: After 9/11, our concerns were focused on preventing nuclear terrorism by non-state actors. The shelling of the nuclear power plant is an act of state-sponsored terrorism. States such as Russia, of course, have access to much more dangerous nuclear and radiological materials and their means of delivery. The United States has worked with Russia in various initiatives to combat global nuclear terrorism, but now we must be concerned about Russia committing nuclear or radiological terrorism.

Mecklin: I'm going to hop subjects a little bit. Everybody's asking you (and they're all asking me): Is Vladimir Putin really going to use a nuclear weapon in Ukraine? And, of course, nobody but Vladimir Putin can really answer that question. I'm interested in what you think the United States should do in response, if Russia uses a tactical nuclear weapon or some other weapon of mass destruction in Ukraine?

Hecker: Well, I think first of all that we need to separate nuclear weapons from other weapons of mass destruction. The only other weapons that we're really concerned about, that would change the course of the war, are chemical weapons. And in my opinion, chemical weapons, as such, are really not weapons of mass destruction. So, let's put chemical weapons aside, although we need to be concerned about that potential, and let's think about nuclear weapons.

Let me first try to answer the question: Why am I concerned that Putin would use nuclear weapons in Ukraine?

I think one of the most important aspects of the whole nuclear era is the no-use-of-nuclear-weapons norm. Since Hiroshima and Nagasaki in 1945, no matter how you might complain about what's happened in the nuclear world, one thing has not happened: A nuclear weapon has not been detonated in wartime. I believe it's essential that we keep that norm. Deterrence has worked, although we have also been lucky. During the Cold War, of course, there were



many scary times, such as the Cuban Missile Crisis. But nevertheless, the norm held up, and then to some extent many of us—certainly me—breathed a big sigh of relief when the Soviet Union dissolved, and it was clear that we're going to walk away from the precipice of using nuclear weapons. The US and Russia dramatically reduced the number of nuclear weapons.

But then what actually happened is through the '90s, through those enormously difficult economic times in Russia, where essentially everything collapsed, including their conventional military, their nuclear doctrine evolved. The most important aspect was they then considered that there was a potential use for nuclear weapons in response to a conventional attack if the existence of Russia was in question. Over the years, Russian military doctrine then evolved to provide a smooth transition from conventional weapons to tactical (non-strategic), to strategic nuclear weapons. It washed out the difference between conventional weapons and tactical nuclear weapons.

We in the United States—and certainly me as a person in the nuclear business over the last 50 years—I always thought there must be a great discontinuity between conventional and nuclear weapons. The Russians don't consider that so anymore. And what we don't know today, for example: Is there some point where Putin would say—because the way the war was evolving, let's say in the eastern part of Ukraine—that he believes there is an existential conventional threat to Russia that he needs to use tactical nuclear weapons to counter.

So, whereas before I would have thought the likelihood of Russia using nuclear weapons was basically zero, I no longer consider it zero, though it's still low. Also, some of my Russian colleagues, my counterparts—their nuclear weapons laboratory directors—contributed a paper to my book, *Doomed to Cooperate*, where they laid out the strategy for tactical nuclear weapons. In essence, what they said was now nuclear weapons are no longer just for strategic use; they are weapons to make sure that there is no major threat to Russia. And they no longer are just used to counter weapons of mass destruction, but they may now be used to counter threats to their country.

And so that's the principal concern that I have. You asked what does the US do in return [if Russia uses a nuclear weapon in Ukraine]? So that was a long way to get to your question, and I would say, we really have to assess what the situation is and what the damage is.

First, it's going to change the face of warfare, because we haven't had a nuclear weapon used in 77 years. But rather than immediately responding with a nuclear weapon, I think we need to assess the damage, and then decide how we're going to respond to Russia. My immediate view at this point without knowing exactly what will happen is that that response should be a conventional military response. And the US has the capabilities to do sufficient damage in retribution with conventional military and not allow this to escalate to a potential strategic exchange. More than anything, what has to drive our thinking is we must avoid a strategic nuclear exchange between Russia and the United States that could eventually imperil the world as we know it.

But that does not mean that there does not have to be a military response.

Mecklin: Do you know of any kind of game, or study, or military exercises where somebody has found that that kind of tit for tat does not escalate to general nuclear war? I haven't run into a scenario somebody was able to come up with that, once escalation started, you could stop it. Are you aware of any?

Hecker: No. Most of these are the type of war games that have been played by governments as well as some nongovernmental organizations. And you're correct that most of those—at least, the ones I'm familiar with—eventually wind up escalating to a strategic exchange. But they are just that, games; they're war games. They don't necessarily represent what actually happens on the ground. So the bottom line, I would say, is: We don't know. But we should do everything that we can to avoid this escalation.

Mecklin: Your talk earlier this week went toward your idea Russian and American scientists need to continue to talk to one another. So this is a two-part question. First, are you still in contact with some of your Russian friends while the war is going on? And second, why do you think that sort of contact is important now?

Hecker: To answer the first question, I have not had direct cooperation with my colleagues at the Russian nuclear weapons laboratories—the equivalent of their Los Alamos, Lawrence Livermore, and Sandia national laboratories—since about 2014. And that was a direct consequence of the Crimea invasion, annexation, and the aftermath. I've stayed in contact with several of my colleagues in the Russian nuclear complex, but no cooperation along the lines of what we did between 1992 and 2014.

At that point, I decided—because I believe so strongly that cooperation between the nuclear scientists and engineers of the two sides is crucial in this global nuclear order—to establish a program engaging the next generation. I called it the Young Professionals Nuclear Forum, where I brought together—Stanford leading the US side, with myself heading that effort, and the Moscow Engineering and Physics Institute heading the Russian side—eight to 10 young professionals from each side who had an interest in the nuclear world. And we got them together twice a year, once in Moscow, once at Stanford, to tackle nuclear issues that we face commonly from a global perspective. Some of their work has been featured in co-authored articles in your *Bulletin*.

That's what I've been doing, essentially since 2016. I've stayed in contact with them. With COVID, we had to go virtual. The last in-person meeting was in late 2019. In 2020 and '21,



we were virtual, and we continued the collaboration. At the end of February this year, with the invasion of Ukraine, we put it on hold. So currently, I contact some of the Russian nuclear folks, but we have no more cooperation.

Mecklin: Okay, going forward, given what's happened, what could cooperation do? I mean, does Vladimir Putin listen to scientists?

Hecker: You asked why is this cooperation so important? I didn't answer that part of the question. If you don't mind, let me answer that question, and come back to Putin. The reason that it's important, as I mentioned already, is that the global nuclear order requires cooperation from the leading nuclear states. Otherwise, you don't have a global nuclear order. It's essential that governments play a role, and the scientists need to play a role. We did some of that during the Cold War. During Soviet Union times there was collaboration between the two sides. Of course, on the political side there was also the arms control, the Non-Proliferation Treaty, etc.

But then, where the scientists-to-scientists interactions really came into play, which showed how crucially important it was, was with the collapse of the Soviet Union. I've described that in the book, *Doomed to Cooperate*. At that point, we had the four loose nuke problems: loose nuclear weapons, loose nuclear materials, loose nuclear experts, and loose nuclear exports. Just to put numbers on that: At one time, the Soviet Union had 40,000 nuclear weapons. We had 31,000 around 1965 and then started decreasing them, although we made them more accurate.

In terms of fissile materials, the Soviet Union had on the order of 1.4 million kilograms of fissile materials. Just to give you a comparison, today I believe that North Korea has less than 50 kilograms of plutonium and less than 1,000 kilograms of highly enriched uranium. There was an immense number of nuclear experts, a couple of hundred thousand or so, together with the civilian [experts], over a million. And then exports: The concern was that, as the economy collapsed, they might sell nuclear material and technologies. It was with the US government help of the Nunn-Lugar Cooperative Threat Reduction Program that we American scientists were able to work hand-in-hand with the Russia nuclear scientists. And today, people ask me, "So was it worth it? Look, Putin has just invaded Ukraine." I've said, "Yes, it was worth it, because we had no loose nukes in Russia, very little leakage of nuclear materials, very, very little leakage of nuclear weapons knowledge. And the exports, they eventually got under control in the 1990s." So that's why it was important then and I believe it's going to stay important for the future, especially now that Putin has sort of blown things up.

But what we're going to have to do is to re-envision what nuclear cooperation is going to look like in the future. To do that we need their scientists, we need their engineers, we need to continue to talk, to work together to make sure that the world avoids a nuclear catastrophe and gets the best out of nuclear energy. I strongly believe that sort of cooperation continues to be imperative. Now I'll let you go on with the question...

Mecklin: Well, Vladimir Putin won't be here forever. But while he's here, I see less for the scientists who cooperate to do, when you have somebody who has been [described by Fiona Hill](#) as a one-man band, somebody who just decides everything thing on Vladimir Putin's terms. But you know more about this than I do. Is it conceivable that over time, even with Putin in power, that a nuclear order could start to be put back together? Do you see that as plausible?

Hecker: Right now, during Putin's rule, what are the nuclear scientists allowed to do? Very little in terms of cooperation. In fact, the story that I just told you about Cooperative Threat Reduction before and how we worked together—over the past 10 years or so, Putin has changed the narrative from these programs having benefitted both sides to claiming they were an American spy operation. As it turns out, that's just totally, totally false. In fact, my book, *Doomed to Cooperate*, shows it to be false—from the Russian side. The Russian scientists themselves tell their stories of how that cooperation helped both sides. So Putin was already on the warpath in terms of cooperative activities. Would he allow it now? I think the answer is absolutely not. There's nothing that we can do right now, in terms of direct nuclear cooperation with the Russians. Perhaps something could be done through third parties, like the IAEA, and perhaps have some cooperation on anti-nuclear terrorism activities. That may be able to keep some cooperation alive.

But in that case, the Western world is going to look at the Russians and say, "you've got this leader who's thrown all protocol out, who now has demonstrated that he's completely irresponsible, in terms of how to deal with other countries and with innocent civilians." I don't see that we can establish any cooperation in the near term. However, what I learned during the time that we worked with the Russians—my contacts started in 1988. In 1992, I went to Russia for the first time, my first of 57 visits to Russia. So with 57 visits, you can see that I believed that cooperation was really imperative for us. What I found when I started working with the Russians is that the Russian nuclear complex, and the nuclear cities that were closed cities and are still closed cities today, are a critical part of the civil society of Russia. The scientists in those cities had no intentions to leave [Russia], they had no intentions to export [nuclear material]. They were patriotic, and they were part of Russia's civil society.

And that's the civil society we're going to need, if we're going to restart cooperation, once the political matters line up. Until then, there isn't much that we can do except to stay in contact.

Mecklin: I have a final, strategic question that's less specific to Russia: Some people say we've just entered a new Cold War, with China and Russia lined up on one side. Maybe now it's not so much communism versus the free world as autocrats versus democracies. To me,



it would be horrible if that happened. Do you think there's a way to avoid the world returning to simmering camps, at each other's throats for decades at a time?

Hecker: In my life, I've watched the dark days of the Cold War. I started at Los Alamos as a young summer intern in 1965, and we were in the middle of that Cold War. And yet I had hopes that someday, we could get out of that situation, and lo and behold, we did. As you say, now we're locked into something else. And I guess I wouldn't call it a return to the Cold War or Cold War 2.0. But it's quite clear now as one looks at all the actions that Chinese President Xi Jinping has taken, long before this issue of the Ukraine invasion, and that Vladimir Putin has taken, also long before the Ukraine invasion, because he certainly showed his stripes with the annexation of Crimea and going into eastern Ukraine—as we look at all of that, it certainly does seem to be that we've constructed a new standoff of autocracies versus democracies.

The big autocracies are being led by Xi Jinping and Russia. China is of greatest concern, because it's not only building up as a nuclear power and technological power, but it has enormous economic impact. Russia has much less of that, and after Ukraine, the Russians are going to be in deep, deep economic difficulty. We have that on one side.

What Ukraine showed is that such autocracies are willing to conduct a brutal, totally unprovoked invasion. How in the world do we get out of this? The two most important things, in my opinion are, first, that democracies must work together. That's one of the bright spots of the invasion of Ukraine. It has brought the Western democracies back together. Before that, relations were greatly frayed, particularly during the Trump administration. And the invasion of Ukraine has brought them back together. We're standing together, and that will be imperative to show that democracies are not weaklings of the past; they can manage and bring their people together for what we see as justice.

That's one of the crucial elements. The second element, which may actually be more important, is how we fix our own democracy in this country. If we're going to be the democracy that the rest of the world looks up to, we need to fix the deep political divisions that greatly weaken America—the overall moral stature of the country, the political stature, economic stature, and then the military stature. In other words, how do we fix our own country?

Let me conclude by stressing that what Putin has done is to blow up the entire global nuclear order. That's really a major hinge, a turning point in the nuclear world. That's as big a hinge as when the Soviet Union dissolved, in my opinion. We were creative in 1989 through '92, and we're going to have to be creative now, as the war hopefully draws down and ends. But it's going to take creativity, because we face a different world situation with the loss of the global nuclear order that's been developed over so many years.

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

Chernobyl is still changing: Four enduring stories and a recent one

By Susan D'Agostino

Source: <https://thebulletin.org/2022/04/chernobyl-is-still-changing-four-enduring-stories-and-a-recent-one/>

Apr 25 – “One of the atomic reactors has been damaged,” a Radio Moscow broadcast [announced](#) about the Chernobyl Nuclear Power Plant on April 28, 1986—nearly three days after the accident. “Measures are being taken to eliminate the consequences of the accident. Aid is being given to those affected. A government commission has been set up.”

World citizens did not know then that the event would register as the world's worst nuclear disaster. They did not know that [two](#) plant workers had died in the explosion at Chernobyl, that [28](#) more would die within weeks from acute radiation poisoning, or that thousands would be diagnosed with thyroid cancer over time. They also did not know then that thousands of workers would need to continue decommissioning work at the plant for decades. And they likely could not have imagined how Chernobyl's legacy would continue to change in dramatic ways over time.

In the 36 years since that day, nuclear experts have learned and incorporated many lessons about nuclear safety. Tourists now frequent the desolate town of Pripyat; some are respectful, others are not. A sizable radius around the plant has transformed into an



ecological reserve in which animals and plants thrive. Chernobyl also now boasts a new logo. Then, last month, the beleaguered site appeared in headlines again when Russian forces seized control of the plant just days after invading Ukraine. Since 1986, much has been written about Chernobyl—both the disaster and the place that lived on after the disaster. Below are four Chernobyl stories published in the *Bulletin* that have endured. The fifth story offers evidence that Chernobyl's story may always be a work in progress.



Alley of abandoned villages - 162 plaques with the names of permanently evacuated settlements during 1986-1991 after the Chernobyl accident. Credit: Margarita Kalinina-Pohl (2018).

[2011: Chernobyl 25 years later: Many lessons learned](#)

By [Mikhail Gorbachev](#), March/April 2011

Mikhail Gorbachev penned this essay on the solemn lessons Chernobyl taught the world about nuclear accident prevention, transparency, and vulnerability to terrorism and violence. He wrote: “[Chernobyl] was a horrendous disaster because of the direct human cost, the large tracts of land poisoned, the scale of population displacement, the great loss of livelihoods, and the long-term trauma suffered by individuals yanked from their homeland and heritage. ... Let us all remember Chernobyl, not only for its negative impact on Ukraine, Belarus, Russia, and Europe, but also as a beacon of hope for a safer and more sustainable future.”

[Chernobyl: A nuclear accident that changed the course of history. Then came Fukushima.](#)

By [Mariana Budjeryn](#) | March 11, 2021

Mariana Budjeryn reminded readers that the Chernobyl nuclear disaster was largely seen as a result of the Soviet Union's “backward” safety culture. But then the Fukushima disaster later happened in “an industrialized, technologically-savvy, wealthy nation with what had been regarded until that point as strong institutional infrastructures.” Budjeryn then notes



that nuclear experts agree that “the question is not whether another nuclear accident will happen, but rather when it does, how prepared are we to minimize the damage and respond quickly and effectively.”

[It's not radioactive Disneyland: Visit Chernobyl, but respect it.](#)

By [Margarita Kalinina-Pohl](#) | April 26, 2021

Margarita Kallina-Pohl looks past the kitschy souvenirs and tourists posing for selfies with Geiger counters to introduce readers to a fox named Simon who is fed by locals and lives in the 19-mile radius ecological biosphere reserve surrounding the defunct power plant. She reminds readers that Chernobyl is not a nuclear theme park but the site of the “largest anthropogenic disaster in the history of humankind.” A must-read for those interested in meaningful and respectful ways to visit.

[Rebranding Chernobyl](#)

By [Julian Hayda](#) | August 25, 2021

Julian Hayda tells the story of Banda, a Kyiv design agency, that held a 2019 company picnic in Chernobyl. Their 20 graphic designers were moved to think more deeply about the site, which then prompted them to design a visual brand for Chernobyl and its legacy. “Banda’s logo is really a series of 78 logos—one released every year—with slices of it disappearing each year, until the image is totally gone. The logo for 1986, the year of the disaster, is a complete, black octagon. The logo for 2064 is a white void. There’s supposed to be a logo there, but it’s invisible—perhaps like radiation, which the eye can’t really see, but is nonetheless ever-present in the lives of those affected by the Chernobyl disaster.”

The changing logo “exemplifies the Zone’s movement from exclusion to rebirth and from darkness into light.” It also enables “the creation of official souvenirs that counteract the more vulgar ones.”

[Russian forces now control Chernobyl, inviting speculation and uncertainty](#)

By Susan D’Agostino | February 25, 2022

Lightning, contrary to the maxim, can and does sometimes strike twice. That’s what appeared to have happened—at least on a metaphorical level—when Russian forces seized control of the defunct Chernobyl Nuclear Power Plant last month, just days into its invasion.

As in 1986, the world’s eyes fixated on Chernobyl and the possibility of another nuclear nightmare. Though Russian forces have since relinquished control, this article captures the confusion, speculation, and concern the world experienced when war intersected with a nuclear disaster site for the first time.

Susan D’Agostino is an associate editor at the *Bulletin of the Atomic Scientists*. Her writing has been published in *The Atlantic*, *Quanta Magazine*, *Scientific American*, *The Washington Post*, *BBC Science Focus*, *Wired*, *Nature*, *Financial Times*, *Undark Magazine*, *Discover*, *Slate*, *The Chronicle of Higher Education*, and others. Susan is the author and illustrator of [How To Free Your Inner Mathematician: Notes on Mathematics and Life](#) (Oxford University Press, 2020). She is a member of the editorial board of the Mathematical Association of America’s *Math Horizons* magazine. Susan earned a PhD in mathematics at Dartmouth College and an MA in science writing at Johns Hopkins University. She has received science writing fellowships from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.

Risks of an Unfamiliar New Nuclear Age

Source: <https://www.homelandsecuritynewswire.com/dr20220426-risks-of-an-unfamiliar-new-nuclear-age>

Apr 26 – High-tech advances in weapons technologies and a return of ‘great power nuclear politics’, risk the world ‘sleepwalking’ into a nuclear age vastly different from the established order of the Cold War, according to new research undertaken at the [University of Leicester](#).

Andrew Futter, Professor of International Politics at the University of Leicester, makes the warning in a research paper for the Hiroshima Organization for Global Peace (HOPe), published today (Friday).

While stockpiles are much reduced from the peak of up to 70,000 nuclear weapons seen in the 1980s, progress in a number of new or ‘disruptive’ technologies threatens to fundamentally change the central pillars on which nuclear order, stability and risk reduction are based.

Modern nuclear weapons – acknowledged to be held by nine countries including the USA, Russia and UK – are more capable and more precise than their Cold War counterparts, and at the same time, are being augmented by a new suite of strategic non-nuclear weapons that might be used against or instead of nuclear weapons.



Advances in offensive capabilities have, however, been matched in increasingly sophisticated sensing, tracking and processing technologies designed to detect, prevent and in some cases respond to a nuclear strike – often using Artificial Intelligence (AI). Professor Futter said: “While we’ve seen a substantial reduction in the number of nuclear weapons held across the world, it’s important to remember that this reduction came about as much as a result of rationalization than a genuine drive to disarm. After all, you can’t destroy a city twice, and it takes an enormous amount of money to build and maintain this technology. “We’ve seen massive advances in the capabilities of these weapons and their support systems in the 30 years since the end of the Cold War, and there’s a danger that this means the established rulebook of nuclear doctrine could be thrown out of the window.” However, there are potential political solutions as the world prepares to enter what Professor Futter terms a ‘Third Nuclear Age’. He continued: “Choosing the correct pathway for our nuclear future was hard enough in the past and there is no suggestion it will become any easier as we move into a new, potentially more complex and dynamic chapter in the nuclear story. “Policy proposals to manage the challenges of the Third Nuclear Age are therefore inherently bound by whether one believes the best approach is to take our nuclear world as it is and seek to manage it through restraint, arms control, and norms; or whether it is possible to transition to a world where nuclear weapons no longer exist through sustained moral, ethical, legal and perhaps technological pressure.”

See:

‘[Deterrence, Disruptive Technology and Disarmament in the Third Nuclear Age](#)’ is published by the Hiroshima Organization for Global Peace. ‘[Disruptive Technologies and Nuclear Risks: What’s New and What Matters](#)’, in which Professor Futter further explores the themes of new nuclear capabilities and their impact, is published in the journal *Survival*.

► The Third Nuclear Age research project is funded by the European Research Council. Find out more at thirdnuclearage.com.

Will Putin go nuclear? A timeline of expert comments

By Susan D’Agostino

Source: <https://thebulletin.org/2022/04/will-putin-go-nuclear-a-timeline-of-expert-comments/>



Apr 27 – “The risk of global nuclear war has practically disappeared,” Mikhail Gorbachev, the last leader of the Soviet Union, [said](#) in his 1991 Nobel Prize acceptance speech, even though Russia and the United States retained their massive nuclear arsenals. Three decades later, nine countries are members of the [nuclear club](#). Even so, many were reassured last summer when Russian President Vladimir Putin and US President Joe Biden during a Geneva summit [reiterated](#) the Gorbachev-Regan statement that “a nuclear war cannot be won and must never be fought.” But ever since Russia’s late-February invasion of Ukraine, political leaders, nuclear arms control experts, and world citizens have tried to



answer some version of the question: Will Putin use nuclear weapons in his war in Ukraine? The utterances by individuals of note listed below might have been responses to this question. These statements, arranged chronologically, offer a still-unfolding existential narrative on whether nuclear war may or may not be imminent.

●► [Read the timeline at the source's URL.](#)

Susan D'Agostino is an associate editor at the *Bulletin of the Atomic Scientists*. Susan is the author and illustrator of [How To Free Your Inner Mathematician: Notes on Mathematics and Life](#) (Oxford University Press, 2020). She is a member of the editorial board of the Mathematical Association of America's *Math Horizons* magazine. Susan earned a PhD in mathematics at Dartmouth College and an MA in science writing at Johns Hopkins University. She has received science writing fellowships from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.

A Nuclear South Korea? Why It Might Be the Best Option

By Robert Kelly

Source: <https://www.19fortyfive.com/2022/05/south-korea-nuclear-deterrence/>

May 03 – [Twice in the last week](#), North Korea has threatened a pre-emptive nuclear strike. We also have growing evidence that Pyongyang will soon test a [nuclear weapon](#) for the first time since 2017. North Korean rhetoric is [still belligerent](#), and Pyongyang has clearly indicated that it intends to develop a full-spectrum nuclear program. This is prompting [difficult discussions](#) in South Korea.

[South Korean President-Elect Yoon Seok-yeol](#) has suggested that pre-emptive strikes on North Korean missile sites would be appropriate in a crisis. That would be a huge risk. In 2017, former U.S. [President Donald Trump](#) considered this option, and he rejected it.

South Korean nuclearization is often criticized as being too risky. Yet even [nuclearization](#) would carry less of a risk than airstrikes.



Thinking the unthinkable

The core problem is that North Korea is not going to stop. Its nuclear, missile, and weapons of mass destruction programs have been growing for decades. They will not slow down anytime soon. As the North's weapons programs mature, the threat they pose to U.S. allies grows. Indeed, North Korean missiles can now reach much of the planet, including the United States and Europe. But countries like Japan and South Korea face the greatest danger. Ideally, Pyongyang would bargain with Seoul and Washington, brokering some manner of negotiated deal to cap its developments. North Korea probably has enough warheads now [to achieve basic deterrence with the U.S.](#) and its allies. If it keeps building and testing, Pyongyang will signal that it has bigger goals for its nukes than mere defense. North Korea has spoken of its desire to build tactical or battlefield nuclear weapons, and leader Kim Jong Un's recent comments hint at a more aggressive doctrine. The Ukraine war suggests one obvious task for North Korean WMD: Keep the United States out of any conflict in Korea. Russian President Vladimir Putin has [successfully leveraged](#) his nuclear weapons to keep NATO from intervening more directly in the Ukraine war. Kim is almost certainly watching, learning, and considering whether his own nukes might purchase the same outcome. These developments prompt a discussion of how South Korea and the United States might fight a conflict that could slide toward the use of nuclear weapons. During the Cold War, debates like this were called "thinking the unthinkable" – considering options against a nuclear-armed state that might spark even greater conflict.

Risky airstrikes

Using American and South Korean airpower to denuclearize North Korea by force is an old and much-debated idea. It is attractive because it would not require North Korean assent. Pyongyang has a [long history of gimmicking negotiations](#). There is always skepticism about whether it will stick to any deal it signs. Airstrikes would solve the problem, and U.S. and South Korean airpower commands the skies in Korea. North Korea's air force is obsolete;



its air defenses are better but should be suppressible. The risk, of course, is North Korean retaliation. Indeed, it is unclear that North Korea would recognize a limited strike on its sites as, well, limited. The air campaign would necessarily be extensive, both because of North Korea's ample stock of WMD, and because of the need to first suppress North Korean surface-to-air missile sites. Pyongyang might easily see this as the start of a full-scale war and respond in kind. This is ultimately why the Trump administration gave up on the so-called [bloody nose](#) option in 2017. The air campaign would have to be so large that the North might not interpret it as limited. This could provoke the very war it is intended to prevent.

South Korean direct deterrence

South Korea's [other options](#) are mediocre. Missile defense does not work well enough to absorb all the incoming missiles we anticipate from the North. And while it is important to continue talks with North Korea, there is [little evidence](#) that Pyongyang will accept a serious arms reduction treaty. American extended deterrence has worked for decades, especially as concerns China's nuclear arsenal. But North Korea's threat to nuke the U.S. homeland in a conflict casts doubt on the American guarantee. To participate in a Korean conflict, an American president would have to be willing to risk a nuclear attack on U.S. cities. It is hard to imagine the psychological and strategic pressures on a leader faced with such a decision.

Given all this, I think South Korean direct nuclear deterrence against North Korea is a growing possibility. In other words, South Korea will likely develop its own nuclear weapons. The U.S. opposes this, and South Korean nuclearization would probably end the Non-Proliferation Treaty regime for good. But South Korea is in a tight spot now, especially with Kim openly talking about pre-emption. Direct nuclear deterrence, for all the anxiety it would create, would be a better solution than airstrikes, which would likely ignite a war.

[Dr. Robert E. Kelly](#) is a professor of international relations in the Department of Political Science at Pusan National University. [Dr. Kelly](#) is now a 1945 Contributing Editor as well.

The Future of Nuclear Waste: What's the Plan and Can It Be Safe?

By Lewis Blackburn

Source: <https://www.homelandsecuritynewswire.com/dr20220510-the-future-of-nuclear-waste-what-s-the-plan-and-can-it-be-safe>

May 10 – The UK is planning to significantly expand [its nuclear capability](#), in an effort to decrease its reliance on carbon-based fossil fuels. The government is aiming to construct up to eight new reactors over the next couple of decades, with a view to increasing power capacity from approximately 8 gigawatts (GW) today to 24GW by 2050. This would meet around 25% of the forecast UK energy demand, compared to around [16% in 2020](#). As part of this plan to triple nuclear capacity, also in the works is a £210 million



investment for Rolls-Royce to develop and produce a fleet of [small modular reactors](#) (SMRs). SMRs are cheaper and can be used in locations which can't host traditional, larger reactors, so this will give more options for future nuclear sites.

New reactors will inevitably mean more radioactive waste. Nuclear waste decommissioning, as of 2019, was already estimated to cost UK taxpayers [£3 billion](#) per year. The vast majority of our waste is held in storage facilities at or near ground level, mostly at [Sellafield nuclear waste site](#) in Cumbria, which is so large it has the infrastructure of a small town.



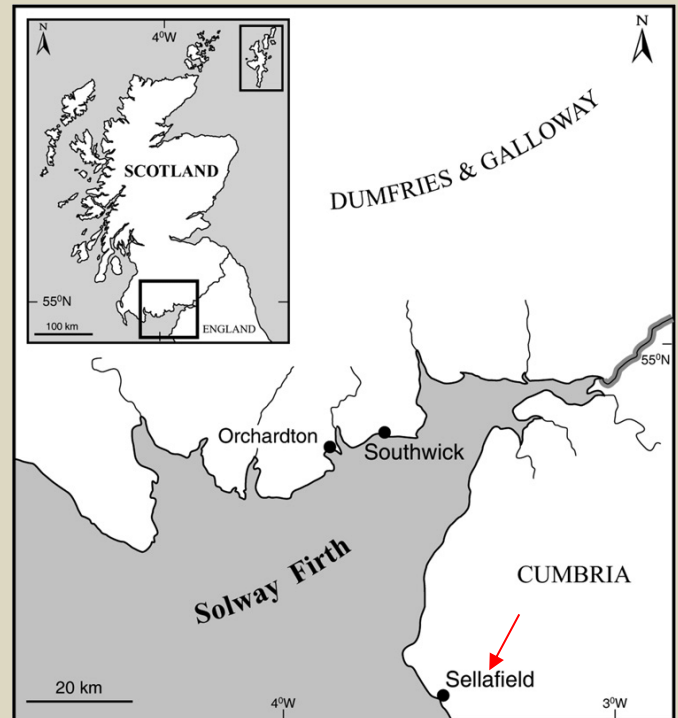
But above-ground nuclear storage isn't a feasible long term plan – governments, academics and scientists are in agreement that permanent disposal below ground is the only long-term strategy that satisfies security and environmental concerns. So what plans are underway, and can they be delivered safely?

The Way Forward

It has taken many decades of international collaboration between academic and scientific institutions and government regulators to identify a feasible route towards the ultimate disposal of nuclear waste. Previous ideas have included disposing of the extra waste [in space](#), in [the sea](#) and below [the ocean floor](#) where tectonic plates converge, but each has been shelved as too risky.

Now, almost every nation plans to isolate radioactive waste from the environment in an underground, highly engineered structure called a [geological disposal facility](#) (GDF). Some models see GDFs constructed at 1,000 meters underground but 700 meters is more realistic. These facilities will receive low, intermediate or high level nuclear wastes (classified as such according to radioactivity and half-life) and store them safely for up to hundreds of thousands of years.

The process for creating such a facility is not simple. The organization responsible for delivering the GDF, which in the UK is [Nuclear Waste Services](#) (NWS), must not only overcome huge environmental and technical issues but also earn the public's support.



Will All GDFs Look the Same?

Although generic design concepts do exist, each GDF will have unique aspects based on the size and constitution of the waste inventory and the geology of where it is installed. Every nation will tailor its GDF to its individual needs, under the scrutiny of regulators and the public.

Underpinning all GDFs, however, will be what is known as the [multi-barrier concept](#). This combines man-made and natural barriers to isolate nuclear waste from the environment, and allow it to steadily decay.

The system for preparing high-level waste for storage in such a system will start with spent nuclear fuel rods from reactors. First, any uranium and plutonium that is still usable for future reactions will be recovered. The residual waste will then be dried and dispersed into a [host glass](#), which is used because glass is tough, durable in groundwater and resistant to radiation. The molten glass will then be poured into a metal container and solidified, so that there are two layers of protection.

This packaged waste will then be surrounded by a backfill of clay or cement, which seals the excavated rock cavities and underground tunnel structures. Hundreds of meters of rock itself will act as the final layer of containment.

How Is the UK Program Going?

The UK GDF program is in its early stages. The siting process operates on a so-called volunteerism approach, in which communities can put themselves forward as potential sites to host the facility. At present, a working group ([Theddlethorpe](#), Lincolnshire) and three community partnerships ([Allerdale](#), [Mid Copeland](#) and [South Copeland](#) in Cumbria) have formed. Whilst working groups are at earlier stages of the siting process, the next steps for community partnerships are to begin more extensive geological surveys, followed by drilling boreholes to assess the underlying rock.

Public support is the basis of the entire GDF program. While some nations may take a more heavy-handed approach and choose a site regardless of public support, the UK GDF mission has community and stakeholder engagement at its core.

Why would residents volunteer? This is a 100+ year project that will require a lot of people working very close by. At the community partnership stage, an investment of up to £2.5million per year, per community, is expected.

The UK program is some way behind certain other nations. The world leader is Finland, which has almost finished the world's first GDF at [Onkalo](#), several hundred kilometers west of Helsinki. [Preferred sites](#) for GDFs have also been selected in the US, Sweden and France.

The UK government aims to identify a suitable site within the next 15-20 years, after which construction can start. The timescale from siting to closing and sealing the first UK GDF is



100 years, making this the largest UK infrastructure project ever. The technology to deliver the GDF is ready; all that remains is to find a willing community with a suitable geology.

Is There Another Way?

It is the scientific consensus, internationally, that the GDF approach is the most technically feasible way to permanently dispose of nuclear waste. Onkalo is an example to the world that scientific collaboration and open engagement with the public can make safe disposal of nuclear waste possible.

The only other approach that has received any traction is the [deep borehole disposal](#) (DBD) concept. At face value, this is not too dissimilar from a GDF approach; drilling boreholes much deeper than a GDF would be (up to several kilometers) and putting waste packages at the bottom. Countries such as Norway are considering this approach.

Lewis Blackburn is EPSRC Doctoral Prize Fellow in Materials Science, University of Sheffield.

A Nuclear Strike Might Not Prompt the Reaction You Expect

By Tyler Cowen | Bloomberg

Source: https://www.washingtonpost.com/business/a-nuclear-strike-might-not-prompt-the-reaction-you-expect/2022/05/10/c4c77d58-d048-11ec-886b-df76183d233f_story.html

May 09 – What if Russia used a tactical nuclear weapon in Ukraine? There has been plenty of speculation as to whether this might happen, or how we should limit the chance that it does. But less has been said about how to react should Vladimir Putin decide to launch a nuclear strike.



I'm not talking about major nuclear war, when those questions might be moot. Instead consider that the Russians deploy a tactical nuke, the Western coalition splinters due to fear of further strikes, and Russia keeps part of Ukraine as Putin claims a daring victory. The battle lines ossify. Putin's likely rhetoric notwithstanding, it would fall somewhere between a Russian win and a Russian loss.

What does that world look like, and how should we prepare for it?

Until recently, my view was that any actual use of a nuclear weapon, no matter the scale, would dramatically change everything. Nuclear use would no longer be considered taboo, and the world would enter a state of collective shock and trauma. Other countries around the world would start frantically preparing for war, or the possibility of war.

But recent events have nudged me away from that viewpoint. For instance, I have seen a pandemic that arguably has caused about 15 million deaths worldwide, yet many countries, including the U.S. haven't made major changes in their pandemic preparation policies. That tells me we are more able to respond to a major catastrophe with collective numbness than I would have thought possible.

I also have seen Trumpian politics operate through the social media cycle. Former President Donald Trump did and said outrageous things on a regular basis (even if you agree with some of them, the relevant point is that his opponents sincerely found them outrageous). Yet the rapidity of the social media news cycle meant that most of those actions failed to stick as major failings. Each outrage would be followed by another that would blot out the memory of the preceding one. The notion of "Trump as villain" became increasingly salient, but the details of Trumpian provocations mattered less and less.

Might the detonation of a tactical nuclear weapon follow a similar pattern? Everyone would opine on it on Twitter for a few weeks before moving on to the next terrible event. "Putin as villain" would become all the more entrenched, but dropping a tactical nuclear weapon probably wouldn't be the last bad thing he would do.

To cite the terminology of venture capitalist Marc Andreessen, the tactical nuclear weapon might stay "the Current Thing" for a relatively short period of time.

Maybe the potency of the nuclear concept, and its instantiation in the actual slaughter of innocents, would create more long-lasting trauma than this, but I am no longer sure.

We don't know how many people such a weapon would exterminate, but it's quite possible that it would kill only a small fraction of the number that have died in the war overall. Russia could either use a small nuke or avoid aiming it at a densely populated area. And it already is the case that Roe v. Wade debates are pushing the Ukraine war out of the forefront of our consciousness, at least in the U.S.

The nuclear strike probably would have foreign policy consequences across the broader world. For instance, more countries might seek to acquire nuclear weapons or other weapons of mass destruction. Those events could become the new outrages, subsuming



Putin's tactical nuke deployment in a broader wave of condemnation. In other words, worries about nuclear war might replace opprobrium directed at Putin's individual act.

The administration of President Joe Biden faces options, including in the realm of communications. One is to let this process operate and allow the world not to freak out so much about the tactical nuclear deployment, which might end up being seen as just another event in a long and bloody war. Many people will feel, perhaps correctly, that the same simply cannot happen to them. Even if you think we ought to instead punish Putin severely, this may not be possible if the NATO coalition has fractured out of fear.

The downside is that we would be normalizing nuclear weapons use while also encouraging Putin to continue in his depredations.

The alternative is to speak repeatedly about Russia's nuclear outrage and to keep the attention of the world focused on it as a special and uniquely evil event. The risk in doing so is that we would elevate Putin's rebellion against Western norms and raise his supposedly heroic profile among those who support him. If you talk about a tyrant but don't punish him, he may end up all the stronger. Furthermore, it isn't obvious whether "trending on Twitter" would support such a Biden strategy in the longer run.

What if they gave a nuclear war and no one came? Or at least no one squawked too loudly? We should start to give this matter some thought.

Nuclear Notebook: How many nuclear weapons does the United States have in 2022?

By Hans M. Kristensen and Matt Korda

Source: <https://thebulletin.org/premium/2022-05/nuclear-notebook-how-many-nuclear-weapons-does-the-united-states-have-in-2022/>

May 10 – At the beginning of 2022, the US Defense Department maintained an estimated stockpile of approximately 3,708 nuclear warheads for delivery by ballistic missiles and aircraft. Most of the warheads in the stockpile are not deployed but rather stored for potential upload onto missiles and aircraft as necessary. We estimate that approximately 1,744 warheads are currently deployed, of which roughly 1,344 strategic warheads are deployed on ballistic missiles and another 300 at strategic bomber bases in the United States. An additional 100 tactical bombs are deployed at air bases in Europe. The remaining warheads — approximately 1,964 — are in storage as a so-called "hedge" against technical or geopolitical surprises. Several hundred of those warheads are scheduled to be retired before 2030. (See Table 1.)

In addition to the warheads in the Defense Department stockpile, approximately 1,720 retired — but still intact — warheads are stored under custody of the Energy Department and are awaiting dismantlement, giving a total US inventory of an estimated 5,428 warheads. Between 2010 and 2018, the US government publicly disclosed the size of the nuclear weapons stockpile; however, in 2019 and 2020, the Trump administration rejected requests from the Federation of American Scientists to declassify the latest stockpile numbers (Aftergood 2019; Kristensen 2019a, 2020d). In 2021, the Biden administration restored the United States' previous transparency levels by declassifying both numbers for the entire history of the US nuclear arsenal until September 2020 — including the missing years of the Trump administration. This effort revealed that the United States' nuclear stockpile consisted of 3,750 warheads in September 2020 — only 72 warheads fewer than the last number made available in September 2017 before the Trump administration reduced the US government's transparency efforts (State Department 2021a). We estimate that the stockpile will continue to decline over the next decade-and-a-half as modernization programs consolidate the remaining warheads.

The US nuclear weapons are thought to be stored at an estimated 24 geographical locations in 11 US States and five European countries (Kristensen and Korda 2019, 124). The location with the most nuclear weapons by far is the large Kirtland Underground Munitions and Maintenance Storage Complex south of Albuquerque, New Mexico. Most of the weapons in this location are retired weapons awaiting dismantlement at the Pantex Plant in Texas. The state with the second-largest inventory is Washington, which is home to the Strategic Weapons Facility Pacific and the ballistic missile submarines at Naval Submarine Base Kitsap. However, if counting only weapons that are part of the stockpile, then Washington would be considered the state containing the most nuclear weapons.

Implementing New START

The United States appears to be in compliance with the New Strategic Arms Reduction Treaty (New START) limits. Its 665 deployed strategic launchers with 1,389 attributed warheads counted as of the most recent data exchange on September 1, 2021 are well below the treaty's limits of 700 deployed strategic launchers with 1,550 warheads (State Department 2021b). This is a decrease of 10 deployed strategic launchers and an increase of 69 deployed strategic warheads over the past 12 months (State Department 2021c). However, these changes do not reflect actual changes in the US arsenal but are caused by normal fluctuations caused by launchers moving in and out of maintenance. The United States has not reduced its total inventory of strategic launchers since 2017 (Kristensen 2020a).



Table 1. United States nuclear forces, 2022.

Type/Designation	No.	Year deployed	Warheads x yield (kilotons)	Warheads (total available) ^a
ICBMs				
LGM-30 G Minuteman III				
Mk-12A	200	1979	1–3 W78 x 335 (MIRV)	600 ^b
Mk-21/SERV	200	2006 ^c	1 W87 x 300	200 ^d
Total	400^e			800^f
SLBMs				
UGM-133A Trident II D5/LE 14/280 ^g				
Mk-4A		2008 ^h	1–8 W76-1 x 90 (MIRV)	1,511 ⁱ
Mk-4A		2019	1–2 W76-2 x 8 (MIRV) ^j	25 ^k
Mk-5		1990	1–8 W88 x 455 (MIRV)	384
Total	14/280			1,920^l
Bombers				
B-52 H Stratofortress	87/46 ^m	1961	ALCM/W80-1 x 5–150	500
B-2A Spirit	20/20	1994	B61-7 x 10–360/-11 x 400 B83-1 x low-1,200	288
Total	107/66ⁿ			788^o
Total strategic forces				
Nonstrategic forces				
F-15E, F-16C/D, DCA	n/a	1979	1–5 B61-3/-4 bombs x 0.3–170 ^p	200
Total				200^q
Total stockpile				
Deployed				1,744 ^r
Reserve (hedge and spares)				1,964
Retired, awaiting dismantlement				
Total Inventory				
				5,428

ALCM: air-launched cruise missile; DCA: dual-capable aircraft; ICBM: intercontinental ballistic missile; LGM: silo-launched ground-attack missile; MIRV: multiple independently targetable re-entry vehicle; SERV: security-enhanced re-entry vehicle; SLBM: submarine-launched ballistic missile.

^aLists total warheads available. Only a portion of these are deployed with launchers. See individual endnotes for details.

^bRoughly 200 of these are deployed on 200 Minuteman IIIs equipped with the Mk-12A re-entry vehicle. The rest are in central storage.

^cThe W87 was initially deployed on the MX/Peacekeeper in 1986 but first transferred to the Minuteman in 2006.

^dThe 200 Mk21-equipped ICBMs can each carry one W87. The estimated remaining 340 W87s are in storage. Excess W87 pits are planned for use in the W78 Replacement Program, previously designated IW-1 but now called W87-1.

^eAnother 50 ICBMs are in storage for potential deployment in 50 empty silos.

^fOf these ICBM warheads, 400 are deployed on operational missiles and the rest are in long-term storage.

^gThe first figure is the total number of nuclear-powered ballistic missile submarines (SSBNs) in the US fleet; the second is the maximum number of missiles that they can carry. However, although the 14 SSBNs can carry up to 280 missiles, 2 vessels are normally undergoing refueling overhaul at any given time and are not assigned missiles. The remaining 12 SSBNs can carry up to 240 missiles, but 1 or 2 of these vessels are usually undergoing maintenance at any given time and may not be carrying missiles. The life-extended Trident II D5LE is replacing the original missile.

^hThe W76-1 is a life-extended version of the W76-0 that was first deployed in 1978.

ⁱAll W76-0 warheads are thought to have now been replaced on ballistic missile submarines by W76-1 warheads, but several hundred are still awaiting dismantlement.

^jThe W76-2 is a single-stage low-yield modification of the W76-1 with an estimated yield of 8 kilotons.

^kAssumes two SLBMs, each with one W76-2, available for each deployable SSBN.

^lOf these SLBM warheads, approximately 944 are deployed on missiles loaded in ballistic missile submarine launchers.

^mOf the 87 B-52s, 76 are in the active inventory. Of those, 46 are nuclear-capable, of which less than 40 are normally deployed.

ⁿThe first figure is the total aircraft inventory, including those used for training, testing, and back-up; the second is the portion of the primary-mission aircraft inventory estimated to be tasked with nuclear missions. The United States has a total of 66 nuclear-capable bombers (46 B-52s and 20 B-2s), but normally only about 50 nuclear bombers are deployed, with the remaining aircraft in overhaul.

^oOf these bomber weapons, only about 300 are deployed at bomber bases. These include an estimated 200 ALCMs at Minot Air Force Base and approximately 100 bombs at Whiteman Air Force Base. The remaining weapons are in long-term storage. B-52H aircraft are no longer tasked with delivering gravity bombs.

^pThe F-15E can carry up to 5 B61s. Some tactical B61s in Europe are available for NATO DCAs (F-16MLU, PA-200). The maximum yield of the B61-3 is 170 kt, while the maximum yield of the B61-4 is 50 kt.

^qAn estimated 100 B61-3 and –4 bombs are deployed in Europe, of which about 60 are earmarked for use by NATO aircraft. The remaining 100 bombs are in central storage in the United States as backup and contingency missions in the Indo-Pacific region.

^rDeployed warheads include approximately 1,344 on ballistic missiles (400 on ICBMs and 944 on SLBMs), 300 weapons at heavy bomber bases, and 100 nonstrategic bombs deployed in Europe.

Table 1: US nuclear forces, 2022



The warhead numbers reported by the State Department differ from the estimates presented in this Nuclear Notebook, though there are reasons for this. The New START counting rules artificially attribute one warhead to each deployed bomber, even though US bombers do not carry nuclear weapons under normal circumstances. Also, this Nuclear Notebook counts weapons stored at bomber bases that can quickly be loaded onto the aircraft, as well as nonstrategic nuclear weapons in Europe.

Since the treaty entered into force in February 2011, the biannual aggregate data show the United States has cut a total of 324 strategic launchers, 217 deployed launchers, and 411 deployed strategic warheads from its inventory (State Department 2011). The warhead reduction represents approximately 11 percent of the 3,708 warheads remaining in the US stockpile, and approximately 8 percent of the total US arsenal of 5,428 stockpiled and retired warheads awaiting dismantlement. The 2018 Nuclear Posture Review (NPR) States that the United States “will continue to implement the New START Treaty” while it remains in effect (US Defense Department 2018, 73). In 2021, the United States and Russia extended the treaty by mutual agreement, until February 2026.

The United States is currently 35 launchers and 161 warheads below the treaty limit for deployed strategic weapons but has 138 deployed launchers more than Russia — a significant gap that is almost equivalent to the size of an entire US Air Force intercontinental ballistic missile (ICBM) wing. It is notable that Russia has not sought to reduce this gap by deploying more strategic launchers. Instead, the Russian launcher deficit has increased by one-third since its lowest point in February 2018.

If either the US or Russia withdrew from New START, both the United States and Russia could upload several hundreds of extra warheads onto their launchers. This means that the treaty has proven useful thus far in keeping a lid on both countries’ deployed strategic forces. Additionally, if New START expired, then both countries would lose a critical node of transparency into each other’s nuclear forces. As of March 3, 2022, the United States and Russia have completed a combined 328 on-site inspections and exchanged 23,369 notifications (State Department 2022). (On-site inspections have been paused since early-2020 due to COVID-19.)

The NPR and nuclear modernization

The Biden administration’s NPR was expected to be completed in late-January 2022 but has been delayed following the Russian invasion of Ukraine. The conclusions are not known but are expected to broadly follow the Trump administration’s 2018 NPR, which in turn followed the broad outlines of the Obama administration’s 2010 NPR to modernize the entire nuclear weapons arsenal — although with several important changes.

The most significant change was a recommendation to increase the types and role of US nuclear weapons. The Trump NPR took a confrontational tone, presenting an assertive posture that embraces “great power competition.” It also included plans to develop new nuclear weapons and modify others. The report backed away from the goal of seeking to limit the role of nuclear weapons to the sole purpose of deterring nuclear attacks. Instead, it emphasizes “expanding” US nuclear options to deter, and, if deterrence fails, to prevail against both nuclear and “non-nuclear strategic attacks.” To be clear, any use of a nuclear weapon to respond to a non-nuclear strategic attack would constitute nuclear first use.

The NPR explained that “non-nuclear strategic attacks include, but are not limited to, attacks on the US, allied, or partner civilian population or infrastructure, and attacks on US or allied nuclear forces, their command and control, or warning and attack assessment capabilities” (US Defense Department 2018, 21). Consequently, US nuclear capabilities will be postured to “hedge against the potential rapid growth or emergence of nuclear and non-nuclear strategic threats, including chemical, biological, cyber, and large-scale conventional aggression” (US Defense Department 2018, 38). To achieve these goals, the NPR stated that “the United States will enhance the flexibility and range of its tailored deterrence options. ... Expanding flexible US nuclear options now, to include low-yield options, is important for the preservation of credible deterrence against regional aggression,” the report claimed (US Defense Department 2018, 34).

The new tailored capabilities included modifying “a small number” of the existing W76-1 90-kiloton two-stage thermonuclear warheads to single-stage warheads by “turning off” the secondary (a technical term representing a part of the warhead) to limit the yield to what the primary (another technical term) can produce (an estimated 8 kilotons). This new warhead (W76-2), the NPR claimed, is necessary to “help counter any mistaken perception of an exploitable ‘gap’ in US regional deterrence capabilities.” The W76-2 was first deployed in the Atlantic Ocean in late 2019 onboard a nuclear-powered ballistic missile submarine (SSBN), the *USS Tennessee* (SSBN-734) (Arkin and Kristensen 2020). Undersecretary of Defense for Policy John Rood told reporters in December 2019 that the low-yield Trident warhead was “very stabilizing” and in no way supported the concept of early use of low-yield nuclear weapons (Kreisher 2019), even though the NPR explicitly stated the weapon is being acquired to provide “a prompt response option” (US Defense Department 2018).

In the longer term, the NPR declared, the United States will also “pursue a nuclear-armed” submarine-launched cruise missile (SLCM-N) to “provide a needed nonstrategic regional presence, an assured response capability, and an Intermediate-Range Nuclear Forces (INF) Treaty-compliant response to Russia’s continuing Treaty violation.” The NPR specifically noted that, “If Russia returns to compliance with its arms control obligations, reduces its



nonstrategic nuclear arsenal, and corrects its other destabilizing behaviors, the United States may reconsider the pursuit of a [submarine-launched cruise missile].” In pursuit of this new missile, the review stated that “we will immediately begin efforts to restore this capability by initiating a requirements study leading to an analysis of alternatives ... for the rapid development of a modern [submarine-launched cruise missile].” The report’s authors believed that “US pursuit of a submarine-launched cruise missile may provide the necessary incentive for Russia to negotiate seriously a reduction of its nonstrategic nuclear weapons, just as the prior Western deployment of Intermediate-Range Nuclear Forces in Europe led to the 1987 INF Treaty” (US Defense Department 2018, 55).

The new nuclear “supplements” proposed by the 2018 NPR are needed, the authors said, to “provide a more diverse set of characteristics greatly enhancing our ability to tailor deterrence and assurance; expand the range of credible US options for responding to nuclear or non-nuclear strategic attack; and, enhance deterrence by signaling to potential adversaries that their concepts of coercive, limited nuclear escalation offer no exploitable advantage” (US Defense Department 2018, 55).

However, the US arsenal already includes nearly 1,000 gravity bombs and air-launched cruise missiles with low-yield warhead options (Kristensen 2017a). The NPR provided no evidence that existing capabilities are insufficient or documented that the yield of US nuclear weapons is a factor in whether Russia would decide to use nuclear weapons. The NPR authors simply claimed that the new capabilities are needed. The US Navy used to have a nuclear submarine-launched cruise missile (the TLAM/N) but retired it in 2011 because it was redundant and no longer needed. All other nonstrategic nuclear weapons — with the exception of gravity bombs for fighter-bombers — have also been retired because there was no longer any military need for them, despite Russia’s larger nonstrategic nuclear weapons arsenal.

The suggestion that a US submarine-launched cruise missile could motivate Russia to return to compliance with the INF Treaty is flawed because Russia embarked upon its current violation of the treaty at a time when the TLAM/N was still in the US arsenal, and because the Trump administration since withdrew the United States from the INF Treaty. Moreover, US Strategic Command has already strengthened strategic bombers’ support of NATO in response to Russia’s more provocative and aggressive behavior (see above); 46 B-52 bombers are currently equipped with the air-launched cruise missile and both the B-52 and the new B-21 bomber will receive the new long-range standoff weapon, which will have essentially the same capabilities as the submarine-launched cruise missile proposed by the 2018 NPR.

Russia’s decisions about the size and composition of its nonstrategic arsenal instead appear to be driven by the US military’s superiority in conventional forces, not by the US nonstrategic nuclear arsenal or by the yield of a particular weapon. Instead, the pursuit of a new nuclear submarine-launched cruise missile to “provide a needed nonstrategic regional presence” in Europe and Asia could reinforce Russia’s reliance on nonstrategic nuclear weapons. It could also potentially even trigger Chinese interest in such a capability as well — especially when combined with the parallel expansion of US long-range conventional strike capabilities including development of new conventional INF-range missiles. Moreover, development of a nuclear sea-launched cruise missile would violate the pledge the United States made in the 1992 Presidential Nuclear Initiative not to develop new types of nuclear submarine-launched cruise missiles (Koch 2012, 40).

One final argument against the submarine-launched cruise missile is that nuclear-capable vessels triggered frequent and serious political disputes during the Cold War when they visited foreign ports in countries that did not allow nuclear weapons on their territory. In the case of New Zealand, diplomatic relations have only recently — 30 years later — recovered from those disputes. Reconstitution of a nuclear submarine-launched cruise missile would reintroduce this foreign relations irritant and needlessly complicate relations with key allied countries in Europe and Northeast Asia.

It is possible that the Biden administration’s NPR will cancel the SLCM-N, but the document had not been published when this article went to print.

The Trump administration significantly increased the nuclear weapons budget. According to an estimate published in May 2021 by the US Congressional Budget Office, modernizing and operating the US nuclear arsenal and the facilities that support it will cost around \$634 billion for the period 2021–2030 (Congressional Budget Office 2021, 1). This is \$140 billion more than the Congressional Budget Office’s 2019 estimate for the 2019–2028 period because modernization programs continue to ramp up, cost estimates are increasing, and the 2018 NPR called for new nuclear weapons (Congressional Budget Office 2019, 1). The nuclear modernization (and maintenance) program will continue well beyond 2039 and, based on the Congressional Budget Office’s estimate, will cost \$1.2 trillion over the next three decades. Notably, although the estimate accounts for inflation (Congressional Budget Office 2017), other estimates forecast that the total cost will be closer to \$1.7 trillion (Arms Control Association 2017). Whatever the actual price tag will be, it is likely to increase over time, resulting in increased competition with conventional modernization programs planned for the same period. The NPR belittles concerns about affordability issues in the nuclear modernization program and instead labels it “an affordable priority,” pointing out that the total cost is only a small portion of the overall defense budget (US Defense Department 2018, XI). There is little doubt, however, that limited resources, competing nuclear and



conventional modernization programs, tax cuts, and the rapidly growing US budget deficit will present significant challenges for the nuclear modernization program.

In addition to the two new “supplement” weapons described above, the National Nuclear Security Administration (NNSA) and the Defense Department have proposed developing several other new nuclear warheads, including the W93 navy warhead. The NNSA’s Stockpile Stewardship and Management Plan from December 2020 doubled the number of new nuclear warhead projects for the next 20 years (NNSA 2020b).

Nuclear planning, nuclear exercises

The changes in the Trump administration’s NPR triggered new guidance from the White House and Defense Department that replaced the Obama administration’s guidance from 2013 (Kristensen 2013a). The first of these was a new Nuclear Employment Guidance document signed by President Trump in April 2019, that in turn was implemented by the Nuclear Weapons Employment Planning and Posture Guidance signed by the Defense Secretary (US Defense Department 2020, 1). The changes in these documents were sufficient to trigger a change of the strategic war plan known as OPLAN 2012–12, the nuclear employment portion of what was previously known as the Single Integrated Operations Plan. The updated OPLAN 8010–12 entered into effect on April 30, 2019 (US Strategic Command 2019).

OPLAN 8010–12 consists of “a family of plans” directed against four adversaries: Russia, China, North Korea, and Iran. Known as “Strategic Deterrence and Force Employment,” OPLAN 8010–12 first entered into effect in July 2012 in response to Operations Order Global Citadel signed by the defense secretary. The plan is flexible enough to absorb normal changes to the posture as they emerge, including those flowing from the NPR. Several updates have been made since 2012, but more substantial updates will trigger publication of what is known as a “change.” The April 2019 change refocused the plan toward “great power competition,” incorporated a new cyber plan, and reportedly blurred the line between nuclear and conventional attacks by “fully incorporat[ing] non-nuclear weapons as an equal player” (Arkin and Ambinder 2022a, 2022b).

OPLAN 8010–12 also “emphasizes escalation control designed to end hostilities and resolve the conflict at the lowest practicable level” by developing “readily executable and adaptively planned response options to de-escalate, defend against, or defeat hostile adversary actions” (US Strategic Command 2012). These passages are notable, not least of which because the Trump administration’s NPR criticized Russia for an alleged willingness to use nuclear weapons in a similar manner, as part of a so-called escalate-to-deescalate strategy.

The 2020 Nuclear Employment Strategy, which reads more like an article than a strategy document, reiterates this objective: “If deterrence fails, the United States will strive to end any conflict at the lowest level of damage possible and on the best achievable terms for the United States, and its allies, and partners. One of the means of achieving this is to respond in a manner intended to restore deterrence. To this end, elements of US nuclear forces are intended to provide limited, flexible, and graduated response options. Such options demonstrate the resolve, and the restraint, necessary for changing an adversary’s decision calculus regarding further escalation” (US Defense Department 2020, 2). This objective is not just directed at nuclear attacks, as the 2018 NPR called for “expanding” US nuclear options against “non-nuclear strategic attacks.”

OPLAN 8010–12 is a whole-of-government plan that includes the full spectrum of national power to affect potential adversaries. This integration of nuclear and conventional kinetic and non-kinetic strategic capabilities into one overall plan is a significant change from the strategic war plan of the Cold War that was almost entirely nuclear. Former US Strategic Command commander Gen. John Hyten, now the Chairman of the Joint Chiefs of Staff, in 2017 explained the scope of modern strategic planning:

“I’ll just say that the plans that we have right now, one of the things that surprised me most when I took command on November 3 was the flexible options that are in all the plans today. So we actually have very flexible options in our plans. So if something bad happens in the world and there’s a response and I’m on the phone with the secretary of defense and the president and the entire staff, which is the attorney general, secretary of state, and everybody, I actually have a series of very flexible options from conventional all the way up to large-scale nuke that I can advise the president on to give him options on what he would want to do. “So I’m very comfortable today with the flexibility of our response options. Whether the president of the United States and his team believes that that gives him enough flexibility is his call. So we’ll look at that in the Nuclear Posture Review. But I’ve said publicly in the past that our plans now are very flexible.

“And the reason I was surprised when I got to [Strategic Command] about the flexibility, is because the last time I executed or was involved in the execution of the nuclear plan was about 20 years ago, and there was no flexibility in the plan. It was big, it was huge, it was massively destructive, and that’s all there. We now have conventional responses all the way up to the nuclear responses, and I think that’s a very healthy thing (Hyten 2017).”

To practice and fine-tune these plans, the armed forces conducted several nuclear-related exercises in 2021 and early 2022. These included Strategic Command’s Global Lightning exercises in March 2021 and January 2022, which is a command-and-control and battlestaff exercise designed to assess joint operational readiness across all of Strategic Command’s



mission areas. To that end, a Global Lightning exercise typically links to several other exercises. In 2021, Global Lightning was integrated with US European Command and US Space Command, and involved the deployment of B-52 bombers from Barksdale and Minot Air Force Bases (US Strategic Command 2021a; Kristensen 2021a). In 2022, Global Lightning was integrated with US Indo-Pacific Command (US Strategic Command 2022a).

In August 2021, Air Force Global Strike Command conducted Exercise Prairie Vigilance, a nuclear bomber exercise at Minot Air Force Base in North Dakota. This was the fourth iteration of this kind of exercise in 2021, which practiced nuclear cruise missile loading and rapid takeoff of B-52 bombers (Spencer 2021; see Figure 1 at top of page).

Prairie Vigilance was the lead-up to Strategic Command's annual week-long Global Thunder exercise in November 2021. The exercise "provides training opportunities that exercise all US Strategic Command mission areas, with a specific focus on nuclear readiness" (US Strategic Command 2021b).

These developments coincide with steadily increasing US bomber operations in Europe since Russia's invasion of Ukraine in 2014. Before that, one or two bombers would deploy for an exercise or airshow. But since then, the number of deployments and bombers has increased, and the mission changed. Very quickly after the Russian annexation of Crimea, Strategic Command increased the role of nuclear bombers in support of European Command (Breedlove 2015), which in 2016 put into effect a new standing war plan for the first time since the Cold War (Scapparotti 2017). Before 2018, the bomber mission was called the Bomber Assurance and Deterrence missions to show the flag, but now the bombers deploy as a Bomber Task Force that brings the full offensive capability to the forward base. Whereas the mission of Bomber Assurance and Deterrence was to train with allies and have a visible presence to deter Russia, the mission of the Bomber Task Force is to move a fully combat-ready bomber force into the European theater. "It's no longer just to go partner with our NATO allies or to go over and have a visible presence of American air power," according to the commander of the 2nd Bomb Wing. "That's part of it, but we are also there to drop weapons if called to do so" (Wrightsman 2019). These changes are important indications of how US strategy has changed in response to deteriorating East-West relations and the new "great power competition" strategy promoted by the Trump administration. They also illustrate a growing integration of nuclear and conventional capabilities, as reflected in the new strategic war plan. The deployment of four B-52s to Royal Air Force Fairford in March 2019, for example, included two nuclear-capable aircraft and two that have been converted to conventional-only missions. NATO's official announcement of the exercise did not notice this feature but said the deployment "shows that the US nuclear umbrella protects Europe" (NATO 2019). The statement also said that the B-52 bombers "can carry both conventional and nuclear weapons" when, in fact, nearly half of them – 41 of 87 – cannot because they have been denuclearized under the New START treaty. The close integration of nuclear and conventional bombers into the same task force can have significant implications for crisis stability, misunderstandings, and the risk of nuclear escalation.

Additionally, as of 2019 US bombers are increasingly practicing an "agile combat employment" strategy, by which all bombers "hopscotch" to a larger number of widely dispersed smaller airfields — including airfields in Canada — in the event of a crisis. This exercise is intended to increase the number of aimpoints for a potential adversary seeking to destroy the US bomber force, thus increasing the force's survivability and raising the ante for an adversary to attempt such a strike (Arkin and Ambinder 2022a). Over the past year, the Strategic Air Command executed 127 Bomber Task Force missions (US Strategic Command 2022b, 14).

Land-based ballistic missiles

The US Air Force operates a force of 400 silo-based Minuteman III ICBMs split across three wings: the 90th Missile Wing at F. E. Warren Air Force Base in Colorado, Nebraska, and Wyoming; the 91st Missile Wing at Minot Air Force Base in North Dakota; and the 341st Missile Wing at Malmstrom Air Force Base in Montana. In addition to the 400 silos with missiles, another 50 silos are kept "warm" to load stored missiles if necessary. Each wing has three squadrons, each with 50 Minuteman III silos. They are collectively controlled by five launch control centers.

The 400 ICBMs as deployed carry one warhead each, either a 300-kiloton W87/Mk21 or a 335-kiloton W78/Mk12A. ICBMs equipped with the W78/Mk12A, however, could theoretically be uploaded to carry two or three independently targetable warheads each, for a total of 800 warheads available for the ICBM force. The US Air Force occasionally test-launches Minuteman III missiles with multiple unarmed re-entry vehicles to maintain and announce the capability to re-MIRV the Minuteman IIIs. On August 4, 2020, for example, a test-launch of a Minuteman III ICBM was equipped with three re-entry vehicles (US Strategic Command 2020). The test came only five days after the Trump administration's arms control envoy tweeted a photo of himself observing a snap exercise at Minot Air Force Base involving a Minuteman equipped with three re-entry vehicles (Billingslea 2020).

The Minuteman IIIs completed a multibillion-dollar, decade-long modernization program in 2015 to extend the service life of the missile to 2030. Although the United States did not officially deploy a new ICBM, the upgraded Minuteman IIIs "are basically new missiles except for the shell," according to Air Force personnel (Pampe 2012).

An ongoing Air Force modernization program involves upgrades to the Mk21 re-entry vehicles' arming, fuzing, and firing component — which validates the President's launch



authorization and unlocks the firing system so that the bomb can detonate — at a cost of slightly over a billion dollars in total. The publicly stated purpose of this refurbishment is to extend the vehicles' service life, but the effort appears to also involve adding a "burst height compensation" to enhance the targeting effectiveness of the warheads (Postol 2014). Priority is on replacement of the Mk21 fuze. A total of 693 fuze replacements were initially planned; however, the new fuzes will also reportedly be deployed on the Minuteman replacement missile, which means that the fuze modernization program is likely to expand significantly to accommodate those new missiles (Woolf 2020, 15–16). The effort complements a similar fuze upgrade underway to the Navy's W76-1/Mk4A warhead. The enhanced targeting capability might also allow for lowering the yield on future warhead designs.

It is possible to do a second life-extension of the Minuteman III. In March 2019, the Air Force's Deputy Chief of Staff for Strategic Deterrence and Nuclear Integration noted in his testimony to the House Subcommittee on Strategic Forces that there was one more opportunity to life-extend the missiles before the Minuteman III would have to be replaced (Clark 2019). However, the Air Force has decided against life-extension, instead opting to purchase a whole new generation of ICBMs.

In August 2017, the Air Force awarded \$678 million worth of contracts to Boeing and Northrop Grumman to develop trade studies for the next-generation ICBM that is currently known as the Ground-Based Strategic Deterrent (Erwin 2018). In October 2019, the Program Manager for Ground-Based Strategic Deterrent noted that the official name for the missile would be selected within 12 months; however, over two years later an official name has still not yet been announced (Bartolomei 2019). On July 16, 2019, the Air Force issued a formal "request for proposals" for the engineering and manufacturing development phase of the Ground-Based Strategic Deterrent program, which includes five production lot options to produce and deploy the system (Bryant 2019).

As the two companies under contract for the Ground-Based Strategic Deterrent's technology maturation and risk reduction phase, Boeing and Northrop Grumman were both expected to bid for the engineering and manufacturing development contract. However, only a week after the request for proposals was issued, Boeing surprisingly walked away from the competition, stating that "the current acquisition approach does not provide a level playing field for fair competition" (Weisgerber 2019). The dispute centers on Northrop Grumman's 2018 acquisition of Orbital ATK, which is one of only two US-based companies that produces solid rocket motors and launch vehicles. Under the terms of the acquisition, Northrop Grumman is required to "make its solid rocket motors and related services available on a non-discriminatory basis to all competitors for missile contracts" (Federal Trade Commission 2018). However, Boeing has expressed concern that Northrop Grumman would not comply with that order. This put Northrop Grumman at a favorable position in the bidding process over Boeing, which does not produce those systems in-house. Boeing stated an intention to not submit a bid for the engineering and manufacturing development contract. Nonetheless, it conducted a substantial lobbying campaign throughout the summer of 2019 in an effort to convince Congress and the Air Force to force Northrop Grumman into submitting a joint "best-of-industry" bid with Boeing (Mehta 2019). However, Northrop Grumman declined Boeing's offer and the Air Force did not intervene to force a joint bid. The Air Force subsequently terminated the remainder of Boeing's technological maturation and risk reduction contract in October 2019 by refusing to allocate any further funding to the contract. This effectively ended Boeing's involvement with the Ground-Based Strategic Deterrent program (Insinna 2019).

The request for proposal deadline for the engineering and manufacturing development contract was December 13, 2019. By that date, the Air Force received only a single bid for the contract, and on September 8, 2020, the Air Force officially awarded the \$13.3 billion engineering and manufacturing development contract to Northrop Grumman. The nationwide team will include Aerojet Rocketdyne, General Dynamics, Collins Aerospace, Lockheed Martin, Textron Systems, HDT Global, Bechtel, Kratos Defense and Security Solutions, Clark Construction, L3Harris, and Honeywell (Northrop Grumman 2020). Aerojet Rocketdyne will produce the system's solid-fuel rocket motors in conjunction with newly acquired Orbital ATK, which is now called Northrop Grumman Innovation Systems.

According to the Air Force's latest milestone requirements, the Air Force must deploy 20 new Ground-Based Strategic Deterrent missiles with legacy re-entry vehicles and warheads in order to achieve initial operating capability, scheduled in fiscal year 2029 (Sirota 2020). The plan is to buy 659 missiles — 400 of which would be deployed, while the remainder will be used for test launches and as spares — at a price between \$93.1 billion and \$95.8 billion, increased from a preliminary \$85 billion Pentagon estimate in 2016 (Capaccio 2020). These amounts do not include the costs for the new Ground-Based Strategic Deterrent warhead — the W87-1 — which is projected to cost up to \$14.8 billion (Government Accountability Office 2020). The Air Force says the Ground-Based Strategic Deterrent will meet existing user requirements but have the adaptability and flexibility to be upgraded through 2075 (US Air Force 2016). The new missile is expected to have a greater range than the Minuteman III. Still, it is unlikely that it will have enough range to target countries like China, North Korea, and Iran without overflying Russia. In June 2021, program officials announced that the first Ground-Based Strategic Deterrent prototype would conduct its first flight by the end of 2023 (Bartolomei 2021).

The Ground-Based Strategic Deterrent will be capable of carrying single or multiple warheads. The Air Force initially planned to equip the Ground-Based Strategic Deterrent with life-extended versions of the existing W78 and W87 warheads. The modified W78 was known as Interoperable Warhead 1. But in 2018, the Air Force and NNSA canceled the W78 upgrade and instead proposed a W78 Replacement Program known as the W87-1. The new



warhead will use a W87-like plutonium pit, “using a well-tested IHE [Insensitive High Explosive] primary design” (Energy Department 2018b). The new warhead will be incorporated into a modified version of the Mk21 re-entry vehicle and be designated as the W87-1/Mk4A.

In order to produce the W87-1 in time to meet the Ground-Based Strategic Deterrent’s planned deployment schedule, the NNSA has set an extremely ambitious production schedule that relies upon its ability to produce at least 80 plutonium pits per year by 2030. However, due to the agency’s consistent inability to meet project deadlines and its lack of a latent large-scale plutonium production capability, the 80-pit requirement was always unlikely to be achieved (Government Accountability Office 2020; Institute for Defense Analyses 2019). In June 2021, the Acting Administrator of the NNSA announced to Congress what external analysts had long predicted — that the security administration’s goal of producing up to 80 pits by 2030 would not be possible (Demarest 2021). This was further confirmed by the NNSA in early 2022 (Demarest 2022). This could mean that despite completing its March 2021 requirements review for the W87-1 — a key milestone that allows the program to progress into the next stage of its development — it is likely that the program will face delays and that new delivery systems will be initially deployed with legacy warheads (Sirota 2021; Department of the Air Force 2020).

In October 2019, Lockheed Martin was awarded a \$138 million contract to integrate the Mk21 re-entry vehicle into the Ground-Based Strategic Deterrent, beating out rivals Boeing, Raytheon, Northrop Grumman, and Orbital ATK (which Northrop Grumman now owns and has been renamed to Northrop Grumman Innovation Systems) (Lockheed Martin 2019). Because the W87-1/Mk21A will be bulkier than the current W78/Mk12A, the Ground-Based Strategic Deterrent payload section would have to be wider to accommodate multiple warheads. Also, Northrop Grumman’s Ground-Based Strategic Deterrent illustration shows a missile that is different than the existing Minuteman III, with a wider upper body and payload section (Kristensen 2019b).



Figure 2: A new underground nuclear weapons storage facility is under construction at F.E. Warren AFB for storage of W78 and W87 warheads for Minuteman III ICBMs. Image: © 2022 Maxar Technologies.

The Air Force faces a tight construction schedule for the deployment of the Ground-Based Strategic Deterrent. Each launch facility is expected to take seven months to upgrade, while each missile alert facility will take approximately 12 months. The Air Force intends to upgrade all 150 launch facilities and eight of 15 missile alert facilities for each of the three ICBM bases; the remaining seven missile alert facilities at each base will be dismantled (US Air Force 2020a). Since each missile alert facility is currently responsible for a group of 10 launch facilities, this reduction could indicate that each missile alert facility could be responsible for up to 18 or 19 launch facilities once the Ground-Based Strategic Deterrent becomes operational. This could have implications for the future vulnerability of the Ground-Based Strategic Deterrent’s command-and-control system (Korda 2020). Once these upgrades begin, potentially as early as 2023, the Air Force must finish converting one launch facility per week for nine years in order to complete deployment by 2036 (Mehta 2020). It is expected that construction and deployment will begin at F. E.



Warren between 2023 and 2031, followed by Malmstrom between 2025 and 2033, and finally Minot between 2027 and 2036. As the Ground-Based Strategic Deterrent gets deployed, the Minuteman IIIs will be removed from their silos and temporarily stored at their respective host bases — either F. E. Warren, Malmstrom, or Minot — before being transported to Hill Air Force Base, the Utah Test and Training Range, or Camp Navajo. The rocket motors will eventually be destroyed at the Utah Test and Training Range, while non-motor components will ultimately be decommissioned at Hill Air Force Base. To that end, five new storage igloos and 11 new storage igloos will be constructed at Hill Air Force Base and Utah Test and Training Range, respectively (US Air Force 2020a). New training, storage, and maintenance facilities will also be constructed at the three ICBM bases, which will also receive upgrades to their Weapons Storage Areas. The first base to receive this upgrade is F. E. Warren, where a groundbreaking ceremony for the new Weapons Storage and Maintenance Facility (also called the Weapons Generation Facility) was held in May 2019. Substantial construction began in spring 2020 and is scheduled to be completed in September 2022 (Kristensen 2020b; US Air Force 2019d). Commercial satellite imagery indicates that construction has made considerable progress as of March 2022 (see Figure 2). In May 2021, the US Congressional Budget Office estimated that the cost of acquiring and maintaining the Ground-Based Strategic Deterrent would total approximately \$82 billion over the 10-year period between 202 and 2030 — approximately \$20 billion more than the Congressional Budget Office had previously estimated for the 2019–2028 period (Congressional Budget Office 2021, 2019). The Air Force conducts several Minuteman III flight-tests each year. The first test of 2021 took place on February 23rd, when a team of airmen derived from all three ICBM bases launched a Minuteman III from Vandenberg Air Force Base to the Reagan Test Site on Kwajalein Atoll in the Western Pacific (Defense Visual Information Distribution Service 2021). The second planned test launch of 2021 was aborted immediately prior to launch on May 5th — an extremely rare incident. In a statement, the Air Force Global Strike Command spokesperson noted that “During terminal countdown, the missile computer detected a fault in the sequence of checks it does prior to launching. Upon detection of this fault, it shut itself down” (Cohen 2021). The final test of 2021 took place on August 11, which “involved a Hi Fidelity Joint Test Assembly re-entry vehicle that detonated conventional (i.e. non-nuclear) explosives prior to hitting the surface of the water” (US Air Force 2021a). The first planned Minuteman III test of 2022 was postponed on March 2nd due to the Russian invasion of Ukraine and associated heightened nuclear tensions. A Pentagon spokesperson stated that this postponement was intended “to demonstrate that we have no intention of engaging in any actions that can be misunderstood or misconstrued” (Garamone 2022).

Nuclear-powered ballistic submarines

The US Navy operates a fleet of 14 Ohio-class ballistic missile submarines, of which eight operate in the Pacific from their base near Bangor, Washington, and six operate in the Atlantic from their base at Kings Bay, Georgia. Normally, 12 of the 14 submarines are considered operational, with the remaining two boats in a refueling overhaul at any given time. But because operational submarines undergo minor repairs at times, the actual number at sea at any given time is closer to eight or 10. Four or five of those are thought to be on “hard alert” in their designated patrol areas, while another four or five boats could be brought to alert status in hours or days. Each submarine can carry up to 20 Trident II D5 submarine-launched ballistic missiles (SLBMs), a number reduced from 24 to meet the limits of New START. Since 2017, the Navy has been replacing the original Trident II D5 with a life-extended and upgraded version known as Trident II D5LE (LE stands for “life-extended”). The D5LE, which has a range of more than 12,000 km (7,456 miles), is equipped with the new Mk6 guidance system designed to “provide flexibility to support new missions” and make the missile “more accurate,” according to the Navy and Draper Laboratory (Naval Surface Warfare Center 2008; Draper Laboratory 2006). The D5LE upgrade will continue until all boats have been upgraded and will also replace existing Trident SLBMs on British ballistic missile submarines. The D5LE will also arm the new US Columbia-class and British Dreadnought-class ballistic missile submarines when they enter service.

Instead of building a new ballistic missile, like the Air Force wants to do with the Ground-Based Strategic Deterrent, the Navy plans to do a second life-extension of the Trident II D5 to ensure it can operate through 2084 (Eckstein 2019). In 2021, the Director of the Navy’s Strategic Systems Program testified to Congress that the D5LE2, as the second life-extended missile is known, is scheduled to enter service on the ninth Columbia-class SSBN, following which it will be back-fitted to the remaining eight boats (Wolfe 2021a). The Navy also announced in 2021 that it would acquire an additional 108 Trident missiles to be used for deployment and testing (Wolfe 2021b).

Each Trident SLBM can carry up to eight nuclear warheads, but they normally carry an average of four or five warheads, for an average load-out of approximately 90 warheads per submarine. The payload of the different missiles on a submarine are thought to vary significantly to provide maximum targeting flexibility, but all deployed submarines are thought to carry the same combination. Normally, around 950 warheads are deployed on the operational ballistic missile submarines, although the number can be lower due to maintenance of individual submarines. The New START data from September 2021, however, indicated there were 944 warheads deployed on 221 SLBM launchers (State Department 2021b). Overall, SSBN-



based warheads account for approximately 70 percent of all warheads attributed to the United States' deployed strategic launchers under New START.

Three warhead types are deployed on SLBMs: the 90-kiloton enhanced W76-1, the 8-kiloton W76-2, and the 455-kiloton W88. The W76-1 is a refurbished version of the W76-0, which is being retired, apparently with slightly lower yield but with enhanced safety features added. The NNSA completed production of the W76-1 in January 2019, a massive decade-long production of an estimated 1,600 warheads (Energy Department 2019a). The Mk4A re-entry body that carries the W76-1 is equipped with a new arming, fuzing, and firing unit with better targeting efficiency than the old Mk4/W76 system (Kristensen, McKinzie, and Postol 2017).

The other SLBM warhead, the higher-yield W88, is currently undergoing a life-extension program that addresses nuclear safety concerns and will ultimately support future life-extension options. The first production unit for the W88 Alt 370 was completed on July 1, 2021 (NNSA 2021a).

In the final weeks of 2019, the Navy deployed a low-yield version of the W76-1 known as W76-2 on the *USS Tennessee* (SSBN-734). The W76-2 only uses the warhead fission primary to produce a yield of about 8 kilotons. The First Production Unit of the W76-2 was completed at the Pantex Plant on February 22, 2019 and reached initial operational capability some time before the end of the fiscal year on September 30, 2019 (NNSA 2019). It is unknown exactly how many W76-2 warheads were produced; however, the NPR says it's a "small number" (US Defense Department 2018, 54). We estimate that no more than 25 were ultimately produced, and that one or two of the 20 missiles on each SSBN is armed with one or two W76-2 warheads, while the remainder of the SLBMs will be filled with either the 90-kiloton W76-1 or the 455-kiloton W88 (Arkin and Kristensen 2020).

The United States is also planning to build a new SLBM warhead – the W93 – which will be housed in the Navy's proposed Mk7 aeroshell (re-entry body). The W93 appears intended to initially supplement, rather than replace, the W76-1 and W88. A second new warhead is planned to replace those warheads.

The US sea-based nuclear weapons program also provides substantial support to the British nuclear deterrent. The missiles carried on the Royal Navy ballistic missile submarines are from the same pool of missiles carried on US ballistic missile submarines. The warhead uses the Mk4A re-entry body and is thought to be a slightly modified version of the W76-1 (Kristensen 2011b); the British government calls it the Trident Holbrook (UK Ministry of Defence 2015). The Royal Navy also plans to use the new Mk7 for the replacement warhead it plans to deploy on its new Dreadnought submarines in the future. Despite a significant lobbying effort on the part of the United Kingdom, including an unprecedented letter to the US Congress from the UK Minister of Defense asking it to support the W93 warhead, the program's status has not yet been settled (Borger 2020).

Since the first deterrent patrol in 1960, US ballistic missile submarines have conducted approximately 4,200 deterrent patrols at sea. During the past 15 years, operations have changed significantly, with the annual number of deterrent patrols having declined by more than half, from 64 patrols in 1999 to 30 to 36 annual patrols in recent years. Most submarines now conduct what are called "modified alerts," which mix deterrent patrol with exercises and occasional port visits (Kristensen 2013b). While most ballistic missile submarine patrols last around 77 days, they can be shorter or, occasionally, last significantly longer. In June 2014, for example, the *Pennsylvania* (SSBN-735) returned to its Kitsap Naval Submarine Base in Washington after a 140-day deterrent patrol, the longest patrol ever by an Ohio-class ballistic missile submarine. In the Cold War years, the overwhelming majority of deterrent patrols took place in the Atlantic Ocean. In contrast, more than 60 percent of deterrent patrols today normally take place in the Pacific, reflecting increased nuclear war planning against China and North Korea (Kristensen 2018).

Ballistic missile submarines normally do not visit foreign ports during patrols, but there are exceptions. Over a four-year period in the late 1970s and early 1980s, US submarines routinely conducted port visits to South Korea (Kristensen 2011a). Occasional visits to Europe, the Caribbean, and Pacific ports continued during the 1980s and 1990s. After Russia's invasion of Ukraine in 2014, the Navy started to conduct one or two foreign port visits per year. A US Navy visit to Scotland in 2015 appeared to be a warning to Russia and was described as a plan to make ballistic missile submarines more visible (Melia 2015). A highly publicized visit to Guam in 2016 — the first visit to the Island by a ballistic missile submarine since 1988 — was a clear warning to North Korea. Port visits have continued every year since, except in 2020, to locations including Scotland, Alaska, Guam, and Gibraltar.

Design of the next generation of ballistic missile submarines, known as the Columbia-class, is well under way. This new class is scheduled to begin replacing the current Ohio-class ballistic missile submarines in the late 2020s. The Columbia-class will be 2,000 tons heavier than the Ohio-class and will be equipped with 16 missile tubes rather than 20. The Columbia program, which is expected to account for approximately one-fifth of the Navy's entire shipbuilding program from the mid-2020s to the mid-2030s, is projected to cost \$109.8 billion (Congressional Research Service 2022, 8). The lead boat in a new class is generally budgeted at a significantly higher amount than the rest of the boats, as the Navy has a longstanding practice to incorporate the entire fleet's design detail and non-recurring engineering costs into the cost of the lead boat. As a result, the Navy's fiscal 2022 budget submission estimates the procurement cost of the first Columbia-class SSBN — the *USS Columbia* (SSBN-826) — at approximately \$15 billion, followed by \$9.3 billion for the second boat (Congressional Research Service 2022, 9). A \$5.1 billion development



contract was awarded to General Dynamics Electric Boat in September 2017, and construction of the first boat began on October 1, 2020 — the first day of fiscal 2021.

General Dynamics expects to receive \$75 billion in revenue over the life span of the Columbia-class project (Medici 2017). Certain elements of construction may be delayed due to the ongoing COVID-19 pandemic, as the Columbia program officer noted in June 2020 that missile tube production had already been delayed by “about a couple of months” due to the pandemic (Eckstein 2020). According to the Congressional Research Service, “Until such time that the Navy can find ways to generate additional margin inside the program’s schedule, the program appears to be in a situation where many things need to go right, and few things can go wrong, between now and 2031 for the lead boat to be ready for its first patrol in 2031” (Congressional Research Service 2022, 15).

The Columbia-class submarines are expected to be significantly quieter than the current Ohio-class fleet. This is because a new electric-drive propulsion train will turn each boat’s propeller with an electric motor instead of louder, mechanical gears. Additionally, the components of an electric-drive propulsion train can be distributed around the boat, increasing the system’s resilience and lowering the chances that a single weapon could disable the entire drive system (Congressional Research Service 2000, 20). The Navy has never built a nuclear-powered submarine with electric-drive propulsion before, which could create technical delays for a program that is already on a very tight production schedule (Congressional Research Service 2022, 19).

In October 2019, the Columbia program manager noted in a presentation that final ship arrangements for the new class of submarines had been completed on September 6, apparently a year ahead of schedule (Bartolomei 2019). The Navy’s revised schedule now indicates that the Ohio-class boats will begin going offline in fiscal 2027, around the same time that the first Columbia-class boat is scheduled to be delivered in October 2027. Sea trials are expected to last approximately three years, and the first Columbia deterrence patrol is scheduled for 2031 (Congressional Research Service 2022, 8). The Columbia deliveries will coincide with the Ohio-class boats being taken out of service, and the Navy projects that they will go from 14 boats to 13 in 2027, 12 in 2029, 11 in 2030, and 10 in 2037, before eventually climbing back to 11 in 2041 and the full complement of 12 boats in 2042 (US Navy 2019; Rucker 2019). The lead boat of the new Columbia-class submarine fleet will be designated the *USS Columbia* (SSBN-826), and the second boat will be designated the *USS Wisconsin* (SSBN-827). The rest of the Columbia-class submarine fleet has not yet been named (US Navy 2020).

Compared with the previous year’s two test launches, six Trident II D5LEs were test-launched in 2021. Four launches were conducted in February 2021 as part of a commander’s evaluation test, while two more were launched from the *USS Wyoming* (SSBN-742) in September 2021 as part of a demonstration and shakedown operation (DASO-30) designed to test both the system and the crew’s readiness for operational deployment (US Navy 2021). The most recent missile launch marked the 184th successful test launch of the Trident II system since its introduction into the US arsenal in 1989 (US Navy 2021).

Demonstration and shakedown operations are conducted after an ballistic missile submarine completes its engineering refueling overhaul — a multi-year operation that takes place around the 20-year point for each boat. The overhaul consists of extensive structural repairs and the refueling of the boat’s nuclear reactor. These efforts resulted in a 20-year life-extension for each boomer. The Navy first completed the *USS Ohio*’s (SSBN-726) engineering refueling overhaul in December 2005, and has since completed 16 additional overhauls, completing the *USS Wyoming*’s (SSBN-742) engineering refueling overhaul in October 2020 (US Defense Department Inspector General 2018; Naval Sea Systems Command 2020). The final ballistic missile submarine to undergo an engineering refueling overhaul is the *USS Louisiana* (SSBN-743), which began the overhaul process in August 2019 and is expected to be completed in the fall of 2022 (Naval Sea Systems Command 2021). The Columbia-class SSBNs will not require nuclear refueling; as a result, their midlife maintenance operations will take significantly less time than their Ohio-class counterparts (Congressional Research Service 2022, 5).

Strategic bombers

The US Air Force currently operates a fleet of 20 B-2A bombers (all of which are nuclear-capable) and 87 B-52 H bombers (46 of which are nuclear-capable). A third strategic bomber, the B-1B, is not nuclear-capable. Of these bombers, we estimate that approximately 60 (18 B-2As and 42 B-52 Hs) are assigned nuclear missions under US nuclear war plans, although the number of fully operational bombers at any given time is lower. The New START data from September 2021, for example, only counted 45 deployed nuclear bombers (11 B-2As and 34 B-52 Hs) (State Department 2021b). The bombers are organized into nine bomb squadrons in five bomb wings at three bases: Minot Air Force Base in North Dakota, Barksdale Air Force Base in Louisiana, and Whiteman Air Force Base in Missouri. The new B-21 bomber program will result in an increase in the number of nuclear bomber bases.

Each B-2 can carry up to 16 nuclear bombs (the B61-7, B61-11, and B83-1 gravity bombs), and each B-52 H can carry up to 20 air-launched cruise missiles (the AGM-86B). B-52 H bombers are no longer assigned gravity bombs (Kristensen 2017b). An estimated 788 nuclear weapons, including approximately 500 air-launched cruise missiles, are assigned to the bombers, but only about 300 weapons are thought to be deployed at bomber bases. The



estimated remaining 488 bomber weapons are thought to be in central storage at the large Kirtland Underground Munitions Maintenance and Storage Complex outside Albuquerque, New Mexico.

The United States is modernizing its nuclear bomber force by upgrading nuclear command-and-control capabilities on existing bombers, developing improved nuclear weapons (the B61-12 and the long-range standoff missile), and designing a new heavy bomber, the B-21 Raider.

Upgrades to the nuclear command-and-control systems that the bombers use to plan and conduct nuclear strikes include the Global Aircrew Strategic Network Terminal. This is a new high-altitude electromagnetic pulse-hardened network of fixed and mobile nuclear command-and-control terminals. This network provides wing command posts, task forces, munitions support squadrons, and mobile support teams with survivable ground-based communications to receive launch orders and disseminate them to bomber, tanker, and reconnaissance air crews. First delivery of the global aircrew strategic network terminals, which the Air Force describes as “the largest upgrade to its nuclear command, control and communication systems in more than 30 years,” was expected in May 2020. However, it appears that this was delayed until Barksdale Air Force Base became the first base to receive the system in January 2022 (US Air Force 2022).

Another command-and-control upgrade involves a program known as Family of Advanced Beyond Line-of-Sight Terminals, which replaces existing terminals designed to communicate with the MILSTAR satellite constellation. These new, extremely high frequency terminals are designed to communicate with several satellite constellations, including advanced extremely high frequency satellites. The 37 ground stations and nearly 50 airborne terminals of the Family of Advanced Beyond Line-of-Sight Terminals will provide protected high-data rate communication for nuclear and conventional forces, including for what is officially called “presidential national voice conferencing.” According to the Air Force (US Air Force 2019b), “[The Family of Advanced Beyond Line-of-Sight Terminals] will provide this new, highly secure, state-of-the-art capability for [Defense Department] platforms to include strategic platforms and airborne/ground command posts via MILSTAR, [advanced extremely high frequency], and enhanced polar system satellites. [The Family of Advanced Beyond Line-of-Sight Terminals] will also support the critical command and control ... of the MILSTAR, [advanced extremely high frequency], and enhanced polar system satellite constellations.”

The heavy bombers are also being upgraded with improved nuclear weapons. This effort includes development of the first guided, standoff nuclear gravity bomb, known as the B61-12, which is intended to replace all existing gravity bombs. The bomb will use a modified version of the warhead used in the current B61-4 gravity bomb. B61-12 integration drop tests have already been conducted from the B-2 bomber (the B61-12 may also be integrated onto US-and allied-operated tactical aircraft, including the F-15E, the F-16C/D, the F-16MLU, and the PA-200 Tornado). Approximately 480 B61-12 bombs, which appear to have limited earth-penetration capability, are expected to cost a total of roughly \$10 billion (Kristensen and McKinzie 2016). The first production unit was initially scheduled for March 2020; however, in September 2019 a NNSA official confirmed that both the B61-12 and the upgraded W88 warhead for the Trident II SLBM would likely face delays during production due to concerns over the longevity of its commercial off-the-shelf subcomponents (Gould and Mehta 2019). The First Production Unit prototype of the B61-12 was completed on August 25, 2020 at the Pantex Plant (NNSA 2020a). The first real First Production Unit was only completed in November 2021, and full-scale production is now scheduled for May 2022 (NNSA 2021b).

The Air Force is also developing a new nuclear air-launched cruise missile known as the long-range standoff missile. It will replace the AGM-86B air-launched cruise missile in 2030 and carry the W80-4 warhead, a modified version of the W80-1 used in the current air-launched cruise missile. In February 2019, the Nuclear Weapons Council authorized the development engineering phase (Phase 6.3) for the W80-4. The production engineering stage (Phase 6.4) is planned for December 2021 (Energy Department 2019b). A solicitation invitation to defense contractors in 2015 listed three potential options for the long-range standoff engine: First, a derivative subsonic engine that improves on current engine technology by up to 5 percent; second, an advanced subsonic engine that improves on current technology by 15 percent to 20 percent; and third, a supersonic engine (US Air Force 2015). In August 2017, the Air Force awarded 5-year contracts of \$900 million each to Lockheed Martin and Raytheon to develop design options for the missile. After reviewing the designs, the Air Force, in December 2019, cleared the two companies to continue development of the missile (Sirota 2019). The Air Force originally planned to down-select to a single contractor in fiscal 2022 during the awarding of the engineering and manufacturing development contract; however, in April 2020, the Air Force selected Raytheon Technologies as the prime contractor for the long-range standoff (US Air Force 2020b). This was a relatively surprising move, as selecting a single-source contractor at this early stage could ultimately result in higher program costs. In July 2021, Raytheon Technologies was awarded up to \$2 billion to proceed with the engineering and manufacturing development stage of the long-range standoff, in order to prepare for full-rate production beginning in 2027 (Insinna 2021).

In March 2019, the Air Force awarded Boeing a \$250 million contract to integrate the future long-range standoff capability onto the B-52 Hs, a process that is expected to be completed by the beginning of 2025 (Hughes 2019). Development and production are projected to reach at least \$4.6 billion for the missile (US Air Force 2019a) with another \$10 billion for the warhead (Energy Department 2018a).



The missile itself is expected to be entirely new, with significantly improved military capabilities compared with the air-launched cruise missile, including longer range, greater accuracy, and enhanced stealth (Young 2016). This violates the 2010 White House pledge (White House 2010) that the “United States will not ... pursue ... new capabilities for nuclear weapons,” though the NPR from 2018 did away with such constraints.

Supporters of the long-range standoff argue that a nuclear cruise missile is needed to enable bombers to strike targets from well outside the range of the modern and future air-defense systems of potential adversaries. Proponents also argue that these missiles are needed to provide US leaders with flexible strike options in limited regional scenarios. However, critics argue that conventional cruise missiles, such as the extended-range version of the Joint Air-to-Surface Standoff Missile, can currently provide standoff strike capability, and that other nuclear weapons would be sufficient to hold the targets at risk. In fact, the conventional extended-range joint air-to-surface standoff missile is now an integral part of Strategic Command’s annual strategic exercises.

Unlike the current air-launched cruise missile, which is only carried by the B-52 H bomber, the long-range standoff missile will be integrated on both the B-52 H and new B-21 bombers (Kristensen 2013c). Warhead production is scheduled from 2025 through 2031. The Air Force plans to buy 1,000 missiles (Reif 2015), but there will only be enough warheads for about half of those. The excess missiles are intended to be used as spares and for test flights over the course of the weapon’s 30-year service life. Moreover, several hundred of the existing air-launched cruise missiles were converted to conventional missiles (AGM-86C/D) and the US Air Force Global Strike Command has previously indicated that it intends to develop a conventional version of the long-range standoff (Wilson 2015).

But given the deployment of several new long-range conventional cruise missiles and the development of even more advanced versions, it remains to be seen if the Air Force can persuade Congress to also pay for a conventional version of the long-range standoff. Indeed, the Air Force has replaced the AGM-86C/D conventional air-launched cruise missile with the extended-range conventional Joint Air-to-Surface Standoff Missile. If Congress will not pay for conventional long-range standoffs, it can probably be assumed that the plan to buy 1,000 missiles can be reduced by several hundred.

Northrop Grumman continues to develop the new B-21 Raider next-generation heavy bomber, as the preliminary design review received approval in early 2017 and the first test vehicle is currently in production. The B-21 is scheduled to make its first flight no earlier than 2022 from its production facility in Palmdale, California, to Edwards Air Force Base (Wolfe 2020). The B-21 is expected to enter service in the mid-2020s to gradually replace the B-1B and B-2 bombers during the 2030s, and it is expected that the Air Force will procure at least 145 of the new bombers at an estimated cost of \$550 million per plane to increase the total bomber force from 175 to 220 aircraft (Tirpak 2020).

The Air Force announced in March 2019 that the B-21 bombers will first be deployed at Ellsworth Air Force Base (South Dakota), followed by Whiteman Air Force Base (Missouri) and Dyess Air Force Base (Texas) “as they become available” (US Air Force 2019c). The upgrade of the non-nuclear B-1 bases to the nuclear B-21 bomber will increase the number of bomber bases with nuclear weapons storage facilities from two bases today (Minot AFB and Whiteman AFB) to five bases by the 2030s (Barksdale AFB will also regain nuclear storage capability) (Kristensen 2020c). Further details about the B-21 program, including updated cost estimates, are still shrouded in secrecy; however, like all previous bomber programs, the costs will most likely increase.

The B-21 is very similar in design to the B-2 but is expected to be slightly smaller and have a reduced weapons capability. The B-21 will be capable of delivering both the B61-12 guided nuclear gravity bomb and the long-range standoff, as well as a wide range of non-nuclear weapons, including the Joint Air-to-Surface Standoff cruise missile.

In early 2022, the Air Force announced that six B-21 bombers were currently in production, and the first assembled bomber was taken to conduct its calibration tests in early March 2022 (Tirpak 2022). This aircraft will be the first B-21 to make a maiden flight, which is expected in mid-2022 from its manufacturing and assembly facility to Edwards Air Force Base in California (Tirpak 2022).

Nonstrategic nuclear weapons

The United States has one type of nonstrategic nuclear weapon in its stockpile: the B61 gravity bomb. The weapon exists in two modifications: the B61-3 and the B61-4. A third version, the B61-10, was retired in September 2016. Approximately 200 tactical B61 bombs of all versions remain in the stockpile. About 100 of these (versions –3 and –4) are thought to be deployed at six bases in five European countries: Aviano and Ghedi in Italy; Büchel in Germany; Incirlik in Turkey; Kleine Brogel in Belgium; and Volkel in the Netherlands. This number has declined since 2009 partly due to reduction of operational storage capacity at Aviano and Incirlik (Kristensen 2015, 2019c). The remaining 100 B61s stored in the United States are for backup and potential use by US fighter-bombers in support of allies outside Europe, including northeast Asia. This includes F-15Es from the 391st Fighter Squadron of the 366th Fighter Wing at Mountain Home in Idaho (Charkhuff 2021).

The Belgian, Dutch, German, and Italian air forces are assigned nuclear strike missions with US nuclear weapons. Under normal circumstances, the nuclear weapons are kept under the control of US Air Force personnel; their use in war must be authorized by the US president. The Belgian and Dutch air forces currently use the F-16 aircraft for the nuclear missions,



although both countries are in the process of obtaining the F-35A to eventually replace their F-16s. The Italian Air Force uses the PA-200 Tornado for the nuclear mission but is in the process of acquiring the F-35A. Like the Tornados, the nuclear F-35As will be based at Ghedi Air Base, which is currently being upgraded. Germany also uses the PA-200 Tornado for the nuclear mission; however, it is planning to retire its Tornados by 2030, and would require a new dual-capable aircraft if it intended to remain part of NATO's nuclear sharing mission.



Figure 3: A B61-12 guided nuclear (practice) bomb is dropped from an F-35A. The B61-12 will enter full-scale production in May 2022 and probably begin deploying to bases in Europe in 2023. Image: USAF.

The new German coalition government announced in November 2021 that it intended to do so, and it is rumored that the German government will issue a letter of request to purchase the Boeing F/A-18E/F Super Hornet in early 2022 to replace its Tornado aircraft (Siebold and Wacket 2021; Jennings 2021). Yet the F-35A is apparently still a candidate (Reuters 2022).

At least until 2010, Turkey was still using F-16s for the nuclear mission, although it is possible that the mission has since been mothballed. In 2019, the Trump administration also halted delivery of F-35As to Turkey — some of which were intended to take over the nuclear mission — because of its plans to acquire the Russian S-400 air-defense system (DeYoung, Fahim, and Demirjian 2019). Legislators and analysts raised concerns about the security of the nuclear weapons at the Incirlik base during the failed coup attempt in Turkey in July 2016; the chairman of the Senate Foreign Relations Subcommittee for Europe stated in September 2020 that “our presence, quite honestly, in Turkey is certainly threatened,” and further noted that “we don’t know what’s going to happen to Incirlik” (Gehrke 2020). Despite rumors in late 2017 that the weapons had been “quietly removed” (Hammond 2017), the New York Times reported in 2019 that US officials had reviewed emergency nuclear weapons evacuation plans for Incirlik, indicating that there were still weapons present at the base (Sanger 2019). The numbers appear to have been reduced, however, from up to 50 to approximately 20. If the United States decided to withdraw the remaining nuclear weapons from Incirlik, it could probably do so with a single C-17 transport aircraft from the 4th Airlift Squadron at Joint Base Lewis-McChord in Washington — the only unit in the Air Force that is qualified to airlift nuclear weapons.

NATO States that do not host nuclear weapons can still participate in the nuclear mission as part of conventional supporting operations, known as Support Nuclear Operations With Conventional Air Tactics — or SNOWCAT.

NATO is working on a broad modernization of the nuclear posture in Europe that involves upgrading bombs, aircraft, and the weapons storage system. The B61-12 is estimated to be 12 feet long, weighing approximately 825 pounds, and is designed to be air-launched in



either ballistic or gravity drop modes (Baker 2020). The B61-12 will use the nuclear explosive package of the B61-4, which has a maximum yield of approximately 50 kilotons and several lower-yield options. However, it will be equipped with a guided tail kit to increase accuracy and standoff capability, which will allow strike planners to select lower yields for existing targets to reduce collateral damage. The increased accuracy will give the tactical bombs in Europe the same military capability as strategic bombs used by the bombers in the United States. Although the B61-12 has not been designed as a designated earth-penetrator, it does appear to have some limited earth-penetration capability. This increases its ability to hold at risk underground targets (Kristensen and McKinzie 2016). Until their new aircraft are ready, Italy and Germany will continue to fly the PA-200, which, due to its age and legacy systems, will not be able to utilize the B61-12s new guided tail kit function. Instead, it will deliver the bomb as a “dumb” bomb akin to the current B61-3s and B61-4s.

In March 2020, the F-15E became the first aircraft to be certified to operate the B61-12, after completing the last in a series of six compatibility tests at Nellis Air Force Base and the Tonopah Test Range (Baker 2020). In addition to the F-15E, integration of the B61-12 on B-2, F-16, and PA-200 aircraft is well under way. In October 2021, the F-35A completed two drop tests of the B61-12 Joint Test Assembly (see Figure 3), thus completing the final stage of its nuclear design certification process (US Air Force 2021b). The B61-12 will begin full-scale production in May 2022, certification with the F-35A before January 2023, followed by training of the nuclear fighter-wings in Europe later in 2023 (Defense Visual Information Distribution Service 2022). Once deployment to Europe begins, possibly in 2023, the B61-3/4 bombs currently deployed in Europe will be returned to the United States.

NATO is life-extending the weapons storage security system, which involves upgrading command and control, as well as security, at the six active bases (Aviano, Büchel, Ghedi, Kleine Brogel, Incirlik, and Volkel) and one training base (Ramstein). Specifically, these upgrades include the installation of double-fence security perimeters, modernizing the weapon storage and security systems and the alarm communication and display systems, and the operation of new secure transportation and maintenance system trucks (Kristensen 2021b). Security upgrades now appear to have been completed at Aviano and Incirlik and are underway at Ghedi.

In addition to the modernization of weapons, aircraft, and bases, NATO also appears to be increasing the profile of the dual-capable aircraft posture. In June 2020, for example, the 31st Fighter Wing at Aviano Air Base conducted the first “elephant walk” ever to display all aircraft in a single visual show of force of its capability to “deter and defeat any adversary who threatens US or NATO interests” (US Air Force 2020c). NATO’s annual Steadfast Noon nuclear force exercise also includes participation from a large number of NATO members every year. In 2021, the exercise involved the participation of 14 countries — including Dutch and Belgian F-16s, and German and Italian Tornados — over southern Europe (NATO 2021).

Having reached 50 ratifications in October 2020, the Treaty on the Prohibition of Nuclear Weapons officially entered into force on January 22, 2021. It is unclear whether the treaty will have an effect on the status of NATO’s nuclear posture over the coming years — and specifically on the forward-deployment of US nuclear weapons on European NATO territory. However, public opinion in Belgium, Germany, Italy, and the Netherlands is firmly opposed to hosting US nuclear weapons (International Campaign to Abolish Nuclear Weapons (ICAN) 2018). To that end, some host country parliaments have already taken actions that challenge the future of US nuclear weapons on their soil; in January 2020, a motion to “draw up, as soon as possible, a roadmap aiming at the withdrawal of nuclear weapons on Belgian territory” was narrowly defeated by a vote of 74–66 in the Belgian parliament (Galindo 2020). It is possible that similar resolutions could be debated and voted upon in other nuclear hosting nations over the coming years. This explains why the United States tried in vain to persuade other countries to withdraw their ratifications, only a week before the Treaty on the Prohibition of Nuclear Weapons reached 50 ratifications (Lederer 2020).

The 2018 NPR recommended rapid development of a nuclear nonstrategic submarine-launched cruise missile to recreate a capability to deploy such a weapon in support of NATO (and Pacific) allies. A previous cruise missile was retired in 2011. The new weapon would likely be intended for deployment on attack submarines. The analysis of alternatives for the nuclear nonstrategic submarine-launched cruise missile was scheduled to be completed in 2021, with development of the missile beginning in 2022. However, it remains unclear whether the Navy has met these deadlines (Wolfe 2021b). It also remains unclear whether the Biden administration will continue the project.

Hans Kristensen is the director of the Nuclear Information Project with the Federation of American Scientists (FAS) in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a co-author to the world nuclear forces overview in the *SIPRI Yearbook* (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has co-authored *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.

The hidden city under Helsinki built for the nuclear apocalypse: Finnish city has 500 bunkers where the entire population of 600,000 people can shelter from the fallout of nuclear war for months

Source: <https://www.dailymail.co.uk/news/article-10813491/Hidden-city-Helsinki-built-nuclear-apocalypse-entire-population-shelter-months.html>

May 13 – This is the incredible scale and intricacy of [Finland's](#) thorough network of nuclear bunkers.

More than **500 underground shelters** carved into the bedrock of capital Helsinki can hold **900,000 people** - a third more than the city's entire population.

And as Finland's bid to join [NATO](#) prompts Kremlin tough talk including vows to take 'retaliatory steps' against Helsinki, officials are preparing for all eventualities.

Anna Lehtiranta, head of communications at Helsinki's city rescue department, said Finns are unfazed by [Putin's](#) threats.



A softball court is built in one of Helsinki's hundreds of underground emergency bunkers

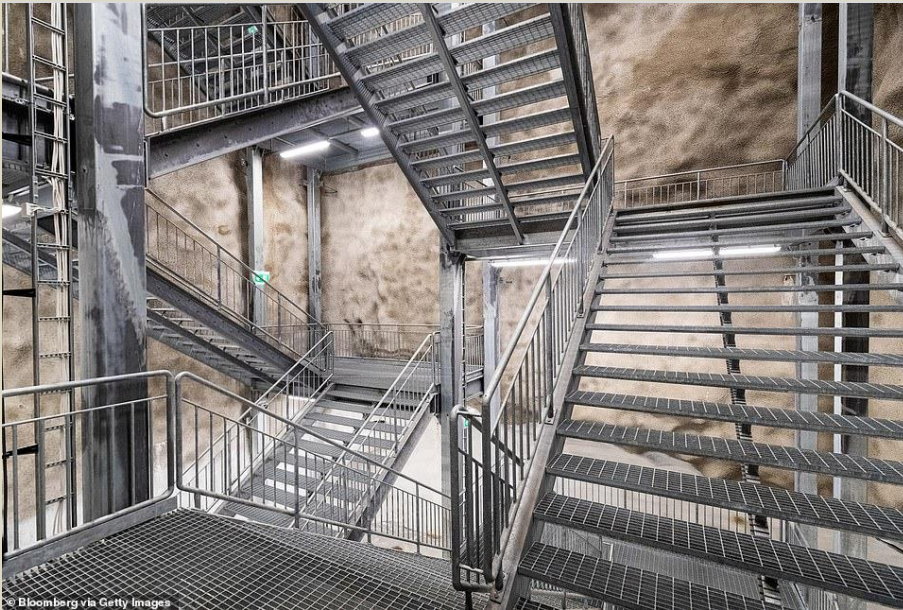
She told MailOnline: 'As a neutral country, we have always felt we need to protect ourselves - and we do.'

'The underground shelters built in the bedrock of Finland come from our experience in the Winter War and during the Second World War. We all have relatives who suffered through those traumas.'

Finland's subterranean habitats include cafes, softball courts, go karting tracks, car parks and thousands of bunk beds.

First built during the 1960s, successive governments have excavated more than 9 million cubic metres of bedrock below Finland.





Stairs take Finns and visitors to the country 25m below ground to the safe underground havens

That's enough space to store 50,000 double-decker buses.

The shelters' entry doors carefully located above ground are so thick a nuclear blast wouldn't leave a dent, officials claim.

The historically neutral Nordic country's bid to join NATO has sparked fury in Moscow, which accuses the Western military alliance of encircling its borders.

Kremlin officials have promised 'retaliatory steps', including moving nuclear weapons closer to Europe.

Finland would become the sixth NATO member to share a land border with Russia.

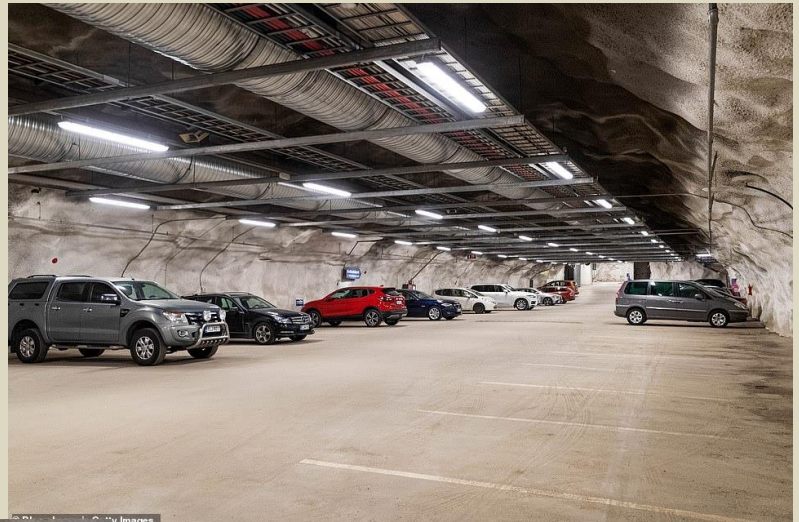
The shelters have space for hundreds of cars so residents are in no rush through entry doors

NATO leader Jens Stoltenberg said the nation would be 'warmly welcomed with open arms' by its member states, which must sign off on Finland's entry before it joins.

The bid has prompted new interest among Finns in the nation's network of underground shelters - and new urgency among civil defence officials to make sure they're ready if - or when - they're needed.

Ms Lehtiranta said: 'We have documents with lists of jobs people will do underground if they're forced to stay for two weeks or longer.'

'There will be a management department, doctors and



nurses, people in charge of looking after children while they parents work, and more.

'People will use the skills they have gained above ground while in the shelters.'

In addition to the hundreds of shelters, Helsinki's 25 metro stations can also be converted into underground bunkers which can hold people for weeks on end.

Official guidelines state 'everybody who stays in Finland', including hotel guests, will have a place in the bunkers.

But the rules also state: 'Alcohol, drugs, weapons, devices that produce heat or anything that smells bad are not allowed in a shelter.'

Ms Lehtiranta stated that the shelters are protected against potential cyber attacks, too.

Finland's president

has warned that Russia could step up its technological warfare on the country if its NATO bid is given the greenlight by alliance members.

But Ms Lehtiranta said: 'Though there will be phone signal below ground, our lower reliance on technology in the shelters means we are entirely safe against cyber attacks.'





EDITOR'S COMMENT: Two simple questions: (1) Helsinki's population is 1,328,000 (2022) while the capacity of underground bunkers is 900,000 people. Will 428,000 people be left out exposed to radiation? Finns or legal and illegal immigrants, refugees and tourists? (2) The distance between Helsinki and in example St. Petersburg, Russia is just 306km. Remember how long it took (minutes) for a nuclear missile to reach European targets in the recent simulations conducted by Russians – a Russian Sarmat based in Kaliningrad (664km from Helsinki) can nuke Berlin in 106 seconds, Paris in 200 seconds and London in 202 seconds? And Helsinki in 20 seconds with Kinzhals! Based on the above, why the very young Finnish PM pretends to be a mighty lion in front of Siberian bear?

New satellite images reveal North Korea has restarted construction on long-dormant nuclear reactor

Source: <https://edition.cnn.com/2022/05/13/politics/north-korea-restarts-construction-nuclear-reactor-satellite-images/index.html>

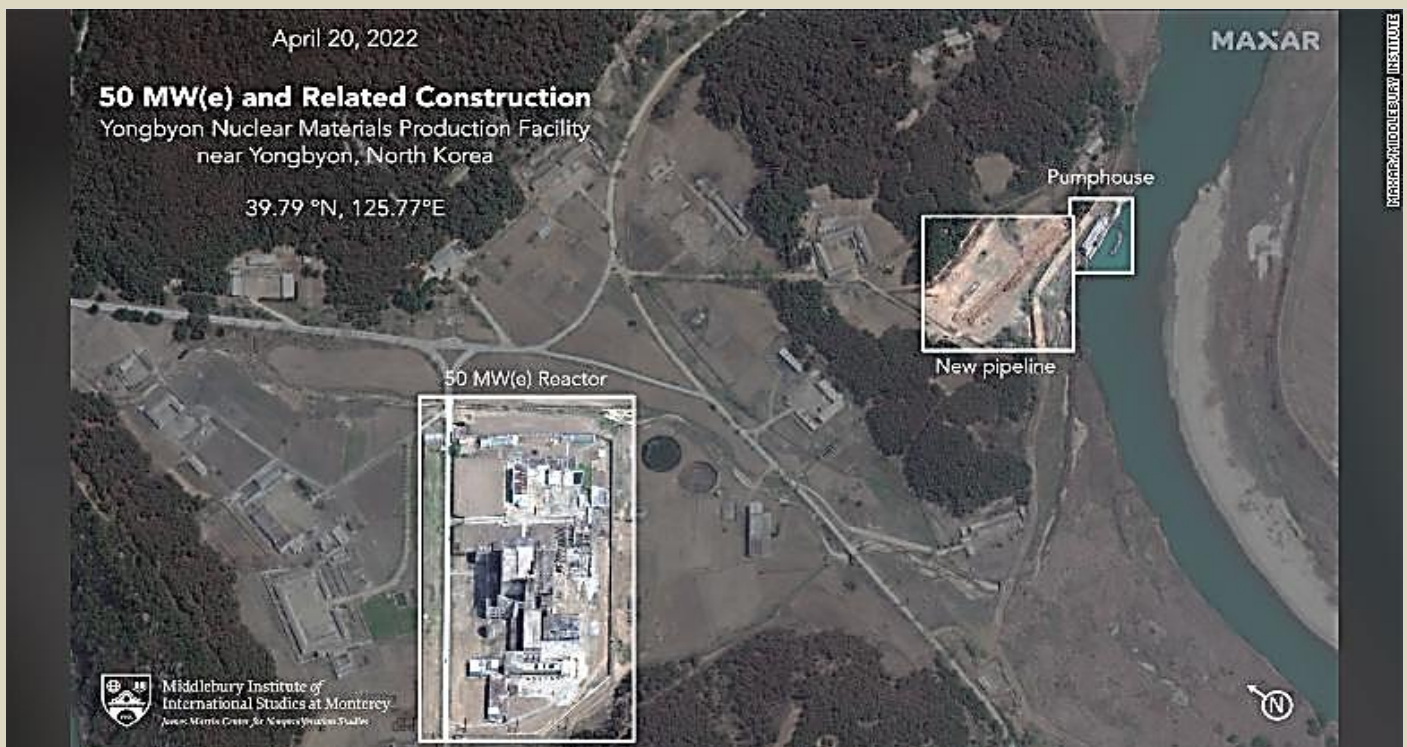
May 13 – [North Korea](#) appears to have resumed construction at a long-dormant nuclear reactor in recent weeks that, if completed, would dramatically increase its capacity to produce plutonium for nuclear weapons, according to new satellite images obtained by CNN and a source familiar with recent US intelligence reporting on the matter.

The satellite images, which were captured by Maxar during April and May of this year, show North Korea has restarted construction of the second reactor at its Yongbyon nuclear complex after years of inactivity, experts at the Middlebury Institute of International Studies who analyzed the photos said.

The reactor is about 10 times larger than the existing nuclear reactor at Yongbyon, which has been operating since the late 1980s. US officials are also aware of and closely monitoring recent activity at Yongbyon, according to a source familiar with the situation, who noted North Korea is not trying to hide its efforts to restart construction on the reactor in question.

This appears to be an outward demonstration of North Korea's nuclear progress and ambitions, the source said, adding that new construction on the Yongbyon reactor aligns with Pyongyang's aim of proving it's a nuclear armed state.





Experts say it is difficult to estimate how quickly North Korea could complete construction of the reactor.

But once operational, it could allow North Korea to increase its production of plutonium for nuclear weapons by a factor of 10, according to Jeffrey Lewis, a weapons expert and professor at the Middlebury Institute.

Lt. Col. Martin Meiners, a Pentagon spokesman, declined to comment when asked if there is specific intelligence suggesting North Korea has taken new steps to complete construction of the reactor at Yongbyon.

"However, we've been very clear on the threat posed by the Democratic People's Republic of Korea (DPRK) nuclear and missile programs, our commitment to the defense of the ROK, Japan, and the U.S. homeland, and our shared objective of the complete denuclearization of the Korean Peninsula," Meiners added.

North Korea halted construction of the nuclear reactor at Yongbyon in 1994 under the framework of its agreement with the US. At that point the reactor was still years away from completion, Lewis said.

Only very limited construction activities were observed at the site in subsequent years but Lewis told CNN that he and his fellow researchers believe the recent satellite images provide "the first unambiguous indicator that North Korea is moving to complete the reactor."

Specifically, the images taken by Maxar show that North Korea is "connecting the secondary cooling loop of the 50 MW(e) reactor to a pumphouse on the river," he said.

"In the image dated April 20, construction equipment is visible, as are what appear to be pipe segments. By May 7, North Korea had buried the pipe," Lewis added.

"The connection of the cooling loop helps explain other activities seen at the 50MW(e) reactor in recent years," Lewis told CNN, pointing to the observed demolition of a building last year that was believed to house a cooling pond for spent fuel.

"Connecting the secondary cooling loop suggests, in hindsight, that the demolition of the apparent spent-fuel building was an early sign that North Korea intends to complete construction of the reactor," told CNN.

The source familiar with the matter also said that there is a lot of preparatory activity required before any country can start construction on a nuclear reactor. "Preparatory activities speak to intent, planning and long held goals," the source added.

CNN [reported earlier this month](#) that US military and intelligence agencies assess North Korea could be ready to resume underground nuclear testing in the near term.

The assessment concludes that Kim Jong Un's government is making preparations at another facility, the Punggye-ri nuclear test site, and could be ready to conduct a test by the end of the May.

Signs of personnel and vehicle activity at the site have been seen through satellite imagery, but the officials do not know if the regime has placed nuclear material in one of the underground tunnels at the test site, which the US has been closely watching.

If North Korea conducts a test, it would be the country's seventh underground nuclear test and the first in nearly five years.



The dangerous business of dismantling America's aging nuclear plants

Source: <https://www.washingtonpost.com/business/2022/05/13/holtec-oyster-creek-nuclear-plant-cleanup/>



A worker at Holtec International's manufacturing plant in Camden, N.J. On the left are steel canisters used to store nuclear waste for decades. (Sarah L. Voisin)

May 13 — The new owner took over the Oyster Creek Nuclear Generating Station in 2019, promising to dismantle one of the nation's oldest nuclear plants at minimal cost and in record time. Then came a series of worrisome accidents.

One worker was struck by a 100-ton metal reactor dome. Another was splashed with radioactive water, according to internal incident reports and regulatory inspection reports reviewed by The Washington Post. Another worker drove an excavator into an electrical wire on his first day on the job, knocking out power to 31,000 homes and businesses on the New Jersey coast, according to a police report and the local power company.

All three incidents occurred on the watch of Holtec International, a nuclear equipment manufacturer based in Jupiter, Fla. Though the company until recently had little experience shutting down nuclear plants, Holtec has emerged as a leader in nuclear cleanup, a burgeoning field riding an expected wave of closures as licenses expire for the nation's aging nuclear fleet.

Over the past three years, Holtec has purchased three plants in three states and expects to finalize a fourth this summer. The company is seeking to profitably dismantle them by replacing hundreds of veteran plant workers with smaller, less-costly crews of contractors and eliminating emergency planning measures, documents and interviews show. While no one has been seriously injured at Oyster Creek, the missteps are spurring calls for stronger government oversight of the entire cleanup industry.

In the nearly three years Holtec has owned Oyster Creek, regulators have documented at least nine violations of federal rules, including the contaminated water mishap, falsified weapons inspection reports and other unspecified security lapses. That's at least as many as were found over the preceding 10 years at the plant, when it was owned by Exelon, one of the nation's largest utility companies, according to The Post's review of regulatory records.

Joseph Delmar, a spokesman for Holtec, defended the company's record, saying it takes safety and security seriously. The recent incidents "are not reflective of the organization's culture," he said, adding that the worker who knocked down the power line "did not follow the proper safety protocols." Delmar said the company has decades of experience building equipment to store nuclear waste and employs veteran plant workers to dismantle reactor sites.

"While the decommissioning organization may seem new, the professionals staffing the company are experienced nuclear professionals with intimate knowledge of the plants they work at," Delmar said in an emailed statement.

Holtec is, however, pioneering an experimental new business model. During the lifetime of America's 133 nuclear reactors, ratepayers paid small fees on their monthly energy bills to



fill decommissioning trust funds, intended to cover the eventual cost of deconstructing the plants. Trust funds for the country's 94 operating and 14 nonoperating nuclear reactors now total about \$86 billion, according to Callan, a San Francisco-based investment consulting firm.

After a reactor is dismantled and its site cleared, some of these trust funds must return any money left over to ratepayers. But others permit cleanup companies to keep any surplus as profit — creating incentives to cut costs at sites that house some of the most dangerous materials on the planet.

Even after reactors are shut down, long metal rods containing radioactive pellets — known as spent fuel — are stored steps away, in cooling pools and steel-and-concrete casks. Nuclear safety experts say that an industrial accident or a terrorist attack at any of these sites could result in a radiological release with severe impacts to workers and nearby residents, as well as to the environment. The Nuclear Regulatory Commission, the independent federal agency tasked with overseeing safety at nuclear sites, conducts regular inspections during the decommissioning process. But state and local officials say the NRC has failed to safeguard the public from risks at shut-down plants, deferring too readily to companies like Holtec.

"The NRC is not doing their job," said Sen. Edward J. Markey (D-Mass.), who has pushed the agency to adopt stricter regulations around plant decommissioning. "We need a guaranteed system that prioritizes communities and safety, and we don't have that right now."

The NRC's leadership is divided over the role regulators should play. The agency was created in 1974, as the first generation of commercial reactors was going online, and its rules were mainly designed to safeguard the operation of active plants and nuclear-material sites. As reactors shut down, the NRC began reducing inspections and exempting plants from safety and security rules.

Last November, the NRC [approved](#) a new rule that would automatically qualify shut-down plants for looser safety and security restrictions. Christopher T. Hanson, a Democrat nominated by President Donald Trump and promoted to the role of chairman by President Biden, has [said](#) the changes would improve the "effectiveness and efficiency" of the decommissioning process.

Commissioner Jeff Baran, also a Democrat, voted against the proposed rule and called for the NRC and local governments to play a bigger role. "Radiological risks remain at shutdown nuclear plants that must be taken seriously," he cautioned in [public comments](#). Baran added that the agency already takes a "laissez-faire" approach to decommissioning and that the new rule "would make the situation even worse, further skewing the regulation towards the interests of industry."

Dan Dorman, the NRC's executive director for operations, said in an email that the agency lifts restrictions at plants only if it determines the plant will continue to be safe. In addition to citing Holtec for violations at Oyster Creek, the agency has required the company to take corrective measures, including external security assessments of all its nuclear sites.

"Our increased oversight and the recent enforcement actions demonstrate our concern about the situation at Oyster Creek," Dorman said.

Holtec faces mounting criticism beyond Oyster Creek. Michigan officials have [said](#) they worry Holtec will leave residents on the hook for cleanup costs at the Palisades plant on the shores of Lake Michigan. Massachusetts officials have protested Holtec's plan to take 1 million gallons of contaminated water from the defunct Pilgrim power plant and dump it into Cape Cod Bay.

While Holtec acknowledges a funding shortfall at Palisades, Delmar says the fund will appreciate in value to cover the cost of the cleanup. At Pilgrim, Holtec has [said](#) the potential radiation dose from the Cape Cod release would be far less than the average traveler receives on a typical cross-country flight.

In the Southwest, Holtec has ignited a different controversy. As the company acquires old plants, it is proposing to ship the highly radioactive spent fuel to New Mexico, where it plans to build a storage facility. Gov. Michelle Lujan Grisham (D) has vowed to fight the plan, telling Trump in a 2020 letter that storing radioactive material in the oil-rich Permian Basin region would be "economic malpractice."

Holtec says it is working in partnership with a group of local officials who believe the benefits of the facility — including new jobs and investment — outweigh the risks. On its website, Holtec [says](#) the facility will provide "a safe, secure, temporary, retrievable, and centralized facility for storage of used nuclear fuel and high-level radioactive waste until such time that a permanent solution is available."

The growing debate marks the latest twist in the tortured saga of nuclear power, which once was hailed as a miracle technology capable of producing large quantities of clean, affordable energy. In the early 1970s, the federal Atomic Energy Commission estimated that about 1,000 reactors would be built in the United States, and that nuclear sources eventually would provide at least half of the world's power.

But those ambitions soon collided with fears about nuclear radiation, especially after disastrous meltdowns at Chernobyl in Ukraine and Fukushima in Japan. Nuclear energy peaked at around 18 percent of global electricity production in the 1990s and now comprises about 10 percent, according to the U.S. Energy Information Association.

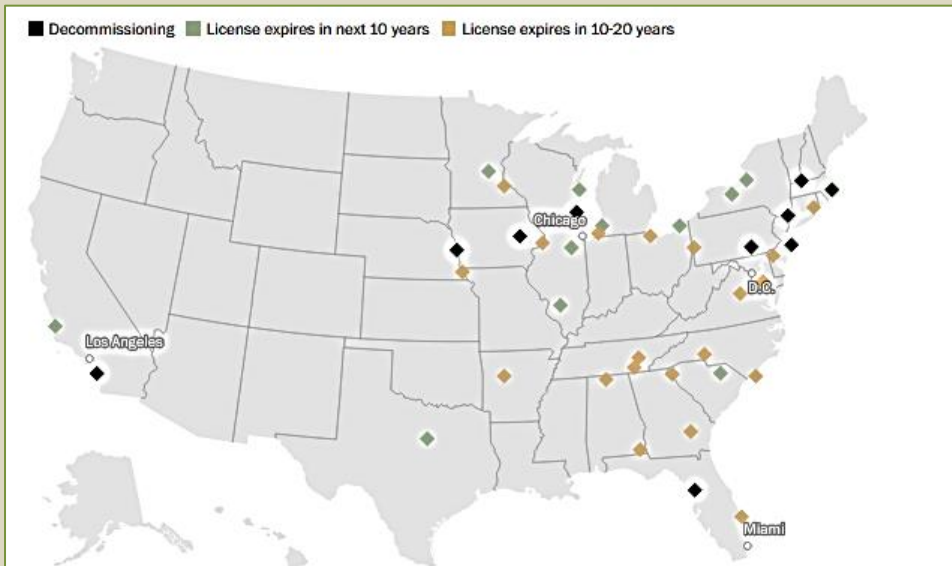


Reactors in the United States initially were licensed for 40 years, and most were renewed for another 20 years. Of 94 reactors that are still active, licenses at over half are set to expire in the next two decades, according to Julia Moriarty, a senior vice president at

Callan.

Recently, worries about climate change have led some governments to embrace nuclear as a low-carbon source of power. Biden has called nuclear essential to the nation's climate goals, and Washington last year set aside \$6 billion for extending the licenses of some plants and \$2.5 billion for developing new nuclear technologies.

But the nation continues to puzzle over the problem of nuclear waste. This material, which emanates invisible but harmful radiation for hundreds of years, is stored in protective containers on the grounds of nuclear plants, scattered in dozens of towns



across the country. A plan to build a national waste repository in Nevada's Yucca Mountain stalled amid decades of political gridlock, leaving these towns saddled indefinitely with the threat of an accidental release or terrorist attack. Holtec is approaching those communities with an offer to clean up the mess.

'Accelerated decommissioning'

Founded and wholly owned by Kris Singh, an inventor and entrepreneur, Holtec says it is pioneering a new model of "accelerated decommissioning." At the 24 U.S. reactors currently undergoing decommissioning, over half are expected to take two decades or more to complete the process, NRC data shows; Holtec pledges to return nuclear sites to safe, clean usable land in as few as eight years.

Singh did not respond to requests for comment, and Holtec did not make him available for an interview.

The company's work at Oyster Creek, its first plant, was meant to be a blueprint for the national expansion, Holtec executives said in interviews with The Post in early 2020. Instead, safety advocates argue, it has served as a warning. Cost-cutting has left employees



feeling overworked and prone to mistakes, according to two former plant workers who were both laid off by Holtec. They spoke on the condition of anonymity to discuss their former employer.

A Holtec worker welds a dry storage canister. Much of the country's nuclear waste is stored in containers such as these at dozens of plants scattered across the country. (Sarah L. Voisin/The Washington Post)

The company has said in regulatory filings it plans to keep about \$85 million in profit from Oyster Creek's \$826 million trust fund. It has already spent about one quarter of the fund.

Shortly after Holtec took over, regulators found problems with the plant's weapons program. All nuclear plants must maintain weapons, such as guns and ammunition used by security personnel, and test them on a regular basis to secure the sites from attacks. According to an NRC investigation, a Holtec manager skipped the annual tests and falsified the weapons inspection reports to give the appearance the tests were conducted. The manager said in a letter to the NRC that he made



mistakes on the company's inspections report because he had been "overwhelmed" following staff cuts, though he denied that anything was intentionally falsified.

"I went from a staff of six to a staff of two, all having extra responsibilities, doubling our workload and learning new criteria of the positions," the manager said in the [letter](#), which was posted on the NRC's website.

In a settlement with the NRC [announced](#) this year, Holtec agreed to pay a \$50,000 civil penalty, hire a new corporate security director and conduct external security assessments.

Delmar, the Holtec spokesman, said the "roots" of some safety incidents "go back to when the plant was operating and under previous ownership," but declined to elaborate. The weapons manager, who was fired by Holtec last year, declined to comment.

Another incident took place in January 2020 on the reactor refueling floor — a cavernous space high up inside the building that houses the reactor, along with the gargantuan steel-and-concrete structures that protect its core. To remove these structures from the site, workers must cut them into smaller pieces.

As they were slicing the 100-ton reactor dome, the structure unexpectedly swung and struck one employee, according to an internal incident report reviewed by The Post. This person was nearly knocked down a 10-story equipment hatch, according to the two former employees, who didn't witness the incident but were briefed on it afterward.

The manager overseeing the work had been responsible for three different teams that day and his "mind may have been elsewhere," according to the report, which blamed the accident on "complacency." The report described the incident as a "near miss" but did not mention the equipment hatch or the possibility of a fall.

Delmar said the accident occurred at least 100 feet from the equipment hatch, which he said had a guardrail around it. "Incidents like this are not normal, and unsafe work practices are unacceptable for any Holtec employee or contractor at our facilities," he said.

The NRC evaluated the incident, but because it did not find any violations of nuclear safety, referred the matter to the Occupational Safety and Health Administration, Dorman said. Holtec said the company has heard nothing from OSHA, and no record of the incident could be found on OSHA's online database. OSHA declined to comment and a request by The Post for such records is pending.

In February 2021, a faulty valve for a nuclear waste container unexpectedly flew into the air, leaking contaminated water on one worker, who took an internal dose of radiation, according to a federal inspection report. This probably means the worker ingested radioactive water through the eyes, nose, mouth or skin, nuclear safety experts said. The worker did not require medical attention because the dose was below the limits for people who work with radiation, Holtec said.

The incident could have been avoided if managers had fixed a problem with the snap rings that held the valve in place, regulators said in the inspection report. Holtec had "replaced the snap rings on prior occasions due to evidence of bending of the ring" but never recorded the action in its system so it would be fixed permanently, the NRC said. The regulators called this a very low-severity violation, because it was not willful or repeated.

Holtec has since modified the valve design and conducted new training, Delmar said.

A 'gamble'

Decommissioning is an unproven business with uncertain profits. The total saved in the nation's decommissioning trust funds is currently smaller than the estimated cost of shutting them all down, according to Callan's Moriarty.

"The gamble under all of this is you can do the cleanup for less than the amount of money that's in the fund. Nobody has proved that yet," said Gregory Jaczko, an appointee of President Barack Obama who headed the NRC from 2009 to 2012.

Some of the firms buying defunct nuclear power plants in the United States are backed by private equity, an industry with expertise in purchasing unwanted assets and improving their value, often by reducing costs. TriArtisan Capital Advisors, the investment firm that partly owns P.F. Chang's and TGI Fridays, now owns the company decommissioning Pennsylvania's Three Mile Island, site of the biggest nuclear meltdown in U.S. history.

Singh founded Holtec in the 1980s, when he saw that nuclear plants were running out of space to safely store radioactive fuel, according to Joy Russell, a senior vice president at Holtec and one of the company's longest-tenured employees. A mechanical engineer who specialized in heat transfer, Singh became a pioneer of the nuclear industry by devising new systems for safely storing spent fuel rods, including metal racks that go inside cooling pools and steel-and-concrete cylinders that can store fuel for decades, Russell said in a 2020 interview.

In 2017, Holtec opened the doors of a stately new manufacturing center in Camden, N.J., that showcases Singh's accomplishments. Employees arriving at the main office building on the Krishna P. Singh Technology Campus walk by a parking space reserved for the CEO's chauffeured Rolls-Royce and into an atrium where more than 100 patents bearing Singh's name are on display.

But the Camden campus also brought controversy. After opening the facility, Singh [complained](#) to an area paper that Camden residents "don't show up to work" and "some of them get into drugs," angering community leaders in the mostly Black and Hispanic city.

Singh later apologized and said his comments were taken out of context.



The NRC has given Holtec permission to pare back safety and security requirements at its plants, including security personnel, cybersecurity, emergency planning, terrorist attack drills and accident insurance, according to documents on the agency's website. In approving these requests, the NRC has accepted Holtec's rationale that such measures are less crucial for retired plants, which experts agree do not carry the same radiological risk.

Some nuclear safety advocates say the NRC is being too deferential to Holtec and other companies. Years of research by the NRC itself shows plants are still vulnerable to a disaster after they shut down. In staff reports, the NRC has [said](#) severe accidents can result from mishandling spent fuel rods and that sites storing nuclear waste [remain vulnerable](#) to sabotage.

A test case

When Holtec announced its deal to acquire Oyster Creek, some local residents were uneasy about the plant becoming a test case for Holtec's corporate expansion, said Janet Tauro, an environmental activist who lives 20 minutes north of the plant.

"When you are dealing with highly radioactive nuclear fuel and taking apart a nuclear power plant, you have to be infallible — there is no room for mistakes," said Tauro, the New Jersey board chair of the nonprofit group Clean Water Action.

For 50 years, the plant's towering gray chimney had been one of the area's most distinctive physical landmarks. Its single reactor generated enough electricity to power 600,000 homes — roughly two New Jersey counties. With the NRC's blessing, Holtec shrank the plant's emergency response staff, documents show. The plant lowered its on-site insurance from \$50 million to \$10 million and stopped providing funds to the surrounding community for emergency equipment, staff and training, because, the company said, hazards at the site had been reduced. While rare, major accidents have occurred at nuclear waste sites with no operational reactor. In 2014, an explosion inside New Mexico's underground repository for "low level" radioactive waste items, such as contaminated clothing and tools, led to 21 workers testing positive for internal contamination and some reporting respiratory problems, according to an [investigation](#) by the Energy Department. The entire site had to close for a three-year, \$2 billion cleanup.

The NRC's Dorman said the agency still requires emergency planning measures on the premises of a shut-down nuclear plant, which he said provides ample resources to respond to accidents. However, the Federal Emergency Management Agency warned the NRC last year that having no dedicated personnel or equipment in neighboring communities "could have unfortunate consequences."

Holtec's Delmar said its exemptions at Oyster Creek "are consistent with other decommissioning sites" and "reflect the reduction in risk at each of the key points in the decommissioning process."

Last summer, Holtec finished moving all of Oyster Creek's spent fuel rods from cooling pools into dry storage containers in just 32 months — a "world record," the company said in a news release. The process normally takes five years or more, but Holtec sped it up by building a fuel canister the company says can accommodate nuclear waste at hotter temperatures. After reviewing the company's calculations, the NRC concluded it was safe to reduce the mandatory minimum cooling time to one year, filings show.

The future of waste

In an empty cow pasture in the New Mexico desert, Holtec is attempting to write the next chapter of the American nuclear story. The company is in the final stages of getting NRC approval for an "interim" waste storage site designed to secure spent fuel from around the country in a shopping-mall-size bunker for up to 40 years. In meetings with New Mexicans, Holtec representatives have said the facility would create jobs and fulfill an important national need. New Mexico Attorney General Hector Balderas (D) has sued the NRC, claiming the regulator "colluded with Holtec" by rubber-stamping its plans and ignoring potential environmental harms.

The NRC's Dorman says the agency's review of the Holtec site has been rigorous. The agency recently [approved](#) a separate, privately owned storage facility in Texas, a project that now faces legal challenges by that state. Holtec declined to comment.

"The NRC has not figured out a permanent solution" to nuclear waste, Balderas said in an interview. "They are using Holtec as a Band-Aid."

Russia moves missiles capable of carrying nuclear warheads to Finland

Source: <https://www.express.co.uk/news/world/1611075/Russia-nuclear-missiles-Finland-NATO>

May 16 – Video posted on Russian social media showed military trucks carrying Iskander ballistic missiles - which can carry nuclear warheads - moving through the country, reportedly on a highway to Vyborg, near the Finnish border.

The apparent deployment came just a day after Finland and Sweden each announced formal plans to apply for membership of Nato. Russia's foreign ministry warned yesterday that the move was a 'grave mistake' and would have 'far-reaching consequences'.

Vyborg is located just 30 miles from Finland and 135 miles from Helsinki, putting it well within missile range.





The Iskander is a short-range ballistic missile developed by Russia that went into service in 2006 to replace the Soviet-era Scud and Tochka rockets.

Iskanders are the workhorse of Russia's missile forces and can perform a wide variety of roles depending on the warhead they are fitted with.

Warheads include thermobaric, cluster, armour piercing, bunker-busters, and electromagnetic for taking out radar systems.

But the most eye-catching of the Iskander's warheads is a nuclear charge, thought to be around four times as powerful as the bomb that destroyed Hiroshima.



The Economist

The missiles have a range of up to 300 miles and are most commonly carried by road-mobile launch vehicles, which makes the missiles much harder to find and destroy. The new deployment to the Finnish border also comes as Nato began staging a huge drill in Estonia to rehearse its response to an attack from Russia.

Read:

Organized Crime, Terrorism and Nuclear Trafficking

Strategic Insights, Volume VI, Issue 5 (August 2007)

By Lyudmila Zaitseva

Source: <https://www.hsdl.org/?view&did=477914>

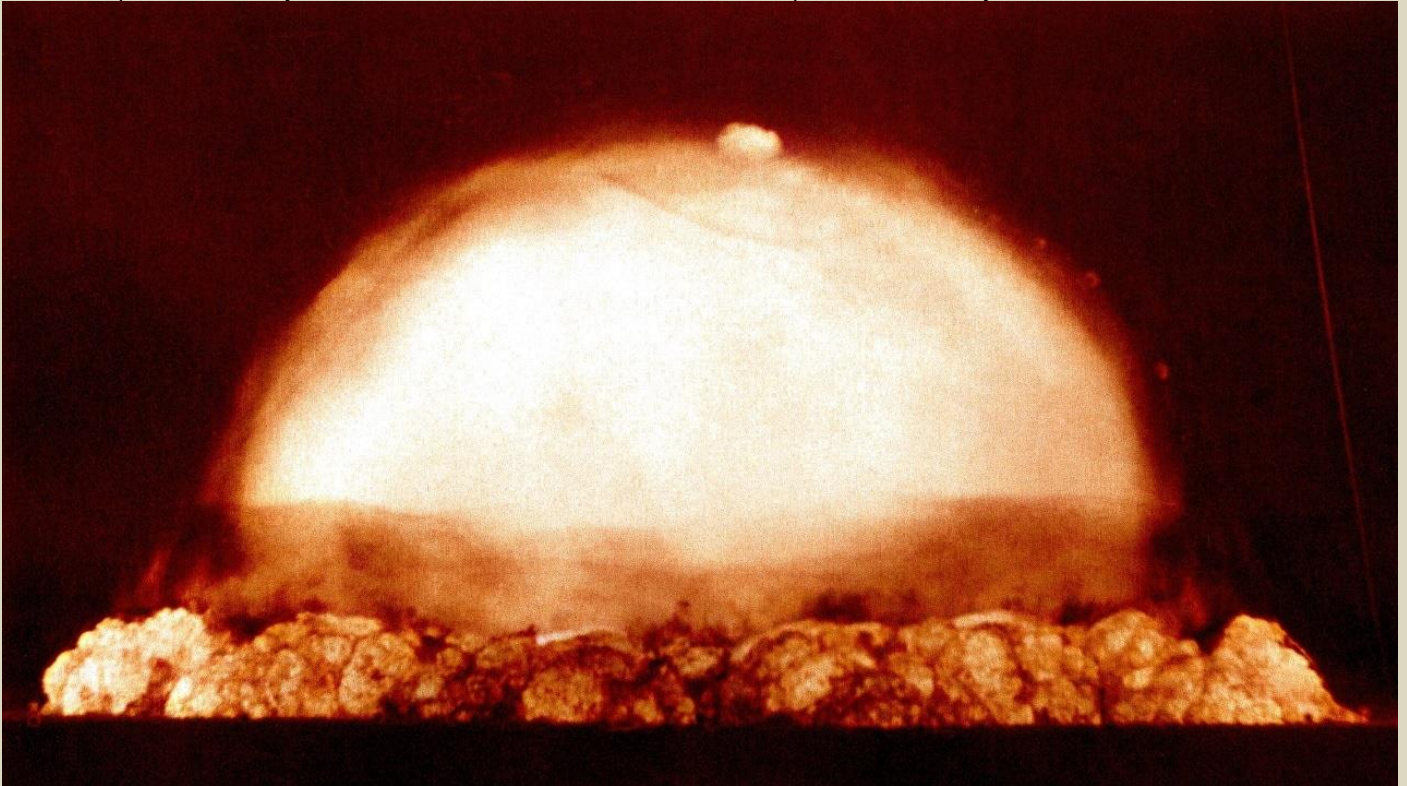
Lyudmila Zaitseva is a Center for International Security and Cooperation (CISAC) Visiting Fellow from the National Nuclear Centre in Semipalatinsk (Kazakhstan). She has worked on documentation and information about nuclear and security issues in the former Soviet Union.



Iran Armed with Nuclear Weapons: Are We Ready?

By Peter Brookes and James Phillips

Source: <https://www.19fortyfive.com/2022/05/iran-armed-with-nuclear-weapons-are-we-ready/>



Trinity nuclear weapons test. Image Credit: Creative Commons.

May 18 – The Biden administration’s [negotiations](#) with the Iranian regime about its increasingly threatening [nuclear program](#) are on the verge of collapse. After more than a year of [meetings](#), the Biden administration has failed to repair the shortcomings that prompted President Trump to [withdraw](#) from the original nuclear deal negotiated by the Obama administration in 2015.

The Vienna talks about reviving the Joint Comprehensive Plan of Action (aka JCPOA or the Iran [nuclear deal](#)) [stalled](#) in March, after Russia [demanded immunity](#) from Ukraine-related sanctions for billions of dollars it will reap for nuclear work in Iran under the deal. After the Biden administration conceded on that issue, negotiations broke down over Iran’s demand that the U.S. lift sanctions imposed on Iran’s Revolutionary Guards due to terrorism. This would have rewarded Iran with extra benefits not included in the JCPOA, which only lifted sanctions related to Iran’s nuclear efforts.

It’s not clear when—or whether—the talks will resume.

Equally disturbing, Secretary of State [Antony Blinken](#) recently testified to Congress that Iran could finish enriching the uranium needed for a nuclear weapon—aka “[breakout](#) time”—in a few weeks if it decided to do so.

That’s deeply troubling.

The “lengthening and strengthening” of the (deeply [flawed](#)) Iran nuclear deal that Team Biden promised was firmly rejected by Tehran. That means that a future nuclear crisis with the Iranian regime remains a strong possibility even if another defective agreement is reached, which itself looks increasingly unlikely.

Now is the right time to start looking at what will likely happen if the Iran nuclear negotiations fail outright.

Nuclear Power #10?

Iran has made significant progress on its nuclear program since it began openly violating the JCPOA in 2019. Tehran has exceeded the limits of the nuclear deal in a number of ways, including restrictions on the size of stockpiles of enriched uranium, levels of uranium enrichment, and the use of advanced centrifuges.

These scientific and technical resources and capabilities put Iran on the path to developing and [fielding](#) a nuclear weapon.

The failure to reach an agreement that permanently ends Iran’s nuclear aspirations would be a major diplomatic failure. It would also destabilize the Middle East and have major



repercussions for U.S. and international security, including Iran becoming a nuclear weapon state—and the trouble that comes with it.

War in the Middle East

Any evidence of Iran moving toward the development and or deployment of a nuclear weapon is expected to provoke a significant reaction in the Middle East due the threat it poses to Israel and the Iran's Arab neighbors, most notably Saudi Arabia.

It is more than likely that Israel would take military action to prevent Iran from developing a nuclear weapon by striking Iranian nuclear facilities, perhaps in cooperation (e.g., overflight rights) with equally concerned Arab partners.

It should also be expected that Iran wouldn't simply absorb the Israeli attacks without a violent response. Tehran has the largest missile arsenal in the Middle East, many of which can reach Israel's major cities.

Iran also has an ally in Syria, which hosts Iranian Islamic Revolutionary Guard Corps bases that could strike Israel. Tehran would also turn to Lebanon's Hezbollah, Gaza's Hamas and Palestine Islamic Jihad, and Iranian-controlled Iraqi militias to assist in meting out its revenge on Israel.

The Iranian regime would certainly blame the United States as being complicit in any Israeli or other attack on Iran over its nuclear program, whether it was involved or not. It should be expected that Iran and its proxies would escalate their [ongoing attacks](#) on U.S. bases and its interests overseas.

Nuclear Proliferation

Another consequence of Iran developing a nuclear weapon is that other states will face strong pressure to follow in its path. The security dilemma created by a nuclear Iran would spur a regional arms race at the conventional—and possibly nuclear—level.

While Israel is widely believed to be a nuclear weapon state, the prime candidates for a cascade of new nuclear proliferation include regional powers Saudi Arabia, United Arab Emirates, and Turkey.

Beyond the increase in regional tensions derived from an Iranian nuclear breakout, efforts at counterbalancing Iran's nuclear weapons arsenal would strain global arms control and nonproliferation treaties, regimes, and norms.

When a country becomes a nuclear weapons state, the perception of its clout, leverage, prestige, and even legitimacy are bolstered significantly, usually at the expense of others, especially regional rivals and enemies.

Due to its new nuclear deterrent, Iran would gain a new freedom of action to escalate its provocative policies, including a drive for regional hegemony, anti-U.S. and anti-Israeli policies, and its support of international terrorist organizations.

Considering Iranian aspirations, a nuclear Iran would significantly shift the balance of power in the Middle East, further destabilizing an important region that plays a critical role in supplying the world's energy.

Unfortunately, the possibility of reaching a peaceful, diplomatic solution to the threats posed by Iran's nuclear program looks remote at this moment, meaning that the United States, its allies, and partners need to start thinking about dealing with more dangerous times ahead.

Dr. Peter Brookes is The Heritage Foundation's Senior Research Fellow for Weapons of Mass Destruction and Counter-Proliferation.

James Phillips, is a senior research fellow for Middle Eastern affairs at The Heritage Foundation, has written extensively on regional issues and international terrorism since 1978.

Five reasons that Russia's nuclear exports will continue, despite sanctions and the Ukraine invasion. But for how long?

By Marina Lorenzini and Francesca Giovannini

Source: <https://thebulletin.org/2022/05/five-reasons-that-russias-nuclear-exports-will-continue-despite-sanctions-and-the-ukraine-invasion-but-for-how-long/>

May 17 – By many measures, Russia's state-controlled nuclear energy company, Rosatom, has primacy in the global nuclear energy market. At any given moment, the firm provides technical expertise, enriched fuel, and equipment to nuclear reactors around the world. The Russian invasion of Ukraine and, more acutely, the Russian military's dangerous actions at [the Zaporizhzhia nuclear power plant](#) and in [the Chernobyl exclusion zone](#) have many countries rethinking their dependence on Russian nuclear products and searching for alternatives. Additionally, the ensuing global effort to cripple Russian access to international



markets calls into question the viability of current contracts, government licensing, and financial instruments involved in Russia's nuclear exports.

Concurrently, the invasion has highlighted the lack of energy source diversification across Europe. Headlines have focused on how several European countries decided to [phase out or delay plans to build new nuclear power plants](#) in the wake of the 2011 Fukushima-Daiichi disaster and, instead, increase imports of Russian oil and natural gas to feed their [electric grids' baseload needs](#). Now, in response to the sudden European effort to minimize dependence on Russian imports, the United States has [sent tankers](#) of liquefied natural gas (LNG) to European ports. Additionally, the United States and partners are releasing a round of [oil from their strategic stockpiles](#) to stabilize market prices. For oil and natural gas supplies to Europe, there are some immediate alternatives available. However, for nuclear power plants, swapping in alternative supplies is causing serious dilemmas and could lead to stranded assets. Disdain for Russia's actions in Ukraine and current sanctions related to the invasion will ultimately exact costs from the Russian nuclear industry, but Russia's dominance in the nuclear energy market will likely endure in the short term for five main reasons.

US and EU reluctance to apply sanctions specifically to the Russian nuclear energy sector

Current US sanctions heavily target Russia, but they are not broad, geography-based designations, like the sanctioning approaches to Iran and North Korea, which target all persons and entities connected to those countries. Without a geography-based designation, various legal authorities currently form a patchwork of sanctions that target Russia in some way—but also, in practice, allow some forms of trade to occur, namely in the [energy sector](#).

Despite the Biden administration's initial [signals](#), Rosatom has yet to be sanctioned explicitly. On March 8, President Biden issued an [executive order](#) focused on inhibiting investment in the Russian energy sector. While one section of the order (“new investment in the energy sector in the Russian Federation by a United States person”) may arguably include the nuclear energy industry, the Biden administration has not yet specifically targeted Russia's mineral, fuel, or equipment exports in the United States and around the world related to nuclear power plants. Plus, the long-term contracts currently in place are not in immediate jeopardy since the executive order focuses on “new investment.”

The European Union has demonstrated similar patterns. Politico [reported](#) at the end of April that five EU diplomats disclosed that the EU is mulling placing sanctions on uranium imports from Russia. This follows [a call](#) on April 7 from members of the EU Parliament for additional punitive measures, including “an immediate full embargo on Russian imports of oil, coal, nuclear fuel, and gas.” The call more explicitly mentions nuclear and would impact current and future contracts, if enacted in its current form. That being said, no such action has yet taken place.

US and EU reliance on Russian fuel

Upon further examination of nuclear fuel supplies, the hesitation to enact an embargo becomes clear. According to the US Trade Commission, in 2019 Russia was the 20th-largest [supplier](#) of imported goods to the United States. But, the most valuable set of imported goods, sitting at a \$13 billion valuation, was mineral fuels, including uranium and enriched nuclear fuel. In 2020, imports of Russian uranium accounted for 16 percent of [uranium purchases](#) for US nuclear power plants, according to the Energy Information Administration. This is just one example of how the United States' nuclear energy industry is greatly intertwined with Russian products.

During her confirmation hearing, a senior adviser in the US Energy Department, Kathryn Huff, [told](#) the Senate's Energy and Natural Resources Committee that “[w]e need to build out capacity for a Western alternative for the Russian component of the uranium market, including conversion and enrichment capacity. There is no question in my mind that we will continue to focus on uranium as an incredibly important fuel.”

While the Energy Department may have the desire to wean US nuclear power from Russian supplies, immediate cost-effective and quick alternatives are not available on the market. Replacing Russia's uranium and related nuclear fuel services alone would require government spending of [\\$1 billion or more](#), Huff stated. Europe faces a similar quandary. The EU imports almost all its uranium from outside the bloc. And, about [20 percent](#) comes from Russia, making the country the second-largest supplier to the EU after Niger.

As of this writing, the [price of uranium](#) sat at close to \$50 per pound and peaked at \$65 in mid-April, a significant jump from around \$26 per pound in August 2021. Increasing the scarcity of uranium supply by sanctioning such products could lead to [a further shock](#) to electric grids at a moment when prices of other sources of energy are also recalibrating due to market volatility.

In addition to legacy fuel sources, [advanced reactor demonstrations](#) expected to come online around 2028 require high-assay, low-enriched uranium (HALEU), which is enriched to contain a higher percentage of the fissile uranium 235 isotope than commercial nuclear power reactors now use. Russia is currently the [singular viable commercial supplier](#) globally of HALEU, and other firms look to be years away from readily providing such fuel. It wasn't until 2021 that Centrus Energy Corporation became the [only licensed HALEU production facility](#) in the United States. The Department of Energy has announced that the company is on track to [produce fuel](#) by this summer.



To address the nuclear fuel situation, on April 7, US senators Joe Manchin and Jim Risch [introduced](#) the [International Nuclear Energy Act of 2022](#). Among other goals, the bill aims to create a Nuclear Fuels Security Initiative that would reduce and eventually eliminate reliance on Chinese and Russian nuclear fuel. If this bill passes, then the US domestic nuclear industry may be better positioned to absorb the consequences of a ban on Russian nuclear products and, in turn, also act as a global supplier. But even if passed and signed into law, this initiative may take several years to be realized.

Most destination countries continue to import nuclear products from Russia

Except for a few circumstances, most countries and companies are continuing their contracts with Russian nuclear companies, whether they are facing public pressure to decouple themselves from the Russian economy or not. These contracts involve many aspects of nuclear power plant construction, operation, and maintenance.

Fuel delivery. For instance, Sweden's nuclear energy company Vattenfall AB, [announced](#) on February 24 that it would not place new orders with Russian companies for nuclear fuel until further notice. In the announcement, the President and CEO Anna Borg noted that the firm has secured alternative deliveries of nuclear fuel. Vattenfall sources its uranium supplies from Australia, Canada, Kazakhstan, and Namibia. So, the decision to not place new orders with Russian companies did not create a significant disruption for procurement of fuel.

Government licensing and project finance. Since the Russian invasion of Ukraine, Finnish officials [have questioned](#) the viability of the planned construction of the Hanhikivi nuclear power plant. The dispute hinged on whether the government would grant a construction permit. A Finnish-Russian consortium (called Fennovoima) commissioned the plant, in which Finnish stakeholders such as Outokumpu, Fortum, and SSAB own two thirds, with Rosatom's subsidiary RAOS Voima holding the remainder. Fennovoima had expected to obtain a construction license from the government by this summer to build the 1.2-gigawatt (GW) reactor, while construction was expected to begin in 2023. In a statement, Rosatom and RAOS Project stated that they would continue to fulfill their obligations from signed agreements and contracts relating to the Hanhikivi I project. On May 2, Fennovoima [terminated](#) the existing contract with RAOS, demonstrating a willingness to absorb financial costs. However, such costs were rather minimal in comparison to the consequences that could have been incurred if the plant were already operating.

Other countries and/or companies may not be in the position to accept the costs of quickly pivoting away from Russian provisions. In fact, even NATO members like Slovakia, Hungary, and Turkey are continuing their operations with Rosatom. These countries house Russian-made nuclear reactors, for which [there is no authorized nuclear](#) fuel alternative to the Russian supply, and terminating a partnership with Rosatom could mean temporarily halting operations at the facility.

Mining and fuel delivery. While Slovakia has said that it has enough nuclear fuel to last through the end of 2023, a ban on Russian imports would be an impending challenge. "This is very concerning as we are 100 percent dependent on Russian nuclear fuel deliveries from the company TVEL," [said](#) Karol Galek, Slovakia's state secretary for energy in the Ministry of Finance. Slovakia has notable uranium deposits in east of the country. But when Canada's Tournigan Energy showed interest in [investing in mining uranium](#), citizens strongly protested in [2006](#) and again in [2013](#). According to amendments in 2010 to Slovakia's [Geological Act](#), citizens of nearby villages can reject an application for uranium exploration. Plus, even if citizens agreed or the government were to further amend the law, it could take several years to start mining operations.

Fuel delivery, loan disbursement, and facility expansion. In Hungary, the challenge goes beyond the fuel itself. Even after opposition parties called for Prime Minister Viktor Orbán to cancel a roughly 12.5 billion euro (\$13.84 billion) deal with Rosatom, Foreign Minister Peter Szijjarto [announced](#) on March 2 that no such action would take place. The deal is set to build another two reactors at the Paks plant to replace the capacity of the current units. The two current reactors are set to be shut down between 2032 and 2037. The existing 2-gigawatt plant, consisting of two Russian-made VVER reactors, accounts for about half of Hungary's electricity generation and was largely financed by a [Russian state loan](#). In fact, even in the thick of the Ukraine war, on April 7, Hungary [received](#) the first shipment of nuclear fuel for Paks nuclear plant from Russia.

In Hungary, not only is Paks reliant on Russian nuclear fuel, but the country also already has contracts in place to expand the facility and finance the project with Russia. This circumstance brings to the fore another traditional strength of the Russian nuclear industry: state-backed financing. For years, Russian companies have out-maneuvered competitors and secured lucrative deals due to their state-backed financing offerings. Many other companies—including Framatome, Mitsubishi Heavy Industries, Siemens, and Westinghouse—typically require robust financial guarantees, partnership arrangements, and power purchase agreements to satisfy their own corporate business standards. Not only is the Paks plant already fit to comply with Russian products, but no other nuclear company or state is likely willing to match the Russian offer.

Russia offers extensive and generous financing structures

In ways not fully realized in Hungary yet, the Akkuyu nuclear power plant in Turkey demonstrates the aggressive financing capacities embedded within the Russian nuclear export strategy. Unlike in Finland, Hungary, Slovakia, and the United States, Turkey's



partnership with Russia involves the ongoing construction of an [estimated \\$22 billion](#) nuclear power plant. (Rosatom would build four VVER-1200 generation 3+ reactors, producing 1.2 gigawatts each.) This plant is set to provide 10 percent of Turkey's annual electricity needs, with the first reactor [undergoing installation](#) and [scheduled](#) to be online in 2023, the 100th anniversary of the founding of the Republic of Turkey, with the other three units to follow by 2026. Even with the ongoing war in Ukraine, on March 16 Rosatom [delivered](#) the main components of a turbine plant, including a stator, turbine generator rotor, and low-pressure cylinder. With such a lucrative and symbolic deal in process, Turkey is unlikely to pull the plug.

The Akkuyu plant was made possible by an innovative Russian creation previously unseen in the nuclear industry: the build-own-operate investment model. After decades of unfruitful efforts to attract foreign nuclear power companies to build Turkey's nuclear energy infrastructure, the Turkish government took a new approach in May 2010—[direct talks](#) between the Russian Federation and the Republic of Turkey that led to an intergovernmental agreement within the same year.

The “build” step of the model is made possible by the Russian-established project company in Turkey called the Akkuyu Nuclear Joint-Stock Company, with stakeholders consisting of Russian companies: Rosatom Energy International JSC (74.915 percent), Rosenergoatom JSC (21.948 percent), Atomstroyexport CJSC (2.267 percent), Inter RAO UES JSC (.820 percent), Atomtechenergo JSC (.025 percent), and Atomenergoremont JSC (.025 percent). Through the stakeholders, Russian banks provide loans to the Akkuyu Nuclear Joint-Stock Company. And some of the banks haven't fared so well under the current U.S. sanctions regime.

To name a few: In 2021, Sberbank announced it would provide a [loan of \\$800 million](#) for a period of seven years to construct the four units at the Akkuyu plant. On February 24, the Biden administration placed sanctions on [Sberbank](#), Russia's largest state-owned bank, which holds a third of all bank assets in Russia. In early May, European Commission President Ursula von der Leyen [announced](#) that the EU will move to cut Sberbank from the SWIFT international payments system.

Sovcombank has also been involved in Rosatom's construction of Turkey's Akkuyu plant, announcing [\\$300 million in loans](#) in March 2021. A year later, the [company](#) and [executives](#) were put on the sanctions list administered by the US Treasury's Office of Foreign Assets Control. Also, as of March 12, Sovcombank will [no longer have access](#) to the Belgium-based SWIFT financial messaging service. Undoubtedly, sanctions will impact the overall financial health of the banks and their ability to continue operations as before. But it remains unclear, based on information in the public press, how the banks have adapted to the current sanctions. Will they be able to fulfill the announced loans in full? What actions are the countries and companies involved taking to shield themselves from [potential exposure](#) to the US sanctions regime? Will companies or countries seek a sanctions waiver from the United States or EU to continue this specific kind of cooperation? Beyond those questions, it also remains unclear to what extent the Biden administration or the EU will prioritize pursuit of sanctions violations on Slovakia, Hungary, or Turkey for their current cooperation with Russian nuclear entities and associated financing vehicles. Only time will tell how sanctions will directly or indirectly impact the banks' ability to deliver on the project finance agreements.

In the event of a halt to construction at the Akkuyu site, whether due to bankruptcy or an import embargo, Turkey would inherit a serious stranded asset problem.

No other supplier is prepared to quickly operate a Russian facility

To date, India has not imposed [any sanctions](#) against Russia. Nonetheless, there is great debate on the extent to which [secondary sanctions](#) could affect India. India hosts two Rosatom-built [reactors](#) (Kudankulam 1 and 2) that are connected to the electric grid and a desalination plant. Rosatom [provides](#) the enriched fuel for this site, and construction is underway for an additional four reactors on the site. If the connection to Rosatom were to be severed, who would supply spare parts for the two operating reactors, which up to now came from Rosatom? Will operation of those two plants cease, at least for a while? And how would work on the four new reactors go forward? If ties with Rosatom were to be cut, the Indian reactors could well become stranded assets. Iran's Bushehr reactor provides a historic example of just how costly such orphaned nuclear facilities can become.

In 1975, West Germany's Kraftwerk Union AG [signed contracts](#) to build a 'turnkey' nuclear power plant and deliver nuclear fuel for the reactor units at Iran's Bushehr nuclear power plant. But in 1979, [construction was interrupted](#) by the fall of the Shah and the Islamic Revolution. Such political conditions, followed by the Iran-Iraq War (1980-1988), dissuaded Kraftwerk Union from continuing operations. It wasn't until 1995 that Iran could solidify a renewed effort on the reactors, via [a contract](#) for approximately \$800 million with the Russian Federation Ministry for Atomic Energy (Minatom) to complete Bushehr's Unit 1, a Russian VVER pressurized water reactor. Because of a variety of difficulties in meshing the work done under the German contract with the Russian reactor, the first Bushehr unit didn't reach [100 percent power generation capacity](#) until August 2012—37 years after the original contracts were signed. The Bushehr site suggests just some of the difficulties that any number of Russian built, operated, or supplied reactors could face, if sanctions were to force plants to cut ties with Rosatom and/or Russian financing vehicles.

The facilities could then also become stranded assets, a source of millions of dollars in lost revenues, to say nothing of the secondary impacts related to the delay in provision of electricity to surrounding populations. Given those impacts, it is likely that most countries



with Russian reactors will continue working with Rosatom in the near term, and perhaps longer.

Will Rosatom be able to reach new nuclear agreements?

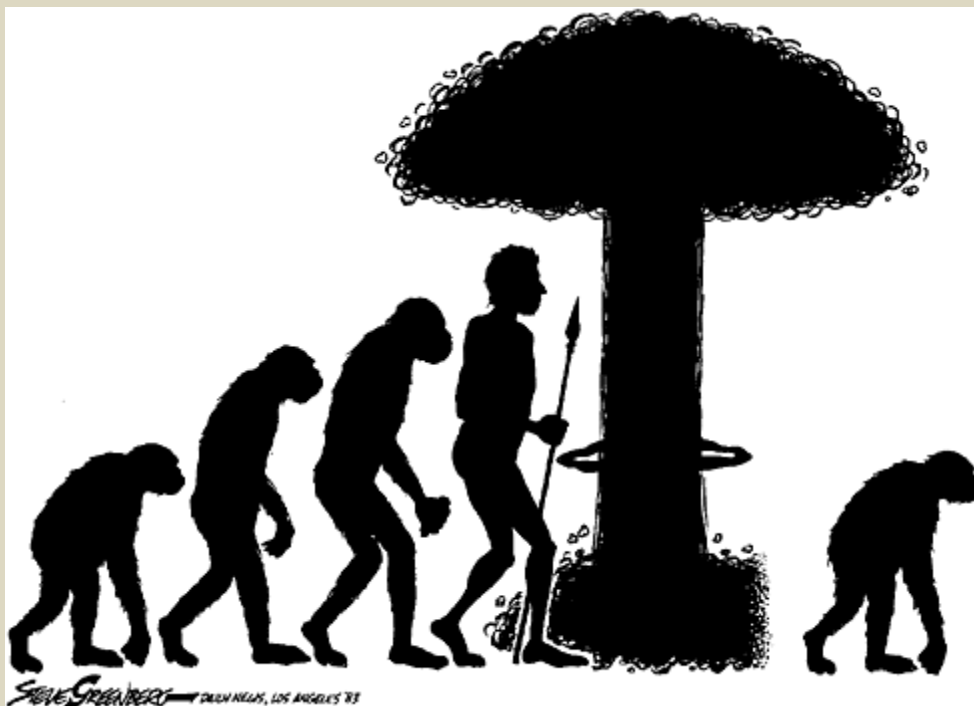
In the short term, the Russians will likely retain most of their nuclear-related commercial agreements and remain a strong player in the global nuclear market. Finland and Sweden seem to be outliers in the field. Still, the political pressure is mounting, and countries may put forth the necessary investments in the coming years to disentangle themselves from Russian provisions. Future long-term contracts with Russian entities may no longer be seen as vital.

Given the political environment and potential loss of revenue streams, Russia has attempted to flex its muscles. To bolster its own currency, it is possible that Russia could sway countries to develop mechanisms to pay in [rubles](#), as we have seen in the oil and natural gas market. Plus, Russian Deputy Prime Minister Alexander Novak announced that Moscow is considering [banning exports of Russia uranium](#) to the United States in retaliation for sanctions. Would Moscow do the same for the EU bloc or any country speaking out against Russian atrocities in Ukraine?

Nonetheless, if Russia cannot continue to fulfill generous loans as sanctions shrink Russian reserves, Rosatom's immense strategic commercial advantage over competitors—France's Framatome and Japan's Mitsubishi Heavy Industries, among others—could be diminished. In this event, other companies may be able to make a stronger case for their products and gain market share in the global nuclear energy industry.

Marina Lorenzini is the project coordinator with the Project on Managing the Atom at the Belfer Center for Science and International Affairs at the Harvard Kennedy School of Government. Her research focuses on arms control agreements, critical infrastructure vulnerabilities, and sanctions across the Eastern Mediterranean and Persian Gulf regions. Prior to joining the Belfer Center, she held positions at McLarty Associates, the Nuclear Threat Initiative, and the International Human Rights Clinic at Harvard Law School. Marina holds a master degree in Law & Diplomacy from the Fletcher School at Tufts University.

Francesca Giovannini is the executive director of the Project on Managing the Atom at the Harvard Kennedy School's Belfer Center for Science & International Affairs. In addition, she is a non-residential fellow at the Centre for International Security and Cooperation at Stanford University. Giovannini served as Strategy and Policy Officer to the Executive Secretary of the Comprehensive Nuclear Test Ban Treaty Organization (CTBTO), based in Vienna. Prior to her international appointment, Ms. Giovannini served for five years at the American Academy of Arts and Sciences in Boston as director of the Research Program on Global Security and International Affairs.



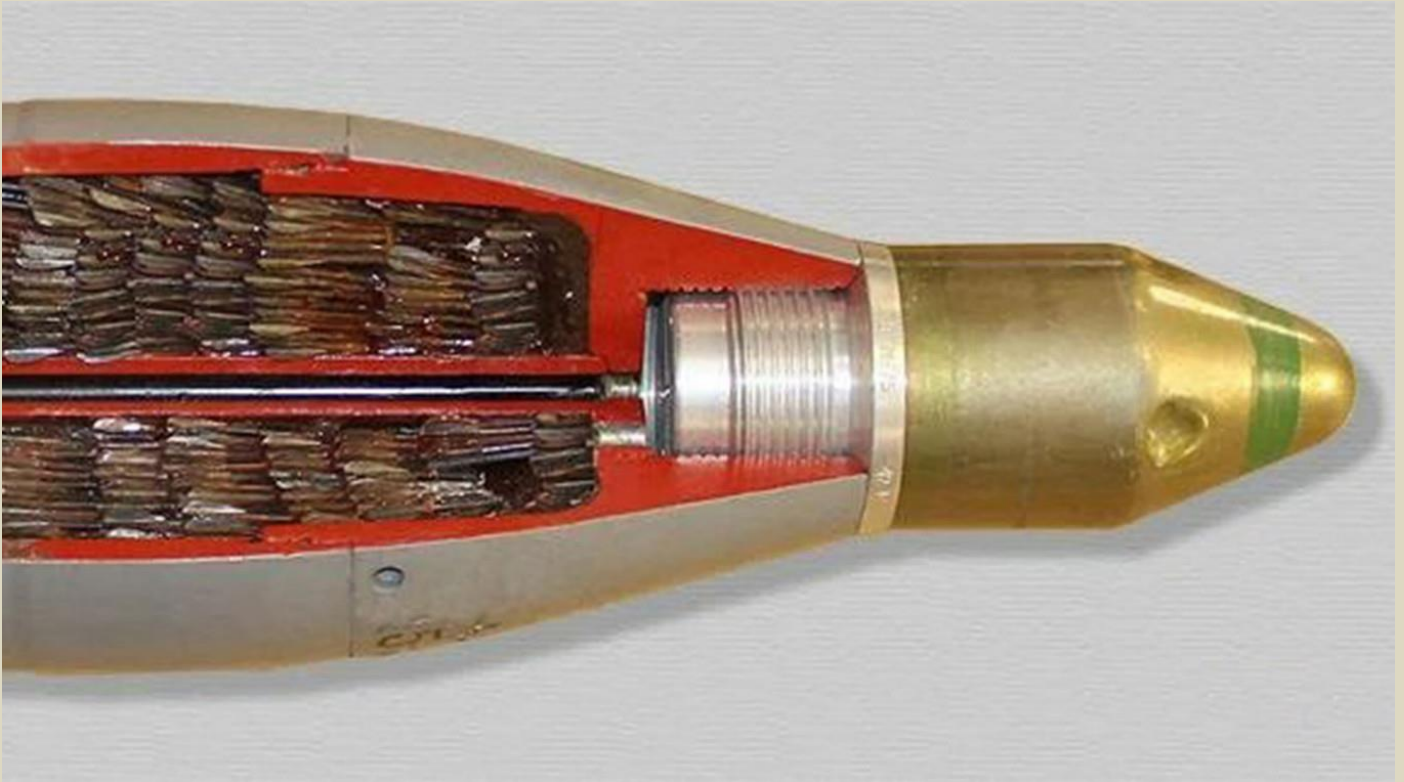
ICI
International
CBRNE
INSTITUTE



EXPLOSIVE NEWS

Dozens of Bucha residents were killed by flechettes. This ammunition was used in the First World War

Source: <https://hindustannewshub.com/russia-ukraine-news/dozens-of-bucha-residents-were-killed-by-flechettes-this-ammunition-was-used-in-the-first-world-war-the-moscow-times-in-russian/>



Apr 25 – Dozens of civilians who died during the Russian occupation of the Ukrainian city of Bucha were killed by flechettes, small metal darts. According to The Guardian, citing forensic experts, Russian artillery shells were stuffed with them.

“My colleagues and I have found several thin, nail-like objects in the bodies of men and women in this region. They are very difficult to find in the body, they are too thin. Most of the bodies were brought from the Bucha-Irpensky district,” Ukrainian forensic expert Vladislav Pirovsky told The Guardian.

Independent weapons experts who examined photographs of metal arrows found in the bodies confirmed that they were flechettes. During the First World War, they were actively used by the armies of Kaiser Germany and the Russian Empire. Flechettes in packs or cassettes were dropped from aircraft onto enemy infantry or cavalry. Due to its shape, a flashette dropped from an aircraft closer to the ground accelerates enough to break through a board up to one and a half centimeters thick. In modern artillery, flechettes are used as ready-made submunitions in some projectiles. **Such ammunition is in service with the US Army (XM580E1) and Russia (3Sh1 projectile with swept GGE, used as part of the 3VSh1, 3VSh3 and 3VSh4 rounds).**

A modern projectile can contain up to 8,000 flechettes. Once fired, the projectiles explode, releasing projectiles above the ground. Flechettes can hit a target at a distance of



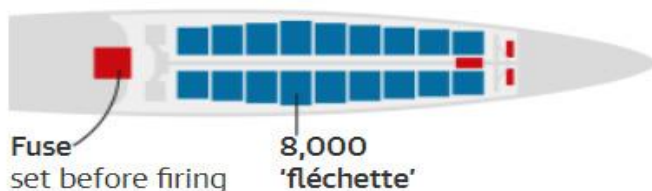


Getty Images

up to 300 meters from an exploding projectile. When hit in the body of the victim, the dart can lose its rigidity, bending into a hook, and part of the plumage can break off and cause additional injuries.

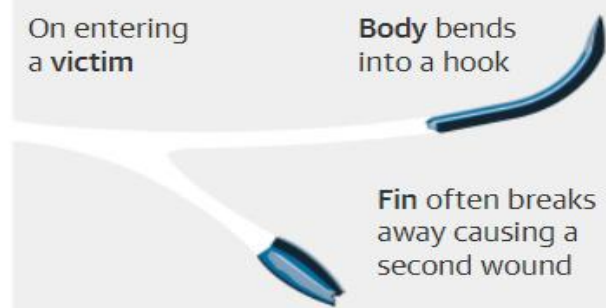
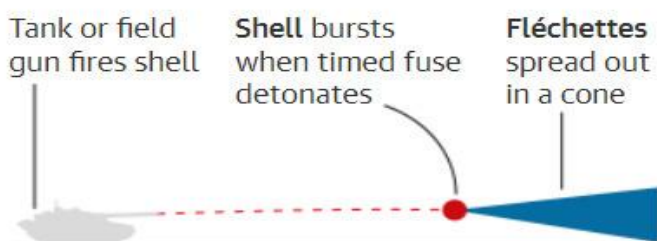
How flechettes work

M546 APERS-T 105mm shell



One of the 8,000 steel flechettes

About 25mm long



Guardian graphic. Source: FAS

Human rights groups have long sought a ban on the use of arrow-shaped projectiles, but these munitions are not prohibited by international law. The use of lethal inaccurate weapons in densely populated civilian areas is a violation of humanitarian law, they recall.



Saint Javelin – war side effects!



Saint Javelin named after the American-made portable anti-tank missile system FGM-148 Javelin

Recognizing the IED Threat – Awareness is Key

By Mr. Richard Carrick

NCT Magazine 5/17

Source: <https://nct-magazine.com/nct-magazine-april-2022/recognizing-the-ied-threat-awareness-is-key>

When considering IED and other explosive threats, the first group that comes to most people's mind is EOD or Bomb Squad. However, the first person to encounter on an IED is rarely an EOD technician, but is likely rather a civilian, law enforcement, or a non-EOD certified soldier. While a First Responder is a trained professional, any of these persons is the true "first responder" in an IED situation. Understanding the components and indicators of a potential IED are crucial first steps in



countering IEDs, giving you the tools to protect yourself and recognize when to call for help from a certified EOD tech. Before we review the physical IED components and characteristics, it is also important to understand what it means to be in a “potential IED environment”. While there are certainly high-risk areas for IEDs, such as active war zones and specific territories with a history of IEDs, it is realistic to accept that almost any location can be a target for an attack. Churches, train stations, sporting events, and other similar places have all been subject to active IED events in recent years. Even inside an airport in locations after security checkpoints, there are announcements to be aware of any abandoned baggage or other suspicious activity. It is valuable to consider your surroundings in terms of a risk percentage, whereas your suburban playground would likely be a lower risk than the subway car in Washington, DC, but ultimately the possibility of an IED attack is never zero percent.

Now that we know when we can potentially be in an IED environment, what does it mean to “See Something, Say Something”? Essentially, if you see something suspicious you should say something to an official (police officer, security team, etc.). Suspicious behavior is a broad topic that can be viewed through a range of topics, however a brief overview on how suspicious behavior pertains to IEDs is valuable to discuss. To start, IEDs can be deployed by a terrorist in several ways:



These examples are not comprehensive, and IEDs can be deployed in almost any fashion imaginable.

- ❖ Person-borne (Suicide vests, backpacks/luggage, hand-thrown munitions May be victim activated (“booby trapped”), remotely detonated, or initiated by terrorists as a suicide device)
- ❖ Vehicle-borne (Motorcycles to large cargo trucks May be driver initiated or attached to a vehicle without the driver’s knowledge)
- ❖ Mail (Small envelopes to large packages)

These examples are not comprehensive, and IEDs can be deployed in almost any fashion imaginable.

●► [Read the full article at the source’s URL.](#)

Richard Carrick is the Vice President of Sales for Inert Products and MAC 7 Training and has over 15 years of experience in providing tailored training solutions to military organizations around the world. He leads a team that includes former US and international military on projects on IED & ordnance recognition, EOD equipment, and CBRNe training. He has established ongoing contracts with the United Nations, US General Services Administration (GSA), and over 30 international distributors. Richard also works with these organizations to develop custom product solutions, including replica training aids, kitting solutions, and curriculum.

We should not forget the dangers hiding under Afghan soil

By Charlotte Slente

Source: <https://www.aljazeera.com/opinions/2022/4/24/we-should-not-forget-the-dangers-hiding-under-afghan-soil>

Apr 24 – Today, due to displacement, economic collapse, and a disintegration of social services including health and education, most Afghans are living in increasingly precarious conditions. **Up to 23 million Afghans are facing acute hunger – more than half of the country’s population.** As the world is rightfully looking at Ukraine, we must not forget Afghanistan.

The current humanitarian crisis in Afghanistan is to some extent the result of the international sanctions introduced after the fall of the Afghan government last August. While sanctions can be a legitimate political tool, they must not put civilians at risk.

Some threats these sanctions pose to the lives of Afghan civilians are very visible, but others are hidden under the soil – waiting to explode.

Decades of conflict have littered Afghanistan with land mines and other explosive remnants of war. As a result, today the country is one of the most contaminated in the world.

A few weeks ago, four children lost their lives in Herat, Afghanistan when an old grenade exploded in their hands. A couple of months ago, [nine children perished in a similar accident](#) in the village of Degnan in Nangahar Province.

Since the beginning of 2022, many more have been killed, hurt and wounded in this way. In 30 years, [more than 41,000 civilians have lost their lives to unexploded ordnances.](#) In 2021, [79 percent of the victims were children.](#)





An Afghan Police official detects and removes land mines in Maiwand district of Kandahar, Afghanistan, July 16, 2017 [Muhammad Sadiq/EPA]

Together with local partners, DRC has worked with humanitarian mine action in Afghanistan since 1999 – conducting mine clearance activities, destroying unexploded ordnance from old battlefields, and providing risk education to civilians to teach them how to avoid being harmed. First and foremost, to save lives, but also because de-mining operations are crucial for Afghanistan's future. Without de-mining, Afghans harmed by decades of war cannot build themselves a safe future in their country. Without effective de-mining operations, farming cannot happen, internally displaced people cannot return to their villages, and education cannot be effective as children cannot go to school.

Now, the efforts to clear Afghanistan of mines and unexploded ordnances are hanging by a thread. With the current international sanctions, it is a more difficult task than ever before to get specialised mine clearance tools into the country. So there is a risk that lifesaving Afghan-led de-mining activities will have to be radically scaled down.

The pressures introduced by sanctions may soon result in the collapse of Afghanistan's de-mining ministry. Such a collapse would be a painful setback for the people of Afghanistan and for the efforts to clear their land of dangerous remnants of war. Capacities built and knowledge gathered over decades could suddenly be lost. The vast majority of the ministry's employees have been in their jobs for years and have worked tirelessly in partnership with the international mine clearance community. Regardless of who is in power in the country, these employees deserve investment and support.

Paradoxically, the risk of collapse is happening at a time where there is a momentum to increase the space in which we can work, and to expand operations into areas that have been left contaminated by deadly weapons for too long. With the decrease in fighting since August 2021, there is now greater access to communities and more of the country than ever before. We are standing in front of a unique window of opportunity to scale up de-mining work, with the potential to save countless lives. It is an opportunity we must seize.

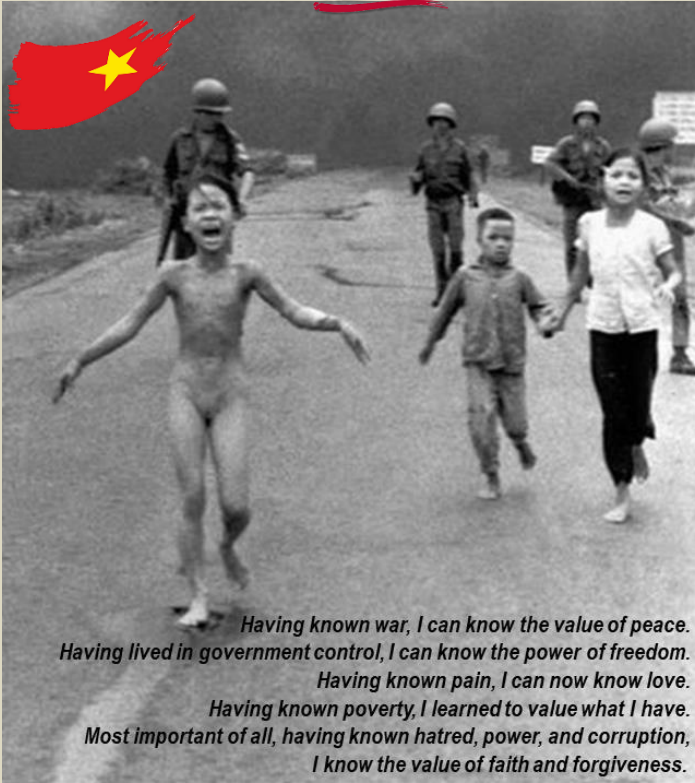
To do this, there is an urgent need for restoring international support to the people of Afghanistan and for immediately introducing sanctions exemptions that clearly allow for the full resumption of de-mining operations in the country. For the sake of Afghanistan's people, the international community should urgently seek ways to engage with and not turn its back



on the successful efforts to build up the country’s de-mining capacity. It is time to act and to implement flexible financial solutions to help sustain the efforts of brave Afghans working to clear their land of mines.

Charlotte Slente is the Secretary General of the Danish Refugee Council (DRC).

The Napalm Girl



*Having known war, I can know the value of peace.
Having lived in government control, I can know the power of freedom.
Having known pain, I can now know love.
Having known poverty, I learned to value what I have.
Most important of all, having known hatred, power, and corruption,
I know the value of faith and forgiveness.*



Kim Phuc

Phan Thị Kim Phúc OOnt, referred to informally as the Napalm girl, is a South Vietnamese-born Canadian woman best known as the nine-year-old child depicted in the Pulitzer Prize-winning photograph taken at Trảng Bàng during the Vietnam War on June 8, 1972.

Jack Russell, Patron, becomes Ukrainian war hero

Source: <https://www.news.com.au/lifestyle/home/pets/jack-russell-patron-becomes-ukrainian-war-hero/news-story/388d4aa580159a33045cf024e6f94c6b>

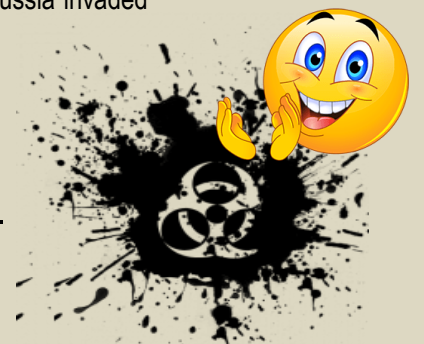


May 02 – This pint-sized dog may be only two years old, but he has earned himself a cult following thanks to his hard work saving lives.

Originally bought as a pet, the life of Patron the Ukrainian Jack Russell was turned upside down when Russia invaded the country on February 24.



Instead of days snuggled with his owner, **two-year-old Patron** (which means “cartridge” or “shell” in Ukraine) was trained to sniff out bombs, missiles and other explosive weapons.



ICI C²BRNE DIARY – May 2022

To date he has sniffed out more than 150 devices, and saved countless lives in the process.

Dressed in his signature State Emergency Service's vest, Patron works with his owner Misha, from Chernihiv, northern Ukraine, and has appeared on the social media accounts of the country's SES, Ukraine's Ministry of Foreign Affairs and the Ministry of Culture and Information Policy of Ukraine.



Misha originally bought Patron from a colleague as a gift for his son, however he was formally trained to find traces of gunpowder around a month into the invasion. Once he's detected the scent, Patron alerts Misha, who is then able to defuse the explosive.

"[Patron] works 24/7, as does a group of pyrotechnicians, and it will take about a year-and-a-half to clean up the city," Misha told US breakfast show, [Today](#).

"He can inspire anyone with his appearance and eyes."

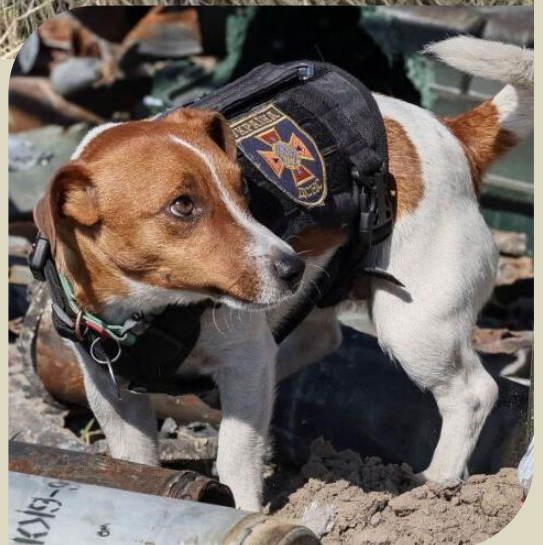
The little dog's energy is so infectious that he's even found an enthusiastic international following, with a line of merchandise which includes stickers on Red Bubble and T-shirts from Support Ukraine.

The Jack Russell is one of more than 600 de-miners working across Ukraine to dismantle the mines, bombs and missiles left by Russia soldiers.

Patron's Instagram boasts more than 187,000 followers, with his dedicated fans sharing drawings of him. Jack Russells are one of the best dog breeds at detecting bombs thanks to their strong sense of smell and background as a hunting dog.

Their lightweight build also means they aren't likely to set off the explosions.

Other breeds suited to the job include German shepherds, labrador retrievers and Belgian malinois (also known as Belgian shepherds)



3DX-Ray

Press Release

Source: <https://counteriedreport.com/3dx-ray-launches-a-range-of-3dx-eod-suits/>

3DX-Ray, specialists in X-ray imaging technology for the security and military markets, have announced the launch of a 3DX range of EOD Bomb Disposal Suits.



They are the 3DX-EOD Bomb Disposal Suit and the 3DX-Search Suit.

The 3DX-EOD Bomb Disposal Suit is a contemporary up-armoured suit offering arguably the best value and highest level of protection. Designed from the outset to be 3E (Economic, Efficient & Effective) compliant, the 3DX suit arguably provides the best value and the highest level of protection of any comparable bomb suit currently manufactured, offering maximum comfort and flexibility to the operator.

The 3DX-Search Suit has been designed specifically for personnel involved in the searching for, and clearing of, suspected terrorist explosive devices. This suit does not offer the higher protection of the EOD Bomb Disposal Suit, it is much lighter in weight, provides all-round 360° protection, whilst at the same time being comfortable to wear and allowing virtually unrestricted movement.

3DX-Ray's Interim CEO, Vince Deery said: "We are talking to both military and civilian EOD customers on a daily basis, and it became clear from

these conversations, that with so many suppliers of equipment available on the market, it is difficult for operators to identify what equipment and suppliers meet the necessary standards of safety and performance that is required, in what are real life and death operational scenarios. There was an obvious need for whole range of EOD equipment from a 'trusted supplier'. We therefore started working with our partners to develop a range of 3DX EOD suits that meet the internationally recognised Standard NATO Agreement (STANAG) 2920. And today I'm pleased to say we have now launched our new range."



●► You can download the product range datasheets at: <https://www.3dx-ray.com/products/security/eod-iedd-equipment/>

Car crashes into Boris Johnson's £1.3 million townhouse in south London

Source: <https://metro.co.uk/2022/05/09/car-crashes-into-boris-johnsons-1-3-million-townhouse-in-south-london-16614710/>

May 09 – A driver crashed into the front garden of Boris Johnson's £1.3 million house in south London in the early hours of this morning. Debris was left strewn across the driveway after the black Vauxhall Astra ploughed into a bush.

Neighbours in Camberwell said the collision at around 1am sounded like 'thunder'.

The car, which was finally towed away at around 5pm, damaged hedges and a tree, and knocked down a small pillar in front of the house.

The driver suffered minor injuries, and appeared to be retrieving his possessions from the side door of the vehicle before it was towed away.

A spokesman for the Metropolitan Police said: 'Officers attended and found a car that had struck the exterior of a property causing minor damage.'



'The driver of the car sustained a minor injury and was assessed by paramedics, but did not require hospital treatment. No offences were identified.'

The prime minister bought the four-bedroom property with his wife Carrie Johnson for £1.2 million in July 2019, according to Land Registry documents.

The Times reported the house was paid for using a buy-to-let mortgage and was undergoing renovation.

The register of MPs' interests states that the PM, who currently resides in Downing Street, has a rental income of at least £10,000 a year.

EDITOR'S COMMENT: What if it was not an ordinary accident but a **VBIED**? Most probably, an empty plot! Sidewalks need fortification; same for windows and doors (glasses) and perhaps something to be installed behind the bushes. They do have a security service or something like that? Don't they?

Flood of weapons to Ukraine raises fear of **arms smuggling**

Source: <https://www.washingtonpost.com/national-security/2022/05/14/ukraine-weapons-trafficking/>

May 14 – President Biden is expected to sign a \$40 billion security-assistance package in the coming days that will supercharge the flow of missiles, rockets, artillery and drones to a war-torn Ukraine.

But what remains unclear is Washington's ability to keep track of the powerful weapons as they enter one of the largest trafficking hubs in Europe.

Ukraine's illicit arms market has ballooned since Russia's initial invasion in 2014, buttressed by a surplus of loose weapons and limited controls on their use.

This uncomfortable reality for the United States and its allies comes amid urgent pleas from Ukrainian President Volodymyr Zelensky to provide artillery needed to counter Russian forces in the country's east and south. The Ukrainian leader's appeals are credited with uniting House lawmakers behind the latest funding request in a [bipartisan 368-to-57 vote](#) on Tuesday. But the unprecedented influx of arms has prompted fears that some equipment could fall into the hands of Western adversaries or reemerge in faraway conflicts — for decades to come.

"It's just impossible to keep track of not only where they're all going and who is using them, but how they are being used," said Rachel Stohl, an arms-control expert and vice president at the Stimson Center.

A State Department spokesman said the United States has conducted thorough vetting of the Ukrainian units it supplies while forcing Kyiv to sign agreements that "do not allow the retransfer of equipment to third parties without prior U.S. government authorization." But the means of enforcing such contracts are relatively weak — and made even weaker by Washington's own mixed history of compliance, as recently as last month.

In mid-April, the United States boosted its involvement in the Ukraine conflict by announcing that it would transfer [a fleet of Mi-17 helicopters](#) to Ukraine that it originally purchased from Russia about a decade ago. The initial sale of the aircraft required the United States to sign a contract promising not to transfer the helicopters to any third country "without the approval of the Russian Federation," according to a [copy](#) of the certificate posted on the website of Russia's Federal Service on Military-Technical Cooperation.

Russia has denounced the transfer, saying it "grossly violates the foundations of international law."

Arms experts say Russia's brutal aggression in Ukraine more than justifies U.S. support, but the violation of weapons contracts chips away at the foundations of counter-proliferation efforts.

"Breaking of those end-use agreements is a serious threat to the underlying, but weak, capacity for countries to control how weapons are used," said Jeff Abramson, an expert on conventional arms transfers at the Arms Control Association.

A Pentagon spokesman dismissed the criticisms, calling Russian charges a distraction and the transfer "permissible under U.S. law and consistent with our national security priorities."



“Russia’s claims are a disingenuous attempt to distract attention from Russia’s unprovoked invasion and its history of aggressive actions against Ukraine since 2014,” said Marine Corps Lt. Colonel Anton T. Semelroth.

The job of ensuring U.S. weapons are used for their intended purpose — a joint responsibility of the departments of State and Defense — is made all the more difficult by the sheer volume of arms making their way to Ukraine.

The emergency spending bill awaiting approval in the Senate will cement Ukraine’s status as the world’s single largest recipient of U.S. security assistance, receiving more in 2022 than the United States ever provided to Afghanistan, Iraq or Israel in a single year. It will add to the stocks of [weapons the U.S. already committed to Ukraine](#), including 1,400 Stinger anti-aircraft systems, 5,500 anti-tank missiles, 700 Switchblade drones, 90 long-range Howitzers artillery systems, 7,000 small arms, 50,000,000 rounds of ammunition, and numerous other mines, explosives and laser-guided rocket systems.

Shoulder-fired Stinger missiles, capable of downing commercial airliners, are just one of the weapon systems experts worry could slip into the possession of terrorist groups seeking to carry out mass-casualty events.

The Biden administration’s funding request includes \$8.7 billion to replenish U.S. stores of weapons shipped to Ukraine, \$6 billion to train and equip Ukrainian forces and \$3.9 billion for U.S. forces deployed throughout Europe in response to the security crisis that’s been set off by the war.

Other NATO countries have transferred billions of dollars in arms and military equipment since the start of hostilities.

“The assistance exceeds the peak year of U.S. military assistance to Afghan security forces during that 20-year war,” said William Hartung, an arms control expert at the Quincy Institute think tank. “In that case the U.S. had a major presence in-country that created at least the possibility of tracking where weapons were ending up. By comparison, the U.S. government is flying blind in terms of monitoring weapons supplied to civilian militias and the military in Ukraine.”

Ukraine’s history as a hub for arms trafficking dates to the fall of the Soviet Union, when the Soviet military left behind large amounts of small arms and light weapons in Ukraine without adequate record-keeping and inventory control. According to the Small Arms Survey, a Geneva-based research organization, a portion of the Ukrainian military’s [7.1 million small arms](#) in stock in 1992 “were diverted to conflict areas” underscoring “the risk of leakage to the local black market.”

The problem grew more acute after Russia’s invasion in 2014, which saw combatants looting arms and munition-storage facilities of Ukraine’s Security Service, Interior and Defense ministries. “Irregular fighters on both sides progressively gained access to a wide range of military-grade equipment, including the full spectrum of small arms and light weapons,” according to a report by the Small Arms Survey in 2017. “Officials estimated that at least 300,000 small arms and light weapons were looted or lost between 2013 and 2015,” providing a boon to the country’s black market run by Mafia-style groups in Donbas region and other criminal networks.

The U.S. government is well aware of the country’s challenges with weapons proliferation, though it has been vague in describing the precautions it’s taking.

Weeks after Russia’s latest invasion of Ukraine on Feb. 24, a group of interagency officials in the Biden administration met with outside arms-control experts to discuss the risk of small-arms proliferation in the conflict. According to Stohl, who attended one of the meetings, U.S. officials offered assurances about vetting Ukrainian security forces and addressing reports of unauthorized transfer — but scant details on how the vetting or monitoring happens.

“It does not inspire much confidence,” said Stohl.

Other arms experts feel similarly in the dark.

“It is unclear what risk mitigation or monitoring steps the U.S. and other countries have taken, or what guarantees they have obtained, to ensure the protection of civilians through these very large transfers,” said Annie Shiel, a senior adviser at the Center for Civilians in Conflict.

Some of the recommended steps include establishing a special investigator as the U.S. government did in Afghanistan, ensuring any weapons transfers contain strong tracking procedures, adding human rights obligations in the terms of sale and including specifics about what units can be authorized to receive such transfers. (In 2018, Congress [banned](#) Ukraine’s Azov battalion, a far-right nationalist group associated with neo-Nazism, from receiving U.S. weapons.)

There are additional concerns among watchdog groups about arms proliferation stemming from Moscow amid reports it has enlisted mercenaries from Libya, Syria and Chechnya, as well as the Wagner Group, a Russian contractor.

During a televised meeting of Russia’s Security Council in March, [Defense Minister Sergei Shoigu](#) said 16,000 volunteers in the Middle East stood ready to fight alongside Russian-backed forces in Eastern Ukraine.

In response, Russian President Vladimir Putin offered his approval, saying, “We need to give them what they want and help them get to the conflict zone.”

At the same meeting, Shoigu proposed handing over captured U.S. Javelin and Stinger missiles to pro-Russian separatists in Donbas region. “Please do this,” Putin told Shoigu.

The introduction of foreign fighters to a conflict runs the risks of weapons returning to those individuals’ countries of origin when the fighting in Ukraine ends. There are [conflicting reports](#)



about the presence of foreign fighters there, however, and it's unclear precisely how many have in fact traveled to Ukraine. The lack of information has spurred calls for answers from the administration and attention from Congress.

"Some of the weapons being provided in the conflict in Ukraine are likely to be found years, and possibly decades later," said Abramson. "Congressional leaders should be asking these questions, in classified briefings if needed, and the public should be better informed."

Mine clearance in Ukraine may take 5-10 years

Source: <https://www.ukrinform.net/rubric-ato/3480545-state-emergency-service-mine-clearance-in-ukraine-may-take-5-10-years.html>



Anti tank mines are displayed on a bridge in Bucha, in the outskirts of Kyiv, Ukraine, Saturday, April 2, 2022. (AP Photo/Rodrigo Abd)

May 11 – "Based on international experience, mine clearance may take from 5 to 10 years," Oleh Bondar, Head of the Pyrotechnic Works and Humanitarian Demining Department of the State Emergency Service of Ukraine, said during a briefing at the Ukraine Media Center–Ukrinform.

According to him, one of the biggest negative consequences of the Russian invasion of Ukraine is the massive contamination of territories and populated localities by explosives, including those prohibited by international conventions.

Bondar clarified that the enemy used remote mining systems, cynically set unguided minefields in populated localities and left a large number of particularly dangerous specially planted explosive devices posing a mortal danger and threatening civilians.

"These mines and ammunition have been discovered in Kyiv, Chernihiv, Kharkiv, Sumy, Mykolayiv, Zaporizhzhia, Dnipropetrovsk, Donetsk, and Luhansk regions. The total number of various mines, cluster munitions, and specially installed explosive devices is about 10% of all detected and neutralized explosive devices," he added.

According to the SES representative, after Ukraine's Armed Forces liberate towns and villages, priority measures are being taken, including inspections of localities, roads and buildings, work of emergency crews on power lines, gas and water mains.

"Currently, the implementation of these measures has allowed us to begin a phased process of inspection and demining of agricultural land. We make every effort to enable agricultural enterprises to carry out the spring sowing campaign," Bondar said.



Ukraine is now using these 200-mile-range electric bikes with NLAW rockets to take out Russian tanks

Source: <https://electrek.co/2022/05/17/ukraine-soldiers-electric-bikes/>

May 17 – Ukrainian electric motorbike company [Delfast has seen its electric bikes](#) used for some vastly diverse tasks, such as breaking [Guinness World Records](#) and [outfitting Mexican police](#). But their latest use is perhaps the bikes' most important mission yet: helping Ukrainian soldiers strike a David vs. Goliath blow against Russia's barbaric invasion of their country.

The image below shows one of many [Delfast electric bikes](#) that have been supplied to Ukrainian armed forces, who are currently using them to defend their country from the over two-month-long Russian onslaught.

The electric bikes, which have functional pedals allowing them push their range to over 200 miles (320 km), have enough speed and power to border on electric dirt bike territory.

A hand throttle means that riders can use the pedals as foot rests when necessary, focusing instead on maintaining speed and navigating tricky terrain.

When pushed hard, the bikes can reach speeds as high as 50 mph (80 km/h).

Their long travel suspension and ability to carry heavy loads has made them particularly useful for navigating forested trails or overlanding when trails are nonexistent.



Autonomy: 320km | Speed: ~80km

The bikes used by Ukrainian defenders have been modified to carry NLAW rockets, or Next Generation Light Anti-Armour Weapons, which are specially designed to allow a single operator to destroy an enemy tank. The rockets are designed to be human-portable and carried by infantry, but the 28 lb. (12.5 kg) weapon is much easier to haul over long distances when carried on the back of an electric bike.



Such portable anti-tank weapons are a game-changer in Ukraine's fight to defend its sovereign territory from a Russian takeover, but their use isn't without significant risk.

Real life isn't like Counterstrike, and this isn't a video game. Getting into position in an open area to fire an NLAW or the similar US Javelin missile is incredibly risky, often exposing the operator to the enemy tank's main cannon or multiple heavy machine guns. The use of a high-power electric bike to quickly and quietly reach a firing position can significantly reduce the soldier's exposure and improve the mission success outlook.



In fact, Ukrainian forces are already employing multiple types of light electric two-wheelers in creative capacities to help repel invading Russian forces.

[Another local Ukrainian company, ELEEK](#), has also supplied its country's armed forces with silent, powerful electric motorbikes for use on the battlefield. In that case, the electric motorbikes were requested for use by sniper teams. They offer similar advantages to these NLAW-carrying electric bikes in that they help Ukrainian operators quietly reach a firing position in less time than rucking in on foot.

Electric motorcycles and e-bikes are rapidly becoming a common tool employed by militaries around the world.

As far back as 2018, we learned that Norway's armed forces began [testing fat tire electric bicycles in border guard patrols](#). Patrol roles were also performed by the [New Zealand Defence Forces in 2020 when they began testing UBCO's electric utility bikes](#).

Australian soldiers [have been documenting stealth electric bikes](#) since last year, and we also saw the first application of [helicopter-mounted electric motorcycles](#) last year in an application designed for quick insertion of special operators on low-signature electric dirt bikes.





[Multiple special forces units in Europe and the Middle East](#) have also tested high-power electric mountain bikes for field use, [with paratroopers even air-dropping electric dirt bikes onto the battlefield.](#)



ICI
International
CBRNE
INSTITUTE



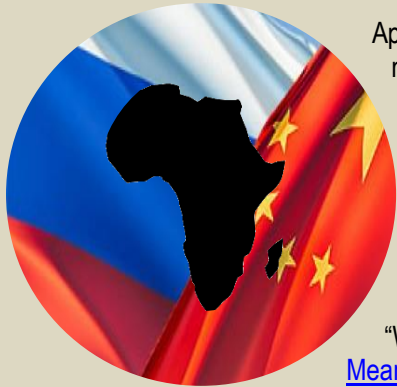
CYBER NEWS



In search of a new world order, Russia and China team up to push Ukraine propaganda

By Cynthia Hooper

Source: <https://thebulletin.org/2022/04/in-search-of-a-new-world-order-russia-and-china-team-up-to-push-ukraine-propaganda/>



Apr 20 – The war in Ukraine is not only about the future of Ukraine. Both Russian and US leaders are making it increasingly clear that the brutal fight for territorial control inside the former Soviet republic is but part of a larger superpower struggle that will determine a new balance of power around the world.

In Iowa to talk about strategies for containing the soaring price of gas, US President Joe Biden [termed](#) Russian leader Vladimir Putin a “dictator” who is committing “genocide.” This came a mere two weeks after Biden [distressed](#) many of his own staffers by going off-script to invoke god in a call for Putin to be removed from power. Meanwhile, in an interview with Kremlin-controlled television channel Russia-24, Russian Foreign Minister Sergei Lavrov announced that one of the goals of his country’s so-called “special military operation” in Ukraine was to [“end the US quest to dominate the world.”](#)

“What we have here is a war between the US and Russia,” warned University of Chicago Professor [John Mearsheimer in a YouTube discussion](#) on April 8. True or not, the power of this idea is one factor in explaining how Putin has been able to shore up domestic public support, with his March [approval rating](#) at an alleged 83 percent. “The [Russian] state media skillfully direct the people’s discontent towards the West,” [commented one Russian journalist](#) opposed to the war, in an interview with a German foundation.

This determination to “just blame Washington” may sound nothing short of pathetic to many US citizens. But Russia’s media strategists do not seem to care. Instead, they are choosing to pivot their attention away from their Western rivals to focus more on winning new audiences in the former Western colonies and developing countries that comprise the so-called “Global South.” In so doing, the Kremlin is partnering with its most powerful ally. Although there are potential competitors for influence in Africa and elsewhere, these days China and Russia have joined together to promote the idea that the United States is to blame for the Ukraine crisis and its consequences. And they are deploying a variety of tools to get this message across, including [cultivating](#) local anti-Western social media “influencers” across Africa, [partnering on stories](#) with specific grassroots media organizations, and employing [for-pay spam services](#) to tweet examples of US racism and hypocrisy.

This campaign is drawing on a deep reservoir of resentment among former colonies towards wealthier, formerly imperialist NATO countries. And it is succeeding in keeping a significant number of the world’s countries, if not actively on Russia’s side, at least reluctant to wholeheartedly endorse “Team USA.”

Russia and China against the West

Inside Russia, the government has banned journalists from using the term “war” to refer to its military actions in Ukraine, [flatly denying](#) that its soldiers have attacked civilians or committed atrocities such as those documented in the town of Bucha. Yet its leaders, from Putin on down, accuse the United States of launching an [“economic war” against Russia by imposing sanctions](#); an “information war” designed to deliberately discredit the actions of Moscow’s armed forces; and a “war of Russophobia” aimed at persecuting Russians abroad and destroying Russian culture.

It’s through this lens that Russian media makers hope people both at home and in developing countries around the world will view the conflict in Ukraine, as a story of a persecuted nation determined to stand up for its interests in the face of US bullying.

And many in China seem to see things the same way.

In diplomatic meetings and state media stories, Chinese establishment figures are siding with Russia on issues like its [false allegations](#) of US-led biological weapons research in Ukraine and its criticisms of post-1991 NATO expansion. “NATO has already messed up Europe, stop trying to mess up Asia and mess up the whole world,” [proclaimed Chinese diplomat Liu Xiaoming](#) in an angry April post on Twitter.

When Russia’s Lavrov travelled to Beijing late last month to meet with his Chinese counterpart Wang Yi, he took the opportunity to direct attention away from news of Russian military losses, casting the Ukraine “conflict” (not “war”) as an opportune moment for China and Russia to challenge past decades of US global leadership. The two countries, he said, planned to work to bring together all nations similarly dissatisfied with “Western hegemony” and, with them, create a new [“multipolar, just, democratic world order.”](#) A Chinese foreign ministry spokesman, Wang Wenbin, enthused, “Our striving for peace has no limits, our upholding of security has no limits, our opposition towards hegemony has no limits.”

One key target of joint Russian and Chinese condemnation is the leveling of economic sanctions on Russia more severe than any ever imposed on a G20 country. [The most recent](#)



[sanctions package](#) bans all new investment in Russia, seeks to disrupt the country's global supply chains, and further tightens restrictions on its banks. Such measures have led to talk of a Russian default on its external debt, and predictions that the Russian economy [could contract by 15 percent in 2022](#).

Meanwhile, US leaders such as Treasury Secretary Janet Yellen are ramping up criticism of China for failing to support such measures. Speaking to the Atlantic Council on April 13, Yellen [endorsed](#) the rather extraordinary strategy of so-called “friend-shoring,” in which “trusted countries” form their own supply chains to reduce dependence on others who could potentially seek to undermine certain foundational values. She also suggested that China risks [being cut out of such relationships](#), saying, “The world’s attitude towards China and its willingness to embrace further economic integration may well be affected by China’s reaction to our call for resolute action on Russia.”

Yellen’s words about the “world’s attitude” seem sure to add fuel to an anger palpable on Chinese social media regarding which countries presume to have the right to speak for that world. In response to pronouncements by Washington last month that “the entire global community” supported sanctions, Zhao Lijian, a combative spokesperson for China’s Foreign Ministry, sarcastically [tweeted a map](#) of what he claimed was the US vision of the world. The map included only part of North America, Europe, Australia and Japan, and it left out, among other locations, China, Africa, and India. Zhao’s comments emphasized that the US-led “West” does not include the majority of the world’s population, and that many of those “overlooked” billions of people often do not share its views. Twitter users, some claiming to be “independent journalists” or “anti-imperialists,” retweeted the post more than 12,000 times in a variety of languages.

Mutually beneficial propaganda deals

Long before the current crisis, Russia and China began joining forces to spread similarly critical visions of US power via information operations directed to both their own citizens and the wider, non-Western world. According to a [recent Brookings Institute report](#), this propaganda partnership launched shortly after Chinese President Xi Jinping took office in 2012, via a series of content-sharing deals between Russian and Chinese media outlets such as Russia’s English-language media network RT and China’s English-language paper *People’s Daily*. Efforts to reinforce each other’s “spin” on global events seems to have [accelerated in the spring of 2020](#), as China scrambled to counter Western stories portraying it as the originator of COVID-19.

After the Russian invasion of Ukraine in February, a Chinese propaganda directive accidentally posted on Weibo revealed yet more signs of behind-the-scenes collaboration. According to the *China Digital Times*, an online outlet founded by Chinese dissident and UC Berkeley School of Information research scientist Xiao Qiang, the memo instructed Weibo’s [army of so-called social media “opinion analysts”](#) (the official term for censors) not to circulate any information [“unfavorable to Russia or pro-West.”](#)

In the face of Western outrage at both Russia’s military slaughter of Ukrainian civilians and a Russian domestic disinformation campaign that casts all atrocities as the work of neo-Nazi Ukrainians, both Russian and Chinese officials—and the journalists who cover them—have swung to attacking the United States for its alleged bias in reporting on the war and its causes.

As part of these efforts, the Russian government is organizing trips for foreign journalists into the Donbass region of eastern Ukraine, ostensibly so they can see with their own eyes signs of damage inflicted by Ukrainian troops on pro-Russian civilians and interview Russian-speaking residents about their experiences.

Almost every night for several weeks, the leading Channel One evening news show *Vremia* has included extensive reports on these excursions, with clips bannered “open your eyes” or “come and see” and featuring soundbites with correspondents from Italy, Iceland, Norway, Greece, and Venezuela, among many others, all testifying to their surprise and shock in discovering the extent of alleged Ukrainian military abuses and of “Western bias” in ostensibly refusing to cover them.

But even as these stories claim to challenge Western censorship, they reveal Russian strategies of information manipulation. Tour guests are described as if they represented respected journalistic establishments from around the world, when in reality, just to take one example, [the German reporter prominently quoted on a March 27 show](#) works for the little-known “Anti-Spiegel” organization (*Der Spiegel* being the Germany’s most prestigious news magazine), which turns out to be an online Russian media company publishing in German.

The same journalist was again featured [in April 12 coverage of a tour to Mariupol](#). In that report, a Channel One correspondent advocated for empowering more “alternative” global media outlets, claiming that appetite was growing around the world for points of view different from those of the Western “establishment.” In a pointed dig at Germany’s *Spiegel* (which means “mirror” in English) and a direct endorsement of its “Anti-Spiegel” challenger, the Channel One reporter continued on to argue that “many Europeans are trying to see more than just their own reflection in the mirror.”

Chinese media, too, has been emphasizing the need for greater variety in points of view on the global stage (arguably an ironic position, given the importance its leaders place on domestic censorship). Government-sponsored outlets accuse US leaders of arrogant overconfidence in their country’s superiority and fault Western journalists for [dismissing](#) any positive coverage of China as “fake.” China’s largest English-language newspaper *China*



Daily—active both inside China and abroad—repeatedly emphasizes these themes. [In a China Daily video interview](#) with Victor Gao, a Chinese Communist Party spokesman, about his country's role in the Russia-Ukraine conflict, Gao stressed that Chinese leaders wanted an end to violence. But he went on to level a blistering, if indirect, critique of Washington, saying that “[w]hat China is opposed to is any country which wants to dictate the terms for the whole world, any country which wants to monopolize power in the world.”

Scramble for Africa

What is important for Westerners to realize is that these narratives are not only staples of domestic propaganda in China and Russia, they are also being deployed by both countries to fuel anti-Western, anti-imperialist sentiments in the developing world and to emphasize differences between rich countries and poor ones. Over and over, Russian and Chinese-funded outlets emphasize that the United States and its Western allies are not listening to developing countries, but instead simply expecting them to obey Washington's commands. Africa is one key region both countries are bombarding with such propaganda.

At first glance, this situation looks paradoxical, as Moscow and Beijing are themselves natural competitors for influence on the continent. Russia has historic ties to a host of countries in Africa and the Middle East dating back to the Cold War, when the Soviet Union took the lead in supporting African independence movements and a global battle against apartheid and imperialism. China's dominance on the continent is more recent, dating back to such things as the 2013 launch of the Belt and Road initiative, a 70-country development project that has led to soaring levels of Chinese investment in African infrastructure.

For the time being, however, the potential rivals appear to be making common cause—prompting the US Congress in April to warn of the [“malign influence and activities”](#) of Russia in Africa, even while [simultaneously worrying about](#) the growing successes of Chinese “soft power” on the continent.

In this battle for hearts and minds, both Russia and China appear to be drawing on a variety of tactics. One is the use of foreign-language, government-funded media tailored to an African audience. Beijing has invested heavily in CGTN Africa, a regional arm of the Chinese Global Television Network founded in January of 2012. *China Daily* launched an African edition later that same year. Today, the stories both outlets run about the Ukraine war focus on the hardship Africans will face as a result of the conflict. One recent CGTN report emphasized that the [price of wheat in Africa](#) rose 19.7 percent in March, alone.

The Kremlin similarly supports a global media network aimed at audiences outside the country. And like CGTN, RT operates inside Africa primarily in English. But RT has also fallen on hard times. Once vastly more popular than its Chinese counterpart, RT has, since the Russian invasion, seen its broadcasts banned in the United States and European Union and its programs thrown off YouTube. But such setbacks in the Western world seem to have encouraged the company to shift its focus. Just weeks before the outbreak of war, [RT announced plans](#) to open a new “African hub” in Nairobi, where both CGTN Africa and China Daily Africa are based. [The company says it is looking to hire journalists](#) with “a nose for narratives and angles that people from across Africa believe in but [which] are dismissed by mainstream media” and “a strong understanding of how to use digital media creatively to build a passionate and dedicated community.”

According to the Paris-based magazine [Africa Report](#), after RT was taken off the air in France, members of the organization's Paris bureau began to consider ideas for expanding French-language media coverage in Africa. Several members of the RT Paris bureau are reportedly considering moving operations to West Africa and have already opened discussions with an online media service in Mali known for its alleged ties to [the Russian paramilitary organization Wagner Group](#), active in that country since 2020.

If these relationships sound convoluted, not to mention sketchy, that is because they are. *Africa Report* has also [documented the emergence](#) of pro-Russian social influencers and bloggers across Africa, and their investigation points to a pattern in which seemingly apolitical organizations (such as “think tanks” or “research centers”) are created to serve as intermediaries between a variety of grassroots (and often very fringe) African media outlets and major Russian propaganda operatives such as Yevgeny Prigozhin, head of the notorious St. Petersburg “troll factory,” [the Internet Research Agency](#) accused of multiple disinformation campaigns and interference in the 2016 US Presidential election.

More recently, groups linked to Prigozhin have, in Africa, been [accused](#) of fabricating scandals to discredit independent journalists, [manipulating public opinion](#) at the behest of local potentates, and mounting coordinated disinformation campaigns [designed to promote Kremlin goals](#). Facebook has also begun to identify significant amounts of suspicious activity originating from Russia and aimed at African social media. In December of 2020, Facebook announced it had [taken down more than 500 “inauthentic” accounts](#) “originating from Russia and France” and “targeting 13 African countries,” while [Facebook's first “adversarial threat report” of 2022](#) mentioned a network originating in St. Petersburg and targeting “primarily Nigeria, Cameroon, Gambia, Zimbabwe, and Congo.”

Since Russia's invasion of Ukraine, a variety of opaque online services appear to be promoting pro-Putin or pro-Russian hashtags and linking them to anti-Western, anti-imperialist, or pan-African commentary. Carl Miller, research director at the Centre for the Analysis of Social Media, [mapped](#) approximately 10,000 accounts that circulated pro-invasion hashtags on March 2 and March 3, and his results suggest that Russian propaganda forces likely rented out pay-to-engage services located in Africa and Asia to boost coverage. His findings, he notes, suggest this operation



was not an isolated incident, but, instead, part of a much larger [“BRICS-solidarity influence strategy”](#) designed to unite poorer countries with growing economies against more established, wealthier ones.

It is worth noting, in this regard, that although China is currently Africa's largest creditor, owed more than \$140 billion, its leaders have—ever since its emergence as a unified Communist state in 1949—always publicly emphasized their country's solidarity with the developing world. [In a recent editorial for the *South China Morning Post*](#), government researcher Zhou Xiaoming stressed his country, too, was an “emerging economy,” called the nations of the Global South “cousins,” and claimed China, like them, had “resisted the pressure to align itself with the West over the war in Ukraine.”

Empathy¹ disrupted

So does such propaganda really work? And, whether covert or overt, does it succeed in transforming people's values, or merely in highlighting opinions deeply rooted in society, if not always openly expressed?

Certainly, the situation in Africa is fraught. In regard to the war, many citizens seem to be struggling to identify the lesser of two evils: They are unhappy with Russia's actions in Ukraine, but even more unhappy with US actions in the wider world. Support for the Kremlin is less than solid. Thirty-seven out of 54 African countries voted to condemn the Russian invasion at the UN, [whereas only 28 voted](#) to condemn the annexation of Crimea in 2014. [Nevertheless, not a single country in Africa](#) (or in the Middle East or Latin America) has joined in on US and EU sanctions.

My colleague at the College of the Holy Cross, history professor Munya Munochiveyi, told me that many Africans perceive sanctions as a neo-colonialist tool, “a sort of 21st century version of European imperialism.” Zimbabwe's acting minister of foreign affairs, in an article for *The Herald*, one of his country's major papers, claimed that sanctions against Russia represent only the will of the United States and its closest allies, noting that his own country has been forced to endure US sanctions for over 20 years. “Unilateral sanctions have never worked to resolve any situation,” he declared. “On the contrary, sanctions unleash untold humanitarian crises and human suffering of the ordinary people.”

It is in the ability to hamstring the construction of a more genuine global alliance, whether today against Russia or tomorrow against a threat like global warming, that anti-US messaging is most powerful. As Munochiveyi told me, “Social media is a perfect vehicle to stir up historical memories of imperialism in the Global South.” And due in part to the very real power of those memories, but also in part to the power of their online amplification, billions of people around the world see the United States as an arrogant and hypocritical country that pursues its own interests, while pretending to a moral superiority it does not deserve. On April 14, the Russian embassy in the United Kingdom [tweeted a comment by Putin](#), in which the Russian president once again accused the United States and its allies of viewing the Ukrainian people as no more than puppets in a larger power struggle. “The main goal of the West is not to help Ukraine,” this particular quote read. “Ukraine is just a means of reaching goals that have nothing to do with the interests of the Ukrainian people.” It's the same line Chinese journalists emphasize when they disparage Washington for allegedly expecting to be able to give the countries of Africa orders and have them fall in line. Africa “has matured and is unwilling to be used as a rubber stamp to undermine or confront other countries,” [proclaimed a March CGTN Africa article](#).

It is, of course, deeply ironic that Russia and China, both superpowers with extensive records of human rights abuse, are expressing outrage over another government's alleged disregard for ordinary people and their opinions. But at the moment, their information war, in order to be successful, merely needs to undermine trust. It is always difficult to persuade countries to act selflessly on a global stage, in a manner at odds with their economic self-interest. But it is all but impossible if citizens are encouraged to believe that the only result of selflessness will be further exploitation.

Cynthia Hooper is an associate professor of Russian History and the head of Russian and Eastern European Studies at the College of the Holy Cross in Worcester, Massachusetts. She is a specialist on Russian media and disinformation strategy, advising businesses and publishing in the *Washington Post*, *Newsweek*, [theconversation.com](#), and *Fortune Magazine*, among others. Her scholarly interests include the Stalin-era Great Terror and the politics of memory. She received her PhD from Princeton University and BA from Harvard University, and has served as a fellow at Harvard's Davis Center and the Woodrow Wilson Institute.

¹ Empathy is the capacity to understand or feel what another person is experiencing from within their frame of reference, that is, the capacity to place oneself in another's position.



France suffers internet outages after fibre-optic cables across the country are sabotaged

Source: <https://www.dailymail.co.uk/news/article-10759943/France-suffers-internet-outages-fibre-optic-cables-country-sabotaged.html>

Apr 27 – France has suffered huge internet outages across the country after fibre optic cables were cut overnight in 'multiple malicious acts' of sabotage.

The apparently coordinated attacks saw multiple cables broken at around 4am, causing massive disruption to internet and phone services.

Free, the worst-affected provider, said: 'The attacks took place overnight at 4am. Our teams have been at work since this morning.'



France has suffered huge internet outages across the country after fibre optic cables were cut overnight in 'multiple malicious acts' of sabotage

In a message on Twitter, the company referred to 'multiple malicious acts' targeting its cables which led to outages and slow connections for many clients.

Competitor SFR said it had experienced 'several fibre cuts' in the Paris region and in Lyon in southeast France.

Other operators such as Bouygues Telecom and market leader Orange were not affected because they use different networks, but problems were reported by users around the country including in regional cities such as Strasbourg, Reims and Grenoble.

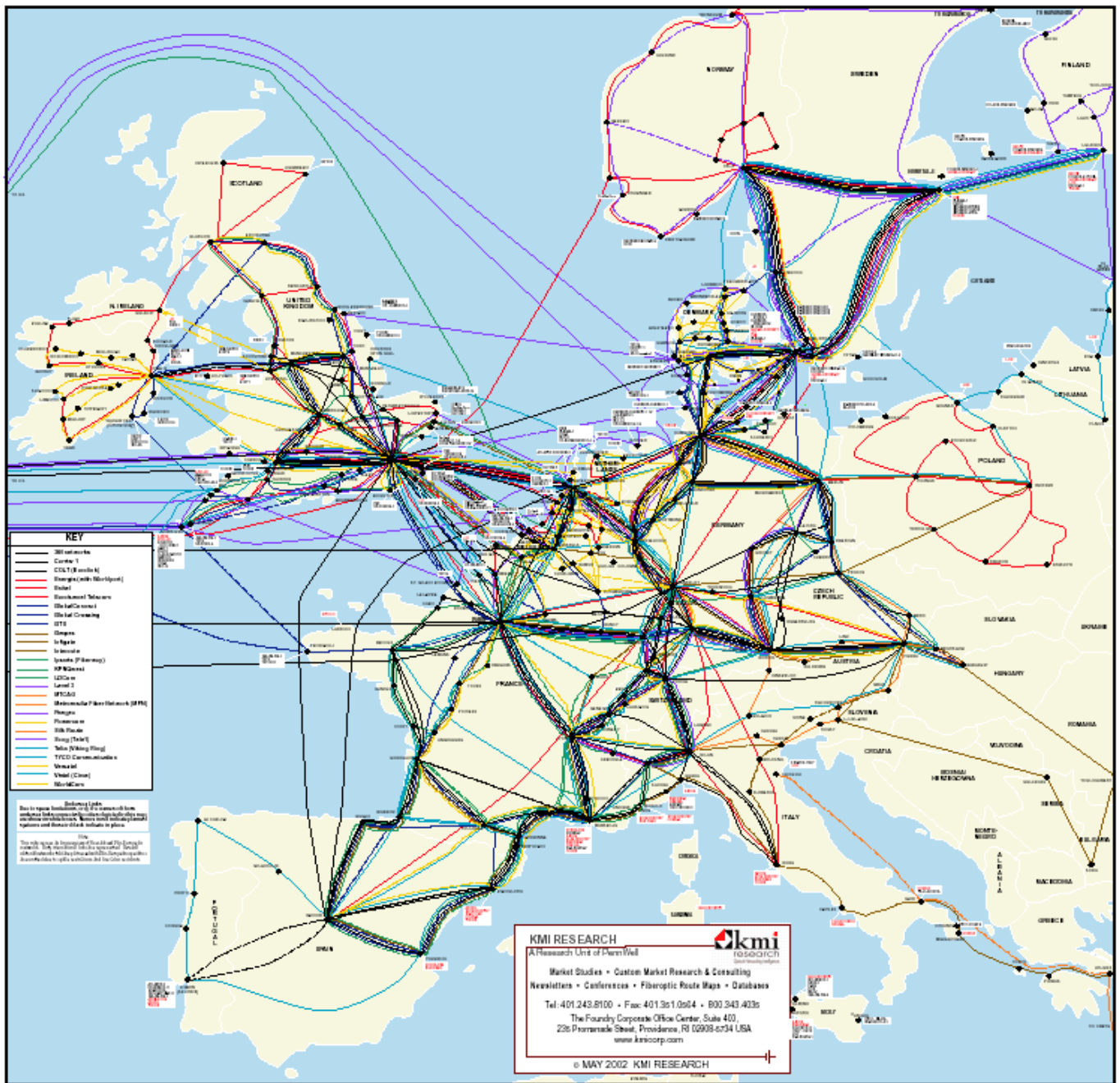
'Cuts to cables have been confirmed in the Paris region affecting fixed and mobile services,' Digital Affairs Minister Cedric O wrote on Twitter.

The source of the problem is unknown at this stage, but experts stressed that apparently coordinated attacks on fibre optic cables were unprecedented.

The apparently coordinated attacks saw multiple cables broken at around 4am, causing massive disruption to internet and phone services

'This sort of incident at this scale never happens,' one security source told AFP on condition of anonymity. 'It's the first time and we don't know who it is for the moment.'





The affected operators said their technicians had been working overnight to restore services, with Free saying the problems were 'contained'.

Other IT companies such as cloud computing groups were also hit by the outages, which forced Free and SFR to move their data on to alternative routes.

'It's at bit like the motorways being blocked and you need to redirect all the traffic on to other roads,' said Sami Slim from the data centre company Telehouse.

'It can result in small outages, but the internet works,' he said.

The cuts targeted so-called 'backbone' cables which carry huge quantities of data between different regions and typically run along motorways or rail tracks.

The Paris-Lyon and Paris-Strasbourg links were apparently targeted.

In March 2020, fibre optic cables used for Orange's network were intentionally cut in the Paris region, depriving tens of thousands of users of internet connections.



Russia's Anti-Satellite Weapons: An Asymmetric Response to U.S. Aerospace Superiority

By Jaganath Sankaran

Source: <https://www.armscontrol.org/act/2022-03/features/russias-anti-satellite-weapons-asymmetric-response-us-aerospace-superiority>

March 2022 – Russia conducted a direct-ascent hit-to-kill anti-satellite (ASAT) test on November 15, 2021, striking a Russian satellite and rendering it into more than 1,500 pieces of orbital debris.¹ Reacting to the test, U.S. Space Command commander Army Gen. James Dickinson claimed that Russia is “deploying capabilities to actively deny access to and use of space by the United States and



its allies.”² He further noted that Russia’s counterspace weapons systems undermine strategic stability.

A Soyuz-2 1b rocket booster carrying the Kosmos-2546 military satellite of the Russian Defense Ministry before launch by the Russian Aerospace Forces from the Plesetsk Cosmodrome in May 2020. That same year, Russia used other versions of Kosmos satellites in anti-satellite (ASAT) weapons tests. (Photo by Russian Defense Ministry/TASS via Getty Images)

Russian military leaders and analysts argue, however, that their counterspace weapons provide a means to restore strategic stability. Russian Defense Minister Sergei Shoigu characterized the test as a routine operation of a “cutting-edge future weapon system” to strengthen Russia’s deterrent and defense against U.S. attempts to attain “comprehensive military advantage” in space.³

Russian leaders believe that a change in the character of warfare has been unfolding over the past three decades. They write that the next generation of warfare will be waged in the aerospace domain with weapons enabled by satellite targeting and navigation.⁴ For instance, in a 2015 speech, President Vladimir Putin asserted that U.S. and NATO forces possess “high-precision long-range non-nuclear weapons comparable in their effect to nuclear weapons.”⁵ Russians fear that, in a conflict, these weapons may be used against them in a coordinated strike against their nuclear and conventional forces.

At a 2013 conference attended by several cabinet ministers and members of the Russian Military-Industrial Commission, Deputy Prime Minister Dmitri Rogozin identified five conflict scenarios that Russia could face in the future.⁶ One of them involved a noncontact war with a technologically advanced adversary, presumably the United States and NATO. In this scenario, the United States would strike the Russian homeland, drawing from its “lightning-fast global strike” weapons using satellite targeting and



navigation. Rogozin suggested that such a strike could destroy 80 to 90 percent of Russia's strategic arsenal, rendering its nuclear deterrent almost useless.

These scenarios reflect a worst-case analysis that may not match reality. As Vladimir Dvorkin, a former Russian military officer with deep involvement in Russian nuclear policies, has noted, "[I]t seems rather fantastical to suggest that the Pentagon could be planning a disarming conventional strike against Russia's strategic nuclear forces: such a measure would not only prove absolutely useless, but would trigger a devastating retaliatory nuclear strike."⁷ Dvorkin suggests Russia's intercontinental ballistic missile silos are hardened to withstand any such strikes, its mobile launchers are difficult to target, and its ballistic missile submarines can be dispersed quickly and are protected by naval forces.

Yet, these fears permeate the Russian debate on the aerospace capabilities of U.S. and NATO forces. Russian military exercises are now designed to "repel a massive" aerospace strike by hypersonic weapons, short- and medium-range cruise missiles, and ballistic missiles with highly mobile anti-air and anti-space units.⁸ Russian planning also includes ASAT weapons to target the critical satellite systems that enable these modern aerospace weapons.⁹

Dissuading Russian ASAT weapons development and testing will require a concerted effort at arms control. In December 2021, the United Nations voted to establish an open-ended working group to prevent an arms race in space.¹⁰ The UN forum may offer a chance to establish norms on space and foster a debate on the linkages between space security and other national security considerations. Likewise, the Biden administration seems inclined to pursue a ban on debris-generating ASAT tests.¹¹ Securing multilateral support for such a ban, however, will require engagement and support from the Russians and Chinese. Such engagement will have to incorporate a discussion on the role of advanced aerospace weaponry, address their perceived vulnerabilities to these weapons, and develop ways to limit them.

Russian Anti-Satellite Weapons

The ASAT test in November is the latest in a series of such actions by Russia. The missile used in the test, Nudol, has been tested several times in the past without a hit-to-kill mission. At the 2021 Reagan National Defense Forum, U.S. Rep. Jim Cooper (D-Tenn.) noted that Russia had attempted to test its ground-launched ASAT missile "several times in recent years and failed, so it was predictable that they would keep trying until they scored a hit."¹² The latest hit-to-kill demonstration indicates that Russia may have perfected its ASAT missile.

In 2014, the Russian Olymp-K satellite demonstrated co-orbital ASAT capabilities in the geostationary orbit where several critical military command-and-control satellites operate.¹³ Additionally, Russia has fielded ground-based lasers and a range of satellite-jamming systems to deny and degrade the capacity of weapons that rely on satellited-enabled information. These weapons are detailed in Russian military literature as a vital mechanism to eliminate Russian vulnerabilities to Western precision weapons.

Russia has also tested co-orbital ASAT systems that target satellites beyond low-earth orbit. In October 2017, three Russian satellites—Kosmos-2519, Kosmos-2521, and Kosmos-2523—conducted high-velocity orbital maneuvers. In January 2020, two Russian satellites, Kosmos-2542 and Kosmos-2543, performed coordinated, close-approach orbital maneuvers in the vicinity of a U.S. military reconnaissance satellite, the KH-11. Six months later, in July 2020, the Kosmos-2543 satellite fired a high-velocity projectile into outer space. Such a projectile could act as a potent ASAT weapon. U.S. Space Force commander Gen. John Raymond has described the orbital experiments performed by these satellites as "Russian nesting doll" satellites and claimed they "exhibited characteristics of a weapon system."¹⁴

A Russian Perspective on Future Wars

Russian military scholars examining U.S. and NATO military campaigns note that high-precision aerospace weapons supported by satellite-enabled data have become indispensable to the U.S. way of war.

Igor Morozov, head of operations at the Russian Space Force, has written that, "[d]uring the Second World War, to destroy such a target as a large railway bridge, it was required to make 4,500 sorties and drop 9,000 bombs. In Vietnam, the destruction of a similar target was achieved with 190 bombs and 95 sorties. In the war against Yugoslavia, the same mission was solved by [one to three] cruise missiles fired from a submarine."¹⁵ Similarly, Russian analysts point out that the ratio of standoff long-distance cruise missiles to aircraft-launched precision weapons has steadily increased "from 1:10 in Operation Desert Storm to 1:1.5 in Operation Desert Fox to 1:1 in Operation Allied Force to 1.8:1 in Operation Enduring Freedom."¹⁶

Russian military literature is replete with discussions about how these high-precision aerospace weapons are changing the nature of warfare. Russians argue that, in past wars, the main burden of any confrontation rested on ground forces tasked to breach the enemy's forward defense and enter the adversary's territory to occupy it. Future wars, they argue, will not be conducted using the massing of armed troops. Instead, their opening salvo will involve massive air missile strikes at targets throughout the adversary's territory. The 1991 Persian Gulf War and the 1999 NATO campaign in Yugoslavia are showcased as evidence.



Russian military commentators studying the Gulf War point out it was the first time in the history of modern warfare that a formidable army of half a million troops was unable to override the aerospace operations mounted by U.S. and allied forces.¹⁷ Moreover, Russian writings note that, by the time the Iraqi army encountered U.S. ground forces, it had been decimated by the weeks of air and missile strikes made possible by satellite-enabled targeting and navigation.¹⁸

Similarly, Russian military commentators conclude that Yugoslavia's disintegration was achieved at the end of the months-long aerospace campaign without a significant force-on-force conflict. Even more concerning for the Russian analysts was that the military intervention was executed without endorsement by the UN Security Council, setting a dangerous precedent for the West's arbitrary use of force against sovereign states and possibly Russia itself.¹⁹

Russian military analysts use these conflicts as a template to write regularly about a future war in which a massive air missile strike campaign could be mounted against Russia. First, they believe that U.S. conventional hypersonic weapons, developed under the Prompt Global Strike program, would start an aerospace assault against crucial Russian government command-and-control posts and mobile and stationary launchers of nuclear-armed missiles.²⁰ Next, U.S. missile defenses would further degrade Russia's retaliatory potential.²¹ These would be followed up quickly with electronic warfare to suppress Russian air and space defense forces. Then, large numbers of standoff high-precision weapons such as cruise missiles, heavy-strike unmanned aerial vehicles, and other strike forces will be used to destroy military facilities and troops, in addition to Russian government administration centers, economic assets, power and energy supply systems, and critical communication nodes.²² Finally, the standoff strikes would coincide with an information warfare campaign to collapse the prevailing political order.²³

Some Russian commentators question the viability of such massive attacks against a significant nuclear power using high-speed, high-precision weaponry as "science fiction."²⁴ One analyst writes that the danger of an attack on Russia with many cruise missiles is improbable and points out that assembling the formations required for such a strike requires lengthy preparations that cannot be done secretly during a crisis.²⁵

Notwithstanding these assessments, most Russian analysts display a severe fear of U.S. and allied technological superiority. Although these fears may reflect an extreme worst-case scenario, many Russian military analysts share them. Therefore, they argue, the dependence of U.S. and NATO forces on space-based assets is a vulnerability of which Russia cannot fail to take advantage in a crisis. Russian military commentators claim ASAT and other counterspace weapons will deter aggression and offer war-fighting advantages if deterrence fails.²⁶



A Russian rocket topped with Kosmos-2543 and Kosmos-2542 satellites is shown as it was erected in November 2019. The following year, Russia deployed both satellites to perform coordinated, close-approach orbital maneuvers in the vicinity of a U.S. military reconnaissance satellite, the KH-11. (Photo by Russian Defense Ministry)

These Russian motivations pose profound challenges to pursuing lasting space arms control measures. Several proposed nonbinding behavioral norms may stall the testing of ASAT weapons for the near term. For instance, U.S. Deputy Defense Secretary Kathleen Hicks recently argued for a global ban on ASAT tests that create debris.²⁷ These norms can be



diplomatically pursued through multilateral dialogues, including at the UN. Meanwhile, U.S. Secretary of State Antony Blinken reiterated a U.S. desire to develop informal norms to standardize acceptable behavior in space operations. In a speech at the UN Conference on Disarmament, he said the United States wants to engage in “developing standards and norms of responsible behavior in outer space.”²⁸ He further noted, “[W]e should be reducing tensions in outer space, not making them worse.”²⁹

Such diplomatic engagements would provide the United States and its NATO allies with some transparency into Russia’s ASAT and counterspace programs and motivations. Similarly, Russia would gain transparency into U.S. and NATO programs and concerns. Diplomatic engagements can also help communicate redlines and establish a shared understanding of pathways that could lead to conflict escalation in space.³⁰

In the end, however, there are limits to what dialogue and voluntary behavioral norms can accomplish. Without mutual restrictions on aerospace weapons and combat operations, Russians will continue to argue that U.S. and NATO forces retain a significant war-fighting superiority that can be offset only with counterspace systems. Addressing Russia’s perceived vulnerabilities to modern aerospace campaigns will require deeper engagement and structured arms control, possibly with an instrument similar to the Intermediate-Range Nuclear Forces Treaty. Such binding agreements are a difficult proposition in the prevailing geopolitical environment, but they are essential to achieve comprehensive space security and strategic stability.

► Endnotes are available at the source’s URL.

Jaganath Sankaran is an assistant professor at the LBJ School of Public Affairs at the University of Texas at Austin.

Analysts Warn Anti-Satellite Weapons Have Evolved Beyond Missiles

Source: <https://www.wired.com/story/analysts-warn-anti-satellite-weapons-have-evolved-beyond-missiles/>

Apr 11 – Last November, three months before Russian forces would [invade Ukraine](#), Russia launched a Nudol missile interceptor that blew up Cosmos 1408, a defunct Soviet satellite, in the process flinging at least [1,400 bits of debris](#) into low Earth orbit. The weapons test unsubtly demonstrated Russia’s anti-satellite military capabilities, which are comparable to those of China and the United States. At the same time, Russia had reportedly been [jamming GPS satellites](#), interfering with radio communications to and from spacecraft, thereby disrupting navigation tools the US military and others rely on. These kinds of electronic weapons, which can be deployed effectively against satellites and satellite-related infrastructure on the ground, are proliferating around the world, according to analysts at the [Center for Strategic and International Studies](#) and the [Secure World Foundation](#).

Last week, the think tanks each released a new annual report assessing what has changed over the past year—and what hasn’t—involving anti-satellite and other “counter-space” weapons, which more and more countries are developing. The counter-space world now extends well beyond the big three military space



actors—the US, China, and Russia—and other newer space powers, like India, Iran, and Japan. Researchers now argue that Australia, South Korea, and the United Kingdom should be considered emerging space powers as well.

“All these countries are laying the groundwork for more indigenous military space capabilities. They’re investing in military space organizations, they’re building resources for electronic warfare capabilities, and they’re building out a policy framework for some sort of military space aspirations,” says Victoria Samson, the Washington office director for the Broomfield, Colorado-based Secure World Foundation, or SWF.

Both reports draw attention to the Russian anti-satellite test, which like previous tests by Russia and other nations, generated long-lasting debris. The cloud of shrapnel from the blown-up satellite even [briefly threatened the International Space Station](#), making the crew take shelter in a SpaceX Crew Dragon docked there, in case there was a collision. Other pieces of [space junk](#) still in orbit from earlier tests have remained there for decades, according to data from the SWF, which means continuing risks of collisions with active satellites.

“That [Russian] test has really galvanized the international space community to continue to [push for a ban](#) on testing that creates this kind of debris,” says Kaitlyn Johnson, a researcher at the Center for Strategic and International Studies (CSIS) and an author of the report.

Samson agrees. Even anti-satellite tests at lower altitudes, like the US’s and India’s, have still thrown hundreds, if not thousands, of bits of space garbage into higher orbits, where they linger longer and could endanger spacecraft. “There’s no such thing as a responsible anti-satellite test,” she says.

In the two reports, the analysts write that they also see nations increasing their investments in, and use of, electronic and cyberweapons. These technologies include the abilities to jam uplinks and downlinks, spoof satellites with fake signals, intercept data, or even possibly [hack a satellite](#) and seize control of it.

From some militaries’ perspectives, these kinds of attacks could be considered advantageous, because they don’t pollute low Earth orbit with junk that could later affect their own spacecraft, and because they can be harder to attribute. “It’s easier, it’s lower cost, it’s less escalatory, and it’s effective—it does the job. Why try to shoot down a satellite when you could just launch a cyberattack and have the same effect with less backlash?” asks Todd Harrison, director of the CSIS’s Aerospace Security Project and an author of their report.

Russia’s invasion of Ukraine cast a shadow over the researchers as they finished writing their reports, and it will surely inform their future analyses. While other countries have also designed electronic weapons, like satellite communication jammers, the reports’ authors say Russia has demonstrated that it has no qualms about using them [against GPS satellites](#) and [against drones](#).

In particular, the CSIS report includes a map of GPS interference throughout the separatist region of eastern Ukraine before the war even started. The CSIS authors used data from the US-based radio frequency analytics company HawkEye 360, which they say indicates the estimated locations of suspected Russian jammers last November and December. And on the first day of the conflict, the US satellite communications provider [Viasat reported a disruption](#) to its ground terminals in eastern Europe; Harrison suspects that Russia is behind that cyberattack, though that has not yet been confirmed.

The Viasat attack could also be a sign of future problems for other companies as the private space industry plays a [growing role in conflicts](#). “This has really driven home to commercial companies that they could become potential targets. If the Ukrainian government is buying imagery from a Planet Labs satellite, I think that makes the satellite a legitimate military target,” says David Burbach, a national security affairs expert at the US Naval War College in Newport, Rhode Island, who was not involved in the reports and was not speaking on behalf of the US Navy.

The reports also detail new weapons that are being researched and developed, mainly by the US, Russia, and China, including lasers and microwave beams that would be fired from the ground or aircraft to temporarily dazzle the sensors on satellites when they try to monitor something sensitive. The effect is like shining a flashlight in someone’s eyes. While the effects from a low-powered beam are reversible, a high-powered weapon could blind a satellite, causing permanent damage to its sensors or circuitry. There’s no known use of such weapons in war—at least not yet.

A close comparison reveals a few differences between the two reports. The CSIS report comes more from a US defense perspective, and unlike the one from SWF, it does not analyze the US’s own capabilities, but focuses more on the nation’s adversaries. (The organization’s funders include US-based aerospace companies and military contractors.) The CSIS analysts include two developments their SWF counterparts decided to leave out: China’s hypersonic weapon test and Israel’s Iron Dome missile defense system.

Last July, China test-launched a [hypersonic missile](#) capable of carrying a nuclear warhead, which made at least a partial orbit before gliding to lower altitudes. It’s technically not a space or counter-space weapon, Harrison says, even if it briefly neared the edge of space. But it did raise questions related to the 1967 Outer Space Treaty, which bans nuclear weapons in space. Missile defense systems also don’t count as counter-space weapons, but similar technologies using ballistic missiles could be used against satellites.



Some space technologies, depending on how they're deployed, create a "dual-use" dilemma, Burbach argues. "Almost anything useful on the civilian or commercial side has a direct military application too," he says.

For example, last year China launched a satellite that [could dock with another orbiter](#), and observers claim that another of its satellites [has a robotic arm](#). While these technologies can have peaceful uses—to service satellites or take dead spacecraft out of orbit—such rapidly advancing technologies could just as easily be used against an adversary's satellite.

To avoid international misunderstandings about how these technologies are being used, Samson, Harrison, and their colleagues support ongoing attempts to develop [norms or new rules for space](#). Debates about what kinds of behavior are allowed—and what are not—will be hashed out at the United Nations next month, as part of a long-term process.

Jessica West, a senior researcher at the research institute Project Ploughshares, based in Waterloo, Canada, says that more work needs to be done to make space safer. "We didn't do arms control, and now we have a big problem," says West, who's not involved with either the CSIS or the SWF.

"Space is a military environment, but it's overwhelmingly a civilian and a commercial environment" she continues. "I think about it like urban warfare: Yes, you have military combatants, but you also have a lot of important infrastructure."

NATO Cyber Game Tests Defenses Amid War in Ukraine

By Catherine Stupp (Reporter, WSJ Pro, The Wall Street Journal)

Source: <https://www.wsj.com/articles/nato-cyber-game-tests-defenses-amid-war-in-ukraine-11650274203>



Apr 18 – NATO's large, multiday cyber defense exercise is set to bring together technical experts from alliance countries and Ukraine nearly two months after Russia's invasion.

The annual cyber wargames, known as the **Locked Shields exercise**, will start Tuesday in Tallinn, Estonia. The North Atlantic Treaty Organization's Cooperative Cyber Defense Centre of Excellence organizes the event, which includes fictional cyberattack exercises that test teams have to fend off under time pressure.

This year's competition is significant for the countries participating because their cyber defense units have been on high alert since the outbreak of the war in Ukraine, said Anett Numa, an international policy adviser in the cyber policy unit of Estonia's ministry of defense.

"Like-minded countries have to work together in order to protect themselves," Ms. Numa said. Ukrainian and Estonian experts will work on the same team in the exercise, she added.

Finland's government websites were attacked on April 8 while the government had been discussing joining NATO. Ukrainian government websites were hacked in January while Russian troops gathered around the country's borders. "Every single political decision can cause an attack," Ms. Numa said, referring to current discussions in Finland about joining NATO. Estonia also experienced a large-scale cyberattack in 2007.

NATO officials have been discussing various ways the alliance could help Ukraine fend off cyberattacks, and gave the country access to its malware information-sharing platform in January. In February, U.S. deputy national security adviser for cyber and emerging



technology Anne Neuberger, traveled to Brussels and Warsaw to discuss Russian cyber threats with officials from NATO, the European Union, Poland and Baltic countries.

The NATO alliance team includes around 30 cyber defenders from different NATO bodies and member countries with specializations such as communications, digital forensics, legal expertise and recovering systems damaged from an attack, said Ian West, chief of the NATO Cyber Security Centre, which defends NATO networks and is a part of the organization's communications and information agency.

The exercise is useful for cyber defenders from different countries to communicate with each other about attacks on the same technology products that several governments use, Mr. West said. "We all use commercial off-the-shelf systems. We're all using the same technology and, as we know, many of these technologies come to market and unfortunately they are vulnerable," he said.

The NATO center organizing Locked Shields doesn't make details of the simulated cyberattacks public. This year's exercise will focus on the "interdependencies between national IT systems," it said in a statement. The wargames don't draw on elements of the recent cyberattacks in Ukraine because those were too recent, but the exercise generally does include scenarios that occurred in real cyberattacks, Ms. Numa said.

In 2021, more than 2,000 participants took part in a simulation that tested how a country might respond to a large-scale cyberattack on its financial system and keep critical functions running, such as payments.

The benefit of the exercises is that it sets a baseline for participants to measure their cyber defense skills against each other, said Stefan Soesanto, a senior cyber defense researcher at ETH Zurich.

The games also help experts get to know their counterparts in allied countries, he said. "They're a huge alliance with partners behind them. If things happen, you can rely on them to assist you," he said.

New Tool in the Fight Against Hackers

Source: <https://www.homelandsecuritynewswire.com/dr20220429-new-tool-in-the-fight-against-hackers>

Apr 29 – People have used codes and encryption to protect information from falling into the wrong hands for thousands of years. Today, encryption is widely used to protect our digital activity from hackers and cybercriminals who assume false identities and exploit the internet and our increasing number of digital devices to steal from us.

As such, there is an ever-growing need for new security measures to detect hackers posing as our banks or other trusted institutions. Within this realm, researchers from the [University of Copenhagen](#)'s Department of Mathematical Sciences have just made a giant leap.

"There is a constant battle in cryptography between those who want to protect information and those seeking to crack it. New security keys are being developed and later broken and so the cycle continues. Until, that is, a completely different type of key has been found", says Professor Matthias Christandl.

For nearly twenty years, researchers around the world have been trying to solve the riddle of how to securely determine a person's geographical location and use it as a secure ID. Until now, this had not been possible by way of normal methods like GPS tracking.

"Today, there are no traditional ways, whether by internet or radio signals for example, to determine where another person is situated geographically with one hundred percent accuracy. Current methods are not unbreakable, and hackers can impersonate someone you trust even when they are far, far away. However, quantum physics opens up a few entirely different possibilities," says Christandl.

Quantum Physics Makes Hacking Impossible

Using the laws of quantum physics, **the researchers developed a new security protocol that uses a person's geographical location to guarantee that they are communicating with the right person.** Position-based quantum encryption, as it is called, can be used to ensure that a person is speaking with an actual bank representative when the bank calls and asks a customer to make changes to their account.

"Ask yourself, why do I trust an employee at the bank counter? Because they're in a bank. Their location creates trust. This explains the principle behind position-based cryptography, where physical location is used to identify oneself," explains postdoc Andreas Bluhm.

The researchers' recipe for securing a person's location combines the information in a single quantum bit – a qubit – followed by classical bits, consisting of the ones and zeroes that we are familiar with from ordinary computers.

Both types of bits are needed to send a message that is impossible for cybercriminals to read, hack or manipulate, and which can confirm whether a person is in your bank's office or in some far-off country.

The quantum bit serves as a kind of lock on the message, due to the role of [Heisenberg's Uncertainty Principle](#) in quantum physics, which causes quantum information to be disrupted



and impossible to decode when trying to measure it. It is also due to what is known as the “[no-cloning theorem](#)”, which makes quantum information impossible to intercept and secretly copy. This will remain the case for quite some time.

“Until a full-fledged quantum computer is built and hackers gain access to one, our method is completely secure and impossible to hack,” says Bluhm.

Could Soon Be a Reality

The researchers highlight the fact that the new method is particularly handy because only a single quantum bit is needed for position verification. So, unlike many other quantum technologies that require further development, this new discovery can be put to use today. Suitable quantum sources that can send a quantum bit of light already exist.

“The particular strength of our technique is that it is relatively straightforward to implement. We’re already able to send individual quantum bits, which is all this technique requires,” says Christandl.

The security ID needs to be developed commercially, by a company for example, before it can be widely adopted. However, its quantum foundation is in place.

The new research result is particularly useful in contexts where communications between two parties need to be extremely secure. This could be payments on the internet or transmission of sensitive personal data.

“Secure communication is a key element of our daily lives. Whenever we communicate with public authorities, our banks or any party that manages our personal data and information, we need to know that the people we’re dealing with are those who we expect them to be – and not criminals,” says Bluhm.

Orwellian “Ministry of Truth” becomes a reality in Biden’s America

Source: <https://ftglobalnews.com/2022/04/28/orwellian-ministry-of-truth-becomes-a-reality-in-bidens-america/>



Apr 28 – Internet users in the US are worried about the USA’s Department of Home Security (DHS) setting up a new Disinformation Governance Board. They feel that this board is going to function as the ‘Ministry of Truth’ from George Orwell’s ‘1984’.

The Orwellian “Ministry of Truth” functions as a propaganda branch of Big Brother, the dictatorial leader of the fictional totalitarian state Oceania in Orwell’s [1984](#).

Though described as the Ministry of ‘Truth’, it happens to control all forms of information – news, education, entertainment and art. The purpose is to delete old historical records and publish new information so that history is brought in line with Big Brother’s current pronouncements.

Parallels between the “Ministry of Truth” and Biden’s Disinformation Governance Board

The board under the Biden administration is being set up to coordinate countering misinformation related to homeland security. The board will focus ‘specifically’ on irregular migration and Russia.



Tim Young
@TimRunsHisMouth



The Biden Administration creating a DHS ‘Disinformation Governance Board’ is nothing more than a Ministry of Truth set up to silence opposition.

The 1st Amendment was designed to prevent the government from doing this... the 2nd Amendment was designed to stop them if they tried.

12:08 AM · Apr 28, 2022



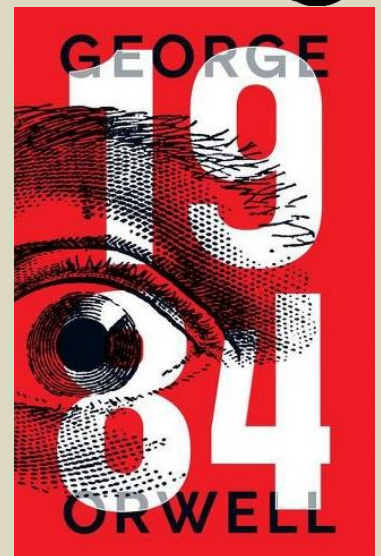
The board is to be designed as a means of ‘countering misinformation’. Again, this is a hyper-partisan effort to remove whatever the other side says as ‘misinformation’ and push through your own propaganda. This is what makes Biden’s Disinformation Governance Board a 21st century “Ministry of Truth”.

And this is exactly what is making Americans worried. Donald Trump Jr tweeted, “...So to make sure there are no abuses of power we are going to create a hyper-partisan government-controlled Ministry of Truth!!!”

Tim Young, a columnist tweeted, “The Biden Administration creating a DHS ‘Disinformation Governance Board’ is nothing more than a Ministry of Truth set up to silence opposition. The 1st Amendment was designed to prevent the government from doing this... the 2nd Amendment was designed to stop them if they tried.”

Why should the Americans be worried about the “Ministry of Truth”?

Jack Posobiec, a veteran Navy intel officer, has explained why the upcoming misinformation board is going to be problematic.



There are very serious issues at hand. The board will be headed by a hyper-partisan Nina Jankowicz – the same woman who had once claimed that armed Trump supporters would show up to the polls to intimidate voters. Really, is she the one who will control misinformation in the United States?

But then, this is how the Orwellian Ministry of Truth works. The very definition of ‘truth’ is reinvented and truth and misinformation are interpreted as per ideological convenience. So, what Jankowicz had said about Trump supporters may be made into truth by the Disinformation Governance Board.

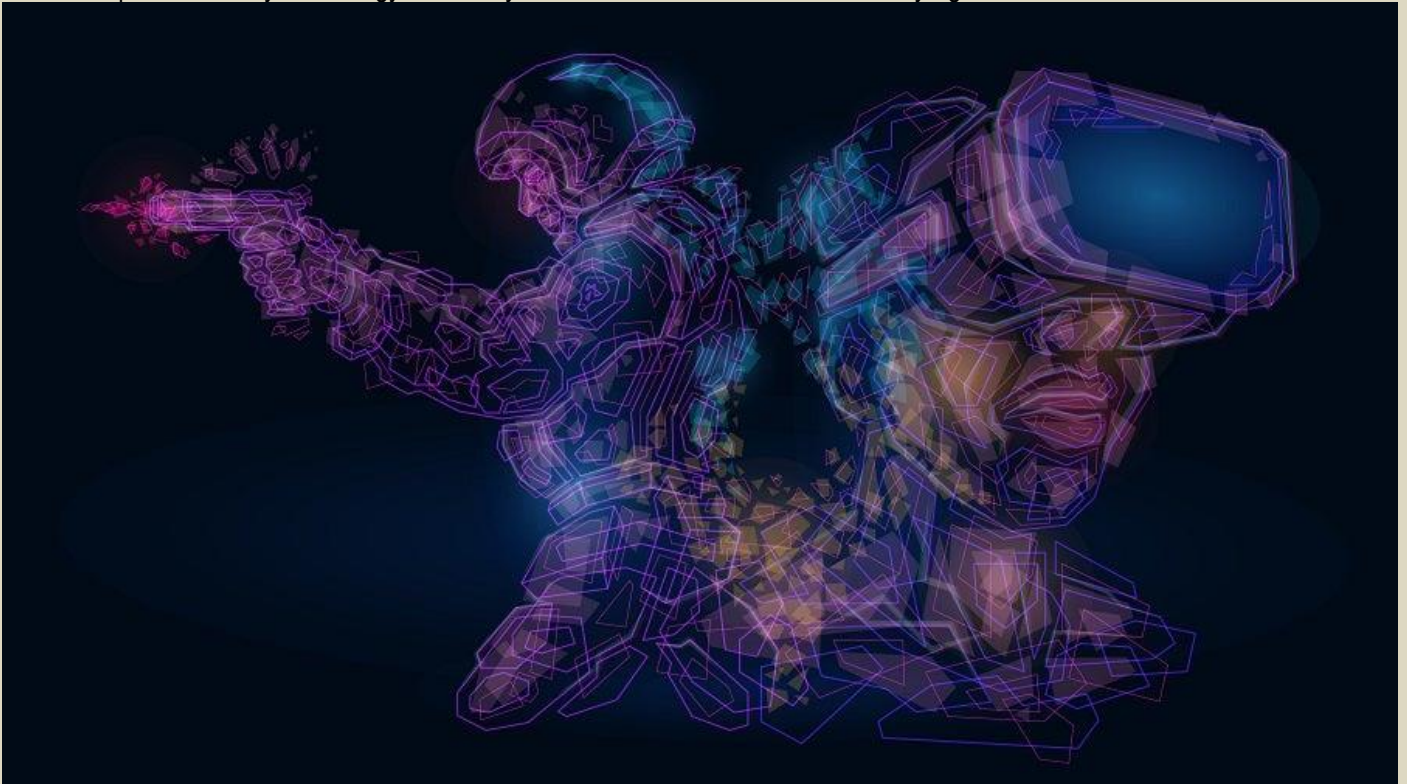
And wait, because it gets even better. Nina Jankowicz has previously worked as an advisor to the Ukrainian government under a Fulbright-Clinton Fellowship. She also has a past record of dismissing Hunter Biden’s infamous [laptop](#) as a fake story and blaming Trump for the controversy instead.

So, we know exactly what kind of ‘misinformation’ [Biden](#) is trying to control. He may utilise Nina Jankowicz, the head of the impending Disinformation Governance Board, to keep information regarding his and his son Hunter Biden’s multiple [misdeeds](#) under control. And this is how Biden is enacting the Orwellian “Ministry of Truth”.

The next level of simulation training: enter the defence metaverse

By Norbert Neumann

Source: <https://www.army-technology.com/analysis/metaverse-simulation-virtual-reality-4qd-hadean/>



May 03 – The idea of metaverse compels excitement in some, while making others cringe. Most of us have seen films or video games where the idea of a synthetic world comes to life, where participants can engage with each other free from the limits of reality. Like it or not, the metaverse did not elude the attention of the defence industry.

What is the metaverse?

There is no consensus around the definition of the metaverse, and explaining it is a bit like trying to define the internet. It is not a singular technology or even a singular concept. But for argument’s sake, this article will use a workable definition provided by *War on the Rocks* writers Jennifer McCardle and Caitlin Dohrman: “A metaverse is a series of interconnected and immersive virtual worlds that afford their users a sense of presence via agency and influence.”

It is similar to virtual or augmented reality in that it provides a spectrum where the physical and digital can meet. In military settings, these platforms are mostly used for the purpose of training. Commercial metaverse technology will not satisfy the military due to the lack of dexterity. But the price of the best available equipment on the market is eye-watering, and



defence departments may adopt technologies in the early stages with the aim of improving them to fit the requirements of the armed forces.

“If there is a greater push for cheaper but higher quality haptics and cheaper things like motion capture, and investments are going into those capabilities, then it could end up yielding something important for the military in the future,” says James Crowley, business development director at immersive urban training expert 4GD. “This will both improve the technology for the civilian market, and will also make it cheaper and much more accessible.”

Defence in the metaverse

Militaries have been using different forms of rudimentary metaverses for training for years. The development of the first simulator networking (SIMNET), where different virtual worlds were stitched together, started in the 1980s by the US military. SIMNET was a wide area network with vehicle simulators and displays for real-time distributed combat simulations that included tanks, helicopters and planes on a virtual battlefield. In the past two decades, the fidelity and effectiveness of simulated training and synthetic environments have grown momentously.

Nick Brown, defence product marketing director at distributed computing company Hadean, says: “Perhaps we can categorise the defence metaverse as an ‘industrial metaverse’. While the more familiar metaverse is focused on entertainment and social interaction of itself, industrial metaverses use the same technology in order to enhance activity in the physical world.”

Brown believes there are three key aspects to the metaverse that make it so appealing to defence. “Firstly, the virtual worlds of the metaverse are getting increasingly better at connecting more people from disparate locations,” he says. “Secondly, they can be used to simulate physical events at a high fidelity such that greater knowledge about the ‘real world’ can be derived.”

The third point, Brown says, is the metaverse’s ability to offer an immersive experience that would be too expensive, logistically or economically unfeasible or simply impossible to conduct physically. Combining these three aspects when placed into the concept of modern military acquisition, force development and training requirements, it is clear why defence is interested in the metaverse.

Crowley expects continued military interest in the metaverse in the future. “There’s an area for influence and an area where we need to be conscious of disparate groups coming together, and perhaps forming either very short-term collectives or of longer-term political groupings and we need to be fairly politically live to that as organisations,” he says.

He says if the metaverse changes the way individuals come together and the way information is exchanged, militaries and governments will need to be aligned to know how those interactions are taking place.

The challenges of the metaverse

It is also very important to consider the operational challenges of the metaverse. Building the computer power and infrastructure capable of running high-fidelity virtual worlds across a range of devices and handling enormous amounts of data will be equally imperative for the metaverse to exist.

“Being able to create these kinds of simulations may be cutting edge, but they’re no good if you need a PC the size of a car seat next to you while you run it,” Brown explains. “Every participant, whose device may vary, needs to be able to view and act within the simulation.”

“This is where distributed cloud and edge computing are set to change the game. If you can dynamically scale computation across cloud and edge environments, then this vastly lowers the requirements needed by devices to run the simulation.”

Crowley echoes the importance of computer power by saying: “This is probably the most impactful part of it. Unless you can reduce your latency to a point that it doesn’t make people ill and feels realistic, unless you can store move and communicate data across various different people in different simulators, you’re not going to provide a practical training tool.”

Another major challenge in developing an open metaverse where militaries of different countries could engage with each other is the aspect of security. “Ultimately, allied operations, for example among Nato countries, will be greatly enhanced by completing training simulations together, incentivising the creation of an open defence metaverse for them,” says Brown. He could envisage an open metaverse for defence where allied forces could all plug into the same virtual version of a given strategic context.

Crowley warns, however, that defence will have to be ruthless and extremely pragmatic when adopting certain technologies. Militaries need to ensure they do not take on new technologies just because they are the most recent on the market, but ensure they can provide the required results.

The development and employment of various metaverses and augmented realities are no new to defence, but the industry still has a long way to go before entering the metaverse for military purposes.

Norbert Neumann is the senior defence writer for Global Defence Technology and its sister websites. He joined after acquiring a degree in journalism and spending a short period with Times Radio’s news team.



Intelligence report identifies transnational security threats

Source: <https://www.securitymagazine.com/articles/97574-intelligence-report-identifies-transnational-security-threats>



May 09 – The U.S. Office of the National Intelligence Director has released the 2022 Annual Threat Assessment of the Intelligence Community, drawing from the findings of national and international intelligence agencies. The report outlined top global threats in 2022, including the risks posed to the U.S. by China, [Russia](#), Iran and North Korea. In addition to in-depth analyses of foreign developments, the report discusses COVID-19 and health security, as well as the effects of climate change in the United States. Intelligence officials highlighted additional transnational concerns facing the global stage in the report, naming many as top priorities to U.S. national interest. Among the transnational threats was technology innovation, which has driven economic development around the world. The report noted the disruptive nature of new technology, saying, “As with any disruption, some will thrive whereas others will struggle, potentially facing increasing inequalities and imbalances.” **The threats posed by new technology, according to the report, include compromising military communications, the wide availability of low-cost cyber tools and unmanned aerial vehicles (UAVs), and the growing use of long range and high accuracy military-grade weapons.** Transnational organized crime also represents a threat to national security, highlights the report. Human trafficking, illicit drugs, financial crime and cybercrime are the top risks involved with international crime. From mitigating ransomware to preventing human trafficking, security leaders can target these top transnational threats as they develop enterprise security plans. Among the other transnational threats outlined by the report were migration and global terrorism. Migration, as a result of transnational conflict, has risen to the forefront of international conversation since the report was released, with the [evacuations](#) caused by the Russian invasion of Ukraine.

► For more insights, download the intelligence report [here](#).

New Method Kills Cyberattacks in Less Than a Second

Source: <https://www.homelandsecuritynewswire.com/dr20220521-new-method-kills-cyberattacks-in-less-than-a-second>

May 21 – A new method that could automatically detect and kill cyberattacks on our laptops, computers and smart devices in under a second has been created by researchers at [Cardiff University](#).

Using artificial intelligence in a completely novel way, the method has been shown to successfully prevent up to 92 per cent of files on a computer from being corrupted, with it taking just 0.3 seconds on average for a piece of malware to be wiped out.

Publishing their findings in the journal [Security and Communications Networks](#), the team say this is the first demonstration of a method that can both detect and kill malicious software in



real-time, which could transform approaches to modern cybersecurity and avoid instances such as the recent WannaCry cyberattack that hit the NHS in 2017.

Using advances in artificial intelligence and machine learning, the new approach, developed in collaboration with Airbus, is based on monitoring and predicting the behavior of malware as opposed to more traditional antivirus approaches that analyze what a piece of malware looks like.

“Traditional antivirus software will look at the code structure of a piece of malware and say ‘yeah, that looks familiar’,” co-author of the study Professor Pete Burnap explains.

“But the problem is malware authors will just chop and change the code, so the next day the code looks different and is not detected by the antivirus software. We want to know how a piece of malware behaves so once it starts attacking a system, like opening a port, creating a process or downloading some data in a particular order, it will leave a fingerprint behind which we can then use to build up a behavioral profile.”

By training computers to run simulations on specific pieces of malware, it is possible to make a very quick prediction in less than a second of how the malware will behave further down the line.

Once a piece of software is flagged as malicious the next stage is to wipe it out, which is where the new research comes into play.

“Once a threat is detected, due to the fast-acting nature of some destructive malware, it is vital to have automated actions to support these detections,” continued Professor Burnap.

“We were motivated to undertake this work as there was nothing available that could do this kind of automated detecting and killing on a user’s machine in real-time.”

Existing products, known as endpoint detection and response (EDR), are used to protect end-user devices such as desktops, laptops, and mobile devices and are designed to quickly detect, analyze, block, and contain attacks that are in progress.

The main problem with these products is that the collected data needs to be sent to administrators in order for a response to be implemented, by which time a piece of malware may already have caused damage.

To test the new detection method, the team set up a virtual computing environment to represent a group of commonly used laptops, each running up to 35 applications at the same time to simulate normal behavior.

The AI-based detection method was then tested using thousands of samples of malware.

Lead author of the study Matilda Rhode, now Head of Innovation and Scouting at Airbus, said: “While we still have some way to go in terms of improving the accuracy of this system before it could be implemented, this is an important step towards an automated real-time detection system that would not only benefit our laptops and computers, but also our smart speakers, thermostats, cars and refrigerators as the ‘Internet of Things’ becomes more prevalent.”

Who hacked the slaughterhouse? When robots and AI take over farms

By Susan D’Agostino

Source: <https://thebulletin.org/2022/05/who-hacked-the-slaughterhouse-when-robots-and-ai-take-over-farms/>

May 23 – Security analysts [warned](#) the US Agriculture Department in May 2021 that a cyberattack could produce more chaos in the food supply chain than COVID-19. Less than a month later, JBS, the world’s largest meat processor, was hit by a Russia-linked ransomware attack that crippled its plants that produce nearly [one-quarter](#) of US beef and food for other countries. JBS paid \$11 million in bitcoin to reestablish itself as a critical link in the food supply chain. Then, a few months later, hackers [demanded](#) \$5.9 million from New Cooperative, an Iowa grain co-op whose computer network manages the feeding schedule of millions of chickens, pigs, and cows. Dozens of malware and ransomware attacks like these have targeted food manufacturers, processors, and packagers in recent years. And last month, the FBI [issued](#) a new alert that cybercriminals are now targeting farms and food producers during critical planting and harvest seasons.

Agriculture today faces many challenges, including climate change, labor shortages, small margins, and [supply chain problems](#) caused by the war in Ukraine and COVID-19. Online data systems like those at JBS and New Cooperative promise to ameliorate some of these challenges by boosting productivity. Sensors that record and transmit agricultural data over the internet help farmers make decisions that might increase their yields at minimal cost. Artificial intelligence (AI) can be used to detect patterns in agricultural data that help reduce expensive [inputs like fertilizer](#) while maximizing crop yields. These advanced technologies, in turn, may help feed the more than [two billion](#) people around the world who struggle with food insecurity.

Yet swift adoption of these technologies may leave computer-aided food systems vulnerable to hacking, according to a recent [paper](#) published in *Nature Machine Intelligence*. Designers of robots and AI in agriculture should assess the risks and establish protocols for problems that can be reasonably anticipated. If not, their inventions may intensify socio-economic inequality and harm the environment.



“If the advantages of AI in agriculture are explicit, so should be [their] associated possible adversities,” Asaf Tzachor, lead author of the paper, said.

The benefits and risks of autonomous robots and AI in farming.

AI and autonomous robots hold potential to be a boon for agriculture. AI, for example, may detect and diagnose plant diseases early, after which algorithms can direct autonomous robots to treat problems. It can predict weather and crop yields, helping farmers plan. It can also automate tilling, planting, fertilizing, monitoring, and harvesting. In most of these tasks, it outperforms humans in processing, synthesizing, and analyzing real-time agricultural data relevant to farmers’ decision making. Also, algorithms can regulate drip-irrigation grids, command fleets of topsoil-monitoring robot swarms, and supervise weed-detecting rovers, self-driving tractors, and combine harvesters, according to Tzachor. These practices often conserve resources, save labor, minimize loss, and increase revenues.

But many of these systems rely on the internet, which means that hackers can attempt to disrupt these digitized food supply chains. Cyberattacks can interfere with AI-driven machinery designed to harvest, inspect crops, or apply fertilizer and pesticides. Such



attacks may affect every link in the food supply chain, including growth, processing, and distribution.

“I’m fascinated with the notion of progress traps,” Tzachor said of his motivation for the research, “...dynamics in which implementing a promising technological fix to one problem inadvertently prompts a novel and far more wicked problem.”

Sometimes a threat, whether inadvertent or intentional, comes from within. For example, before a self-driven machine can head out to a field, it must be programmed by a human who is susceptible to making mistakes.

An entire crop may suffer if a program

directs an autonomous robot to apply an inadequate amount of water or too much of an herbicide, pesticide, or fertilizer. Even when a device performs as intended, a poor design may leave a food system vulnerable. For example, wireless sensors that detect pests and robots that apply chemicals may be programmed in such a way that prioritizes short-term crop productivity over the long-term health and integrity of the environment. Automated tilling, which is known to harm topsoil, may exacerbate soil erosion. In short, AI’s narrow focus on agricultural yields may, in fact, ignore problems with pests, biodiversity, and pollution, according to the study.

Who reaps the benefits of AI and robots in agriculture?

Some agricultural AI relies on data kept by national and international research institutions. This data must be relevant to be useful. But decades’ worth of this institutional data has focused on staple crops from wealthy countries such as wheat, rice, and corn, according to Tzachor’s study. Large data sets focused on crops like quinoa, cassava, and sorghum produced by low-income, subsistence farmers around the world are much harder to find. Similarly, indigenous farmers’ sustainable approaches to planting, pest control, and harvest are often overlooked.

“Small-scale growers who cultivate the majority of farms worldwide and feed large swaths of the so-called global south are likely to be excluded from these AI-related benefits,” Tzachor said. Even if the relevant data existed, many small farmers live in remote regions where the internet access on which digitized farming relies is poor. As a result, the burgeoning use of artificial intelligence in agriculture may widen the gap between commercial and subsistence farmers.

In some cases, the private sector and NGOs have partnered with underserved agricultural regions to help minimize this technology gap. In sub-Saharan Africa, for example, more than [60](#) percent of the land consists of small farms and 23 percent of the GDP hails from agriculture. In Ghana, the private [Farmerline Group](#) has funded technology that supports distribution networks. “We think of ourselves as the Amazon of farmers... a digital and physical infrastructure powering a marketplace that allows the movement of goods and services to and from rural areas,” Alloysius Attah, Farmerline’s co-founder, [told TechCrunch](#). For his efforts, Attah was [named](#) a 2021 Bloomberg New Economy Catalyst.



Still, even farmers with access to digitized tools are encountering problems, according to Diana Moss, president of the American Antitrust Institute. Farmers who sign technology agreements with big agricultural biotech companies often sign away their rights to the data, leading to what's known as a "closed cropping system."

"The closed cropping system basically says, 'Look, you get to use Monsanto products only. Or you get to use Dow products only,'" Moss said of farmers' choices for the proprietary seeds, chemicals, and more that go hand-in-hand with corporate data collection. "The big ag biotechs are engineering their cropping systems to be non-interoperable with rival technologies."

Once farmers are locked into a company that holds their data, both farmers and consumers will pay higher prices, Moss said: "It contributes to a very, very fragile agricultural supply chain."

How can the risks of automated agriculture be minimized?

Advanced technology in agriculture is not inherently bad and is poised to deliver benefits. That said, problems arise when humans fail to predict and prevent the unintended consequences of its use.

"Much like in the digital tech sector with Facebook, Amazon, and Google, it's all about having just a few or a single dominant player with really strong incentives to use data to control competition, to the detriment of growers and consumers," Moss said. "Merger control and strong antitrust enforcement is really the starting point for controlling all of this."

[CGIAR](#), a global research partnership of agricultural research institutes, encourages the use of findable, accessible, interoperable, and reusable—FAIR—data principles. Farmers should be able to own their data and share it at their discretion, without compromising their privacy or introducing security risks. But democratizing data in this way requires sophisticated cooperatives. Brookings has [recognized](#) efforts worthy of emulation, including [Twiga Foods](#) in Kenya and the [Tanihub Group](#) in Indonesia, both of which are at work digitizing the small-farm-to-table supply chain.

Tzachor and his team also suggest the use of "digital sandboxes" in which researchers and farmers can assess risks and make



recommendations for oversight before the systems go live. The [HandsFree Hectare](#) at Harper Adams University, for example, operates a hybrid cyber-physical space in which they test for unintended consequences.

Rural anthropologists, applied ecologists, ethicists, and data scientists should also be invited to collaborate with computer scientists who are at work developing robots and AI for agriculture, Tzachor suggests. This may act as an insurance policy against environmental harm and socio-economic inequities resulting from their use.

Last month, the FBI [warned](#) the food

and agricultural sector that cybercriminals are now timing their attacks on the industry to coincide with critical seasons such as planting and harvesting. Such attacks may increase the victims' willingness to pay ransom, given that any delay could result in an unrealized or spoiled harvest. The FBI recommended [steps](#) to prevent cyberattacks, such as backing up data, using multifactor authentication and strong passwords, updating antivirus and antimalware software, and designing a recovery plan.

"Some 50 malware and ransomware attacks targeting food manufacturers, processors and packagers were registered over the past two years," Tzachor said while acknowledging that none to date have been catastrophic. "That may be attributed to the fact we have not yet delegated a great deal of autonomy to machines to administer our farms."

Susan D'Agostino is an associate editor at the *Bulletin of the Atomic Scientists*. Her writing has been published in *The Atlantic*, *Quanta Magazine*, *Scientific American*, *The Washington Post*, *BBC Science Focus*, *Wired*, *Nature*, *Financial Times*, *Undark Magazine*, *Discover*, *Slate*, *The Chronicle of Higher Education*, and others. Susan is the author and illustrator of [How To Free Your Inner Mathematician: Notes on Mathematics and Life](#) (Oxford University Press, 2020). She is a member of the editorial board of the Mathematical Association of America's *Math Horizons* magazine. Susan earned a PhD in mathematics at Dartmouth College and an MA in science writing at Johns Hopkins University. She has received science writing fellowships



from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.



ICI
International
CBRNE
INSTITUTE



& Robotic

DRONE NEWS



Electronic Warfare to Cyber and Beyond: How Drones Intersect with the Information Environment on the Battlefield

By Zachary Kallenborn

Source: <https://mwi.usma.edu/from-electronic-warfare-to-cyber-and-beyond-how-drones-intersect-with-the-information-environment-on-the-battlefield/>



Apr 27 – In the ongoing war in Ukraine, both sides have used drones. The [Ukrainian military](#) has used Bayraktar TB-2 drones to carry out strikes, conduct reconnaissance, and collect video that features in propaganda. Even Ukrainian civilians have joined the effort—just as civilians from widely divergent backgrounds have volunteered by [assembling Molotov cocktails](#), [manning defensive positions](#), and [facilitating the movement of supplies](#), an [NGO made up of volunteers](#) is customizing drones used daily in the war. On the other side of the blurred front lines, the Russian military is also using small drones to [direct artillery](#), while the [Orion](#) carries out occasional strikes.

Together, the unfolding conflict offers a glimpse into the future of drone warfare. But what we're seeing is just the beginning. Global militaries are building unmanned ground vehicles like the Russian [Uran-9](#), [large unmanned surface vessels](#), unmanned undersea vehicles, and large aerial swarms like the [Perdix](#).

Drones have become an increasingly broad category of platforms—and will only become more so as technology continues to advance. They can be used on land, at sea, or in the air, and will soon [likely feature in space](#). Beyond all of these domains, drones' interaction with warfare's information environment requires special attention. In particular, how do they relate to specific dimensions of information warfare—from electronic warfare to psychological operations? And how do they intersect with the information components of the space and cyber domains? Modeling, simulation, wargaming, exercises, policy analysis, strategic analysis, and everything in between—all are needed to fully understand the military implications of drones. All of these, however, need to be based on a fundamental initial understanding of the nexus between drones and the information environment, both where that nexus is today and where it will migrate in the future.

Electronic Warfare

Drones typically depend on the electromagnetic spectrum to receive commands. This may include where to move; when, what, and where to attack; and everything in between. Jamming those signals would disrupt the drone, regardless of whether it's flying in the air, sailing at sea, or driving on land. Soldiers can think for themselves and strategize without communications, but drones cannot. Unsurprisingly, jammers are the most common form of counterdrone system with over 70 percent of [counterdrone systems](#) incorporating jamming as a standard feature.



Greater autonomy may reduce dependence on the electromagnetic spectrum, because fewer commands are needed for operation. Yet, greater autonomy may also increase cyber and space warfare vulnerabilities, because the system will require more complex computing, perhaps using GPS to navigate. Greater autonomy may also mean the drone is more vulnerable to manipulation: In 2011 Iranian forces captured an American [RQ-170 Sentinel](#) drone, claiming to have sent it false GPS signals to get it to land. US officials [publicly dismissed Iran's claim](#), saying instead that operators lost control of the drone—but the episode nonetheless draws attention to the very real prospect that increased autonomy could lead to increased vulnerability.

Cyber Warfare

Drones rely on complex computer systems for operation. Drone operators use specialized software often on specially designed ground control stations to issue commands. Onboard the drone, microcontrollers—basically, small computers—manage the drone's operation. Drone operators issue commands and the microcontroller adjusts the motors, rotors, or other mechanical components as required. Microcontrollers also allow preprogrammed autonomous flight and obstacle avoidance.

Cyber dependence means [cyber vulnerability](#). An adversary could use cyberattacks to deauthenticate the drone from the ground control station, disable the drone engines or propellers, or issue false commands. In July 2015 researchers used cyberattacks to disable the brakes on a [Jeep Cherokee](#). Similar cyberattacks could disrupt drone operations, cause the drones to crash, collect information to inform future attacks, or redirect the drones to attack friendly targets.

Space Warfare

Compared to electronic and cyber warfare, the relationship between drones and space warfare is at a more rudimentary stage, making projections on the form that relationship might take more variable. Satellites support drones by providing communication links for flight that extends beyond visual line of sight and localization through GPS. Small aerial drones use GPS to support autonomous navigation, to include simple actions like hovering over an area; however, GPS is not technically required (though in the United States, it is required to meet various [Federal Aviation Authority](#) regulations). Larger systems like the MQ-9 Reaper that fly thousands of miles from their operators definitely need GPS, though the Air Force is developing [technology](#) for navigation in GPS-denied areas. Targeting satellite constellations would allow an adversary to disrupt numerous unmanned systems over a broad area, in addition to whatever systems rely on those satellites.

Psychological Warfare

Drones are great vehicles for collecting and disseminating propaganda. The Ukrainian military has [released](#) several videos of Bayraktar TB-2 drones loitering above—and then destroying—Russian vehicles. Ukrainian patriots even wrote an [uplifting ballad](#) using the videos to celebrate the TB-2. The Ukrainians are not the first to recognize this potential. The Islamic State has also [used drones](#) to photograph, record, and [share its battlefield successes](#). Drones can also be propaganda themselves by helping an organization show itself as a powerful, modern power.

At the same time and also related to the information effects of drone use, there is growing public concern around the use of autonomous weapons. A January 2016 [Ipsos](#) poll found 61 percent of respondents opposed autonomous weapons, including strong majorities in several NATO countries. As autonomous weapons scale into drone swarms those concerns are likely to grow. And as these swarms grow in size, weaknesses of artificial intelligence may result in drone swarms becoming future [weapons of mass destruction](#). Weapons of mass destruction carry significant normative and policy implications, where use may bring into play international treaties, economic and diplomatic sanctions, and military interventions. This would likely incentivize states to use information campaigns to tap into those norms and weaken adversaries' political standing. The challenges of [verifying](#) autonomous weapons use offer ripe opportunities for disinformation to create uncertainty around the fundamental question of whether an autonomous weapon was really used.

Policy Recommendations

All of this means several things for the US military. First, at the tactical level, commanders need to consider the information environment when deploying drones on the battlefield, especially in mass. Commanders may need to deploy dedicated defenses against electronic warfare, take appropriate countermeasures to protect a range of vulnerabilities, and at times perhaps even rethink the deployment. Commanders also need to think about how information warfare systems interact with other systems in countering drones. For instance, if a platoon faces a mixed swarm of ground and aerial drones, how might jamming support anti-air and anti-vehicle weapons? Commanders will require appropriate training and education prior to battle—and be able to rely on appropriate doctrine when challenges emerge—to help them make informed decisions.

Second, larger, technical analyses are needed to better understand how information warfare interacts with drones in various situations. The descriptions above are simply a starting point.



Modeling and simulation should be conducted to identify the most effective information warfare means to counter different types of drones, in different numbers, working across different (or multiple) domains. Wargames, exercises, and simulations may also explore the effects of unmanned systems in various offensive information roles, like electronic attack, to better understand the trade-offs between unmanned and manned systems and develop attendant concepts of operations.

Third, to the degree unmanned systems will increasingly define the future of warfare, the US military must also prioritize information warfare. Developing new technical, doctrinal, and strategic approaches to waging information warfare—electronic warfare, in particular—and to refining concepts for both cyber and space warfare will help the United States defend against adversary measures while protecting friendly unmanned systems. Because the United States faces [significant challenges](#) and [competition](#) across [each dimension](#) of [information warfare](#), this may require significant new investments and organizational developments. Specifically, the United States should conduct a review across the armed forces and critical supporting civilian agencies of information warfare capabilities and gaps.

Ultimately, we can confidently predict that the nexus between drones and information warfare will become an increasingly significant one on the future battlefield. Yet, although that connection is critical to the future use of drones, our understanding of it is rudimentary. That needs to change.

Zachary Kallenborn is a policy fellow at the Schar School of Policy and Government, a research affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism, an officially proclaimed US Army “Mad Scientist,” and national security consultant. His research on autonomous weapons, drone swarms, and weapons of mass destruction has been published in a wide range of peer-reviewed, wonky, and popular outlets, including the Brookings Institution, *Foreign Policy*, *Slate*, *War on the Rocks*, and the *Nonproliferation Review*. Journalists have written about and shared that research in the *New York Times*, NPR, *Forbes*, the *New Scientist*, and *Newsweek*, among dozens of others.

DJI Statement On Military Use Of Drones

Source: <https://www.dji.com/sg/newsroom/news/dji-statement-on-military-use-of-drones>



Apr 21 – More than 15 years ago, DJI was founded to explore the astonishing new possibilities of drone technology. From our first attempts at building tiny helicopters to our latest cutting-edge drones for professionals, we have been driven not just by the technical challenge of robotic innovation, but by how this new technology can help people. And with every improvement and advance, our drones have helped make the world better. Our products have enabled new ways to see our world, a new storytelling language for creators, new business and job opportunities, new techniques for growing food and protecting our environment, and new capabilities for responding to emergencies. Our drones have preserved endangered species, saved global landmarks from destruction, and saved lives all over the world.

With that in mind, we want to reiterate a position we have long held: our products are made to improve people’s lives and benefit the world, and we absolutely deplore any use of our products to cause harm. DJI has only ever made products for civilian use; they are not designed for military applications. Specifically:

- DJI does not market or sell our products for military use.
- DJI does not provide after-sales services for products that have been identified as being used for military purposes.
- DJI has unequivocally opposed attempts to attach weapons to our products.
- DJI has refused to customize or enable modifications that would enable our products for military use.

DJI believes strongly in these principles. Our distributors, resellers, and other business partners have committed to following it when they sell and use our products. They agree not



to sell DJI products to customers who clearly plan to use them for military purposes, or help modify our products for military use, and they understand we will terminate our business relationship with them if they cannot adhere to this commitment.

DJI is dedicated to creating products that benefit society. We take great pride that our drones have rescued people who were lost and near death, enabled scientists to protect our environment, enabled enterprises to improve workflows and reduce risk in challenging times, and created enjoyment for millions of people around the world. We will never accept any use of our products to cause harm, and we will continue striving to improve the world with our work.

How Concerned Should We Be about the Iranian Drone Threat?

By Seth J. Frantzman

Source: <https://www.meforum.org/63215/how-concerned-should-we-be-about-the-iranian>

May 05 – The US House of Representatives voted last week to pass the **Stop Iranian Drones Act**.

"It shall be the policy of the United States to prevent Iran and Iranian-aligned terrorist and militia groups from acquiring unmanned aerial vehicles, including commercially available component parts, that can be used in attacks against United States persons and partner nations," the bill says.



Iranian drones, such as the Shahed 129 (photo) threaten the region's stability by giving Iran an instant air force.

The move was an important step in highlighting the increased Iranian drone threat to the region. It is also important because the bipartisan legislation was sponsored by Reps. Michael McCaul (R-Texas), Gregory Meeks (D-New York), Ted Deutch (D-Florida) and Joe Wilson (R-South Carolina). US lawmakers are

beginning to understand how drones, and various versions of what are called UAVs and unmanned aerial systems (UAS), are playing an emerging role in the Middle East.

Iran got its start in drone warfare relatively early, back in the mid-1980s. The country had recently gone through the Islamic Revolution of 1979 and was fighting a vicious war against Iraq. Iraq had a plethora of military equipment, especially Soviet arms. Iran, by contrast, was stuck with American military supplies left over from the shah's era. Without spare parts, it couldn't fight the war without mass human wave attacks and high casualties. Some Iranians understood that drones, which Israel had used with effect against Syrian air defenses in 1982, were the wave of the future. In those days drones resembled large model airplanes, operated by remote control. In Iran's hands the drones were used to do surveillance of the front.

Fast-forward 20 years to the 2000s and we find Iran beginning to build larger, more sophisticated drones. These were often modeled on captured drones or blueprints of foreign UAVs. This included Iran's attempt to copy the American Predator and secretive Sentinel drone. Iran's copies were slower, had less of a range and had worse cameras than the US models. But Iran was showing that, despite sanctions, it had success with these futuristic weapons.

Iran's investment in drones in the last decade appears to be an outcome of the Iran deal and the US decision to leave that deal. In 2015 Iran's regime believed that, through sanctions relief, it might get access to trade and more advanced weapons and hi-tech from abroad. However, it soon realized this might not happen, and the Islamic Revolutionary Guard Corps took advantage of the regime waiting for sanctions relief and the relief's failure to materialize to showcase new drones to the ayatollah. The result was that the IRGC got the upper hand in an arms race and received some benefit from a window of appeasement of Iran after 2015 that enabled it to move more drones to the Houthis in Yemen and to Hezbollah. As the Syrian regime began to turn the tide in Syria, Iran also moved more drones to Syria's T4 air base in 2017 and then to the Golan area in 2018 and 2019.



Meanwhile, in [Iraq](#), as the pro-Iranian Shi'ite militias such as Kataib Hezbollah became empowered after the war against ISIS, they also received new drone technology. Soon the Hashd al-Sha'abi or PMU, the umbrella group that Kataib Hezbollah operates under, was using drones. Kataib Hezbollah used them to threaten Saudi Arabia and later the UAE between 2019 and 2022. These groups also began to threaten US forces in Erbil, the capital of the Kurdistan autonomous region. Iran also used drones in Syria to threaten US forces, first in 2017 and then in 2021 when it threatened the Tanf garrison of US forces that are in Syria near the Jordanian border.

What is clear is that Iran set its goal as perfecting several cheap kamikaze munitions, called "loitering munitions," which are a combination of drone and cruise missile technology. The Houthis in Yemen turned this into the Qasef line of drones, modeled on one of Iran's lines of Ababil drones. Hezbollah and Hamas also operated similar drones, as does the PMU in Iraq.

Soon these drones were threatening Saudi Arabia. In September 2019 Iran went one step further and carried out an attack on Saudi Arabia's Abqaiq energy facility, using drones and cruise missiles. This lifted the veil on a new Iran strategy using kamikaze drones against sensitive infrastructure.

Iran also began to test Israel's defenses with drones flown from Syria in February 2018, the aforementioned Hezbollah drone use near the Golan in August 2019, a drone flown from Iraq in May 2021 and other threats emanating from Iran in early 2021, as well as early 2022. This coincided with the rising Iran drone threat against US forces in Iraq in 2021 and the use of a drone against a commercial ship in July 2021.

Iran uses drones in part because this gives it a kind of instant air force, when it can't acquire new warplanes. These cheap weapons also enable it to threaten the whole Middle East over thousands of kilometers, attacking at a place and time of its choosing. It can base drones, such as the V-shaped Shahed 136, in places like Yemen and threaten Israel without even needing to use the drones. Drones also let Iran empower proxies and partners such as Hezbollah and Hamas.

When Iran moves the technology to these groups, it can deny that it is behind the drone attacks. Furthermore, drone attacks enable Iran to not risk its own soldiers, and it can claim plausible deniability when its drones slam into ships or other places.

When Iran uses drones, if there are no casualties, the country being attacked can also refrain from retaliating, meaning the use of drones sometimes means less urgency for countries to go to war.

This new drone war has been on display, with [Hezbollah](#) using drones to try to penetrate Israel's airspace as well. Hezbollah wants a propaganda public relations coup in these incidents. It may not even care about how well its drones perform.

While Hezbollah has a large number of drones, the real goal of Iran and its proxies may sometimes be to test Israel's defenses, rather than use them to destroy things.

Nevertheless, the threat is rapidly rising. Hamas used new drones in the May 2021 conflict. The attacks against US forces in Iraq and Syria, and against a ship in the Gulf of Oman in July 2021, as well as reports the US downed drones over Iraq that were heading to Israel, are all examples of the rising threat.

[Seth Frantzman](#) is a Ginsburg-Milstein Writing Fellow at the Middle East Forum and senior Middle East correspondent at [The Jerusalem Post](#).

EDITOR'S COMMENT: Shahed 129 is a big drone (length 8m; wingspan 16m). Therefore it requires an equal big runway for takeoff and landing and this is something that can easily betray the location of the Hezbollah drone base. Unless they use public roads or the Beirut-Rafic Hariri International Airport; something difficult to hide.

Iran's Drones Tip the Balance of Power in the Middle East

By **Dr. Uzi Rubin** (expert on missile defense and the resilience of Israel's home front)

Source: <https://jiss.org.il/en/rubin-irans-drones-tip-the-balance-of-power-in-mideast/>



Jan 2022 – Iran has been developing and expanding its Unmanned Air Vehicles¹ fleets ever since the 1980s.

They now comprise a wide spectrum of types that range in size and function from aircraft size, high flying reconnaissance UAVs to small, low-cost "suicide" ones. Until fairly recently, Israel's military regarded the threat from Iran's UAVs – either operated by Iran's armed forces or by their proxies in the region – as a minor component of the overall military threat, compared to the major strategic threat from Iran's fleet of ballistic missiles and its proxies' rockets deployed in Iraq, Syria, Lebanon, Yemen, and Gaza.

This view seems to have changed dramatically, judging by recent reports in the Israeli and US media and strong statements made by Israel's leadership. Amos Harel, Haaretz daily military analyst, reported that "Iran relies on UAVs as a counterweight to Israel's air superiority", adding that "Israel's military High Command is worried by the spread of Iran's UAV capabilities to more and more of Iran's proxies."²



Three months later, the same concern was expressed by top Israeli leaders. In his September 12, 2021 speech to the Reichman University's Institute for Counter-Terrorism, Israel's Minister of Defense Benny Gantz disclosed that "One of Iran's most potent weapons is its fleet of UAVs." According to Gantz, "This is an array of lethal and precise weapons, that like ballistic missiles can traverse thousands of kilometers. The Iranians produce and provide these air vehicles to their proxies, who in turn use them in coordination with and under the command of the Revolutionary Guard and its Quds Brigades."³ Gantz, in fact, thereby elevated Iran's UAVs to the top rank of threats, on par with Iran's nuclear threat.

Israel's Prime Minister Naftali Bennett was even blunter. In his September 27, 2021 speech to the UN General Assembly, he emphatically stated that "Iran has recently established a new terror weapon unit.... swarms of armed UAVs carrying lethal weapons that can strike anywhere, anytime." Moreover, he warned that "Iran has already used these lethal UAVs, dubbed "Shahed 136" to attack Saudi Arabia, US bases in Iraq and cargo ships on the open seas." He warned that "Iran intends to arm its proxies in Yemen, Iraq, Syria, and Lebanon with hundred – and later with thousands – of this kind of UAVs."⁴ Remarkably, Bennett made no mention of the Iranian missile threat. Taken together, Bennet's and Gantz's statements testify to the mounting concern in Israel over the threat of Iran's UAVs, a threat that by itself is not new but which has now reached a kind of "critical mass" that render it equivalent to the nuclear threat and that overshadows the missile and rocket threats from Iran and its proxies.

Apparently, Iran's UAVs have evolved into an issue of concern for the US administration too. A recent Wall Street Journal article, titled "Iran Armed Drone Prowess Reshapes Security in the Middle East" discloses that "Teheran uses off the shelf materials to manufacture armed drones that challenge the US and its allies in the region." The article proceeds to quote unnamed sources in Europe, the United States, and Israel who say that Iran's fast-expanding capabilities to design, manufacture and deploy UAVs "Are altering the balance of power in the region."⁵

Following the October 10, 2021 attack by Iranian-made UAVs on US troops in the El Tanf base in Syria, the administration sanctioned Iranian persons and industries engaged in UAV design and manufacturing. It seems, then, that US and Israel share similar views about this new threat.

Threat Evolution

Iran's engagement in developing, deploying, and transferring UAVs to its proxies is not a new phenomenon. Iranian UAVs operated by Hezbollah penetrated Israeli airspace already 16 years ago, even before the 2006 Lebanon War. In July 2006, while that war was still raging, Hezbollah launched three or four bomb-laden UAVs towards central Israel. One suffered a technical failure and crashed near the Lebanese border, while two more were shot down by air-to-air missiles fired from Israeli F-16 fighter jets. The fate of the fourth one – if there was a fourth – is not known. Following the 2006 war, Hezbollah's Iranian-supplied UAVs made several attempts to reconnoiter Israel, all being intercepted and shot down. In addition, Iran itself tried to send its own UAVs into Israel's airspace at least twice, once in February 2018 from an Iranian-operated airbase in Syria and again in May 2021 from Iraq. On both occasions, the UAVs were destroyed before penetrating Israeli airspace.

Since almost a decade ago, Iran's proxies in Gaza have been stoking up with locally made – but Iranian designed – armed UAVs. As early as 2012, during Operation Pillar of Defense, the Israel Defense Forces (IDF) destroyed a Hamas UAV poised to take off from the old Gaza airport runway. During the July – August 2014 escalation (operation Protective Edge), Hamas launched several UAVs into Israel, which managed to cross the Gaza border. Two or three of them were shot down by Patriot air defense systems.

In the recent May 2021 escalation (Operation Guardian of the Walls), Hamas unveiled a new type of suicide UAV – unseen before in Gaza, but familiar from Iran's proxies operations in Yemen and Lebanon. Hamas launched five or six of them towards Israeli border towns. Most, if not all were shot down by the Iron Dome short-range air and missile defense system. Hamas claimed that one of its new UAVs managed to break through Israel's defenses, hitting a "chemical plant" within Israel. A video clip released by Hamas shows a UAV diving and exploding near the Nirlat paint factory in Kibbutz Nir Oz, about 3 km (1.9 miles) from the Gaza perimeter.

The proficiency of Iran's UAVs and their operators have been demonstrated repeatedly in the region ever since the onset of the war in Yemen in 2014. Iran's UAVs operate in the skies of Saudi Arabia, the Persian Gulf, Iraq, and Syria. They have been extensively used in a broad spectrum of operations, including retaliation against ISIS bases, battlefield support of the Assad regime forces in their campaign to regain control in Syria, in attacking cities, national infrastructures, and oil targets in Saudi Arabia, and in targeted killing of high-ranking officers and officials of the internationally recognized Yemeni government.

Scant attention was paid to the role of Iranian originated, Quds brigade smuggled UAVs in the fighting inside Yemen and the war of attrition against Saudi Arabia. However, this changed abruptly after the surprise attack by Iran's UAVs on September 14, 2019, against two of Aramco's main oil facilities in Saudi Arabia. In a meticulously planned operation that surprised most if not all Intelligence services in the West (Including Israel's Mossad), less than 30 low-cost Iranian UAVs caused tremendous damage to two of Saudi Arabia's key oil installations, reducing oil exports capacity by more than one-half for several months. This brilliantly conceived operation, a veritable "mini-Pearl Harbor" used mainly of the Shahed 136 suicide UAVs later mentioned by Israel's PM's UN speech. The Iranian UAV swarms reached their targets in the depth of



Saudi Arabia's hinterland with complete surprise, remaining undetected by Saudi Air defenses. Hence, no attempt was made to intercept them. Their precision in hitting their targets was exceptional.⁶

In July 2021 Iran's UAVs starred once again in the world media when for the first time in ever a suicide UAV managed to hit and cause casualties a moving commercial ship at sea. The oil tanker MT "Mercer Street" sailed from Dar-el-Salaam, Tanzania to the UAE oil terminal of Fujairah when it was attacked on July 28 and then again on July 29 by unmarked UAVs. While the first attack or attacks on July 28 failed, the next day was they were successful. The diving UAV achieved a bull's eye on the ship's bridge, killing the British captain and his Romanian bodyguard.

The stricken ship was escorted by warships of the US Navy Fifth Fleet and continued on its voyage to Fujairah. Upon arrival, the US Central Command (CENTCOM) conducted a thorough investigation and released some of its results to the public. One of the key findings was that the debris of the attacking UAV was identical to that of the Iranian Shahed 136 UAVs that had devastated the Saudi oil installation in Abqaiq two years earlier. This proved the Iranian connection to the attack on a civilian ship on the high seas. As a result, Israel, the US, the UK, and Romania named Iran the perpetrator of this outrage. The international media defined it as an act of terror.

The Japanese-owned, Liberian- flagged MT Mercer Street is operated by "Zodiac Maritime", a London-based company owned by the Israeli tycoon Eyal Ofer. The Israeli connection brought forth a theory that the Iranian action against this ship was part of a broader covert war between the two countries. One source in the Iranian media claimed that the attack was in retaliation for unspecified Israeli attacks on Iranian installations in Syria. Iran's government, however, washed its hands from the whole affair. As in the case of the attack on the Saudi oil installations in 2019, no smoking gun could conclusively prove Iran's guilt, since the UAV launch point remained unknown.

At the time of the attack, Mercer Street was sailing close to the Omani coastline about 480 km (298 miles) away from the nearest Iranian coast. Its distance from the Omidiyeh Iranian Air Force Base for which the September 2019 UAV attack on Saudi oil installation originated, was about 1500 Km (932 miles) – about twice as far as the distance traveled by the Iranian UAVs during the September 2019 oil attack. One Western source hypothesized that the attack on the Mercer Street originated in Houthi-held Yemen, but this is highly doubtful. The distance between Houthi-held territory and the point where Mercer Street was struck is about 1700 km (1056 miles). It would be more reasonable to the Houthis to strike at the ship when it was closest to the Yemeni coast in its voyage from Dar-el-Salam to Fujairah, which is about 1300 km (808 miles) from Sana'a, rather than attacking it when it was almost beyond reach nearing the Strait of Hormuz.

It is therefore more reasonable to assume that the attack originated in Iran. In November, Minister of Defense Gantz identified the location of two Iranian UAV bases at Chabahar and the Island of Queshm that he said were being used for sea control. Chabahar and the Queshm Island bases are located 410 km (255 miles) and 670 km (416 miles) respectively from the attack site on Mercer Street. If indeed these were the launch points for the attack on Mercer Street, it would allow the same Shahed 136 that had been used against the Saudi oil installation to be used against Mercer Street too. Nevertheless, Israeli media sources reported that the range of the Shahed 136 was indeed doubled to 1500 km (932 miles). With such a range capability, the Shahed 136 could attack Israel directly from Iran –which is about 1200 km (746 miles) away from Israel at its closest point. Perhaps this was Gantz's mind when he warned about lethal Iranian UAVs "that could traverse thousands of kilometers."

While the number of UAVs that attacked Mercer Street – two or three – was much smaller than the swarms that assaulted the Saudi oil installations two years earlier, the later operation was almost as impressive technically and operationally. The Iranian perpetrators had no difficulty identifying the target ship from the general sea traffic in the busy sea lanes. This is because ships at sea must constantly broadcast their locations. At the same time, the ability to intercept and strike it with precision while in motion was far from a trivial achievement. This required some feats of navigation and the ability to home on a moving target, either by onboard sensors or by remote pointing from another air or sea vessel. In contrast to the attack on the Saudi oil installations, the Mercer Street attack took place in broad daylight. It stands to reason that a daylight operation was mandatory to correctly identify the target ship and avoid erroneously attacking an uninvolved ship. This in turn could indicate that the Iranian operators maintained real-time data and visual links with the attacking UAV, hundreds of kilometers from the launch point – a capability hitherto the domain of the more industrialized countries.

Possibly, the attack on Mercer Street was part of a broader operation that was ultimately aborted. Five days later, a group of armed persons boarded and took control of the Asphalt Princess, another oil tanker on its way to Fujairah, but which had no connection with Israel. The armed persons – who conversed among themselves in Persian- instructed the captain to sail towards the Iranian coast. About one hour later, without any explanation, the group debarked the ship and let it resume its original course. It could be significant that the two ships – Mercer Street and Asphalt Princess – had some similarities and almost identical painting schemes. During the incident, some neighboring ships reported interrupted communication. The Iranians denied any connection to the aborted hijacking of the Asphalt Princess, other than offering to send help.



Did the Iranians plan to hijack Mercer Street? There is no evidence of this. Yet it is not unreasonable to speculate that the UAV attack on Mercer Street was part of a larger plan that was aborted, perhaps due to the death of uninvolved nationals of countries who maintain cordial relations with Iran. Moreover, the abduction of the ship after those killings could have caused diplomatic complications that Iran was anxious to avoid, hence the rest of the operation – if such existed – was aborted.

Mercer Street was not the first Israeli-linked ship to be attacked in that region. On February 26, 2021, the MV Helios Ray, an Israeli-owned car transporter, was attacked in the Gulf of Oman while sailing from Dubai to Fujairah. The damage forced the ship to return to the port of origin for repairs. Less than one month later, on March 25, 2021, the MT Lorry, an Israeli-owned container ship, was attacked in the Arab Sea while sailing to Gujarat harbor in India. There were no casualties, the damage was light, and the ship continued its voyage. Three weeks later, on April 3, 2021, the MT Hyperion Ray, another Israeli-owned car transporter was attacked while sailing in the Gulf of Oman towards Fujairah. In this case, too, there were no casualties and the damage was light.

Thus, the July attack on Mercer Street was the fourth consecutive attack on vessels associated with Israel. The first attack on the Helios Ray was carried out by attaching small explosive charges to the ship's side above the waterline – a method used previously by Iran's navy to attack oil shipping several years ago. The latter attacks, however, were done differently. Initial reports of the second and third attacks cited "missile attacks", but later it was reported that at least one of them was executed by a UAV. It seems that the Mercer Street incident was the third Iranian UAV attack on Israeli-linked shipping in the seas near Iran, and the first one was successful, albeit on the second attempt.

It can be assumed that the Iranian planners intended to cause enough damage to draw media attention and force the attacked ships to seek shelter for repairs, but not to cause the death of uninvolved civilians. In this assumption, the killing aboard the Mercer Street was undesirable collateral damage.

Major Features of the UAV Threat

Apart from the above-described land and sea operations, Iran's UAVs are busy almost daily in attacking Saudi targets in the southern and central region of the Kingdom. They are also active against US forces in Iraq and Syria (Nine attacks at the time of writing and counting) and in a sporadic incursion into Israeli airspace. The improving performance of Iran's UAVs as well as the burgeoning expertise of their Iranian controllers is turning them into a significant strategic threat to Israel. This threat is fast becoming no less severe than that from the rockets and missiles of Iran and its proxies.

In his September address to the UN, Israel's Prime Minister Bennett cited the attacks on Israeli shipping as a confirmation of the decisiveness of the new UAV threat and was quite explicit about its nature: Swarms of hundreds, if not thousands of Iranian supplied UAVs to its proxies in Yemen, Iraq, Syria, and Lebanon, could be used for attacking Israel. To evaluate the significance of this threat we need to assess the growing importance of UAVs in Iran's military force structure – but to do this, it first needs to define "what is a UAV?"

Manned aircraft come in an extraordinary variety of forms and functions: From single-seat, single motor, propeller-driven private Cessnas to Boeing jumbo jets carrying hundreds of passengers across the world's oceans and to the giant nuclear bombers such as the US B-52. Likewise, UAVs come in an almost infinite variety of forms, functions, and purposes. Strictly speaking, any flying object that can fly stably to any distance – even a short one – but without a human pilot on board, is a UAV. This includes balsa wood, rubber band powered model aircraft, quadcopters purchased in toy shops as well as giant remotely piloted aircraft like the US Global Hawk that can fly non-stop from the US to the Middle East, one example of which was shot down by an Iranian air defense missile in June 2019 over the Straights of Hormuz. The term "UAV" has become even more ambiguous with the appearance of the so-called "Cruise Missile" which is essentially nothing but a UAV that is powered by a Jet engine. Iran, for example, has at least two types of jet-driven UAVs, which are designated by the media (as well as by some analysts) as "cruise missiles." This paper will apply the term "UAV" to all militarily significant unmanned aircraft, whether propeller or jet-driven. Quadcopters and multi-copters of any kind- sometimes called "drones" – are a class of their own and will not be included in the following discussion.

As in Israel and the US, Iran's early generation UAVs were designed for use as reconnaissance aircraft to obtain real-time battlefield intelligence. They carried video cameras and transmitted back still photos and video footage about enemy positions, deployment, and movements. Later, they had air-to-ground weapons fitted under their wings, enabling them to strike the targets identified through their optical sensors. Once the art of navigation by satellites was perfected and with GPS and GLONASS satellite navigation systems coming online, the Iranian turned some of their simpler and cheaper reconnaissance UAVs into suicide UAVs that destroy targets by crashing into them, rather than by aiming air to ground munitions at them.

Suicide UAVs are favored by the Iranians since their simpler versions can be manufactured in the improvised workshops of their proxies all over the Middle East, including the Hamas and Islamic Jihad in Gaza. The Wall Street Journal article already cited above reveals that the Iranian purchase off-the-shelf commercial-grade components and materials for the production of UAVs both by themselves and by their proxies. Piston engines, for example, are purchased from China's Ali Baba for \$500 per piece, free of any export license since this small air motor has wide civilian use,



including for powering model aircraft built by enthusiasts in the US and Europe. The servo motors used to move the control surfaces of their UAVs originate in the South Korean toy industry. One of the critical components of the Shahed 136 of the Saudi oil installation FAME was made in Sweden and is used in the food industry. Software for guidance and control – created by Western enthusiasts – can be freely downloaded from ArduPilot, a site that offers such software for remotely controlled air and ground vehicles.⁷

The manufacturing of such rudimentary yet effective suicide UAVs could be simpler than the production of precision rockets, hence the growing use of UAVs in regional wars. In Yemen, the Houthi insurgents initially used unguided rockets to harass Saudi Arabia's southern cities but have later shifted to suicide UAVs since the Saudi ground-based defense systems have more difficulty intercepting them – but perhaps also because such UAVs are easier to mass-produce in the workshops of Houthiland. Following the 2020 six weeks war of Nagorno Karabakh where Azeri attack and suicide UAVs devastated the Armenian armed forces, Iran held a giant arms exposition where it showed off and flew UAVs of all three varieties: Reconnaissance, ground attack, and suicide attack. As the unnamed Iranian official said to the Wall Street Journal: “Developing a nuclear weapon would take years. With drones, just a few months. Drones have changed the balance of power in the Middle East.”

The main drawback of combat UAVs – whether releasing air to ground weapons or crashing into the target – is the relatively small weight of explosives carried aboard. Heavy Iranian rockets like the Zelzal or its precision sibling the Fatah 110 carry warheads of more than half a ton of explosives. The Shahed 136s that hit the Saudi Oil installation and the Mercer Street carried about 20 kg (44 lbs) of explosives. At the same time, all suicide UAVs are precision weapons with pinpoint accuracy. Therefore, the cumulative damage from a large number of even small warheads can be decisive, as shown in the case of the Saudi oil installation.

UAVs have an advantage over rockets and ballistic missiles because of the unpredictability of their flight path. A rocket or ballistic missile travels along a direct line between the launch point and the target. Hence, since the prospective launch zone of Hezbollah rockets from Lebanon and Hamas rockets from Gaza are well known, Israel's defense system can deploy in the directing of the incoming threats. In contrast, UAVs can follow any route selected by their operators, and with sufficient fuel in their tanks can approach their targets in roundabout routes. For example, a Hamas UAV taking off from Gaza could theoretically approach Tel Aviv from the north. Hence, detection of and defense against UAVs must be circumferential – 360° – rather than focusing on one specific direction. The 360 degrees exposure dilutes the defense's assets. Moreover, most UAVs have small dimensions, and many are made from low signature composite materials – presenting reduced radar signatures. Their small piston engine has a tiny heat signature, hard to detect by thermal sensors. Flying low and slow, they prove hard to detect by radars tuned to provide early warning against fast, high flying manned aircraft – as may have happened in the recent Nagorno Karabakh war.

UAVs are not launched in salvos but rather take off and fly individually. When arriving separately at the target area, they can be picked off one by one. To overcome this vulnerability, operators developed “Swarming” techniques by which bunches of UAVs fly in a coordinated manner and can, for example, synchronize their arrival at the target area – each arriving from its own unique direction – saturating the defenses both temporally and directionally. This technique was already employed by the Iranians in the September 2019 attack on the Saudi oil installations, where all the attacking UAVs were probably synchronized to arrive at their target within a concise time window. The Iranians demonstrated this capability in a recent military exercise (“Great Prophet 15”) in January 2021, which featured a swarm of 4 Shahed 136s simultaneously diving and crashing into various ground targets with remarkable precision. Thus, as PM Bennett noted, the most ominous feature of the UAV threat on Israel is from mass raids by synchronized swarms of hundreds if not thousands of UAVs.

Tippling the Balance of Power in the Middle East?

The success of Iran's UAVs in Saudi Arabia and the Azeri ones in the Nagorno Karabakh war shows that Israel must assume that in any war situation, Iran's proxies in Syria, Lebanon, and Gaza will deploy armed and suicide UAVs that could precisely strike and take out key targets within Israel's homeland, such as military reserve storage depots and force concentrations. Moreover, the UAVs of Iran's proxies will have the capability to hit armor and supply vehicles in motion, thereby disrupting maneuvering forces. Above all, they are likely to target Israel ground-based air defenses as their first priority. The accumulated damage to Israel's warfighting capability from swarms of hundreds of precise UAVs might equal if not surpass that from salvos of rockets and missiles.

The strategic significance of the growing UAV threat seems to be debated within Israel's defense establishment. According to an unnamed military source quoted in Harel's article, the Iranian UAVs “are not game-changers. UAVs can harass, gather intelligence and deter, but cannot achieve victory.” The Armenians, soundly defeated by Azerbaijan's fleets of ultra-modern UAVs would have agreed with the quoted opinion of the unnamed Israeli officer. Decades ago, the IDF made the same mistake of underestimating the significance of an earlier threat, when it determined that “missiles and rockets don't win wars” and tried to block the development of anti-missile defenses. It seems that the political leadership of the country does not share the optimistic assessment of the quoted Israeli officer, expressing their concerns in high-level international forums. In fact, Prime Minister Bennet dedicated as much time to the UAV threat as to the Iranian nuclear threat in his recent UN speech thereby indicating that he does not see Iran's UAVs as secondary weapons of “Harassment, intelligence gathering, and



deterrence” but as a viable strategic threat. It may well be that the Israel Defense Forces have in the meantime rethought its position as indicated by recent media reports. An article on the international air exercise held on October 2021 in Israel, stated that “Israel’s Air Force is closely tracking two issues of concern: the deployment of Iranian ground-based air defenses in Syria, and their enhanced use of UAVs.”⁸

A recent article in an Israeli daily disclosed that Israel has been acting in the last few months to mobilize the international community to combat the spread of Iran’s UAVs, assigning it equal weight to Iran’s nuclearization in the struggle against Iran’s quest for hegemony in the Middle East.⁹ Judging by these reports it seems that the top Israeli leadership does perceive Iran’s UAVs as a veritable game-changer.

The Challenge of UAV Defense

Roughly speaking, combat UAVs come in two classes: The first one includes medium to large UAVs flying at medium altitudes, used for reconnaissance and for attacking ground targets with precisely guided air to ground missiles or glide bombs. UAVs of this class operate individually rather than in swarms and are designed to return to base after completing their missions – in other words, they are multi-use systems designed for repeated operations. The challenge of defending against them is rather similar to that of defending against manned aircraft, except that UAVs generally fly at lower speeds.

The second class includes single-use suicide or “kamikaze” UAVs. Generally speaking, they tend to be smaller and less sophisticated than Class 1 UAVs. They fly at low to very low, ground-hugging altitudes, and can operate in swarms. From the aspect of the defender, their threat is more akin to precision rocket salvos.

The UAVs launched against Israel to date by Hezbollah, Hamas and the Iranians themselves were mainly (but not exclusively) of the first class and were intercepted and shot down by Israel’s air force. Initially, hostile UAVs were shot down by air-to-air missiles fired from fighter aircraft. On one occasion, an Iranian UAV arriving from Syria was shot down by gunfire from an Apache helicopter. Later, during the 2014 operation Protective Edge and the 2021 operation Guardian of the Walls, Hamas UAVs were shot down by ground-based air and missile defenses – “Patriot” and “Iron Dome” respectively.

UAVs of both classes are not immune to air defenses, whether ground-based or airborne. If anything, the opposite is true: It is relatively easy to shoot down a slow-flying UAV, provided that it is detected in time and provided that the defender uses the appropriate weapons against small and stealthy targets. The challenge is timely detection and tracking and in the case of UAV swarms – avoiding being overwhelmed. Moreover, UAVs are precision weapons, hence it is not enough to kill some of them or even many of them: The operational requirement is to kill them all – in the language of missile defense, to achieve a zero or near zero leakage rate. Defending against swarms of UAVs arriving simultaneously from every direction at treetop levels is a formidable challenge to any air defense system, a challenge that may well require the development and fielding of new technologies and operational doctrines.

UAVs in Adjacent Arenas

“UAV Wars” where air defenses were pitted against ground attack UAV have gone on in northwest Syria, in Libya, in the South Caucasus, in Saudi Arabia, in Yemen, and most recently – in Ethiopia. In the Second Nagorno Karabakh War of October–November 2020, Azerbaijan threw into the battle its newly purchased fleet of ultra-modern class 1 and class 2 UAVs, practically obliterating the Armenian’s Soviet-era ground-based air defense systems. Losing the capacity to defend the airspace paved the way to a crushing Armenian defeat. In the still-ongoing civil war in Libya, Turkish class 1 UAVs deployed in support of the internationally recognized government in Tripoli, demolished the ground-based air defenses of the rival government of Benghazi, proceeded to wreak havoc on the Benghazi ground forces thereby allowing the Tripoli government to break the siege on its capital city and regain control of large tracks of the country. During the 7 days long “Operation Spring Shield” in February – March 2020, Turkish Class 1 UAVs demolished the opposing Syrian air defenses, then proceeded to destroy Syrian tanks, troop concentrations, and command posts.¹⁰ Recent reports from the ongoing civil war in Ethiopia are painting a similar picture. The Ethiopian government, on the verge of defeat by the Tigray rebels, has recently turned the table with the aid of Class 1 UAVs of Chinese, Turkish and Iranian origins.

The situation in Saudi Arabia is more complex. Since 2015 the Houthis in northern Yemen have been conducting a war of attrition against the Kingdom, using rockets, ballistic missiles, and UAVs –mainly of class 2 – to harass population centers, military installations, economic value targets, and state symbols across the length and breadth of Saudi Arabia. In the south, close to the Yemeni border, the targets are mainly towns, airports, and oil facilities. In the Kingdom’s deeper hinterland, the Houthis target state symbols (e.g., royal palaces) and oil industry infrastructure, such as pumping stations serving oil pipelines. The Iranians surreptitiously intervene in this harassment campaign, by launching “Houthi looking” UAVs from their territory into Saudi Arabia. The Saudi extensive air defenses are vigorously battling the incoming UAVs using ground-based defenses (Patriot) and airborne defenses combining early warning aircraft with manned interceptor fighter aircraft. The information offered by the media on the evolution of the air campaign in Saudi Arabia is at best sketchy, providing an



incoherent picture of the situation due to the heavy use both sides make of verbal and photographic data for propaganda purposes. All the same, some general conclusions can be gained even from the incomplete and biased information published hitherto.

One conclusion is that Saudi Arabia encounters some difficulties defending its hinterland against Class 2 UAVs, especially when they arrive from unexpected directions. The most outstanding example was the failure to detect and engage the Class 2 UAVs coming from Iran's direction that struck the oil installations in September 2019. This however was not the only case. In February 2021, for example, three suicide UAVs launched from Iraqi territory struck a royal palace in Riyadh, the capital city.¹¹ It seems that in both cases Saudi Arabia air defenses failed to detect the incoming UAVs and were powerless to intercept them.

Another conclusion is in the southwestern regions of the kingdom. Its air defenses enjoy some success against the Houthi UAVs (according to Saudi and US sources – an outstanding success). From the photographic evidence released by the Saudi military, it seems that they use both ground-based defense using Patriot batteries and airborne defense, using Saab 2000 early warning aircraft and air-to-air armed F-15 fighter jets. The Saudis sometimes claim the destruction of dozens of Houthi UAVs in a single day and release convincing-looking video footage on the media. Nevertheless, there is no doubt that some UAVs manage to penetrate through the defensive shield. For example, the Abha International Airport, about 150 km (93 miles) away from the closest Yemeni border, sustained casualties and damages from Houthi UAVs during the summer and fall months of 2021 (The Saudis claim that the UAVs were intercepted and that the casualties and damages were inflicted by the falling debris). This highlights the requirement from the defense to achieve an extremely high success rate against the incoming UAVs, since the damage from the “leakers” that get through overshadows the success in preventing damage from the destroyed UAVs that don't get through.¹²

Saudi Arabia, whose huge territory is almost the size of Western Europe, lacks a nationwide early warning system against low and slow UAVs. This leaves its borders practically open to incursion by low or medium-altitude aircraft. Its ground-based air defenses, consisting mainly of the older generation Patriot 2 and the newer Patriot 3, are optimized for intercepting high flying combat aircraft and ballistic missiles rather than low flying UAVs. The prospects of the Kingdom buying “Iron Dome” systems (initially optimized against rockets, and only recently upgraded for UAV interception) are practically nil, but it may yet emulate the Emirates by purchasing the newly developed South Korean M-SAM II, a joint development with Russia's defense industry. Acquiring and fielding those systems may take years. Saudi Arabia's nascent military industry announced in 2020 that it is developing an anti-UAV system. Still, from the published details it seems that the new system will offer only localized defense against quadcopters (“drones”) rather than horizontal flight UAVs of both categories.¹³ It seems that Saudi Arabia has no immediate military option to seal its skies against the incursion of hostile UAVs from Yemen, Iran, or Iraq. Perhaps this is what compelled the Kingdom to seek a diplomatic solution and to open negotiations with Iran. It is perhaps not too far-fetched to conclude that the simple, unsophisticated UAVs originating in Iran managed to humble the powerful Royal Saudi Air Force, gaining for Iran a significant strategic achievement. The statement of the unnamed Iranian official quoted above that the UAVs are tipping the military balance in the Middle East was not far off the mark.

Meanwhile, in another corner of the Middle East UAVs have been battling Russian air defenses in Syria. When Russia acquiesced to Bashar Assad's entreaties to save his regime against the then victorious insurgents, the latter granted Moscow an airbase in Khmeimim and a naval base in Tartus, both in the northwestern corner of Syria. As soon as the Russian intervention commenced, those two bases – but mostly the airbase – came under frequent insurgent attacks, initially from mortars and later from UAVs. On December 31, 2017, the Khmeimim airbase suffered a major insurgent strike, initially thought to come from mortars but later confirmed as coming from UAVs. The attack caused the death of two Russian persons and damaged several aircraft. Unofficial sources claimed that eight aircraft were hit, two of which were total losses. One week later, on the night between January 5 and 6, 2018, 13 insurgent UAVs attacked both Russian bases (Ten UAVs attacked Khmeimim and three attacked Tartus). It seems that this time the Russians were ready. According to their statements, the attack was completely foiled, with seven UAVs being downed by ground-based air defenses and the rest forced to land by a Russian cyber operation. The photographic evidence released by the Russians shows two types of UAVs: One is a Chinese-made, hand-launched UAV sold to all buyers through Ali Baba under the name “Skywalker.” The other was a rather largish, rudimentary balsa wood radio-controlled model aircraft of unknown provenance carrying tiny bombs under its wings and probably built by the Insurgents themselves. The UAV attacks on the Russian bases are still going on sporadically. For example, in July 2021 the Russian reported downing 13 hostile UAVs, and a month later, in August, they reported the downing of a formidable number – 45 in all. Russia claims a 100% success rate and no losses or damages in the ongoing battle against the insurgents' UAVs.

The Russian military is largely silent about its doctrine and weapons for combating UAVs, but non-Russian sources report that it consists of three major components: First, the Russians re-tuned their radars to detect the small size, low and slow air vehicles. Second, they set up systems to interfere with navigation satellite communication (GPS and perhaps Russia's own GLONASS), and third, they use Electronic Warfare (EW) to disrupt communication between the UAVs and their operators. It is also possible that the Russians are using cyber warfare to hijack control of incoming UAVs and land them safely away from their targets. The ground-based air defenses of the Russian enclaves are based largely on the SA-22 Pantsir which is equipped with two 30mm rapid-firing anti-aircraft guns – a legacy of WWII – and twelve small,



short-range, heat-seeking ground to air missiles. While Pantsirs operated by Syrian and Libyan forces have been overwhelmed by modern Turkish UAVs, it seems that in the case of the Russian bases in Syria, the Pantsir remains effective against the rudimentary UAVs launched from the last anti- Assad enclave in North-Western Syria.

Comparing the UAV defense of Saudi Arabia and the arguably more effective Russian defense, four parameters stand out: the size of the defended area, the suitability of the defensive weapons to the mission of killing UAVs, the role of electronic and cyber warfare, and the sophistication of the aggressor's air vehicles and operators. Territorial size seems to be decisive: The immense territory of Saudi Arabia and its extremely long borders make it difficult to erect a hermetic early warning fence against low flyers and practically allow an almost free ingress of UAVs into its territory. In contrast, the two Russian bases in Syria have the size of small towns, facilitating impermeable early warning fences around them.

As for weapons, Saudi Arabia relies on heavy manned fighter aircraft and Patriot air defense systems, both designed to engage high flying manned aircraft rather than low, slow and cheap UAVs. Using expensive Patriot interceptor missiles against fiberglass, propeller-driven model aircraft mass-produced in the workshops of Sana'a is tantamount to using a sledgehammer to kill gnats: Feasible but highly inefficient. The Russians, in contrast, are using lower-tech ground-based air defenses combining anti-aircraft guns with what is essentially shoulder-launched anti-aircraft missiles. The Russians are using electronic countermeasures (ECM) to disrupt the hostile UAVs and perhaps also cyber warfare (CW) to force them down. There is no information on the similar use of ECM or CW by the Saudis. Finally, the aggressor's level of sophistication seems also to play a part. The Iranian have demonstrated high skill in inserting swarms of UAVs into Saudi Arabia's hinterland, circumventing defensive systems, remaining unseen by early warning systems, and avoiding ground obstacles. The Syrian insurgents in the Idlib enclave that keep attacking the Russians with their simple UAVs lack the Iranian sophistication – so it stands to reason that their UAVs fly in straight lines along the shortest route – and hence the most predictable route – from the Idlib enclave to the Russian bases.

Elements of Effective Defenses Against Iran's UAVs

Today, the burgeoning UAV threat is an issue of concern not only in Israel but to the West at large. The Western defense industries are proposing a welter of new anti UAV weapons, some realistic and some bordering with science fiction. Of the cutting-edge weapons being developed, the closest to maturity is the high-power solid-state laser in which significant progress has recently been achieved both in Israel and abroad. A development program of 300 Kw mobile laser system has recently been initiated in the US. Since the level of power of the laser beam is directly proportional to its rate of kill, it may well be that such powerful lasers will be able to deal even with synchronized UAV swarms. Another cutting-edge technology being experimented with is Microwave beams, aimed to "fry" the electronics of incoming UAVs. One US company came up with the idea of reusable kinetic interceptors that kill the target UAV by metal-to-metal collision, without any explosives. The spent interceptor is then parachuted down for recycling. Other companies propose interceptor UAVs that shoot air-to-air missiles at the incoming hostiles or physically crash into them.

Class 1 UAVs that are generally used for reconnaissance and ground attack tend to be relatively large and heavy, necessitating takeoffs from and landings on suitable runways. Repeatedly damaging such runways by offensive actions could slow down Class 1 UAV operations. In contrast, the smaller types of Class 2 UAVs are launched from zero-length rails or catapults and are accelerated to take-off speed by small rockets or pressurized air bottles. Zero-length catapults of the types unveiled by Hamas during the May 2021 operation "Guardian of the Walls" can be assembled in a few minutes before the launch and disassembled immediately after it. Hence, they present temporary, quickly vanishing targets. Accordingly, the chances to hit them while deployed are slim, to say the least. As a result, the response to most Class 2 UAVs – i.e., the smaller types of suicide UAVs – will probably be defensive rather than offensive. In the case of Israel, the defensive brunt will befall on the shoulders of Israel's Air Defense Command.

Unlike Saudi Arabia, Israel's small territory facilitates the establishment of a seamless early warning perimeter around all its borders. Detection of low, slow, and small UAVs is the cornerstone of effective defense, without which no viable defense is feasible as we see in Saudi Arabia. Israel's air defenses had already made significant steps in this direction when it upgraded the Iron Dome radars to detect small, low flying UAVs, proving its effectiveness during the 11-day long operation "Guardian of the Walls."

The UAV threat does not replace the rocket and missile threat, but rather adds to it. Adding the mission of UAV defense to the already existing mission of rocket and missile defense could overwhelm the defense systems. It is therefore necessary to take quantitative measures to beef up the defensive shield. The number of defensive systems capable of dealing with both kinds of threats must be increased. Even then, synchronized UAV swarms coming from every direction could locally overwhelm the defense. Hence, the addition of new cutting-edge kill systems should be investigated, such as laser (already in development in Israel) and microwave systems. ECM systems might be able to destroy UAVs in masses. hence their integration in the defensive array should be pushed forward. Israel's army has already employed ECM during the May 2021 operation "Guardian of the Walls", but it seems they were of the local, short-range "Drone Dome" type made by Rafael, basically optimized against short-range quadcopters. Disrupting horizontal flying UAVs at long distances will probably require more powerful ECM systems, such as the Israel



Aerospace Industry Elta Division “Scorpius” recently unveiled by the Israeli Ministry of Defense.

Finally, and most importantly: The cost per kill must be driven down. In combating rockets and missiles, the cost of defense has always been and remains higher than the cost of offense, giving the aggressor a financial advantage. This disparity becomes even more pronounced in the case of UAV when descending the technological ladder by the aggressor – i.e. switching from relatively expensive guided missiles and rockets into toy-like, fiberglass made small air vehicle powered and guided by amateur grade systems – forces the defender to climb up the technological ladder, from interceptor missiles to lasers and microwaves.¹⁴ Ultimately, it will be battlefield economics, as expressed by the cost per kill, that will determine who will have the upper hand: the aggressor or the defender.

Conclusion

Iran’s UAV can no longer be seen as secondary weapon systems that can merely “harass, gather intelligence and deter.” Rather, they have grown into a major weapon system that when applied properly can be a game-changer by themselves, as potent as the new generation of precision rockets and missiles of the Islamic Republic. The concerns voiced by Israel’s Prime Minister and Minister of Defense are justified and timely. It can only be hoped that Israel’s defense establishment will learn from the experience of others and will rapidly deploy the required offensive and defensive means to prevent Iran’s UAVs from tipping the military balance in the region.

●► Notes are available at the source’s URL.

Undefined's next-gen "silent" ion propulsion drone: still noisy

Source [+video]: <https://newatlas.com/drones/ion-propulsion-drone/>



The Ventus drone ionizes air to create lift without moving propulsors – Undefined Technologies says it'll be quiet next to current propeller-driven drones (Undefined Technologies)

May 02 – With two successful flight tests in the bag, and just under US\$2 million in seed funding, Florida company Undefined Technologies has unveiled the next generation of its "silent" commercial drone, which uses ionic propulsion instead of propellers. The new design is certainly a step up visually from previous efforts, but at the end of the day, an ionic propulsion system is going to look like an ionic propulsion system; by necessity it'll feature a large grid of electrodes with at least two layers, such that the top and bottom layers can be fed high and opposing voltages in order to accelerate ionized air downwards and produce thrust. So while the wraparound cover is a nice touch, it still looks like a flying dish rack underneath.



[We had a lot of questions](#) when we first saw this company's promises – ionic propulsion has proven very useful in space, but could it really be an efficient replacement for propellers closer to Earth? MIT has published research on its [ion-drive fixed-wing plane](#), but you need a lot more thrust and a lot more onboard energy storage for vertical-lift aircraft. Undefined Technologies has certainly chosen its name judiciously; a year and a half later, we still know very little about its "novel Air Tantrum™ technology," which the company says will be extremely quiet. But its December 2021 flight video and a [presentation given by company CEO Tomas Pribanic](#) at a logistics conference in January do turn up an interesting nugget or two. The company's original proof of concept, as shown in the last video we published, flew for around 25 seconds, and made about 90 decibels, says Pribanic. The new prototype, he claims, has flown for around two and a half minutes, and was measured at 85 decibels. The ultimate target is around 70 decibels, or about the same as a DJI Mavic, but presumably in a larger airframe with some cargo carrying capability. It's unclear how the company expects to continue reducing noise on a device that already has no moving parts in its propulsion system. The company doesn't make any promises around range or endurance either at this stage.



Previous "flying pallet" designs have been flown for up to two and a half minutes (Undefined Technologies)

In the video below you can see the new prototype airborne, but the company has chopped the footage up so we can't verify the full length of the flight. It looks a little more stable than the proof of concept, although it's flying indoors without any wind to contend with. Noise-wise, there's an interesting high-pitched whine involved, and the drone bends in a somewhat worrying way when it lands, just due to the size and light weight of its structure. It does not look heavy duty, and we imagine it'll be tough to scale these things up without making them fragile. It certainly won't achieve high altitudes; as MIT's Steven Barrett and a number of astute commenters on our previous piece point out, the breakdown voltage of air rises with altitude. But most use cases for today's drones keep them close enough to the ground that this is unlikely to be the dealbreaker. We're not convinced the Silent Ventus will be silent or energy-efficient enough to compete with regular multicopters, but we're watching with interest.

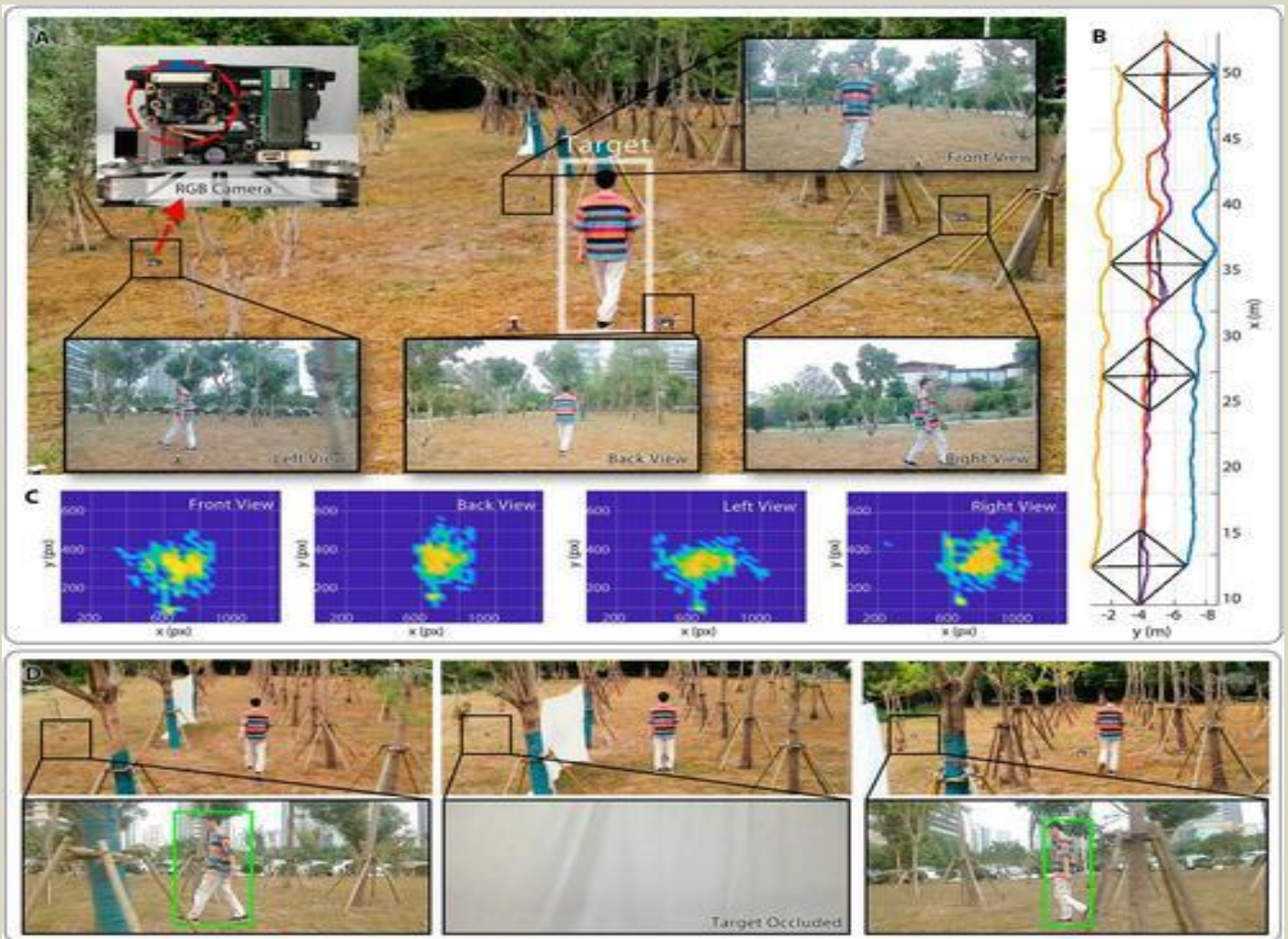


Autonomous drones fly through Chinese bamboo forest

Source: <https://www.youtube.com/watch?v=rPuI9WKQ6oQ>

This swarm of 10 autonomous drones can manoeuvre through a bamboo forest in China. They are the first to successfully fly outdoors and navigate unprogrammed obstacles, according to researchers at Zhejiang University who led the experiment.





 **Remember slaughter bots? [video](#)** (watch 05:30)
 ● Visit also <https://autonomousweapons.org/>



Molecular Robots Are Now Able to Work Cooperatively in Swarms

Source (+video): <https://i-hls.com/archives/114329>

Apr 24 – Researchers from Hokkaido University in Japan demonstrated that molecular robots can perform cargo delivery by using a swarming strategy, achieving five times the transport efficiency of individual robots.

Robot swarms provide robots with capabilities that are not possible in individual robot activity, such as splitting work among themselves, responding to different risks, and establishing complex structures as the environment changes. A micro-robot or machine at the micro or nano scale may be perceived as only being suited for a limited set of tasks, but their swarming capabilities could permit them to perform a variety of complex tasks and be integrated in a variety of solutions.

Researchers used five million molecular machines, which are made up of two biological components: microtubules, which can swarm, and kinesins, which can transport



microtubules. Swarming was controlled by combining DNA with a light-sensitive compound called azobenzene, which functions as a sensor. They also added cargo consisting of polystyrene beads ranging in diameter from micrometers to tens of micrometers, enabling control of swarming also at the loading stage.

Swarms of molecular robots, according to sciencedaily.com, have demonstrated the ability to cope with thirty micrometers of polystyrene beads, and even achieved five times the efficiency of individual robots.

It showed that molecular machines can operate in a swarm-like strategy and perform high-efficiency missions together, and its impact on microrobotics will likely be significant. There is a possibility that microrobot swarm technology will soon be applied in a variety of industries and fields, including medicine and military, when molecular robot cooperation could lead, among other things, to the effective manufacture of drugs and the development of defense technologies against chemical and biological warfare.

Russia uses new laser weapons in Ukraine, Zelenskiy mocks 'wonder weapon'

Source: <https://www.reuters.com/world/europe/russia-touts-new-generation-blinding-laser-weapons-2022-05-18/>

May 18 – Russia on Wednesday said it was using a new generation of powerful lasers in Ukraine to burn up drones, deploying some of Moscow's secret weapons to counter a flood of Western arms.

Russian President Vladimir Putin in 2018 unveiled an intercontinental ballistic missile, underwater nuclear drones, a supersonic weapon and a laser weapon.

Little is known about the specifics of the new laser. Putin mentioned one called **Peresvet**, named after a medieval Orthodox warrior



monk Alexander Peresvet who perished in mortal combat.

Yury Borisov, the deputy prime minister in charge of military development, told a conference in Moscow that Peresvet was already being widely deployed and it could blind satellites up to 1,500 km above Earth.

He said there were already more powerful systems than Peresvet that could burn up drones and other equipment. Borisov cited a test on Tuesday which he said had burned up a drone 5 km away within five seconds.

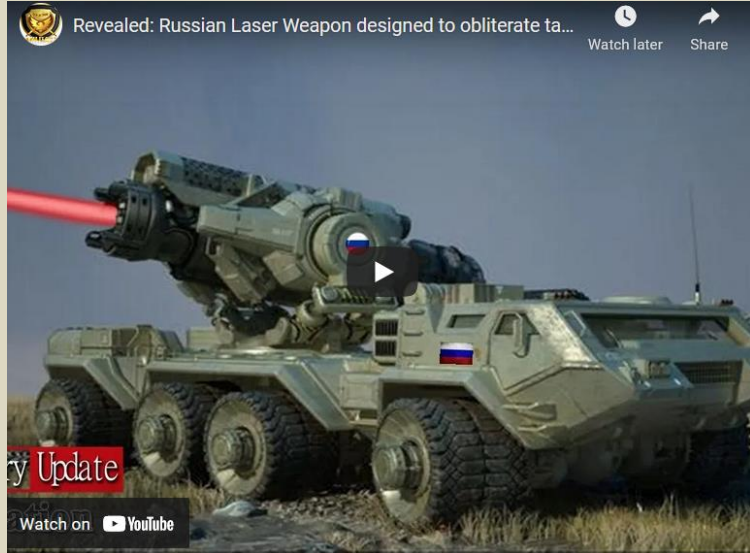
"If Peresvet blinds, then the new generation of laser weapons lead to the physical destruction of the target - thermal destruction, they burn up," he told Russian state television.

Asked if such weapons were being used in Ukraine, Borisov said: "Yes. The first prototypes are already being used there." He said the weapon was called **"Zadira"**.



Ukrainian President Volodymyr Zelenskiy mockingly compared news of the lasers to the so-called wonder weapons that Nazi Germany unveiled in a bid to prevent defeat in World War Two.

"The clearer it became that they had no chance in the war, the more propaganda there was about an amazing weapon that would be so powerful as to ensure a turning point," he said in a late night video address.



"And so we see that in the third month of a full-scale war, Russia is trying to find its 'wonder weapon' ... this all clearly shows the complete failure of the mission."

Almost nothing is publicly known about Zadira but in 2017 Russian media said state nuclear corporation Rosatom helped develop it as part of a programme to create weapons-based new physical principles.

The invasion of Ukraine has illustrated the limits of Russia's post-Soviet conventional armed forces, though Putin says the "special military operation" is going to plan.

Borisov's remarks indicate Russia has made significant progress with laser weapons, a trend of considerable interest to other nuclear powers such as the United States and China.

Using lasers to blind satellites was once a fantasy from the realm of science fiction, but the United States, China and Russia have been working on variants of such weapons for

years. Besides the benefit of burning up drones, blinding reconnaissance systems has a strategic impact too as satellites are used to monitor intercontinental ballistic missiles carrying nuclear weapons.

Borisov said he had just returned from Sarov, which is a centre of Russia's nuclear weapons research. He said a new generation of laser weapons using a wide electromagnetic band would ultimately replace conventional weapons. "This is not some sort of exotic idea; it is the reality," Borisov said.

Spotting drones over the Aegean Sea



The Aladin H2020 system developed by the Hellenic National Center for Research and Technological Development (EKETA) recently won the NATO competition in the field of drone detection.



Eaglet Air-Launched Drone Aims To Help Its Mothership Survive In Army Tests

Source: <https://www.thedrive.com/the-war-zone/eaglet-air-launched-drone-aims-to-help-its-mothership-survive-in-army-tests>



May 19 – General Atomic's new air-launched drone, dubbed 'Eaglet,' is set for an Army demonstration this summer, a company official told *The War Zone*.

Eaglet is designed to be launched from either the company's [MQ-1C Gray Eagle ER](#) or [MQ-9 Reaper](#). Though program work is still ongoing, its first flight is scheduled for later this year and General Atomics "will be demonstrating Eaglet for the U.S. Army this summer," C. Mark Brinkley, Senior Director Strategic Communications & Marketing for General Atomics, Aeronautical Systems, or GA-ASI, told *The War Zone* Wednesday.

Brinkley on Wednesday also exclusively told *The War Zone* the name and specification details about [the new drone](#), developed by General Atomics to [keep its legacy unmanned aerial assets relevant](#) in modern, contested airspace.

The vehicle - which General Atomics [first disclosed the existence of](#) last year - was on display in full-sized mockup form at the 2022 Special Operations Forces Industry Conference in Tampa, which began on Monday and wrapped up today.

The propeller-driven Eaglet weighs less than 200 pounds, has a span of 10.5 feet with its pop-out wings deployed, and can fly at a maximum airspeed of 115 knots with a range of about 700 kilometers (435 miles) or about eight hours with a payload of about 20 to 30 pounds. Its maximum service ceiling is about 15,000 feet.

The mock-up shows the same general layout as had been seen in artwork and smaller models that General Atomics has displayed in the past. It is now even more apparent that the design has at least some low observable (stealthy) features, with what appears to be a flush exhaust port on the top rear portion of the drone's body. What may be two air intakes are seen at the front on either side of the propeller shaft. A stealthy chined fuselage with sloped sides and v-tail round out the reduced signature design.

Eaglet is one of the newest entries in General Atomics' Evolution Series of advanced UAS concepts, said Brinkley

The goal of Eaglet is to be able to allow the company's now-vulnerable legacy drone fleet to continue providing reconnaissance and strike capabilities at a safe distance from enemy anti-access/area denial systems.

"It's a survivable, air-launched effect (ALE) designed for use with the [MQ-1C Gray Eagle ER](#) or [MQ-9 Reaper](#)," said Brinkley. "Eaglet provides capability for multispectral sensing and survivability on the future battlefield."

For the better part of the past 20 years, America's drone fleet has ruled the skies, raining down death and destruction, and soaking up intelligence largely unmolested because they were operating in permissible environments against adversaries with no air defenses or electronic warfare systems.



But those days are over and the U.S. military and defense contractors have been seeking new ways to continue to provide those capabilities while leveraging existing systems.

U.S. drones have been vulnerable for a while, even to non-state actors. In 2017, for instance, Yemen's Houthi rebels brought down a U.S. Air Force Reaper. You can read more about that incident, depicted in the video below, [here](#).

Russia's war in Ukraine - where unmanned systems from both sides have been vulnerable to air defense and electronic warfare systems not fielded by insurgents in Afghanistan and Iraq - has only hammered home those concerns.

The inevitability of such vulnerability is why the Army launched its ALE program two years ago. Its goal is to develop a family of smaller drones that can be launched from larger manned or unmanned aircraft that are able to work together in networked swarms. "Army Futures Command (AFC) has identified a future fight in an Integrated Air Defense Systems (IADS)-rich environment where platforms must be survivable, attritable, or expendable to deliver sensing capabilities effectively where 1) The MQ-1C Gray Eagle flies racetrack patterns tangential to the IADS threat, at 80 km [~50 miles] distance, 2a) ALEs deploy from the MQ-1C Gray Eagle as the forward most element of the advanced team in areas of expected enemy contact in order to detect, identify, locate and report (DILR) and attack/disrupt/decoy threat assets to initiate disintegration of the IADS," according to an official 2020 Army contracting notice.

The Army wants that capability to provide ISR, electronic attack, and even lethal strikes. All while remaining "outside the range of enemy sensors and weapon systems," [according to the Army](#), which wants them to be survivable, but small and cheap enough to be expendable if needed.

ALE drones should also be designed to allow rapid integration of new technologies.

You can read more about the ALE effort [here](#).

Brinkley told *The War Zone* that Eaglet can meet those criteria.

"Imagine a Gray Eagle ER carrying four Eaglets is flying an ISR mission near hostilities," he postulated. "The UAS can launch its Eaglets forward into hostile airspace, where this ALE quartet can work in four-part harmony to extend the sensing envelope of the host UAS, provide electronic or kinetic warfare options, or simply disrupt an adversary's mission planning."

The Eaglet, he added, is "affordable and recoverable," allowing it to be used for multiple missions. "We don't have pricing to announce yet, but the whole point is to balance affordability with performance," he said. "We anticipate Eaglet's price point to fit within the budget of expendable or attritable options. Eaglet will give commanders a variety of options when examining mission needs and risk, while holding the larger UAS at a safe standoff distance."

GA-ASI is working on several Artificial Intelligence/Machine Learning advancements "to help UAS pilots manage and control Eaglet during missions," Brinkley said. "These ALEs could be launched one at a time, or all at once, depending on the need."

Eaglet is one of several ALE systems the Army is taking a look at.

The Army has [previously experimented with](#) a small drone called the Area-I small Agile-Launch Tactically Integrated Unmanned System drone, or ALTIUS. That system has already been launched from Army [Gray Eagle](#) as well as an Air Force [XQ-58A Valkyrie](#) stealthy unmanned aircraft.

Even if the Army doesn't agree to purchase Eaglet, it is the kind of drone that, if it does what the company claims, could be attractive to the U.S. Marine Corps, [which has its own Reaper](#) that faces similar challenges in the new world of contested airspace. The USAF is also likely interested in squeezing more relevancy out of its large MQ-9 fleet, especially as work to [transition to a more survivable type](#) could drag on. Using Eaglet on [ship-deployed MQ-9 conversions](#) is another possible option as is selling them to other nations operating Reaper variants. (The U.S. is the only nation operating the Gray Eagle).

The MQ-9A Reaper is operated by U.S., UK, Italy, France, Spain and the Netherlands, said Brinkley. The customer list for the MQ-9B SkyGuardian and SeaGuardian continues to grow, with UK, Belgium, and Japan awaiting delivery, and many other nations in various stages of request and approval. The Eaglet can fit on both of those variants, Brinkley said.

For a number of years now, the future of using large, unstealthy, slow drones for many combat applications has become questionable. General Atomics is betting that Eaglet can help keep them in the fight.

That future should come into greater focus as the Army continues its ALE testing.

China launches an autonomous mothership full of autonomous drones

Source ([+video](#)): <https://newatlas.com/marine/china-autonomous-mothership/>

May 23 – China christened a remarkable new 290-foot ship last week – the world's first semi-autonomous drone carrier. It'll carry, launch, recover and co-ordinate the actions of more than 50 other autonomous aerial, surface and underwater vehicles.

The Huangpu Wenchong Shipyard began construction on the Zhu Hai Yun last July in Guangzhou. According to the [South China Morning Post](#), it's the first carrier of its kind, a



self-contained autonomous platform that will roll out with everything necessary to perform a fully integrated operation including drone aircraft, boats and submersibles.



The Zhu Hai Yun is designed to carry and co-ordinate its own integrated autonomous research and surveillance fleet, with more than 50 autonomous aircraft, boats and submersibles capable of working in concert (CSSC Huangpu Wenching Shipbuilding Company Limited)

China doesn't expect it to navigate busy seaports by itself, like the [Japanese autonomous container ship Suzaku](#) we wrote about last week. Instead, the Zhu Hai Yun will run on remote control until it's out in the open water, and then its self-driving systems will take over to execute whatever mission it's running.

It's kitted out with everything it needs to deploy its own boats, subs and aircraft, communicate with them, and run co-ordinated missions, including conducting "task-oriented adaptive networking to achieve three-dimensional views of specific targets," according to the shipbuilding company. The aerial drones can land back on its deck, and it stands ready to retrieve the boats and subs once they've made their rounds.

"The Intelligent, unmanned ship is a beautiful new 'marine species' that will bring revolutionary changes for ocean observation," said Professor Dake Chen of the Chinese Academy of Science's School of Oceanography.

While it's mainly pitched as an ocean research platform, the SCMP also reports that it has "military capability to intercept and expel invasive targets," a capability at the forefront of many autonomous marine projects, including the [extraordinary spider-legged WAM-V boats](#) we looked into on Friday.



IOI
International
CBRNE
INSTITUTE



C²BRNE
DIARY



EMERGENCY RESPONSE



E-SPONDER

EU-sponsored project | 2010-2014

Source: <https://cordis.europa.eu/project/id/242411/reporting>



The E-SPONDER is a suite of real-time data-centric technologies which will provide actionable information and communication support to first responders that act during abnormal events (crises) occurring in critical infrastructures. This information will enable improved control and management, resulting in real time synchronization between forces on the ground (police, rescue, firefighters) and out-of-theater command and control centers (CC). The approach guiding the E-SPONDER project is based on the fusion of variable forms of field-derived data within a central system which will then provide information analysis and decision support applications at designated CC locations in order to provide in situ support to first responders that operate in Critical Infrastructures. Statistics show that efficient emergency system can reduce accident losses to 6%, compared with situations without emergency system. As a result, an efficient emergency system is a key to cope with all kinds of sudden events and improve safety of cities and countries. To do this, E-SPONDER will achieve the following objectives: i) Improvement of front end data collection technologies installed both on portable and fixed platforms, providing a flexible yet comprehensive coverage of the affected area; ii) this data will then be fused and analyzed to provide real-time decision support; iii) E-SPONDER will make these resources readily available to commanders through the use of easily accessible web-portals but lastly and most important it will provide significant support based on Information and Communication Technologies to the First Responders. Thus, E-SPONDER will minimize the uncertainty that characterizes crisis events, thereby limiting their scope. Once E-SPONDER elements are ready for deployment they will be integrated and extensively field tested.



ICI
International
CBRNE
INSTITUTE



**Because
international
CBRNE First Responders
need a common roof!**



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