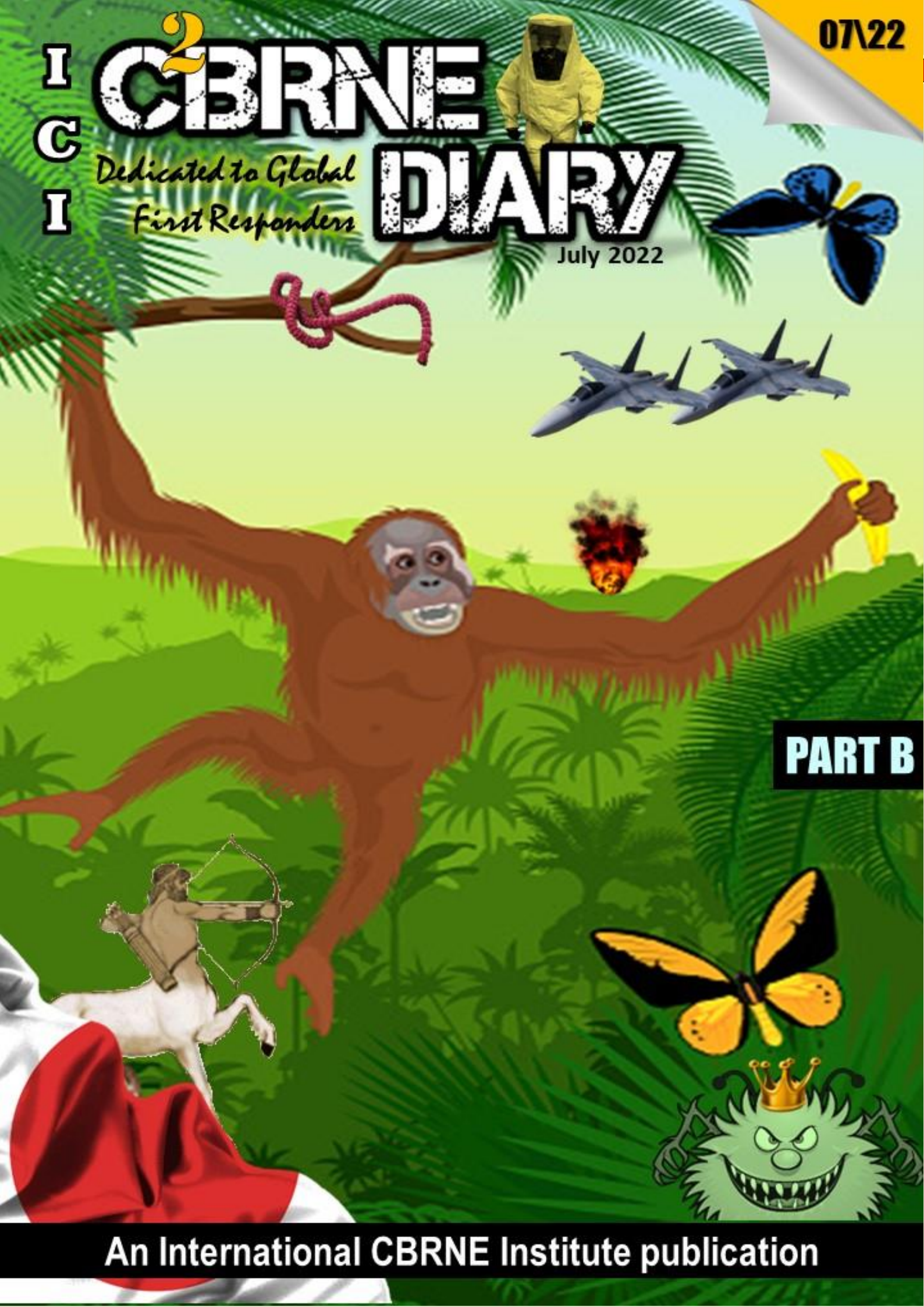

07\22
I C I
C²BRNE DIARY
Dedicated to Global First Responders
July 2022
PART B
An International CBRNE Institute publication

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

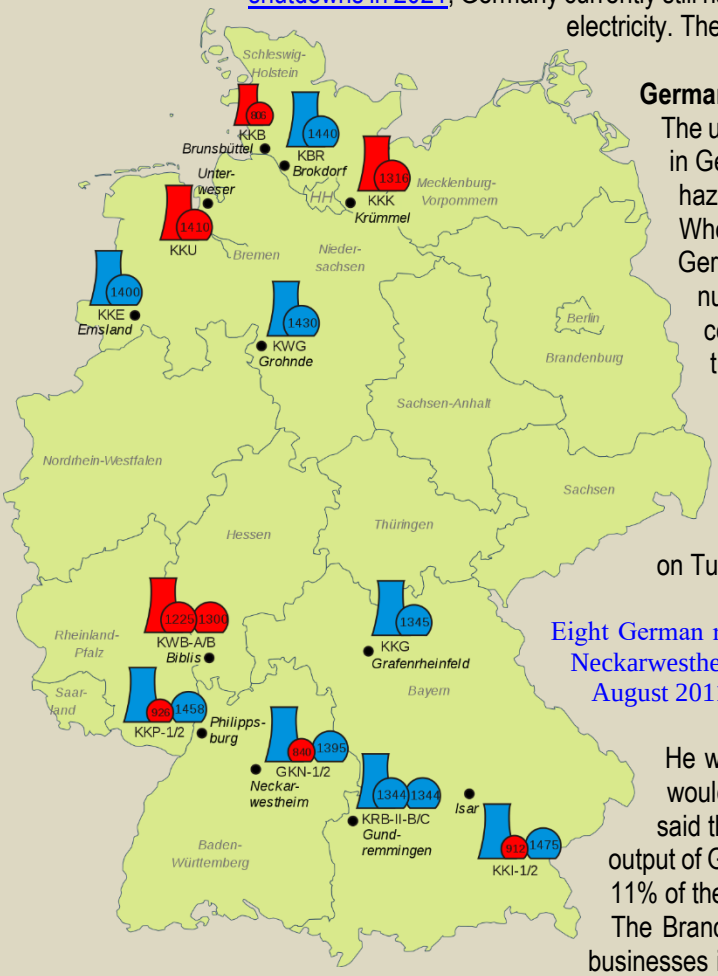
C2BRNE DIARY

DIRTY R-NEWS

Will Germany Return to Nuclear Power?

By Elizabeth Schumacher (DW *journalist)*
Source: https://www.homelandsecuritynewswire.com/dr20220623-will-germany-return-to-nuclear-power

June 23 – Germany is heading into an energy crisis as Russia cuts gas supplies in retaliation for sanctions over its invasion of Ukraine. Finance Minister Christian Lindner warned this week that the country was on the brink of a "very serious economic crisis," and the government needed to explore all avenues to plug the gaps in the nation's energy supply.
To that end, Linder's business-focused Free Democrats (FDP), the smallest party in Berlin's governing coalition alongside the Green Party and the center-left Social Democrats (SPD), have called to postpone Germany's nuclear energy phaseout. After several shutdowns in 2021, Germany currently still has **three nuclear power stations** running to provide 11% of the country's electricity. They are all set to be switched off by the end of the year.



Germany's Opposition to Nuclear Power

The use of nuclear energy as a "green" alternative to fossil fuels is controversial in Germany. The Green Party has argued for decades that the environmental hazards of disposing of nuclear waste vastly outnumbered the benefits.
When they came to power in a coalition government under SPD Chancellor Gerhard Schröder in 1998, they pushed successfully for the phaseout of nuclear energy. The subsequent conservative government under the center-right Christian Democrat Chancellor Angela Merkel first rolled back the timeline, but the 2011 Fukushima nuclear disaster in Japan turned the tide again and Merkel pushed her party toward the phaseout after all.
The CDU is now Germany's largest opposition party, and has been demanding that the nuclear phaseout be called off. "It is technically and legally possible" for the three remaining reactors to keep on operating beyond the end of this year, said CDU chairman Friedrich Merz on Tuesday.

Eight German nuclear power reactors (Biblis A and B, Brunsbüttel, Isar 1, Krümmel, Neckarwestheim 1, Philippsburg 1 and Unterweser) were permanently shut down on 6 August 2011, following the Japanese Fukushima nuclear disaster

He was contradicting Chancellor Olaf Scholz of the SPD, who had argued it would be too hard to source the necessary nuclear fuel rods in time. Scholz said that "no one has provided me with a feasible plan" to quickly increase the output of Germany's three remaining nuclear plants — which as of now provide only 11% of the country's electricity.
The Branchenverband Kernenergie, an umbrella organization for nuclear energy businesses in Germany, told the *Müncher Merkur* newspaper that an extension was indeed possible, but called for quick decision-making. "The power plants are in the process of shutting down. The longer you wait, the more difficult it will be to start them up again," it said.
According to Christian von Hirschhausen, an expert in energy and infrastructure at the German Institute for Economic Research, Scholz has the most scientifically sound grasp of the situation.
Bringing nuclear energy back online was technically and legally "impossible," von Hirschhausen told DW. There was no way to revert the decommissioning process over the next 18 months, he said, due to the time it takes to order, deliver and install equipment as well as enriched uranium.
"They would also need to implement a new set of safety standards and checks," von Hirschhausen added, to replace those that have not been carried out in years due to the phaseout, and new laws to govern the power plants' use.

Gas Crunch

As it was winding down its use of nuclear power over the past decade, Germany's reliance on Russian energy sources was ratcheted up. Almost all of the country's heavy industry is reliant on natural gas, as are about half of German homes for their source of heating.

Early this year, around 65% of natural gas in Germany came from Russia. Now, that has dropped to below 40%. In 2021, about 53% of Germany's coal needed for power and industrial production was imported from Russia, which is to be reduced to zero after an EU-wide ban takes effect in August.
In order to head off an energy crisis, Berlin is looking to fill up its gas reserves from the current 60% to at least 80% by October, and to total capacity before the winter.
This plan has left politicians scrambling to secure new import partners for oil and gas and speed up the expansion of solar and wind energy. They have also reluctantly extended the lifespan of the country's coal plants, despite promises to phase out coal entirely by 2030.
Many worry, however, that all this may not be enough, and they have been looking even further afield for new sources of energy. FDP lawmaker Torsten Herbst and Bavaria's center-right state premier, Markus Söder, were among the first to suggest Berlin lift its ban on fracking, a method of extracting shale gas that is popular in the United States but highly controversial for the amount of methane it leaks into the groundwater.
Economy and Climate Minister Robert Habeck, of the Green Party, remains opposed to nuclear energy and fracking, and finds it hard to advocate for something as destructive to the climate as coal.
But increasing the use of coal, von Hirschhausen said, "is just a temporary measure. It makes sense if we want to build up reserves…so that there aren't major shortages in the energy supply."
In an interview with public broadcaster ZDF on Tuesday, Habeck vowed that the government's ambitious plan to completely exit coal in the next eight years was still on track.
The coalition is set to debate ways to avert a potentially disastrous lack of energy supply in the next two weeks, with an eye to presenting a new plan at the beginning of July.

EDITOR'S COMMENT: My question is if Germany will be (now) interested in nuclear weapons as well and if yes, who will stop her from becoming a nuclear power like France or UK?

Has the Russia-Ukraine war blown up the global nuclear order?

By Lauren Sukin
Source: https://thebulletin.org/2022/06/has-the-russia-ukraine-war-blown-up-the-global-nuclear-order/

June 28 – The Russian nuclear saber-rattling that has accompanied the invasion of Ukraine represents a level of nuclear risk unprecedented since the end of the Cold War. One wonders how global nuclear politics will adapt to these changing circumstances.

The ongoing Russia-Ukraine war poses major challenges for several core international institutions and issues, from the upcoming Non-Proliferation Treaty review conference to President Biden's proposed arms control efforts with Russia and China.

Illustration by Thomas Gaulkin

Perhaps the most pressing nuclear security question coming out of the war is whether Russia will use nuclear weapons in Ukraine. Russian President Vladimir Putin and various spokesmen for the Kremlin have repeatedly made statements threatening the use of nuclear weapons and defining conditions for their use that could allow the Russian military to attack Ukrainian forces with nuclear weapons. Indeed, Russia has used the same language in the context of the invasion as can be found in its nuclear doctrine. Russian nuclear doctrine specifically reserves the right to use nuclear weapons in response to any "existential threats," including any non-nuclear threats that meet a nebulous 'existential' threshold.
Unfortunately, Russian disinformation around non-existent Ukrainian efforts to develop weapons of mass destruction, the Russian intellectual tradition that thinks of Ukraine as rightful Russian territory, and Putin's personalistic leadership style all mean this criterion could fairly easily be met. At a recent workshop held by Stanford University's Center for International Security and Cooperation and the Global Security

Institute, former US ambassador to Ukraine Steve Pifer explained: "The concern I have is that, if Russia is losing this war… that is not existential for Russia, but it is perhaps existential for Putin, and that is where I start to get concerned about the use of nuclear weapons." That Putin might be willing to use nuclear weapons to preserve his own power is a harrowing possibility—one that his position as an autocratic leader may enable. If Putin favors nuclear use, he is unlikely to experience pushback either from within his government or from the general Russian public. Dissuading and deterring Russian nuclear use, then, must remain an essential political objective for the United States and its NATO allies.

While some have argued that any nuclear use from Russia would likely be limited to a single demonstration—such as a high-altitude test, which would be intended not to cause any direct casualties—others have predicted more dire forms of possible Russian nuclear use. For example, Siegfried Hecker, a former director of the Los Alamos National Laboratory, says that "if Putin is going to use a nuclear weapon, he's going to use it. He's not going to do a demonstration." After all, Russia has little need to demonstrate its nuclear capabilities; the extent of its resources is well known. A nuclear demonstration could even be counterproductive, showing that Russia is unwilling to use nuclear weapons tactically and thereby undermining nuclear deterrence.

These complex dynamics suggest that, should Putin feel the need to use nuclear weapons to offset military losses (or simply to stay in power), Russia could ultimately use nuclear weapons on the battlefield. And we may already be edging closer to that possibility. Former deputy secretary general of NATO and former US under secretary of state for arms control and international security Rose Gottemoeller puts the chances of Russian nuclear use at "greater than one percent." After all, Russia has already suffered significant losses, including—by Ukrainian estimates—up to 30,000 fatalities, the ascension of Finland and Sweden to NATO's ranks, as well as damage and destruction to thousands of pieces of its heavy military equipment, including the sinking of Moskva, the flagship of Russia's prized Black Sea fleet.

Philip Taubman, the former Moscow bureau chief for *The New York Times*, tells me: "I think it's impossible to over-state the pathetic performance of the Russian military during the initial stage of its invasion in Ukraine. Combine that with the American rhetoric about degrading the [Russian] military to the point where they can no longer pose a threat, and you are inevitably pushing the Kremlin toward nuclear weapons. That is the singular danger of this war, more than anything." Even a limited nuclear strike on an isolated military base or in a remote area would do irreparable and long-term environmental damage, shatter expectations around civilian immunity and the non-use of nuclear weapons in warfare, and even potentially spiral out of control.

Fortunately, there are some steps the United States can take to reduce the possibility of Russian nuclear use. The United States can work to make it clear to Russian leaders that there would be a major global response if Russia were to use nuclear weapons. Engaging Russia's partners—including China, India, and states throughout the Global South—to reaffirm the threat of political and economic fallout from any nuclear use would be essential. The United States can also continue to reiterate its security guarantees to its allies in order to strengthen extended deterrence. "The best way to prevent [Russian nuclear use is by] thinking about how to deter a crisis like this from ever happening again," says Stanford University professor Scott Sagan. "All of the options now are very risky and very frightening. We should be privately telling the Russians that the use of nuclear weapons against a city is a war crime, and we have a history of tracking down war criminals."

Unfortunately, even if Putin refrains from using nuclear weapons in Ukraine, the course of the war has already contributed to eroding the nuclear taboo, or the tradition of the non-use of nuclear weapons. Russia's nuclear threats and its attacks on nuclear facilities, including the Chernobyl exclusion zone and the Zaporizhzhia nuclear power station, represent major departures from the norms that guided previous conflicts. Rebuilding these norms will be a critical global challenge moving forward.

Russian attacks on nuclear power plants may also complicate the future of energy security. European states are now faced with an important conundrum. To reduce reliance on Russian oil and gas, they may need to revitalize their domestic energy programs, including nuclear power and renewables. But energy transitions can take decades. At the same time, Russia has long held a central role in the global construction of nuclear power plants, exporting nuclear technology and nuclear fuel as well as managing nuclear waste. Continued global development of nuclear power will be exceedingly difficult to do independently of Russia. Moreover, Russian actions have stressed one of the many possible risks of operating nuclear power plants. By attacking nuclear power plants and even forcing operators to work multi-day shifts at gunpoint, Russia not only violated a critical norm against warfighting at or near nuclear facilities but also emphasized the vulnerability of these facilities to terrorists, mercenaries, and foreign militaries. Gottemoeller even likens Russia's actions against Ukrainian nuclear facilities to "nuclear terrorism."

The ongoing war in Ukraine is also likely to shape the development of military strategy in Europe, including through the decision-making process around the new NATO Strategic Concept. NATO's current doctrine was designed with a focus on developing new goals and areas of cooperation for its members during peacetime. But today's wartime conditions will demand a different strategic design for the new Concept. A regrouped effort to counteract Russian aggression and a renewed focus on nuclear deterrence are both likely to be up for discussion at the Madrid summit to be held June 28-30, 2022, where NATO members will write and adopt the new Concept. At the summit, NATO states will be challenged to devise a strategy that at once highlights the importance of deterring Russian nuclear

aggression and, at the same time, promotes norms and policies of nuclear restraint, including through arms control and disarmament efforts.

While the war highlights the pressing need for expanded arms control arrangements with Russia, returning to the agreement made by Presidents Biden and Putin to conduct strategic stability dialogues will be exceedingly difficult. Can the conditions for productive arms control with Russia be restored? Pifer tells me he is pessimistic. "There are two things that would have to change," he says. "Putin has to leave [office] and there have to be real policy changes by his successor to demonstrate that Russia is changing course." Yet continuing to push for limits on non-strategic nuclear warheads and designing ways to integrate European allies into the monitoring and verification processes for future arms control efforts will be critical, even if there is an uphill battle ahead. The United States can also continue to work toward disarmament and nonproliferation efforts elsewhere around the world, including through arms control dialogues with China. These efforts can help contribute to global strategic stability, even if cooperation with Russia is, for the moment, unlikely.

However important, international arms control and nonproliferation efforts will be more difficult in the wake of the Russian invasion of Ukraine. Hecker explains that Putin has "blown up the global nuclear order… 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." That fallout will undoubtedly extend to the Non-Proliferation Treaty review conference, which begins on August 1, 2022, as Russia's nuclear threat-making has exacerbated demands for strengthened extended deterrence and shaped warming interest in nuclear proliferation among NATO and other US allies. Managing dual pressures from the need for stronger nuclear deterrence alongside condemnations of the failure of the United States and other nuclear powers to progress toward disarmament will force US officials to walk a thin tightrope throughout the review conference.

The Russia-Ukraine war will have dire consequences for the future of the nuclear order. Not only has the war raised the specter of possible nuclear use, but it has also devolved norms around the use of nuclear weapons and the protection of nuclear facilities during wartime. Russian nuclear aggression has decimated the chances of continued cooperation on arms control, nuclear power production, and nonproliferation efforts. But if the United States is to work toward the challenging, yet the all-important goal of global strategic stability, it cannot do so alone. Cooperation between the United States and Russia has long been a cornerstone of the global nuclear order. Restoring and reinforcing that order will require finding ways to bring Russia once again to the negotiating table.

Lauren Sukin is a MacArthur Nuclear Security Postdoctoral Fellow at Stanford University's Center for International Security and Cooperation and an incoming Assistant Professor of International Relations at the London School of Economics and Political Science. Her research examines the role of nuclear weapons in alliances, crisis politics, and public opinion. She holds a Ph.D. and MA in political science from Stanford University and ABs in political science and literary arts from Brown University.

Iran's Centrifuges: Models and Status

Source: https://www.iranwatch.org/our-publications/weapon-program-background-report/irans-centrifuges-models-status

June 24 – Iran possesses thousands of gas centrifuges that are the mainstay of its nuclear program. Gas centrifuges spin uranium hexafluoride gas (UF_6) to separate uranium isotopes suitable for nuclear fuel, a process known as uranium enrichment.[1] The number and capacity of these machines determine Iran's "breakout" time: how long it would take Iran—if it decided to do so—to produce the fuel for a small nuclear arsenal. The machines are also key to Iran's ability to "sneak out" by producing nuclear weapon fuel at secret sites.

In recent years, Iran has developed and deployed centrifuge models that can enrich greater amounts of uranium with fewer machines relative to its original IR-1 design. Iran's increasing mastery of centrifuge design and manufacturing raises the risk of a "sneak out," and it reflects an acquisition of knowledge that cannot be reversed.

The table below sets out the capacity and primary materials of each of Iran's currently-deployed centrifuge models, as well as the number of each model known from publicly-available IAEA reports[2] to be installed and/or enriching uranium at Iran's three declared enrichment sites: the Fuel Enrichment Plant (FEP) and Pilot Fuel Enrichment Plant (PFEP) at Natanz and the Fordow Fuel Enrichment Plant (FFEP) at Fordow.
In addition to the models listed in the table, Iran has developed several other centrifuge designs that are not currently installed at any of its declared sites, including the IR-2, IR-3, IR-6m, IR-6sm, IR-6smo, IR-8s, and IR-9s.
The information in the table about the number of centrifuges installed or operating is based on IAEA reports. The information on centrifuge capacity and rotor material is based on a November 2021 Iran Watch report, Beyond the IR-1: Iran's Advanced Centrifuges and their Lasting Implications, which contains analysis of each centrifuge model.

●▶ Click on the source's URL for more details on centrifuges models.

The US Nuclear Posture Review in limbo

ISS | Vol 28; June 2022
Source: https://www.iiss.org/publications/strategic-comments/2022/the-us-nuclear-posture-review-in-limbo

The 2022 Nuclear Posture Review (NPR) in the United States has been written and shared with Congress in its classified form, but unusually, an unclassified version has not been made public. This is reportedly due to a dispute with some lawmakers over the pending cancellation of a programme to develop a nuclear-armed submarine-launched cruise missile – which the US Navy appears to support – and because the National Security Strategy written by officials in the administration of US President Joe Biden has not yet been finalised. The brief summary of the 2022 NPR that has been released suggests that it is largely a continuation of the nuclear policy adopted in 2010 by former President Barack Obama.
On 28 March 2022, United States President Joe Biden submitted his Nuclear Posture Review (NPR) to Congress. The classified document establishes his administration's policies regarding nuclear forces and doctrine and was submitted alongside a Missile Defense Review and an overarching National Defense Strategy. The NPR is traditionally written during a new president's first year in office, with an unclassified version made public shortly after transmission to Congress. The NPR process was delayed several months, in part because of the discovery of the extent of China's nuclear build-up and Russia's invasion of Ukraine on 24 February, and while the US Department of Defense released a one-page summary of the NPR, an unclassified version has not been released. This is reportedly because the administration may revise it after its National Security Strategy is finalised, and because there is an ongoing dispute between the administration and Congress about at least one issue: the cancellation of the programme to develop a nuclear-armed submarine-launched cruise missile (SLCM-N).
The 2010 and 2018 NPRs released by the administrations of Barack Obama and Donald Trump, respectively, showed a surprising degree of continuity. They did not make significant changes to the 25-year 'program of record' for nuclear weapons, even if the former emphasised arms control and the latter deterrence. There has been more interest than usual in the 2022 NPR, largely driven by hopes in the disarmament community that long-standing US policies on nuclear weapons might be revised, including the adoption of a 'sole purpose' policy – a declaratory limitation on when these weapons would be used. Biden said as a presidential candidate that he supported the adoption of such a policy. The wording of the one-page summary of the NPR, however, indicates that a 'sole purpose' policy will not be adopted. Russia's aggressive actions in Ukraine and elsewhere, together with recent Chinese behaviour, were probably major factors in this outcome, alongside a realisation that such policies would meet strong congressional opposition and prove controversial among the public.

Modernisation programmes
According to a summary released in March, the National Defense Strategy describes threats to the US as following a 1:1:3 format. China is the 'most consequential strategic competitor' of the US, followed by Russia, which poses 'acute threats'. These are followed by three 'persistent' threats: Iran, North Korea and 'violent extremist organizations'. This is the framing that has been used in drafting the 2022 NPR.
The NPR is expected to support the continuing modernisation of US strategic nuclear-weapon systems, which involves replacing the entire nuclear triad. The proposed National Defense Budget for Fiscal Year 2023 includes US$34.4 billion towards this end (with a 30-year cost approaching US$2 trillion). This ambitious programme was set in motion by Obama and continued under Trump. (Obama agreed to modernisation as a concession to some US senators, who in exchange voted for the 2010 New Strategic Arms Reduction Treaty (START).) The primary elements of the programme include:

- 400 new 35A *Sentinel* intercontinental ballistic missiles
- 12 new *Columbia*-class ballistic-missile submarines
- at least 100 new B-21 *Raider* dual-capable heavy bombers
- replacement of the F-15E and allied dual-capable aircraft with the new F-35, in conjunction with the improved B61 bomb
- capability to produce new plutonium pits – the hollow metallic spheres inserted into warheads that produce a nuclear explosion – with at least 30 to be produced per year at Los Alamos National Labs by 2026 and 50 per year at the Savannah River Site by 2030
- upgrades to nuclear infrastructure
- continuation of life-extension programmes for existing nuclear warheads

"There has been more interest than usual in the 2022 NPR, largely driven by hopes in the disarmament community that long-standing US policies on nuclear weapons might be revised."

The 2022 NPR reportedly does not mention the SLCM-N programme, suggesting that it will be cancelled. Indeed, in testimony before Congress on 4 April 2022, Defense Secretary Lloyd Austin stated that 'the marginal capability that [the SLCM-N] provides is far outweighed by the cost'. And the US Navy's most recent budget request did not include funding for related research and development, which would cost US$2.1bn over five years. The SLCM-N was first proposed in Trump's 2018 NPR and essentially revived the nuclear-armed *Tomahawk* Land Attack Missile that had been retired by Obama's 2010 NPR. Some US allies – particularly Japan – disagreed with this decision, because in their view the *Tomahawk* provided the US with unique military capabilities that could be used in a crisis. The Trump administration viewed the SLCM-N programme as an important part of its nuclear agenda, presenting it as a response to China's changing nuclear posture and to Russia's development of a new nuclear-capable ground-launched cruise missile – the 9M729 (SSC-8) – in violation of the 1987 Intermediate-Range Nuclear Forces Treaty.
Circumstances have changed since the demise of that treaty in 2019. Russia and China have continued arms-racing in this area, while the US has sought to catch up by developing an army ground-launched conventional cruise missile with a range that had been prohibited by the treaty. (Several other countries already possess these types of missiles, including India, Iran, Israel, North Korea, Pakistan and South Korea.) Separately, it appears that the Biden administration will attempt to re-retire the megaton-class B83 bomb – another programme resurrected by Trump – and its support for creating new plutonium pits at the Savannah River Site follows the 2021 cancellation of a troubled programme there that would have turned excess plutonium into fuel for a mixed-oxide reactor.

Doctrine
A major point of interest in the 2022 NPR concerns the role of nuclear weapons – what is known as 'declaratory policy'. For years, there has been pressure from disarmament advocates within and outside the government to declare that the US will not use nuclear weapons first in any conflict, or at least to declare that the 'sole purpose' of US nuclear weapons is to deter the use of nuclear weapons by others. The 2010 NPR punted on this question by promising to 'work to establish conditions under which such a policy could be safely adopted', rather than by making changes to the policy itself. After Russia rejected further nuclear reductions offered by the US in Obama's Berlin speech in 2013, nothing further transpired in this direction, including during the Trump administration. Biden expressed support for the 'sole purpose' doctrine as vice president, and in 2020 during his presidential campaign he wrote in *Foreign Affairs* that 'the sole purpose of our nuclear arsenal should be to deter – and, if necessary, retaliate against – a nuclear attack'.
In recent years, however, opposition to adopting a 'sole purpose' policy has grown in Congress, among security-policy professionals in government and among US allies to which it extends nuclear guarantees. Opponents of this policy say that it would weaken deterrence vis-à-vis Russia and China at the wrong time. For example, Russia's stockpile of dual-capable missiles is growing, Russian President Vladimir Putin introduced a new set of nuclear-delivery systems in a March 2018 speech – including the *Poseidon* (*Kanyon*) autonomous, uninhabited underwater vehicle – and, in 2021, it became publicly known that China has been expanding its nuclear programme significantly beyond what had been expected while arms-racing in dual-capable medium-range missiles. The concern among some US allies in NATO and in Asia is that such a change would weaken US security guarantees and lead to nuclear proliferation. South Korea, for example, might consider developing its own nuclear weapons if the US were to proceed down this path.
The 2022 NPR is expected to leave US policy largely unchanged. A 'sole purpose' policy will almost certainly not be adopted, given that the one-page summary of the 2022 NPR adopted the same declaratory policy as the Obama administration: 'As long as nuclear weapons exist, the *fundamental role* of U.S. nuclear weapons is to deter nuclear attack on the United States, our allies, and partners' (emphasis added). This is a moderate shift from the Trump administration, which focused on the 'ladder of escalation' and the need to dominate adversaries at each rung of this ladder. A key sentence from the summary states that 'the United States

would only consider the use of nuclear weapons in extreme circumstances to defend the vital interests of the United States or its allies and partners'. This is consistent with the declaratory policies of France, Russia and the United Kingdom. It is worth noting that, among the P5 powers, only China has declared a 'no first use' policy, even as it continues to build nuclear-delivery systems that appear inconsistent with that policy.

Comparison to Russian military doctrine

Russia's declaratory nuclear policy, last updated in 2014, is closer to US and NATO doctrine than is generally recognised. The Russian Federation reserves the right to use nuclear weapons in response to the use of nuclear weapons or other weapons of mass destruction against it or its allies, or in response to aggression using conventional weapons that 'threatens the very existence of the state'. The latter phrase is almost certainly drawn from a 1996 Advisory Opinion of the International Court of Justice, which stated that the court 'cannot conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake'.

There has been much speculation in the West about whether Russian doctrine also includes the possibility of using nuclear weapons in a conventional war that is going badly – the so-called 'escalate to de-escalate' use. Russia's first official unclassified nuclear doctrine does not refer to this possibility and government officials have consistently denied that it is part of Russian strategy. But it remains unclear whether any leader of a nuclear-armed state on the brink of losing a large conventional war would be restrained from using low-yield nuclear weapons because of their declaratory policies alone.

Arms control

The summary of the NPR declares that the US should be a leader in arms control, but it is unclear whether the unclassified version will offer specific recommendations in this area, considering the lack of Chinese and Russian interest in the topic. There is a sour mood in Washington regarding arms control, given the partisan divide on the subject domestically, differences among US allies, and a growing frustration with China and Russia on so many issues.

"In recent years… opposition to adopting a 'sole purpose' policy has grown in Congress, among security-policy professionals in government and among US allies to which it extends nuclear guarantees."

The unclassified NPR is expected to affirm the famous 1985 Reagan–Gorbachev statement that 'a nuclear war cannot be won and must never be fought'. This statement was also affirmed by Biden and Putin in June 2021 and again by all P5 countries of the United Nations Security Council on 3 January 2022. It is interesting to reflect on the relevance of this statement to reality, especially in the context of the Chinese and Russian diversification of their nuclear arsenals and the potential for low-yield weapons to be used in conflicts such as the Ukraine war. It is not known whether the NPR mentions the Treaty on the Prohibition of Nuclear Weapons (the Ban Treaty), which entered into force in 2021. This treaty bans all nuclear weapons but has no procedures for achieving this or for creating a verification regime. There are currently 65 state parties to the treaty and 21 additional signatories, many of which are in Africa, Latin America and Southeast Asia. No nuclear weapon possessor states or US treaty allies support the treaty. The Biden administration may attempt to ignore the treaty, rather than to actively oppose it like the Trump administration.

Outlook

Once the NPR is finalised, presumably before the end of 2022, it will offer a comprehensive picture of the role of US nuclear strategy, policy, forces and postures in fulfilling the National Defense Strategy. This does not mean that all questions related to nuclear weapons will soon be settled. Difficult choices and trade-offs remain, and the US has substantial but not unlimited resources available to address these problems. Developments in China and Russia have generated a broader US consensus, particularly in Congress, about the need to strengthen deterrence. If the SLCM-N programme is cancelled, as seems likely given that the Navy's budget request indicates it would rather spend the funds elsewhere, it will be controversial and may force the administration to search for concessions it might make to legislators in other areas of the nuclear portfolio.

The administration will next prepare its classified nuclear-employment guidance, which will provide an opportunity for officials to clarify operational plans and other details. Final negotiations over a new NATO Strategic Concept are underway. It will be released at the end of the 2022 NATO Summit in Madrid in late June and is expected to adhere closely to US nuclear declaratory policy.

"Developments in China and Russia have generated a broader US consensus, particularly in Congress, about the need to strengthen deterrence."

The future for arms control does not look bright. One possibility is that, once the Ukraine crisis is resolved, the world will follow the precedent provided by the 1962 Cuban Missile Crisis, which precipitated the agreement of bilateral and multilateral arms-control measures: the Hotline Agreement and the Partial (Limited) Test Ban Treaty in 1963; the Outer Space Treaty in 1967; and bilateral talks that led to the successful negotiation of the Nuclear Non-Proliferation Treaty, Strategic Arms Limitation Talks, the Anti-Ballistic Missile Treaty, and the Agreement on the Prevention of Nuclear War. Conditions today are different, however. After Cuba, both sides recognised that serious mistakes had been made and had brought the world perilously close to nuclear war. Most expect that Russian foreign policy will proceed on a belligerent course for the foreseeable future, which will make it difficult for most NATO member countries to have functional relations with Moscow, let alone to negotiate meaningful arms-control agreements.

Agron's product update: Upgrade to Mirion ADM300A V1b Simulator

Source: https://www.argonelectronics.com/adm300av1b-sim-radiation-training-simulator

Argon has released a major upgrade to its Mirion ADM300A V1b training simulator that provides a significant and welcome improvement to the simulated Gamma and Beta Gamma simulation performance of the training system.

The upgrade implements Argons' latest generation Gamma simulation technology to deliver advanced simulation of inverse square law response and shielding effects and can be applied to all existing customer ADM 300A V1b simulators.

The realism and repeatability of the simulated inverse square law response and the ability to create scenarios where the source is hidden behind a brick wall, inside a vehicle or within solid packaging is especially impressive and provides instructors with significant, advanced exercise creation flexibility.

The associated simulation gamma source employs Argon's proprietary signalling technology and can be detected by the ADM 300A V1b simulator at distance of typically 60 metres (200 feet) line of sight. All previously supplied legacy gamma survey simulators can be similarly upgraded and all newly released Argon gamma survey simulators will also employ this advanced simulation technology.

ADM300A V1b SIM can also be used with PlumeSIM to respond to scenarios involving wide area radiological releases including ground deposition and hot spot areas.

Argon manufactures a wide range of CBRN and HazMat training simulators, many of which can be used independently or with PlumeSIM, their wide area file exercise / virtual Tabletop exercise system. Simulation systems have been delivered to numerous military and non-military organisations worldwide to enhance CBRN and HazMat response training.

●▶ Download the ADM300A V1B-SIM Radiation Training Simulator product sheet

How commercial satellite imagery could soon make nuclear secrecy very difficult—if not impossible

By Igor Moric

Source: https://thebulletin.org/2022/07/how-commercial-satellite-imagery-could-soon-make-nuclear-secrecy-very-difficult-if-not-impossible/

July 05 – Emerging capabilities of commercial satellite imagery are enabling high-resolution observation of objects and activity over large areas or territories of entire states with a sub-hourly frequency. Existing constellations are being expanded and new ones are planned promising even higher resolution and frequency of observations, on a global scale. Coupled with AI-powered automatic monitoring and detection capability, this rapid technology development and deployment of advanced commercial satellites could soon make it very difficult—if not impossible—to establish secret nuclear programs or maintain secrecy around existing ones.

The burst of open-source intelligence

Satellites operated by private companies located in more than 30 countries now provide imagery that once was accessible only to a handful of governments. One must look no further than the daily coverage of the Russian invasion of Ukraine; satellite images captured the massing of Russian forces on the Ukrainian border, columns of military units, destroyed buildings, burning vehicles, and bodies scattered over streets. These images of war are now on our screens with unprecedented speed and detail. They are shared over social media by

open-source investigators and combined with ground imagery of geo-located events captured by civilians with camera phones and soldiers with drones—a framework often referred to as open-source intelligence or OSINT.
Beyond conflicts, commercially available satellite images also provide an unobtrusive and cost-effective way to monitor the activity of civilian or military nuclear programs, as shown by the many recent analyses of sites in Iran and North Korea. Imagery is part of the International Atomic Energy Agency's toolkit, with the agency's inspectors combining commercial imagery with open-source information to look for direct and indirect signs of nuclear activities.

Underground construction activities were detected in late 2020 using commercial satellite imagery south of the Natanz nuclear facility, Iran (Google, Image CNES / Airbus).

According to the Union of Concerned Scientists' database, as of January 1, 2022, there were 4,852 satellites in orbit, 72 percent of which being commercial systems. The civilian space industry is experiencing extraordinary growth made possible by advancements in technology, increased governmental and public demand for services, and cheaper space launches. Following this growth and relaxation of distribution restrictions, providers of commercial satellite imagery are launching new constellations and encouraging the development of novel applications of overhead imagery.

Capabilities of earth observation systems

Satellites can view ground objects only if they are larger than the sensor's resolution, nothing is obstructing their view, and they are visible within the sensor's observation bandwidth. In addition, the capacity to view the activity as it occurs or map out trends depends on the revisit time, that is the time interval between subsequent observations of the site. The quality of ground coverage during a given period of observation, therefore, mainly depends on spatial resolution the sensor can achieve from the altitude of the satellite, spectral information the sensor can acquire during the observation interval, and frequency of repeated observation.
Current commercial systems can acquire data with a 30-centimeter (cm) and 31-cm resolution in the panchromatic (black and white), respectively. By comparison, US government-owned spy satellites can produce imagery with a top resolution at the level of 10 cm; as evidenced by former President Trump's tweet showing a failed Iranian missile launch in 2019.
Rather than trying to reach the highest level of image quality, commercial providers deploy instead multiple satellites built with cheaper, off-the-shelf components which they can easily replace if they malfunction or technology advances. In addition, using multiple sensors observing from different angles and orbits results in a higher persistency of coverage.
For example, the US company Planet operates more than 150 Dove satellites with up to 3.7-meter resolution. The constellation is being constantly expanded and upgraded, and the data is combined to get a more comprehensive view of the surface.

Sensors with a wider spectral range make it possible to see details beyond the capabilities of the human eye, classify observed material and distinguish human-made from natural objects. Some sensors can also image in the infrared spectrum, allowing them to detect thermal sources on the surface, especially useful for tracking activity inside facilities. But most optical systems won't see the Earth's surface during the night or in conditions of poor illumination. Clouds cover most of the land surface at any moment in time, and some locations remain permanently hidden. This makes it difficult to observe any location on demand.
Synthetic-aperture radar (SAR) systems can fill the observation gaps. Here, the image is produced by the radar antenna which transmits microwave pulses that bounce from ground targets and are then bounced back to the satellite. By measuring the phase and the intensity of the returned signal, the system can construct an image of the surface and accurately derive distances between objects, after a relatively extensive image conversion process. Atmospheric and illumination conditions will not affect the quality of the image. SAR systems are always watching.

Satellite super-constellation imagery

If all commercial satellites currently in operation were to be combined into one super-constellation, they would provide global coverage of the Earth's surface with a frequency of only a few hours. Recent work has simulated what type of coverage can be provided by a super-constellation formed by 300 systems—265 optical imaging satellites and 35 SAR-equipped satellites. These systems were selected under the condition that they offer some form of public access to their data and have an imaging ground resolution of five meters or less, at which it becomes possible to identify many objects from space—even though lower-resolution imagery can and was regularly used for nuclear verification and monitoring.
The simulation calculates the ground coverage of the constellation over territories of states with active nuclear programs for a duration of 14 days. A successful pass was not defined simply as a ground track revisit but as a successful observation of some site considering orbit and sensor properties. For optical systems, it considers the effect of statistical cloud coverage and sun illumination, while for SAR it assumes this has no effect on observation quality. Coverage was calculated for different ground resolution intervals, equivalent to levels of detectability of ground objects. Optical and SAR systems were simulated separately because observations in different bands are not equivalent and do not provide the same type of information for a given resolution, even though data from different bands can be merged to provide more than the sum of its parts. Results from the simulations show that with combined commercial systems, it would be possible to observe most locations on the planet every 15 hours on average in the optical and under five hours with SAR, with a sub-meter resolution.

Applications in nuclear verification and monitoring

The current fleet of commercial imagery satellites allows inspectors to detect, identify and monitor most objects relevant to nuclear arms control and nuclear proliferation analysis. They also allow identifying signatures of activities associated with the development, acquisition, and maintenance of operational nuclear weapons capabilities. Commercial imagery satellites can also reveal the absence of items that are necessary for the normal operation of a site that was declared to have some other non-nuclear uses.
High resolution and high frequency of observation are not necessary for the detection of new structures and most immobile objects. Commissioning of nuclear facilities takes years and can easily be detected even with low-resolution sensors. For example, in 2006, imagery taken at a monthly rate was used to detect the construction of a nuclear reactor in Pakistan and later produce a three-dimensional model of the facility and estimate its plutonium production capacity. Even before construction begins, a future site of a nuclear facility can be recognized by tight security, the stockpiling of equipment and increased traffic at a remote location, or proximity to other sites of similar characteristics.
Satellite observations of a site at a weekly frequency provide more information on the facility operation and surrounding activity. Multispectral monitoring of thermal and vapor plume emissions and steam discharges enables monitoring of the operational state of a nuclear facility and can even help estimate the existing stockpile. Satellites can also be used as a tool to track the nuclear fuel cycle. For example, civilian inspectors were able to monitor the operation of North Korea's nuclear reactor and Yongbyon radiochemistry laboratory. Established durations of activity match IAEA's estimated time required to reprocess irradiated fuel and produce plutonium.
Even more frequent observation allows for more confident mapping of trends and an increased probability of detection of attempts at deceiving the observer. Using imagery taken daily, researchers from Stanford's Center for International Security and Cooperation (CISAC) were able to count trucks at a border crossing between China and North Korea, and in that way track trends in trade activity between the two countries.
With the enormous amount of data being downlinked to ground stations each day, AI algorithms are increasingly used for the processing of raw imagery, object classification, and identification of correlations and irregular behavior. For example, the retail industry uses such algorithms to count cars on parking lots and help companies evaluate commercial activity, whereas analysts use them to count the number of

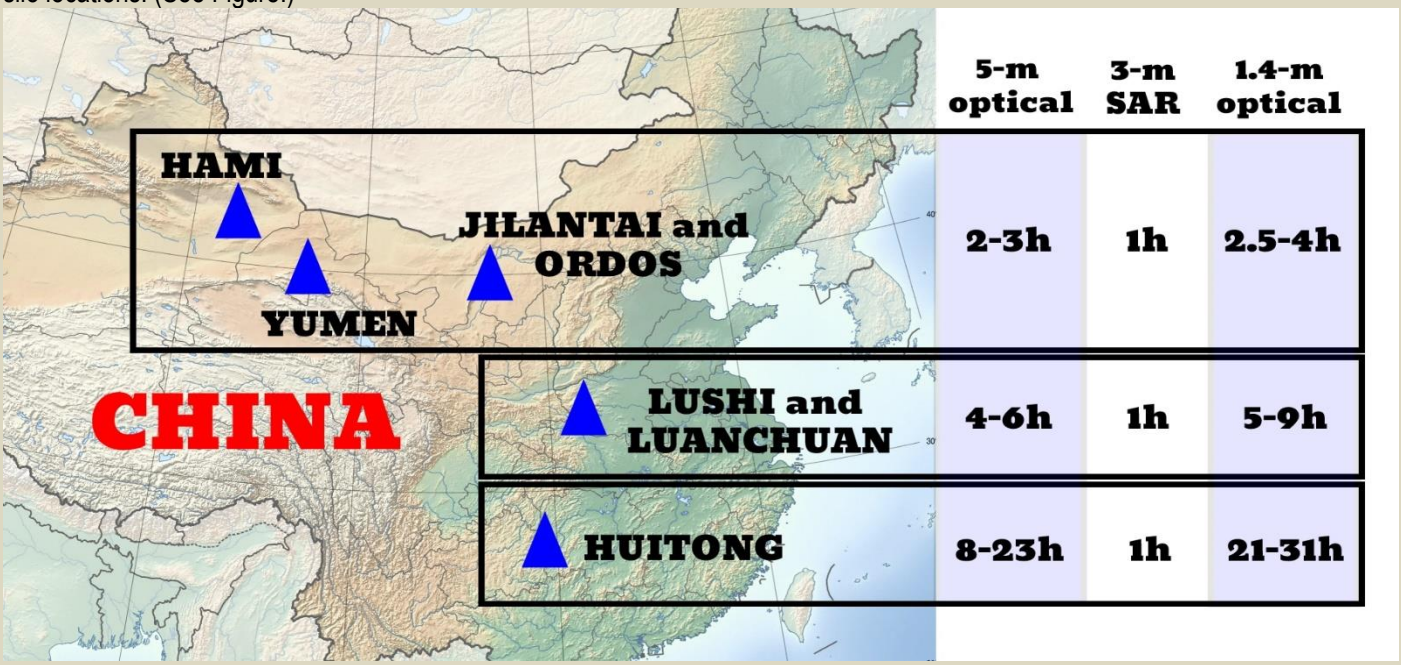
new oil well pads to predict global supply. Similar AI-powered detection capabilities can be used for nuclear verification and monitoring.

Integration of AI in data analysis

With the help of AI algorithms, researchers from open-source defense intelligence agency Janes and Stanford's CISAC used imagery taken at a monthly rate between mid-2020 and early 2021 to automatically count vehicles on a parking lot of a nuclear facility in Iran. From this information, they inferred site personnel fluctuations and then the progress in the construction of a possible underground centrifuge assembly facility—despite the facility not being directly visible from space. Higher persistency of coverage could permit detection and tracking of individual vehicles entering and leaving nuclear facilities with much higher confidence. This can reflect staffing and material demand, allowing remote inspectors to evaluate the production status without the need to visit the site or place intrusive electronic sensors.

Monitoring of state nuclear activities can be performed even without satellites. Citizens can often see what is happening in their area and share information over the Internet. For example, Nukewatch—a volunteer-based civilian organization—tracks British nuclear warhead convoys. Then, crossing the observed level of activity and movement of trucks with official reports and publications, Nukewatch can analyze UK's nuclear modernization and estimate the armament of their nuclear-capable submarines. But this kind of information gathering by concerned citizens is not possible in all countries. Even otherwise democratic societies often work hard to keep their nuclear programs far from the public eye.

Another simulation was performed with a satellite super-constellation by focusing the coverage on the territories of China and North Korea. Chinese and Russian providers that might have objected to imaging of sensitive areas were removed from the sample of available systems. A similar analysis can be performed for other territories, such as the United States and Russia, by removing satellites operated by companies located in those countries. The results showed that on average all locations for every ground resolution in China and North Korea can be imaged at least once every 24 hours. If using the SAR technology, the entire territory of China can be imaged every few hours. This would, for example, allow detection of missile uploading at all known Chinese missile silo locations. (See Figure.)



Example of coverage achieved through satellite super-constellation imagery at locations of known missile silo sites in China. Observation resolutions were selected to allow detection of new construction (5-m optical), vehicles (3-m SAR), and missile uploading (1.4m optical). Image Igor Moric.

Outlook

Even though confidence in what is observed typically scales with sensor advancements and the increased number of satellites, there are inherent limitations to what a sensor can observe from the Earth's orbit. Hosts can attempt to obfuscate their activities, camouflage objects, or otherwise deceive the observer. But hiding will become increasingly difficult as more data is collected, and persistency of coverage is improved.

Advanced satellite imagery allows counting objects of sufficient size, but cannot reveal sensitive information about their structure, chemical composition, or other confidential characteristics. This technical limitation could act as an advantage in nuclear inspection, as the host does not need to worry about the unintended disclosure of information.
Within the next few decades, swarms of commercial surveillance satellites could make real-time multispectral satellite imagery available to everyone. Aided by AI, this could be exploited to create an automated system that monitors sites and detects the appearance or removal of objects relevant to civilian and military nuclear programs, for all atmospheric conditions and during the night. Satellites may be able to track all vehicles entering or leaving nuclear sites anywhere in the world, be they uranium mines, enrichment plants, nuclear reactors, or weapons assembly, deployment, maintenance, storage, and dismantlement sites. Establishing secret nuclear programs—both for energy and weapons—and maintaining secrecy around existing ones could soon become extremely difficult, if not impossible.

Igor Moric is a postdoctoral research associate in the Program on Science and Global Security (SGS) at Princeton University. Prior to joining Princeton, he worked as a postdoctoral researcher on the MIMAC and PandaX dark matter detectors at Tsinghua University in Beijing and SJTU in Shanghai, respectively. During his PhD at CNES and Paris Sorbonne he worked on characterization and optimization of the space atomic clock PHARAO. He also holds an advanced master in "Space Systems Engineering" from ISAE-SUPAERO in Toulouse.

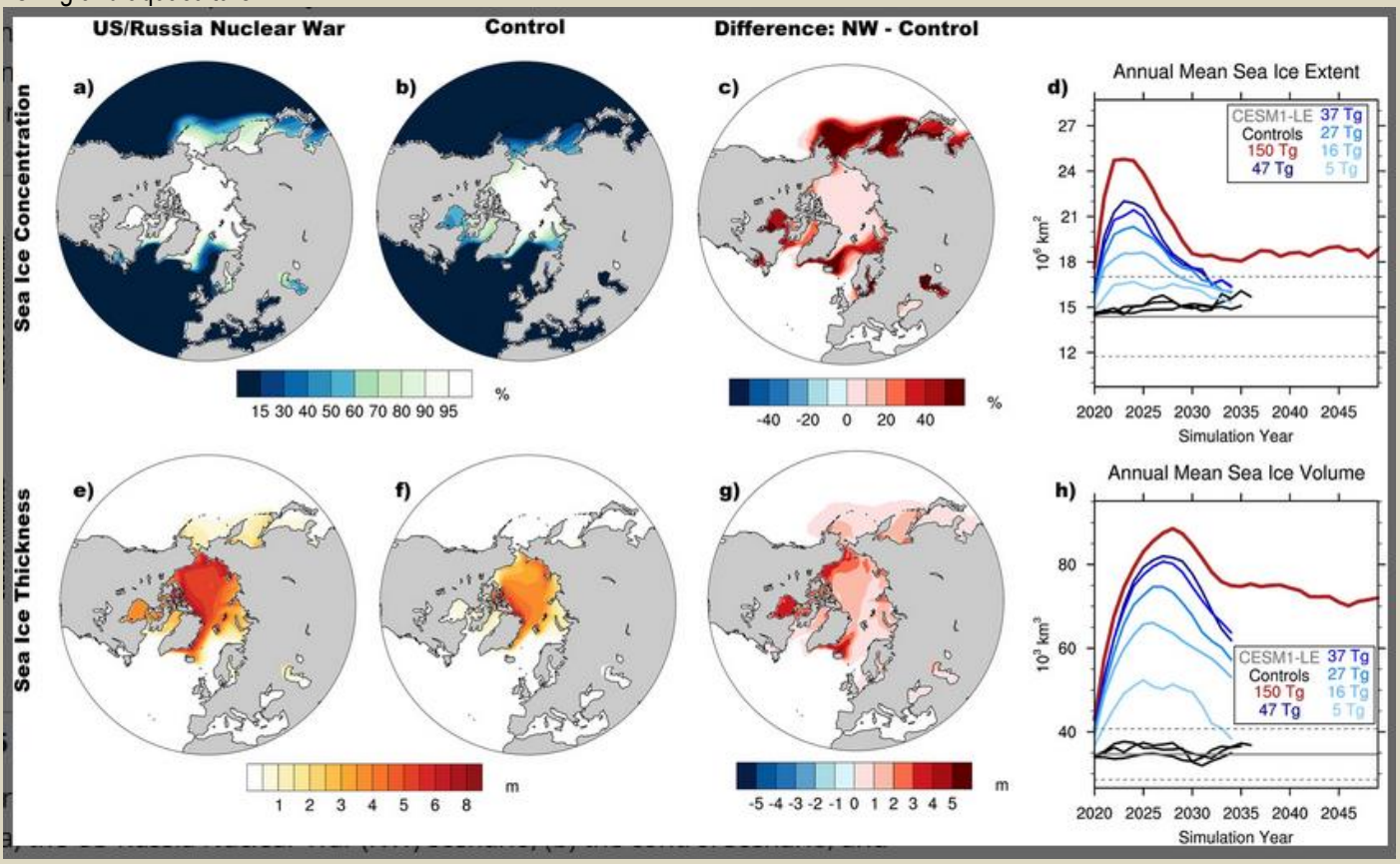
How nuclear war would affect earth today

Louisiana State University
Source: https://www.eurekalert.org/news-releases/958087

LSU Department of Oceanography & Coastal Sciences Assistant Professor Cheryl Harrison presents recent research findings on the impacts of nuclear war on Earth's systems at the Nuclear Threat Initiative conference. view more (Credit: Matt Mendelsohn, NTI)

July 07 – Russia's invasion of Ukraine has brought the threat of nuclear warfare to the forefront. But how would modern nuclear detonations impact the world today? A new study published today provides stark information on the global impact of nuclear war.
The study's lead author LSU Department of Oceanography & Coastal Sciences Assistant Professor Cheryl Harrison and coauthors ran multiple computer simulations to study the impacts of regional and larger scale nuclear warfare on the Earth's systems given today's nuclear warfare capabilities. Nine nations currently control more than 13,000 nuclear weapons in the world, according to the Stockholm International Peace Research Institute.
In all of the researchers' simulated scenarios, nuclear firestorms would release soot and smoke into the upper atmosphere that would block out the Sun resulting in crop failure around the world. In the first month following nuclear detonation, average global temperatures would plunge by about 13 degrees Fahrenheit, a larger temperature change than in the last Ice Age.
"It doesn't matter who is bombing whom. It can be India and Pakistan or NATO and Russia. Once the smoke is released into the upper atmosphere, it spreads globally and affects everyone," said Harrison, who has a joint appointment at the LSU Center for Computation & Technology.
Ocean temperatures would drop quickly and would not return to their pre-war state even after the smoke clears. As the planet gets colder, sea ice expands by more than 6 million square miles and 6 feet deep in some basins blocking major ports including Beijing's Port of Tianjin, Copenhagen and St. Petersburg. The sea ice would spread into normally ice-free coastal regions blocking shipping across the Northern Hemisphere making it difficult to get food and supplies into some cities such as Shanghai, where ships are not prepared to face sea ice.

The sudden drop in light and ocean temperatures, especially from the Arctic to the North Atlantic and North Pacific oceans, would kill the marine algae, which is the foundation of the marine food web, essentially creating a famine in the ocean. This would halt most fishing and aquaculture.



Post-war Arctic sea ice evolution. Arctic 2020–2025 mean sea ice concentration (%) for (a) the US-Russia Nuclear War (NW) scenario, (b) the control scenario, and (c) the difference in concentration between the two scenarios, and Arctic mean sea ice thickness (m) for (e) the US/Russia Nuclear War scenario, (f) the control scenario, and (g) the difference in thickness between the two scenarios. The Northern Hemisphere annual mean time series of (d) sea ice extent and (h) sea ice volume is shown for all war scenarios (colors) and control scenarios (black), where the Community Earth System Model-Large Ensemble experiment mean (solid gray line) and standard deviation (dashed) over the preindustrial period are given to demonstrate the natural, internal variability within the model

The researchers simulated what would happen to the Earth's systems if the U.S. and Russia used 4,400 100-kiloton nuclear weapons to bomb cities and industrial areas, which resulted in fires ejecting 150 teragrams, or more than 330 billion pounds, of smoke and sunlight-absorbing black carbon, into the upper atmosphere. They also simulated what would happen if India and Pakistan detonated about 500 100-kiloton nuclear weapons resulting in 5 to 47 teragrams, or 11 billion to 103 billion pounds, of smoke and soot, into the upper atmosphere.

"Nuclear warfare results in dire consequences for everyone. World leaders have used our studies previously as an impetus to end the nuclear arms race in the 1980s, and five years ago to pass a treaty in the United Nations to ban nuclear weapons. We hope that this new study will encourage more nations to ratify the ban treaty," said co-author Alan Robock, Distinguished Professor in the Department of Environmental Sciences at Rutgers University.

This study shows the global interconnectedness of Earth's systems, especially in the face of perturbations whether they are caused by volcanic eruptions, massive wildfires or war.

"The current war in Ukraine with Russia and how it has affected gas prices, really shows us how fragile our global economy and our supply chains are to what may seem like regional conflicts and perturbations," Harrison said.

Volcanic eruptions also produce clouds of particles in the upper atmosphere. Throughout history, these eruptions have had similar negative impacts on the planet and civilization.

"We can avoid nuclear war, but volcanic eruptions are definitely going to happen again. There's nothing we can do about it, so it's important when we're talking about resilience and how to design our society,

that we consider what we need to do to prepare for unavoidable climate shocks," Harrison said. "We can and must however, do everything we can to avoid nuclear war. The effects are too likely to be globally catastrophic."

Oceans take longer to recover than land. In the largest U.S.-Russia scenario, ocean recovery is likely to take decades at the surface and hundreds of years at depth, while changes to Arctic sea ice will likely last thousands of years and effectively be a "Nuclear Little Ice Age." Marine ecosystems would be highly disrupted by both the initial perturbation and in the new ocean state, resulting in long-term, global impacts to ecosystem services such as fisheries, write the authors.

Ukraine helped North Korea in building nuclear weapon

By Sohail Choudhury

Source: https://www.weeklyblitz.net/international/ukraine-helped-north-korea-in-building-nuclear-weapon/

July 11 – While the entire world, especially the United States and the West are feeling threatened by North Korea (DPRK), which possesses nuclear weapons, it is still unknown to many that one of the key player's behind North Korea's nuclear capabilities is Ukraine. According to media reports, its development would not have been possible without Pyongyang's access to Soviet technology, specifically nuclear-capable hardware that remained in Ukraine following collapse of the USSR. It was Ukraine that played key role in making North Korea a major threat to the United States, and its Asian allies, particularly Japan and South Korea.

It may be mentioned here that, the US, South Korea and Japan share a lot of common goals, one of them being the complete de-nuclearization of the Korean Peninsula. US President Joe Biden has once again made this point clear at the 2022 NATO summit in Madrid. Meanwhile, Washington's allies in Asia have recently found a new reason for concern – on June 14, South Korean Foreign Minister Park Jin announced that North Korea had completed preparations for a new nuclear test.

Prior to that, in March 2022, North Korean Supreme Leader Kim Jong-un effectively ended his country's self-imposed 2018 moratorium on testing intercontinental ballistic missiles (ICBMs) capable of reaching US soil. Now, both Seoul and Washington are worriedly awaiting news about new test launches.

Russian media RT in a report said: "Today, we can say with near absolute certainty that, when designing and constructing its intercontinental ballistic missile, the DPRK used RD-250 rocket engines produced at the Ukrainian Yuzhmash machine-building plant in the city of Dnepropetrovsk.

Like most of the still-functioning industrial enterprises in Ukraine, Yuzhmash is part of the Soviet legacy. The plant was built in 1944 with World War II in full swing; later, during the Cold War, its engineers designed and produced the USSR's most advanced missiles to compete with the US in the arms race.

In the 21st century, Washington once again feels threatened by certain Yuzhmash products – despite the fact that Ukraine, following its 2014 coup, became a satellite of the US, and the plant has since signed contracts with the Americans (to produce rocket stages, engines for these stages, as well as various hardware used in their launch vehicles).

In August 2017, The New York Times, citing Michael Elleman, a missile expert with the lobby group Institute of International Strategic Studies (IISS), reported that the DPRK had most likely used the RD-250 engines to design its own intercontinental ballistic missile.

"It's likely that these engines came from Ukraine – probably illicitly… The big question is how many they have and whether the Ukrainians are helping them now. I'm very worried," Elleman said. The experts at the IISS, however, believed that the official authorities in Kiev were not involved in the smuggling operation.

The design bureaus of Yuzhmash, as well as Yuzhnoye Design Office, a similar enterprise in Dnepropetrovsk, were emphatic in their denial of any collaboration with Pyongyang and its nuclear missile program. Secretary of the National Security and Defense Council of Ukraine Aleksandr Turchynov even suggested that the accusations were part of an 'anti-Ukrainian campaign' carried out by Russian intelligence. He claimed it was Moscow's way of concealing its own assistance to North Korea.

However, in a 2018 report by the 1718 Sanctions Committee (DPRK), the Ukrainian authorities admitted that, in all likelihood, the engine for North Korea's ballistic missiles was created using components of the RD-250 engine produced by Yuzhmash. They added that, in their opinion, the deliveries must have been made through Russian territory. Of course, they would say this.

Vasily Kashin, Director of the Center for Comprehensive European and International Studies at the National Research University Higher School of Economics (HSE), told RT that this controversy about North Korea receiving liquid-fuel engines from Yuzhmash remains the only incident officially on record.

"It wasn't Ukraine sending their engines to North Korea – it was the work of North Korean scientific and technical intelligence in Ukraine that made it all happen. Apparently, the liquid-fuel rocket engines had been acquired there illegally even prior to 2014," the expert concluded.

At the same time, relations between Kiev and Pyongyang have never been friendly and heartfelt enough to suggest Ukraine's willingness to provide North Korea with powerful nuclear weapons. However, there is documentary evidence of Ukraine's corruption-based cooperation with other countries in the nuclear missile field at the turn of the 21st century, which may invite precisely this kind of thinking.

In 1994, Kiev finally discarded the last of its remaining nuclear arsenal, of around 1,000 missiles it had retained after the collapse of the USSR. The plan was to pass half of them on to Russia and to destroy the rest – as part of the US-funded disarmament program. But in 2005, ex-president of Ukraine Viktor Yushchenko confirmed that the previous administration had sold X-55 cruise missiles capable of carrying a nuclear warhead to Iran and China *"through several figureheads,"* as he put it. The range of these missiles is 2.5 thousand kilometers, so this scam practically meant an increased threat of nuclear attack for Israel and Japan.

However, it seems that North Korea had other ways of getting what it wanted.

Starting from the 1990s, representatives of North Korea were caught red-handed trying to get hold of Soviet nuclear missile technology on many occasions. Kashin believes Pyongyang has been conducting scientific and technical intelligence in Ukraine for quite a while now.

"According to declassified KGB documents, North Korean scientific and technical intelligence efforts in Ukraine date back to Soviet times. There was a criminal case, for example, involving their agent, a worker of the Arsenal Factory in Kiev, who was caught stealing parts of anti-tank missiles. North Koreans had ample opportunity to get hold of Soviet military technology in the 1990s and early 2000s in Dnepropetrovsk where they were snooping around all the time. And the Ukrainian government was not involved in any of this. There is nothing to confirm that they were selling their technology deliberately, of course. They just took advantage of the gaps in Ukraine's flawed counter-intelligence system", Kashin said.

Mikhail Khodarenok, a military analyst and retired colonel, reminded RT about the chaos and anarchy that reigned in post-Soviet Russia and Ukraine, affecting many areas of life in the 1990s.

"Back then, Ukraine saw much of its critically important technology leak out of the country. We can trace Ukrainian influence in both China's and Iran's strategic cruise missile arsenals. And it's not surprising – everyone did their best to survive in those turbulent times. And many things may indeed have been done without the involvement of [the] Ukrainian leadership".

"But I don't believe North Koreans were able to steal much. I am inclined to think that, in many cases, it was all based on deals, on mutual agreement. It's just that the government was not part of it", Khodarenok concluded.

And 20 years after the Soviet Union collapse, espionage attempts by North Korea continued.

On 12 December 2012, the DPRK became the 10th nation to join the global space club by placing its Kwangmyongsong-3 (or KMS-3) satellite in Earth orbit. It was the same year when a high-profile spy case involving North Korean nationals was investigated in Ukraine.

It resulted in two citizens of North Korea (employees of a trade mission in Belarus) being sentenced to eight years in prison. They were caught trying to buy technical documentation and scientific works containing important R&D results from the staff of the Yuzhnoye Design Office in Ukraine. And they offered to pay a modest fee of $1,000 for every research paper on liquid-fuel engine systems. An unnamed source later informed the Strana.ua web portal that the Koreans had taken a particular interest in the design of the legendary R-36M (or Satan) intercontinental ballistic missile engine. It's the most powerful missile of its kind".

Another issue that has likely played into the hands of North Korean technology hunters is the 'brain drain' phenomenon, with dozens of Soviet engineers fleeing abroad after the Belovezh Accords were signed in 1991, disbanding the USSR.

The post-Soviet de-industrialization of Ukraine took stable income and career prospects away from dozens of professionals working at the Ukrainian aerospace manufacturer Yuzhmash. So these people were forced to look for other ways to make a living.

Choices were limited. They could either try their luck in the wild post-Soviet labor market (attempting to start a business or becoming a salesperson) or agree to a tempting –albeit questionable in terms of patriotism and legality– offer to help other countries with their nuclear missile programs.

Many of them found themselves in difficult circumstances –personally and professionally– after the fall of the Soviet Union. It's even believed that some of them went to North Korea, Iran and Pakistan.

Former US Ambassador to Ukraine Carlos Pascual later admitted that the importance of this phenomenon, when top-level specialists lost their jobs, was overlooked. It wasn't just a matter of their personal turmoil – this was an important factor for the non-proliferation of weapons of mass destruction.

The US and EU, however, took some initiatives in the mid-1990s. They funded the Science and Technology Center in Ukraine, an intergovernmental organization that was supposed to make sure that expertise and experience in the area of weapons of mass destruction didn't leak.

Executive Director Curtis Bjelajac admitted that there was a point where the center basically gave out money to certain specialists. In the end, millions of dollars were spent on former Soviet engineers and scientists specializing in missile and nuclear technology. The general consensus is that this helped stop the flow of professionals into countries that are toying with dangerous technology. But were there any 'leaks'?

According to Mikhail Khodarenok, there is an understanding within the community of experts that it was the work of Yuzhmash specialists that helped North Korea develop its missiles.

"You can't really judge Yuzhmash engineers – everyone tried to survive back then, and those countries paid good money. I think that many went there for work. North Korea would not have made such advances without the expertise in the critical technology. The Soviet Union also had to borrow – it used Wernher von Braun's research after the war", Khodarenok said. (Von Braun was a German aerospace engineer and Nazi Party member who later worked in the US".

With the past record of selling nuclear technology and hardware to a number of countries such as North Korea, Iran and Pakistan, Ukraine should remain in watch-list of the Western nations as they may start selling sophisticated weapons and military assets to any dubious buyer, including Islamist militancy groups such as Al Qaeda, Islamic State, Hezbollah and Hamas.

Sohail Choudhury is the Executive Editor of Blitz

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

By Hans M. Kristensen and Matt Korda

Source: https://thebulletin.org/premium/2022-07/nuclear-notebook-how-many-nuclear-weapons-does-india-have-in-2022/

Editor's note: The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Matt Korda, a senior research associate with the project. The Nuclear Notebook column has been published in the Bulletin of the Atomic Scientists *since 1987. This issue examines the status of India's nuclear arsenal, which includes approximately 160 warheads. India continues to modernize its nuclear arsenal, with at least four new weapons systems now under development to complement or replace existing nuclear-capable aircraft, land-based delivery systems, and sea-based systems. Several of these systems are nearing completion and will soon be combat-ready. India is estimated to have produced enough military plutonium for 140 to 210 nuclear warheads but has likely produced only 160. Nonetheless, additional plutonium will be required to produce warheads for missiles now under development, and India is reportedly building several new plutonium production facilities. India's nuclear strategy, traditionally focused on Pakistan, now appears to place increased emphasis on China, and Beijing is now in range of Indian missiles.*

July 11 – Collecting and analyzing accurate information about India's nuclear forces is a more challenging effort than for many other nuclear-armed states. India has never disclosed the size of its nuclear stockpile, and Indian officials do not regularly comment on the capabilities of the country's nuclear arsenal. Although some official information can be derived from parliamentary inquiries, budget documents, government statements, and other sources, India generally maintains a culture of relative opacity regarding its nuclear arsenal. India has previously refused to divulge the costs of certain nuclear weapon programs, and in 2016, the Indian government added Strategic Forces Command – the agency responsible for operating the country's nuclear arsenal – to a list of security organizations exempt from the India's Right to Information Act, thus inhibiting journalists, researchers, and the public from getting access to critical information about India's nuclear arsenal (Sarkar 2021; Government of India 2016).

In the absence of official information from the Indian government and military, local news and media outlets tend to embellish details about the country's nuclear arsenal; for example, some outlets regularly claim that certain weapon systems are "nuclear-capable," despite a lack of any official evidence to that effect. To that end, we generally rely on official sources and images – as well as commercially or freely-available satellite imagery – to analyze India's nuclear arsenal and, whenever possible, try to corroborate the credibility of any unofficial claims with multiple sources. In particular, the research of open-source analysts such as *@tinfoil_globe* have proven to be highly valuable in analyzing Indian military bases using satellite imagery.

India continues to modernize its nuclear weapons arsenal and operationalize its nascent triad. We estimate that India currently operates eight different nuclear-capable systems: two aircraft, four land-based ballistic missiles, and two sea-based ballistic missiles. At least four more systems are in development, most of which are thought to be nearing completion and to be combat-ready soon. Beijing is now in range of Indian ballistic missiles.

India is estimated to have produced approximately 70 – plus or minus about 150 kilograms – of weapon-grade plutonium, sufficient for 138 to 213 nuclear warheads (International Panel on Fissile Materials 2022); however, not all the material has been converted into nuclear warheads. Based on available

information about its nuclear-capable delivery force structure and strategy, we estimate that India has produced 160 nuclear warheads (see Table 1). It will need more warheads to arm the new missiles that it is currently developing.

Table 1. Indian nuclear forces, 2022.

Type/designation	No. of launchers	Year deployed	Range (km)[a]	Warheads x yield[b]	No. of warheads
Aircraft	48[c]				48
Mirage 2000 H	32	1985	1,850	1 x 12 kt bomb	–
Jaguar IS	16	1981	1,600	1 x 12 kt bomb	–
Rafale	(32)	2022	2,000	[1 x 12 kt bomb][d]	–
Land-based missiles	64				64[e]
Prithvi-II	24	2003	250[f]	1 x 12 kt	24
Agni-I	16	2007[g]	700+	1 x 10–40 kt	16
Agni-P	–	(2025)	1,000–2,000	1 x 10–40 kt[h]	–
Agni-II	16	2011[i]	2,000+	1 x 10–40 kt	16
Agni-III	8	2018	3,200+	1 x 10–40 kt	8
Agni-IV	–	(2023)	3,500+	1 x 10–40 kt	–
Agni-V	–	(2023)	5,000+	1 x 10–40 kt	–
Agni-VI	–	(2026)	6,000+	1 x 10–40 kt	–
Sea-based missiles	3/14[j]				16
Dhanush	2	2013	400	1 x 12 kt	4[k]
K-15 (B-05)	1/12[l]	2018	700	1 x 12 kt	12
K-4	–	(2025)	3,500	1 x 10–40 kt	–
Total stockpile	128				128
Other stored warheads					32[m]
Total inventory					160

[a]Range listed is unrefueled combat range with drop tanks, and is intended for illustrative purposes. Actual combat range will vary depending on flight profile, payload, and other circumstances.

[b]The yields of India's nuclear warheads are not known. The 1998 nuclear tests demonstrated yields of up to 12 kt. Since then, it is possible that boosted warheads have been introduced with a higher yield, perhaps up to 40 kt. There is no open-source evidence suggesting that India has developed two-stage thermonuclear warheads.

[c]Aircraft listed in this table are only those estimated to hold nuclear strike roles in the Indian Air Force. Indian Air Force squadrons typically include 18 aircraft per squadron; however, we estimate that not all of the available aircraft will necessarily be fully operational or assigned a nuclear strike role.

[d]The Rafale is used for the nuclear mission in the French Air Force, and India could potentially convert it to serve a similar role in the Indian Air Force, with an eye towards taking over the air-based nuclear strike role in the future. However, as of May 2022 there has been no official confirmation that the Rafale will be used for the nuclear strike role with the Indian Air Force.

[e]The missile and warhead inventory may be larger than the number of launchers, some of which can be reused to fire additional missiles. This table assumes an average of one warhead for each launcher.

[f]The US Air Force's National Air and Space Intelligence Center (NASIC) has estimated the range of the Prithvi-II as 250 kilometers (155 miles) but we assume the range has probably been increased to about 350 kilometers (217 miles) as stated by the Indian government.

[g]Agni-I first began induction with the 334th Missile Group in 2004 but did not become operational until 2007.

[h]The Agni-P test-launch in 2021 was rumored to carry two decoy warheads to simulate a MIRV payload; however, if true then this reflects a largely aspirational capability; India would still be many years away from equipping its ballistic missiles with MIRVs. Once the Agni-P becomes operational, it will likely take over the nuclear strike mission from India's Prithvi-II and Agni-I SRBMs, each of which can carry one warhead.

[i]Agni-II first began induction with the 335th Missile Group in 2008 but did not become operational until 2011.

[j]The first figure is the number of operational vessels – two ships and one nuclear-powered ballistic missile submarine (SSBN); the second is the maximum number of missiles that they can carry. India has launched three SSBNs, but only one – INS *Arihant* – was believed to be operational as of May 2022, and was believed to probably have only a limited operational capability.

[k]Each Sukanya-class patrol ship equipped with Dhanush missiles was thought to have possibly one reload. The effectiveness of these vessels in combat nuclear strike roles is highly questionable given their slow speed and relative vulnerability, and they will likely be retired once India's SSBN program matures.

[l]Each of India's first two SSBNs has four missile tubes, each of which can carry three K-15 submarine-launched ballistic missiles (SLBMs), for a total of 12 missiles per SSBN. India's subsequent SSBNs will likely have eight missile tubes. As of May 2022, we estimate that only one SSBN—the INS *Arihant*—is operational with the Indian Navy, although the INS *Arighat* will likely be operational within the next year.

[m]In addition to the 128 warheads estimated to be assigned to fielded launchers, approximately 32 warheads for K-15 SLBMs on the second SSBN, additional Agni-III MRBMs, and future Agni-IV MRBMs and Agni-V IRBMs are thought to have been produced or be in production for an estimated total stockpile of 160 warheads.

Table 1: India's nuclear forces, 2022

India's source of weapon-grade plutonium has been the operational Dhruva plutonium production reactor at the Bhabha Atomic Research Centre complex near Mumbai, and until 2010 the CIRUS reactor at the same location. India has plans to significantly expand its plutonium production capacity by building at least one more plutonium production reactor. Moreover, the unsafe-guarded 500-megawatt Prototype Fast Breeder Reactor (PFBR) under construction at the Indira Gandhi Centre for Atomic Research near Kalpakkam could potentially increase India's plutonium production capacity even further. The PFBR was originally scheduled to reach criticality in 2010; however, it has been marked by significant delays and is now expected to go critical by October 2022 (Government of India 2021a). The director of the research center has additionally stated that six more fast breeder reactors will come online within the next 15 years (Kumar 2018). Construction of the first two, to be located on-site at the center, will reportedly begin in October 2022 and are scheduled to become operational by the early 2030s (*World Nuclear News* 2022).

Nuclear doctrine

Tensions between India and Pakistan constitute one of the most concerning nuclear hotspots on the planet. These two nuclear-armed countries engaged in open hostilities as recently as November 2020, when Indian and Pakistani soldiers exchanged artillery and gunfire over the Line of Control, resulting in at least 22 deaths. The clash followed another incident in February 2019, when Indian fighters dropped bombs near the Pakistani town of Balakot in response to a suicide bombing conducted by a Pakistan-based militant group. In retaliation, Pakistani aircraft shot down and captured an Indian pilot before returning him a week later. The skirmish escalated into the nuclear realm when it triggered a convening of Pakistan's National Command Authority, the body that oversees Pakistan's nuclear arsenal. Speaking to the media at the time, a senior Pakistani official noted, "I hope you know what the [National Command Authority] means and what it constitutes. I said that we will surprise you. Wait for that surprise. You have chosen a path of war without knowing the consequence for the peace and security of the region" (Abbasi 2019).

In this context, the risk of conflict escalation between India and Pakistan remains dangerously high. In March 2022, India accidentally launched what appeared to be a BrahMos ground-launched cruise missile 124 kilometers (77 miles) into Pakistani territory, damaging civilian property. Pakistani officials subsequently claimed that India did not alert them using the high- level military hotline, and India did not even issue a public statement about the accident until two days later (Dawn 2022). Although the BrahMos is a conventional weapon, the unprecedented incident – as well as India's deficient response – has serious implications for crisis stability between the two countries. In the absence of any de-escalation measures from India, Pakistan reportedly suspended all military and civilian aircraft for nearly six hours and placed frontline bases and strike aircraft on high alert (Bhatt 2022). If this same accidental launch had taken place during a period of heightened tensions, it is possible that the incident could have escalated into a very dangerous phase (Korda 2022).

While India's primary deterrence relationship is with Pakistan, its nuclear modernization indicates that it is putting increased emphasis on its future strategic relationship with China. In November 2021, India's then-Chief of Defence Staff stated in a press conference that China had become India's biggest security threat (Sen 2021). Additionally, nearly all of India's new Agni missiles have ranges that suggest China is their primary target. This posture is likely to have been reinforced after the 2017 Doklam standoff during which Chinese and Indian troops were placed on high alert over a dispute near the Bhutanese border. Tensions have remained high in subsequent years, particularly following another border skirmish in June 2020 that resulted in the deaths of both Chinese and Indian soldiers.

Further casualties have been reported due to Chinese-Indian military skirmishes as recently as January 2021 (BBC 2021).

The expansion of India's nuclear forces against a militarily superior China (in terms of both conventional and nuclear forces) will result in significant new cap- abilities being deployed over the next decade. This development could potentially also influence how India views the role of its nuclear weapons against Pakistan. According to one analyst, "we may be witnessing what I call a 'decoupling' of Indian nuclear strategy between China and Pakistan. The force requirements India needs in order to credibly threaten assured retaliation against China may allow it to pursue more aggressive strategies – such as escalation dominance or a 'splendid first strike' – against Pakistan" (Narang 2017).

India has long adhered to a nuclear no-first-use policy. This policy, however, was weakened by India's 2003 declaration that it could potentially use nuclear weapons in response to chemical or biological attacks – which would therefore constitute nuclear first use, even if it were in retaliation. Moreover, amid the 2016 border skirmishes with Pakistan, India's then-defense minister Manohar Parrikar indicated that India should not "bind" itself to the no-first-use policy (Som 2016). Although the Indian government later explained that the minister's remarks represented his personal opinion, the debate highlighted the conditions under which India would consider using nuclear weapons. Current defense minister Rajnath Singh has also publicly questioned India's future commitment to its no-first-use policy, tweeting in August 2019 that "India has strictly adhered to this doctrine. What happens in the future depends on the circumstances" (Singh 2019). Recent scholarship has further called India's commitment to its no-first-use policy into question, with some analysts asserting that "India's NFU [no-first-use] policy is neither a stable nor a reliable predictor of how the Indian military and political leadership might actually use nuclear weapons" (Sundaram and Ramana 2018). Despite questions about the future

of India's NFU policy, it might have served to limit somewhat the scope and strategy of Indian nuclear forces for the first two decades of its nuclear era.
Additionally, although India has long been thought to store its nuclear warheads separately from deployed launchers, some analysts have speculated that India may have increased the readiness of its arsenal over the past decade by "pre-mating" some warheads with missiles in canisters for a subsection of the ballistic missile launchers, and possibly also storing some bombs at air bases (Clary and Narang 2018, 36–37; Narang 2013). There is still uncertainty about the readiness of the arsenal on a day-to-day basis, since the only two canistered missiles – Agni-V and Agni-P – are not yet operationally deployed. But this trend will likely strengthen with deployed of canistered launchers and India's development of a sea-based leg of its nuclear triad, which, at least in the way the United States and Russia operate ballistic missile submarines, has typically involved mating warheads with missiles.

Aircraft
Fighter-bombers were India's first and only nuclear strike force until 2003, when the Prithvi-II nuclear-capable ballistic missile was fielded. Despite considerable progress since then in building a diverse arsenal of land-and sea-based ballistic missiles, aircraft continue to serve a prominent role as a flexible strike force in India's nuclear posture. We estimate that three or four squadrons of Mirage 2000H and Jaguar IS aircraft at three bases are assigned nuclear strike missions against Pakistan and China.
The Mirage 2000H Vajr ("divine thunder") fighter- bombers are deployed with the 1st, 7th, and possibly the 9th squadrons of the 40th Wing at Maharajpur (Gwalior) Air Force Station in northern Madhya Pradesh. We estimate that one or two of these squadrons has a secondary nuclear mission. Indian Mirage aircraft also occasionally operate from the Nal (Bikaner) Air Force Station in western Rajasthan, and other bases might potentially function as nuclear dispersal bases as well.
The Indian Mirage 2000H was originally supplied by France, which used its domestic version (Mirage 2000N) in a nuclear strike role for 30 years, until its retirement in the summer of 2018. The Indian Mirage 2000H is undergoing upgrades to extend its service life and enhance its capabilities to include new radar, avionics, and electronic warfare systems; the modernized version is called Mirage 2000I. Although the modernization program for 51 Mirage 2000I aircraft was scheduled to be completed by the end of 2021, the program is behind schedule, with only about half of the aircraft having been modernized by the expected deadline (Philip 2022). India also intends to purchase 24 Mirage 2000 aircraft that had been previously phased out of the French Air Force and will use the scavenged parts to maintain the Indian Air Force's existing Mirage squadrons (*The Print* 2021).
The Indian Air Force also operates four squadrons of Jaguar IS/IB Shamsher ("sword of justice") aircraft at three bases (a fifth squadron flies the naval IM version). These include the 5th and 14th squadrons of the 7th Wing at Ambala Air Force Station in northwestern Haryana, the 16th and 27th squadrons of the 17th Wing at Gorakhpur Air Force Station in northeastern Uttar Pradesh, and the 6th and 224th squadrons of the 33rd Wing at Jamnagar Air Force Station in southwestern Gujarat. We estimate that one or two of the squadrons at Ambala and Gorakhpur (one at each base) might be assigned a secondary nuclear strike mission. Jaguar aircraft also occasionally operate from the Nal (Bikaner) Air Force Station in western Rajasthan. The Jaguar, designed jointly by France and Britain, was nuclear-capable when deployed by those countries.
The Jaguar is getting old and might be retired from the nuclear mission soon – if this hasn't happened already. Half of the Jaguars have received the so-called DARIN-III precision-attack and avionics upgrade since 2017 (Ministry of Defence 2017), but the upgrade of the second half of the inventory was scrapped in August 2019 due to its prohibitive cost and long timeline. Instead, the air force will reportedly phase out its Jaguar fleet over the next 15 years. In October 2019, India's Air Chief Marshal declared that the Indian Air Force's six Jaguar squadrons of approximately 108 fighters would begin retiring in early 2020 (Shukla 2019); however, this may have been pushed back to 2024 in order to bring India closer to its goal of maintaining enough squadrons to simultaneously deter both Pakistan and China over the coming decade (Shukla 2021a).
On September 23, 2016, India and France signed an agreement for delivery of 36 Rafale aircraft (Ministry of Defence 2017). The order was considerably reduced from initial plans to buy 126 Rafales. The Rafale is used for the nuclear mission in the French Air Force, and India could potentially convert it to serve a similar role in the Indian Air Force, with an eye towards taking over the air-based nuclear strike role in the future. The Indian defense minister formally received the first Rafale (tail number RB-001) at a special ceremony in France in October 2019, followed by two more a month later. After initial delays due to the Covid-19 pandemic outbreak and subsequent lockdowns in both France and India, the full shipment of the 36 aircraft was completed on-schedule by April 2022 (*Hindustan Times* 2022). All 36 Rafales are outfitted with 13 "India-Specific Enhancements," which include new radars, cold-weather engine start-up devices, 10-hour flight data recorders, helmet-mounted display sights, and electronic warfare and friend-or-foe identification systems (Dominguez 2019).
The Rafales are being deployed in two equally-sized squadrons of 18 fighters and four dual-seat trainers: one squadron (17th "Golden Arrows" Squadron) at Ambala Air Base Station, located only 220 kilometers (137 miles) from the Pakistani border, and the other squadron (101st "Falcons of Chamb and Akhnoor" Squadron) at Hasimara Air Force Station in West Bengal. New infrastructure developments to

accommodate the planes are being constructed at both bases, and the Indian Air Force has reinstated the squadrons to active duty after they had both been decommissioned years earlier (Indian Air Force 2021).

Land-based ballistic missiles

India has four types of land-based, nuclear-capable bal- listic missiles that appear to be operational: the short-range Prithvi-II and Agni-I, the medium-range Agni-II, and the intermediate-range Agni-III. At least three other Agni missiles are in development and nearing deployment: the medium-range Agni-P, the intermediate-range Agni-IV, and the near-intercontinental-range Agni-V.

It remains to be seen how many of these missile types India plans to keep in its arsenal. Some may serve as technology development programs toward longer-range missiles. Although the Indian government has made no statements about the future size or composition of its land-based missile force, short-range and redundant missile types could potentially be discontinued, with only medium-and long-range missiles deployed in the future to provide a mix of strike options against Pakistan and China. Otherwise, the government seemingly appears to be planning to field a diverse missile force that will be expensive to maintain and operate.

The Prithvi-II missile was "the first missile to be developed" under India's Integrated Guided Missile Development Program for "India's nuclear deterrence," according to the government (Press Information Bureau 2013). The missile can deliver a nuclear or conventional warhead to a range of 350 kilometers (217 miles). Given the relatively small size of the Prithvi missile (nine meters long and one meter in diameter), the launcher is difficult to spot in satellite images and therefore little is known about its deployment locations. It is thought India has four Prithvi missile groups (222, 333, 444, and 555) with about 30 launchers deployed close to the border with Pakistan. Possible locations include Jalandhar in Punjab, as well as Banar, Bikaner, and Jodhpur in Rajasthan.

The two-stage, solid-fuel, road-mobile Agni-I missile became operational in 2007, three years after its induction into the armed forces. The short-range missile can deliver a nuclear or conventional warhead to a distance of approximately 700 kilometers (435 miles). The mission of Agni-I is thought to be focused on targeting Pakistan; we estimate that up to 20 launchers are deployed in western India, possibly including the 334th Missile Group. In September 2020, India used an Agni-I booster to conduct a test of its developmental scramjet-powered Hypersonic Technology Demonstrator Vehicle (Jha 2020).

The two-stage, solid-fuel, rail-mobile Agni-II – an improvement on the Agni-I – can deliver a nuclear or conventional warhead to a distance of more than 2,000 kilometers (1,243 miles). The missile may have been inducted into the armed forces in 2008, but technical issues delayed its operational capability until 2011. Around 10 launchers are thought to be deployed in northern India, possibly including the 335th Missile Group. Targeting is probably focused on western, central, and southern China. Although the Agni-II appeared to suffer from technical issues and failed several of its previous test launches, more recent successful tests in 2018 and 2019 indicate that previous technical issues could have since been resolved (Liu 2018; *The Hindu* 2019).

The Agni-III – a two-stage, solid-fuel, rail-mobile, intermediate-range ballistic missile – can deliver a nuclear warhead to a distance of over 3,200 kilometers (1,988 miles). The Indian Ministry of Defence declared in 2014 that the Agni-III is "in the arsenal of the armed forces" (Ministry of Defence 2014) and the Strategic Forces Command conducted its fifth user trial on November 30, 2019, from Abdul Kalam Island on India's east coast. The Agni-III failed its first night trial – deemed a "very crucial" test – with the missile falling into the sea after the first-stage separation (Rout 2019). No test launches of the Agni-III have been publicly reported since this failed test in 2019.

It is still early in the Agni-III deployment; there are probably fewer than 10 launchers deployed, and the full operational status is uncertain. The longer range potentially allows India to deploy the Agni-III units further back from the Pakistani and Chinese borders. More than a decade ago, while the missile was still under development, an army spokesperson remarked, "With this missile, India can even strike Shanghai" (*India Today* 2008) – although this would require launching the Agni-III from the very northeastern corner of India. From that region, the Agni-III would, for the first time, bring Beijing within range of Indian nuclear weapons.

India is also developing the Agni-IV missile – a two-stage, solid-fuel, road- and rail- mobile intermediate-range ballistic missile with the capability to deliver a single nuclear warhead to a distance of over 3,500 kilometers (2,175 miles), with the Ministry of Defence listing the range as 4,000 kilometers (2,485 miles) (Ministry of Defence 2014). Following the final development test in 2014, the ministry declared that Agni-IV "serial production will begin shortly." Since then, three user launches have been conducted by the Strategic Forces Command, the most recent in December 2018, but the missile is not yet fully operational.

Although the Agni-IV will be capable of striking targets in nearly all of China from northeastern India (including Beijing and Shanghai), India is also developing the longer-range Agni-V – a three-stage, solid-fuel, road-mobile, near-intercontinental ballistic missile (ICBM) capable of delivering a warhead to a distance of more than 5,000 kilometers (3,100 miles). The extra range will allow the Indian military to establish Agni-V bases in central and southern India, further away from the Chinese border. The Agni-V has been successfully flight tested eight times in total, with the most recent test launch conducted in October 2021. The 2021 test was the first user trial for the Agni-V, and additional tests will likely be required before the missile becomes operational (Government of India 2021b; Philip 2021a).

The Agni-V missile brings an important new capability to the Indian strike force. Unlike current Indian land-based ballistic missiles, the Agni-V is carried in a sealed canister on the launcher. The first two test-

launches used a rail launcher, but since 2015, all launches have been conducted from a road-mobile launcher. The launcher, which is known as the Transport-cum-Tilting vehicle-5 (TCT-5), is a 140-ton, 30-meter, 7-axle trailer pulled by a 3-axle Volvo truck (DRDO Newsletter 2014). The canister design "will reduce the reaction time drastically . . . just a few min- utes from 'stop-to-launch,'" the former head of India's Defence Research and Development Organisation said in 2013 (Times of India 2013). Several Agni-V transporter erector launchers (TELs) are clearly visible on commercial satellite imagery of the Defence Research and Development Organisation's (DRDO) integration center north of Hyderabad, as well as at other sites across the country (see Figure 1).

Figure 1— Left: Photograph of an Agni-V TCT-5 transporter-erector launcher (TEL) during a missile test-launch. Image: DRDO. Right: Satellite imagery of Agni-V ICBM TELs at DRDO missile complex near Shampirpet, India. Image: © 2022 Maxar Technologies.

In June and December 2021, India test-launched its new two-stage, solid-fuel, Agni-P medium-range ballistic missile, which the Indian Government calls a "new generation" nuclear-capable ballistic missile (Government of India 2021c). The Agni-P is India's first shorter-range ballistic missile (SRBM) to incorporate more sophisticated rocket motors, propellants, avionics packages, and navigation systems found in India's newer, longer-range missiles like the Agni-IV and Agni-V. Importantly, the Agni-P is also carried in a sealed canister, similarly to the Agni-V (Korda and Kristensen 2021). One senior DRDO official remarked during the early stages of the Agni-P's development that, "As our ballistic missiles grew in range, our technology grew in sophistication. Now the early, short-range missiles, which incorporate older technol- ogies, will be replaced by missiles with more advanced technologies. Call it backward integration of technology" (Shukla 2016). Statements like these, coupled with the Agni-P's clear capability upgrade over the early Agni-I and Agni-II missiles – which utilize older and less robust propellants, airframes, and hydraulic actuators, as well as less accurate guidance systems – suggest that the Agni-P will eventually replace these older missiles once it becomes operational (Shukla 2021b).

India is also developing a conventional SRBM known as the Pralay. The Pralay was most recently tested in December 2021 and is reportedly intended to take over the conventional role currently occupied by the dual-capable Prithvi-II and Agni-I SRBMs (Government of India 2021d; Unnithan 2021). The splitting of these nuclear and conventional short-range missions between the new Agni-P and Pralay missiles, respectively, could help reduce the risk of misunderstanding (conventional-nuclear entanglement) during a conflict. This could be

further bolstered by the fact that the new Agni-P will likely be operated by Strategic Forces Command – which is responsible for India's nuclear arsenal – while the Pralay will be operated by the Indian Army's artillery corps (Philip 2021b).
The June 2021 test of India's Agni-P missile was rumored to have carried two maneuverable decoys to simulate a payload equipped with multiple independently targetable reentry vehicles (MIRVs); however, this was not confirmed by the Indian Ministry of Defence (Pandit 2021). Similarly, press reports surrounding the Agni-V user trial in October 2021 claimed that the missile could be equipped with MIRVs (Rout 2021). However, there is good reason to doubt that India can or will add MIRVs to its missiles soon. There are no official reports that the Indian government has approved a MIRV development program, and loading multiple warheads on the Agni-V would reduce its extra range – a key purpose of developing the missile in the first place.
The Agni-V is estimated to be capable of delivering a payload of 1.5 tons (the same as the Agni-III and Agni-IV), and India's first- and second- generation warheads, even modified versions, are thought to be relatively heavy compared with warheads developed by other nuclear-armed states that deploy MIRVs. However, it took the Soviet Union and the United States hundreds of nuclear tests and 25 years of continued effort to develop re-entry vehicles small enough to equip a ballistic missile with MIRVs. Moreover, deploying missiles with multiple warheads would invite questions about the credibility of India's minimum deterrent doctrine; using MIRVs would reflect a strategy to quickly strike multiple targets and would also run the risk of triggering a warhead race with adversaries. Unless China develops an efficient missile defense system with capability against intermediate-range ballistic missiles, there seems to be no military need for MIRVs on Indian missiles (Kristensen 2013).
It seems likely, though, that China's recent decision to equip some of its ICBMs with MIRVs, and Pakistan's announcement in January 2017 that it had test-launched a new Ababeel medium-range ballistic missile with MIRVs, could strengthen the hand of those in the Indian military-industrial complex who favor development of a MIRV capability, if for no other reason than to avoid falling behind in MIRV technology development.
Although Ministry of Defence officials a few years ago indicated that India's strategic missile force will be "capped for the present with the Agni-V, with no successor or next series on the horizon or even on the drawing board" (Gupta 2018), India apparently has also begun development of a true ICBM, known as Agni-VI. Official data is scarce, but an article posted on the government's Press Information Bureau website in December 2016 claimed the Agni "will have a strike- range of 8,000–10,000 kilometers" (4,970 to 6,210 miles) and will "be capable of being launched from submarines as well as from land" (Ghosh 2016). Whether these claims are accurate remains to be seen for a range improvement of roughly 50 percent to nearly 100 percent of that of the Agni-V seems exaggerated. The US Air Force's National Air and Space Intelligence Center estimates the range to be closer to 6,000 kilometers (3,730 miles) (National Air and Space Intelligence Center 2020).
India has also converted some of its ballistic missile technology into an anti-satellite interceptor. In March 2019, the Defence Research and Development Organisation completed its first successful anti-satellite test "Mission Shakti" against one of its own satellites. According to the Indian Ministry of Defence, the interceptor was a three-stage missile with two solid rocket boosters, derived from its indigenous ballistic missile defense program (Ministry of Defence 2019, 96). The destruction of the satellite created a large debris field of hundreds of pieces, and while most reentered the Earth's atmosphere, dozens were kicked into higher orbit by the impact (Grush 2019). Unidentified Indian military sources have also speculated that the interceptor likely utilizes the same propulsion system as that of the Agni-V ballistic missile, which is still in development (Bedi 2019).

Sea-based ballistic missiles

India operates a ship-launched and a submarine-launched, nuclear-capable ballistic missile and is developing a second submarine-launched ballistic missile for eventual deployment on a small evolving fleet of nuclear-powered ballistic missile submarines.
The ship-based ballistic missile is the Dhanush, a 400-kilometer (249-mile) single-stage, liquid-fuel, short-range ballistic missile designed to launch from the back of two specially configured *Sukanya*-class patrol vessels (*Subhadra* and *Suvarna*); each ship can carry two missiles. The Dhanush is a ship-based variant of the Prithvi-II. The Dhanush has not been test launched since February 2018 and its utility as a strategic deterrence weapon is severely limited by its relatively short range; the ships carrying it would have to sail dangerously close to the Pakistani or Chinese coasts to target facilities in those countries, making them vulnerable to counterattack. The two *Sukanya*-class ships are homeported at the Karwar naval base on the Indian west coast. We suspect the Dhanush will be retired (if it hasn't happened already) once one or two of the Arihant-class nuclear submarines become fully operational.
India's first indigenous nuclear-powered ballistic missile submarine (SSBN), the INS *Arihant*, was commissioned in August 2016, but spent most of 2017 and the first half of 2018 undergoing repairs after its propulsion system was crippled by water damage (Peri and Joseph 2018). In November 2018, Indian Prime Minister Narendra Modi announced that the *Arihant* had completed its first deterrence patrol, officially marking the completion of India's nuclear triad. He additionally stated that the deployment constituted "a fitting response to those who indulge in nuclear blackmail" (Singh 2018). The "deterrence patrol" lasted approximately 20 days; however, it is unclear whether the boat was actually equipped with nuclear weapons. The *Arihant* appears to bear a strong

resemblance to the Russian-built *Kilo*-class attack submarines that are operated by the Indian Navy, with the exception of a unique missile compartment designed to accommodate India's submarine-launched ballistic missiles (Sutton 2021).

Although the INS *Arihant* conducted two submerged unit trials of nuclear-capable K-15 missiles in August 2018, sources indicate that it will primarily serve as a training vessel and technology demonstrator and that it will not be deployed for nuclear deterrence patrols as additional SSBNs come online (Gady 2018). These claims are further bolstered by the fact that the Arihant has rarely been seen, photographed, or written about in recent years, despite it being a significant technological achievement for India's Navy (Sutton 2021).

A second SSBN, the INS *Arighat* (previously intended to be named *Aridhaman*), was launched on November 19, 2017, and was expected to be commissioned into the Indian Navy in 2020 (Pubby 2020); however, the *Arighat* only began sea trials at the beginning of 2022, and as of May 2022 there had been no announcement to confirm the boat's commissioning, indicating that it has likely been delayed (Bhattacharjee 2022). The *Arighat* will be followed by two more SSBNs, temporarily designated S4 and S4 (Bedi 2017), which are scheduled to enter service before 2024 (Pubby 2020); however, it is likely that these boats will be delayed as well. The first of these, the S4, was launched in November 2021, and is noticeably longer and wider than India's first two SSBNs (Biggers 2021). Satellite images indicate the S4 is approximately 18 meters longer than the first two SSBNs and equipped with eight missile tubes, twice the number on the *Arihant* and *Arighat*.

India also appears to be developing its next generation of SSBNs – the S-5 class. A series of tweets by the Indian vice president during his visit to the country's Naval Science & Technology Laboratory revealed some details about what this new class of submarines might look like (Vice President of India 2019). Photos indicate that the new submarines will be significantly larger than the current Arihant-class and could have eight or more launch tubes. Analysts speculate that this new class of submarines could enter service in the late 2020s, after the completion of all four *Arihant*-class boats (Sutton 2019). A naval base for the SSBNs named INS *Varsha* is currently under construction near Rambilli on the Indian east coast, and will reportedly be located near a facility associated with the Bhabha Atomic Research Centre – India's primary nuclear research institution, which is also tied to its nuclear weapons program. The INS *Varsha* base is undergoing extensive construction with numerous tunnels into a mountain, large piers, and support facilities (see Figure 2).

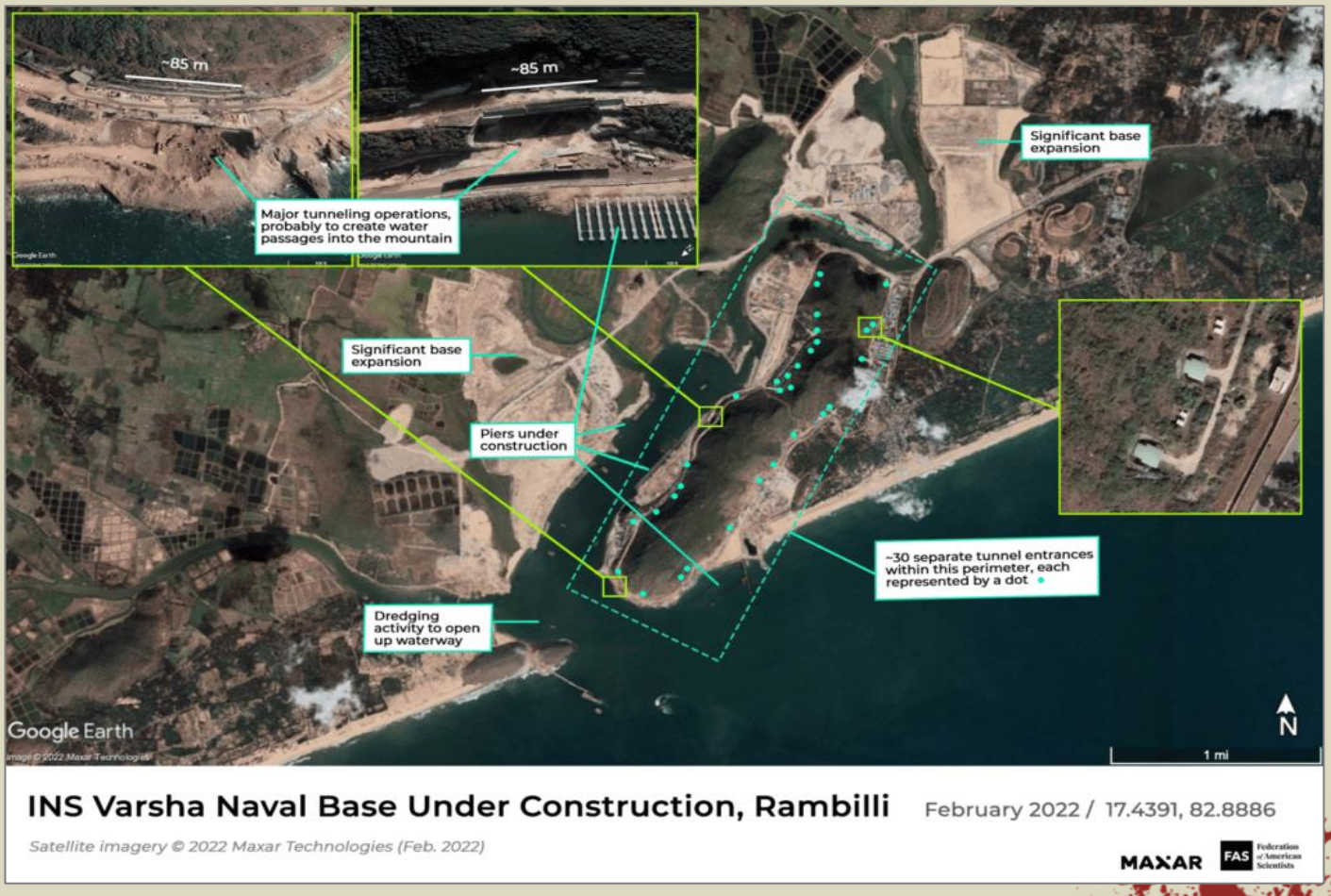


Figure 2 — The INS Varsha naval base under construction near Rambilli, India. Image: © 2022 Maxar Technologies.

To arm the SSBNs, India has developed one nuclear-capable sea-launched ballistic missile, and is working on another: the current K-15 (also known as Sagarika or B-05) submarine-launched ballistic missile (SLBM) with a range of 700 kilometers (435 miles), and the future K-4 SLBM with a range of about 3,500 kilometers (2,175 miles).
The relatively short range of the K-15 would not allow the SSBNs to target Islamabad, only southern Pakistan, and the submarines would not be able to target China at all unless they sail through the Singapore Strait, deep into the South China Sea. Therefore, despite its induction in the summer of 2018, the K-15 should be seen primarily as an intermediate program intended to develop the technology for future more capable missiles.
The K-4, which reportedly has similar characteristics to the Agni-III intermediate-range ballistic missile, has undergone six test launches – two of which took place only five days apart in January 2020 – and is reportedly "virtually ready" for serial production (Pandit 2020).
Launch videos of the K-4 SLBM indicate that rather than the cold launch system typically used by most SLBMs – through which the missile gets ejected from the launch tube via a gas generator – the K-4 uses two small motors on the front end of the missile to pull it several meters above the surface of the water before the main engine ignites (DRDO 2015). Rumors about the K-4 claim that it is highly accurate, reaching "near zero circular error probability," according to the Defence Research and Development Organisation (Panda 2016), and one official reportedly claimed: "Our Circular Error Probability is much more sophisticated than Chinese missiles" (Peri 2020). Such claims, however, should probably be taken with a grain of salt.
With a range of 3,500 kilometers (2,175 miles), the K-4 will be able to target all of Pakistan and most of China from the northern Bay of Bengal. Each SSBN launch tube will be capable of carrying one K-4 or three K-15s. As is usual with nuclear programs, there are rumors and speculation that each K-4 SLBM will be capable of carrying more than one warhead, but that seems highly unlikely.
In addition, senior Indian defense officials have stated that the Defence Research and Development Organisation is reportedly planning to develop a 5,000-kilometer (3,107-mile) range SLBM that matches the design of the land-based Agni-V and would allow Indian submarines to target all of Asia, parts of Africa, Europe, and the Indo-Pacific region, including the South China Sea. The missile will carry the same K- series label as the two other SLBMs currently in development and was initially expected to be tested sometime in 2022 (Gupta 2020), although as of May 2022 no such launch had taken place.

Cruise missiles
India is developing a ground-launched cruise missile – the Nirbhay. The missile looks similar to the American Tomahawk or the Pakistani Babur and might also be intended for air- and sea- based deployment. The Indian Ministry of Defence describes the Nirbhay as "India's first indigenously designed and developed long-range subsonic cruise missile having 1,000-kilo- meter (621-mile) range and capable of carrying up to 300-kilogram warheads" (Ministry of Defence 2019, 100). After a series of failed tests dating back to 2013, successful flight tests in November 2017 and April 2019 indicate that some of the technical challenges have been resolved.
Although there are many rumors that the Nirbhay is dual-capable, neither the Indian government nor the US intelligence community has publicly stated such (Pandit 2017). A test of the Nirbhay cruise missile fitted with an indigenous propulsion system was scheduled for April 2020; however, the test was postponed until August 2021, and resulted in a partial success, as the engine fired correctly but the delivery platform subsequently crashed (Gupta 2021).
The Defence Research and Development Organisation confirmed in early 2020 that additional variants of the Nirbhay cruise missile – including submarine-launched and air-launched versions – are in the early stages of planning and development (Udoshi 2020)

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

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

By Lucia Bisceglia and Pirous Fateh-Moghadam

Source: https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(22)01203-X/fulltext

July 16 – The ongoing conflict in Ukraine confirms how wars and armed conflicts are a serious threat to public health and environmental integrity. The crisis has made clear that nuclear war is closer than ever.

As people working in the biomedical field, we are urged to stress that any reasoning about just causes of war loses any hypothetical meaning when compared with the destructive potential of modern nuclear technology. The very concept of defence is not applicable to nuclear weapons, which, by their very nature, clearly violate all of the principles enshrined in international humanitarian law and the protocols of the Geneva Conventions.

Nuclear weapons cause immediate damage by death and injury that far exceeds the capacity for health care even in well organised settings. Global health-care infrastructure is not, and cannot, be prepared for the humanitarian catastrophe that would result from the use of these weapons.

The long-term damage to the health of the population and the environment could easily be beyond the resilience, not only of individual countries or territories, but of the entire world. As long as these weapons of mass destruction exist, humanity's survival is under threat.

The Treaty on the Prohibition of Nuclear Weapons entered into force on Jan 22, 2021, and the first meeting of state parties took place in June, 2022. In an open letter to the Italian Government, the Italian Association of Epidemiology urged the Italian government to attend the meeting, with the ultimate goal of signing and ratifying the treaty as soon as possible.[1]

As the Italian historian of medicine, Giorgio Cosmacini, opportunely pointed out in reference to the two world wars: "The fact that no one—or very few—among the protagonists of medicine...has posed the problem of the prevention of one of the deadliest pandemics in the history of human societies should make us reflect on the actual coherence of a medical science that, while professing to be at the service of life, refuses to take sides and declares itself neutral...If ideology and politics in power bring with them, or do not effectively contrast, a social and biological calamity such as war, medicine...must exercise a brave critique of the calamitous ideological and political context...Physicians must explore a new province of preventive medicine: the prevention of war."[2]

Joint action of the international public health community is needed to prevent future historians from having to make similar reflections on the time period that lies ahead of us.

Lucia Bisceglia is on the board of the Italian Association of Epidemiology (AIE).
Pirous Fateh-Moghadam is a member of the AIE Peace Working Group.

Khamenei adviser says Tehran 'capable of building nuclear bomb,' Al Jazeera reports

Source: https://www.reuters.com/world/middle-east/khamenei-adviser-says-tehran-capable-building-nuclear-bomb-al-jazeera-2022-07-17/

July 17 – Iran is technically capable of making a nuclear bomb but has not decided whether to build one, a senior adviser to Iranian Supreme Leader Ayatollah Ali Khamenei told Qatar's al Jazeera TV on Sunday. Kamal Kharrazi spoke a day after U.S. President Joe Biden ended his four-day trip to Israel and Saudi Arabia, vowing to stop Iran from "acquiring a nuclear weapon." read more

Kharrazi's comments were a rare suggestion that Iran might have an interest in nuclear weapons, which it has long denied seeking.

"In a few days we were able to enrich uranium up to 60% and we can easily produce 90% enriched uranium ... Iran has the technical means to produce a nuclear bomb but there has been no decision by Iran to build one," Kharrazi said.

Iran is already enriching to up to 60%, far above a cap of 3.67% under Tehran's 2015 nuclear deal with world powers. Uranium enriched to 90% is suitable for a nuclear bomb. In 2018, former U.S. President Donald Trump ditched the nuclear pact, under which Iran curbed its uranium enrichment work, a potential pathway to nuclear weapons, in exchange for relief from economic sanctions.

In reaction to Washington's withdrawal and its reimposition of harsh sanctions, Tehran started violating the pact's nuclear restrictions.
Last year, Iran's intelligence minister said Western pressure could push Tehran to seek nuclear weapons, the development of which Khamenei banned in a fatwa, or religious decree, in the early 2000s.
Iran says it is refining uranium only for civilian energy uses, and has said its breaches of the international deal are reversible if the United States lifts sanctions and rejoins the agreement.
The broad outline of a revived deal was essentially agreed in March after 11 months of indirect talks between Tehran and Biden's administration in Vienna.
But talks then broke down over obstacles including Tehran's demand that Washington should give guarantees that no U.S. president will abandon the deal, the same way Trump did.
Biden cannot promise this because the nuclear deal is a non-binding political understanding, not a legally-binding treaty.
"The United States has not provided guarantees on preserving the nuclear deal and this ruins the possibility of any agreement," Kharrazi said.
Israel, which Iran does not recognise, has threatened to attack Iranian nuclear sites if diplomacy fails to contain Tehran's nuclear ambitions.
Kharrazi said Iran would never negotiate its balistic missile programme and regional policy, as demanded by the West and its allies in the Middle East. read more
"Any targeting of our security from neighbouring countries will be met with direct response to these countries and Israel."

EDITOR'S COMMENT: Just an expected surprise!

This is an official New York City video about how to survive a nuclear attack.
Please do not freak out.

Nuclear Egypt

El Dabaa Nuclear Power Plant is the first nuclear power plant planned for Egypt and will be located at El Dabaa, Matrouh Governorate, Egypt, which is about 130 Kilometers northwest of Cairo. The plant (by ROSOATOM Group), will have four VVER-1200 reactors, making Egypt the only country in the region to have a Generation III+ reactor.


ICI International
CBRNE INSTITUTE
CBRNE-Terrorism Newsletter
W M O D
C2BRNE DIARY
EXPLOSIVE NEWS

3D X-Ray Makes it Easier to Detect Hidden Explosive Weapons

Source: https://www.homelandsecuritynewswire.com/dr20220624-3d-xray-makes-it-easier-to-detect-hidden-explosive-weapons

June 24 – As summer officially kicks off, many people are preparing to travel for vacations, to visit loved ones, or for business. To make these trips seamless and safer, the Science and Technology Directorate (S&T) says it is developing, implementing, and ensuring the effectiveness of cutting-edge screening equipment and protocols that help protect the public and keep security lines moving. Soon, new S&T-funded screening technologies will be available that will do this and more, while also supporting first responders and the dedicated Department of Homeland Security (DHS) staff tasked with ensuring each step of your trip is smooth sailing (or flying … or driving).

As travelers pass through border crossings, ports of call, airport checkpoints, and various precautionary measures in both federal and private venues, their safety and wellbeing are constantly ensured through various forms of screening technologies that have one critical goal: to identify and alert the proper authorities to potential threats. And, while these technologies do their jobs very effectively, it is important to ask the question: "How can we continue to make these technologies better?"

Xoran demonstrates how a robot can be used to transport the 3D X-ray to a package of interest in the field.

To answer this question, S&T has teamed up with Xoran Technologies, LLC, to develop a one-of-a-kind, compact, 3D X-ray scanner.

"DHS staff and first responders in the field need imaging capabilities that will enable them to safely, effectively, and efficiently scan and detect hidden explosive devices, such as bombs or improvised explosive devices (IED), that can be easily concealed in a small container or bag," said S&T Program Manager Karen "Maua" Johnson. "The 3D X-ray could potentially help us meet this critical security need by greatly enhancing the ability of our frontline operators to find and intercept these dangerous devices before they can be used to harm the general public."

The 3D X-ray is a user-friendly, portable, durable, prototype imaging tool that uses a combination of both 2D and 3D computed tomography (CT) imaging capabilities to quickly and accurately detect the presence of explosive devices and related components in backpack-sized containers or bags—without needing to open them.

"The 3D X-ray stands out from other existing screening technologies because of how multi-functional and adaptable it is out in the field," said Xoran President David Sarment. "It is designed to quickly perform any type of X-ray scan—no matter what a first responder might be looking for, what environment they're working in, and what level of detail they might need."

Built to be the size of a roller bag when disassembled, and weighing in at 70 pounds, the 3D X-ray scanner can be used by one or two first responders and taken anywhere it may be needed in the field. The 3D X-ray can either be carried to a small container or bag of interest via a remote-controlled robotic truck or be manually wheeled there by a responder. Once on site, it can be assembled; placed on an accompanying tripod and gantry; positioned for use; powered up; and synced with a laptop for wireless operation—all within five minutes.

"The 3D X-ray scanner has a number of unique capabilities," explained Sarment. "If a responder feels that only a simple scan of a container or bag is necessary, they can utilize the 3D X-ray's traditional 2D X-ray function to quickly take basic images of it. However, if they decide that they need more detailed imaging, they can utilize the gantry to rotate the 3D X-ray as needed and shoot more complex images—such as series (or sets) of 2D X-rays, partial 3D reconstructions, and complete 3D CT scans."

The 3D X-ray's ability to take CT scans is its most cutting-edge feature. When the 3D X-ray is used in CT mode, it operates very similarly to a medical CT scanner and takes hundreds of X-rays (up to 600) at different angles while the gantry rotates it a full 360 degrees around a container or bag of interest. The software associated with the 3D X-ray then processes this data and quickly compiles a detailed rendering of the contents inside the container or bag, providing vital information revealing whether a bomb or IED, along with any associated components and parts, may be concealed in its contents.

Preliminary testing data from Xoran's lab indicates that the 3D X-ray has the potential to be a promising screening tool at a wide variety of security checkpoints. However, before it is implemented in the field and commercialized, Xoran's team is working to finalize two prototypes of the scanner and deliver them to S&T at the end of September. S&T will then place these prototypes with two law enforcement groups for further pilot testing in the field. Feedback from this testing will be used to improve the 3D X-ray and prepare it for the marketplace.

Johnson noted that in addition to being useful to DHS frontline staff and first responders, the 3D X-ray could also be utilized in other fields and venues.

"Should this technology be commercialized, it has the potential to be effective in many other settings, such as courthouses, sporting arenas, correctional facilities, government buildings, and any other highly-trafficked areas where the security and safety of the public are of the utmost priority."

Ukraine's Bomb Squads Have a New Top Dog

Move over, mine-sniffing pups. Robots are taking your job.

By Jack Detsch, *Foreign Policy*'s Pentagon and national security reporter. FP subscribers can now receive alerts when new stories written by this author are published. Subscribe now | Sign in

The robot Spot during a demonstration in Versailles, France, on June 10, 2021. BERTRAND GUAY/AFP VIA GETTY IMAGES

Iran Missile Milestones: 1985-2022

June 29, 2022

Source: https://www.iranwatch.org/our-publications/weapon-program-background-report/iran-missile-milestones-1985-2022

1985: Then-speaker of the Iranian Majlis Ali Akbar Hashemi Rafsanjani leads a high-level delegation to Libya, Syria, North Korea, and China, reportedly to acquire missiles.

1985: Iran receives its first Scud-Bs from Libya.

1987: China sells Iran "Silkworm" anti-ship cruise missiles.

1987: Iran reportedly receives approximately 100 Scud-B missiles from North Korea. Iran had allegedly agreed to finance North Korea's longer-range missile program in exchange for missile technology and the option to buy the finished missiles.
1988: China agrees to provide Iran with equipment and know-how to develop and test medium-range ballistic missiles.
1988: Iran successfully tests the 160 km range Mushak-160 missile.
1990: China and Iran reportedly sign a 10-year agreement for scientific cooperation and the transfer of military technology.
1991: Iran test-fires a ballistic missile identified by U.S. intelligence as a North Korean Scud-C.
1991: Syrian chief of staff General Hikmat Shihabi reportedly visits Tehran to discuss building a factory in Syria for joint development and production of surface-to-surface missiles.
1992: The U.S. Department of State sanctions Iran's Ministry of Defense Armed Forces Logistics (MODAFL) for engaging in "missile technology proliferation activities" with North Korea.
1995: Iran receives four Scud Transporter Erector Launchers (TELs) from North Korea.
1996: The State Department sanctions North Korea's Changgwang Sinyong Corporation and Iran's Ministry of Defense Armed Forces Logistics (MODAFL) and State Purchasing Office for "missile technology proliferation activities."
1996: Iran test-fires a Chinese-built C-802 surface-to-surface cruise missile.
1996: U.S. Rep. Benjamin Gilman (R-NY) states during a Congressional hearing that U.S. intelligence believes China has "delivered dozens, perhaps hundreds, of missile guidance systems and computerized tools to Iran."
1996: The *Washington Times* reports that, according to a Central Intelligence Agency (CIA) report entitled "Arms Transfers to State Sponsors of Terrorism," China has supplied Iran with missile technology, including gyroscopes and accelerometers, as well as test equipment and components for an advanced radar system.
November 1996: Iran reportedly fires, for the first time, a Chinese C-802 anti-ship missile from one of its ten Chinese-built "Houdong" patrol boats.
June 1997: Iran reportedly tests two Chinese-built C-801K air-launched cruise missiles from a vintage F-4 Phantom, marking the country's first successful test of an air-launched cruise missile.
September 1997: The Russian INOR Scientific Center reportedly agrees to supply Iran's Instrumentation Factories Plan with a high-strength steel alloy and three types of alloy foil used to shield missile guidance equipment.
December 1997: U.S. satellite reconnaissance reportedly picks up the heat signature of a missile engine test at the Shahid Hemat Industrial Group (SHIG) research facility, south of Tehran.
January 1998: According to the National Council of Resistance of Iran (NCRI), an Iranian opposition group, Iran completes development of the Shahab-3 medium-range missile and readies it for production.
July 1998: Iran tests the Shahab-3 missile. According to Iranian sources, the 16-meter long missile can carry a 1,000 kg payload 1,300 km. The missile is believed to be a single-stage, liquid-fueled, scaled-up version of North Korea's Nodong missile.
July 1998: The State Department imposes sanctions on seven Russian entities for engaging in "proliferation activities related to Iran's missile programs." Designated entities include Baltic State Technical University, Europalace 2000, Glavkosmos, Grafit, INOR Scientific Center, MOSO Company, and Polyus Scientific Production Association.
September 1998: Iran publicly displays the Shahab-3 missile at a military parade. Also on display are five air-to-air missiles, Chinese C-801 and C-802 anti-ship missiles, and three Iranian-built, solid propellant surface-to-surface missiles, including the Zelzal-2, the Nazeat, and the Shahin.
January 1999: The State Department imposes sanctions on Russia's D. Mendeleyev University of Chemical Technology of Russia, Moscow Aviation Institute (MAI), and The Scientific Research and Design Institute of Power Technology for engaging in "proliferation activities related to Iran's nuclear and/or missile programs."
February 1999: Iran's defense minister Ali Shamkhani announces that the Shahab-4 missile is in production not for military purposes, but for launching a satellite. U.S. intelligence reportedly believes the missile is derived from the 1950s-era Soviet SS-4 "Sandal" medium-range missile, which had a maximum range of 2,000 km.
April 1999: Iran announces the successful test fire of the Sayyad-1, an advanced anti-aircraft missile designed and manufactured by the Aerospace Industries Organization (AIO).
October 1999: Iran reportedly sells Scud-B and Scud-C missiles to the Democratic Republic of the Congo (formerly Zaire). Iranian military officers and technicians are on hand to help assemble the missiles.
November 1999: U.S. intelligence reportedly believes that North Korea sold Iran 12 Nodong missile engines.
January 2000: Iran commissions three production lines at the Education and Research Institute of the Ministry of Defense. They will allegedly help Iran become self-sufficient in the production of HTPB resin, aluminum powder, and potassium chlorite—all of which are useful in the production of solid rocket propellant.
February 2000: Iran reportedly tests a Shahab-3 missile equipped with a North Korean engine. The missile was launched from a transporter erector launcher (TEL) at an IRGC airbase. Iranian sources say

the missile has an inertial navigation guidance system and a circular error probable (CEP) of approximately three kilometers.
March 2000: Israeli and U.S. officials reportedly agree that Iran can deploy the Shahab-3 missile.
March 2000: The Iran Nonproliferation Act of 2000 (P.L. 106-178) is signed into law, authorizing sanctions against persons transferring to Iran materials and technology capable of contributing to Iran's cruise and ballistic missile programs.
April 2000: The State Department imposes sanctions on Changgwang Sinyong, a North Korean company, and Iran's Ministry of Defense Armed Forces Logistics (MODAFL), Aerospace Industries Organization (AIO), Shahid Hemat Industrial Group (SHIG), and SANAM Industrial Group for missile technology proliferation activities.
July 2000: Iran successfully tests the Shahab-3 missile, according to Iranian state media.
August 2000: In its report on worldwide proliferation, the CIA says Iran has made considerable progress in the development of ballistic missiles, and that entities in Russia, North Korea, and China continued to supply the largest amount of ballistic missile-related goods, technology, and expertise to Iran.
September 2000: Iran tests the Shahab-3 missile, but the missile reportedly explodes shortly after launch.
May 2002: Iran tests the Shahab-3 missile. According to Iranian authorities, the test is successful.
July 2002: Iran tests the Shahab-3 missile. The test is reportedly unsuccessful.
September 2002: Iran claims to have successfully flight tested the Fateh-110, a single-stage, solid-fueled missile, with at least a 200 km range. Iran's state media reports the inauguration of a facility to produce the Fateh-110.
May 2003: The State Department imposes sanctions on two Moldovan companies, Cuanta S.A. and, Computer and Communicatti SRL, on a Moldovan national, Mikhail Pavlovich Vladov, and on Iran's Shahid Hemat Industrial Group (SHIG) for contributing to missile programs in Iran.
July 2003: On July 20, a ceremony is held to mark the distribution of the Shahab-3 to the (IRGC). The ceremony follows by several weeks what an Iranian foreign ministry spokesman calls the "final test" of the Shahab-3 missile.
November 2003: Iran's defense ministry announces that Iran does not have any program "to build the Shahab-4 missile."
November 2003: In its report to Congress on worldwide proliferation, the CIA says that Iran's ballistic missile inventory is among the largest in the Middle East and that entities in the former Soviet Union, North Korea, and China have helped Iran progress in ballistic missile production.
January 2004: Iran begins production of the Raad cruise missile and the DM-3b active-radar sensor for the Noor anti-ship missile.
May 2004: Iran says it has begun manufacturing a cruise missile called the Kowsar (Kosar), an indigenous stealth anti-ship missile made by the Aerospace Industries Organization (AIO). The missile is said to have three variants: shore-launched, air-launched, and ship-launched.
August 2004: Iran announces the successful test of an upgraded Shahab-3 medium-range ballistic missile, which reportedly is longer than the original version, with a larger fuel tank, a "baby bottle-shaped" reentry vehicle, and an increased range.
September 2004: Iran displays a number of missiles during the Sacred Defense Week military parade, including the Zelzal, Nazeat, Shahab-2, and Shahab-3. Reportedly, two Shahab-3 variants, featuring a triconic warhead, and assessed to have improved ranges of 1,500 km and 2,000 km, respectively, are displayed.
October 2004: Iran claims that it has successfully tested a more accurate version of the Shahab-3 missile.
December 2004: According to NCRI, Iran's Aerospace Industries Organization (AIO) is developing several clandestine missiles, including the Ghadr, the Shahab-4, and the Zelzal 2, and is working on nuclear and chemical warheads.
2005: North Korea allegedly supplies Iran with 18 missile assembly kits for the BM-25 (or Musudan), a modified version of Russia's SS-N-6. The SS-N-6 is a single-stage, liquid-fueled, submarine missile with a range of 2,400 to 3,000 km.
June 2005: President George W. Bush issues Executive Order 13382 on Blocking Property of Weapons of Mass Destruction (WMD) Proliferators and Their Supporters. The order freezes the assets of specially designated proliferators of WMD and WMD delivery systems, as well as members of their support networks; four Iranian entities are designated under this Order, including Aerospace Industries Organization (AIO), Shahid Hemat Industrial Group (SHIG), Shahid Bakeri Industrial Group, and the Atomic Energy Organization of Iran (AEOI).
December 2005: According to NCRI, Iran is using underground facilities to hide missile command and control centers and to build nuclear-capable missiles.
March-April 2006: Iran holds "Holy Prophet" war games in the Persian Gulf involving the IRGC Naval Force and Iran's regular naval and armed forces. According to Iran, missiles tested include the Shahab-2, the Kowsar, the sonar-evading Hoot (Hud, Hut) underwater missile, the surface-to-air Fajr-3, and an upgraded Nour cruise missile. Reportedly, the Nour (Noor) may be a variant of the Chinese C-802, the Kowsar a variant of the Chinese C-801, and the Hoot based on the Russian-developed Shkval rocket-powered torpedo.
June 2006: Pursuant to Executive Order 13382, the U.S. Department of the Treasury imposes financial sanctions on four Chinese companies, Beijing Alite Technologies Company Ltd. (ALCO), LIMMT Economic and Trade Company, Ltd., China Great Wall Industry Corporation (CGWIC), and China

National Precision Machinery Import/Export Corporation (CPMIEC), and on the U.S.-based CGWIC representative, G.W. Aerospace, Inc., for supplying Iran with missile-related and dual-use components.

July 2006: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on SANAM Industrial Group and Ya Mahdi Industries Group for their ties to missile proliferation; both are Iranian companies subordinate to Iran's Aerospace Industries Organization (AIO).

August-September 2006: During "Blow of Zolfaqar" war games, Iran claims to have successfully tested a radar-evading, ship-launched missile called the Sagheb, and a new surface-to-surface missile called the Saeqeh. U.S. military intelligence reportedly determines that the video of the Sagheb test released by the Iranian government is actually of an earlier Chinese missile test.

November 2006: Iran tests several missiles during the IRGC-led "Great Prophet 2" military maneuvers, including the Shahab-2, Shahab-3, Fateh-110, Zelzal, and Scud-B. Iran claims the Shahab-3 was tested with cluster warheads and achieved a range of approximately 1,900 km. Anti-ship missiles, including the Noor, Kosar, and Nasr, are also reportedly tested.

December 2006: The U.N. Security Council adopts resolution 1737, imposing sanctions to prevent the transfer to Iran of materials, as well as technical or financial assistance, which might contribute to Iranian nuclear and ballistic missile development. The resolution designates eight Iranian entities involved in missile activities, for which financial resources must be frozen.

January 2007: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on Bank Sepah, a state-owned Iranian financial institution. Bank Sepah is described by Treasury as "the financial linchpin of Iran's missile procurement network."

February 2007: Iran tests the Tor-M1 short-range air defense system provided by Russia. The Tor-M1 system has a reported range of 12 km, which may be increased to 20 km. Iran's IRGC Air Force Commander claims that the system is capable of tracking 48 targets and engaging eight targets using electro-optic and infrared systems.

February 2007: Iran claims to have tested a suborbital research rocket as part of the country's space program, which may include an effort to develop an independent satellite launch capability. U.S. missile launch sensors reportedly detect no such test.

March 2007: The U.N. Security Council adopts resolution 1747, imposing further sanctions to prevent the transfer of arms and provision of financial assistance to Iran, and designating additional Iranian entities involved in ballistic missile activities, for which financial resources must be frozen.

June 2007: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on two Iranian companies involved in missile work for Iran's Aerospace Industries Organization (AIO), which directs Iran's missile program. Fajr Industries Group is an AIO subordinate involved in the production of missile guidance systems and Mizan Machine Manufacturing Group is an AIO front company involved in procurement.

September 2007: Iran displays the Ghadr-1 (Qadr-1) missile during a military parade, claiming it to be an upgraded version of the medium-range Shahab-3 with a range of 1,800 km. Experts say the Ghadr-1 appears identical to a Shahab-3 variant displayed in 2004. The Ghadr-1, along with other missiles displayed during the military parade, including the Shahab-3, the Fateh-110, and Zelzal-3, are in possession of the IRGC Air Force.

November 2007: Iran says it has built a new missile, the "Ashura" (or Ashoura), with a range of 2,000 km. Descriptions of the Ashura vary from a multi-stage, solid-propellant missile to a missile that uses non-Scud technology. It is reportedly depicted in a U.S. Missile Defense Agency (MDA) report as a stretched version of the liquid-propelled Shahab-3, fitted with larger tail fins, and in an April 2008 Israeli report as a two-stage solid-propellant missile with a triconic nose shape.

February 2008: Iran claims to have successfully launched its Kavoshgar-1 rocket into space. Iran claims that the Kavoshgar is a two-stage rocket, that it reached an altitude of 200 km, and that it successfully made contact with the ground station. Private analysts believe that the Kavoshgar is a single-stage, liquid-fueled missile and that the space center, located 230 km southeast of Tehran, has the potential to be used in developing long-range missiles. Iran also inaugurates a space center with a satellite control and tracking station and displays its "Omid" satellite.

March 2008: The U.N. Security Council adopts resolution 1803, extending travel restrictions and asset freezes to—and in some cases instituting a travel ban on—additional Iranian entities, and barring Iran from buying almost all nuclear and missile-related technology.

July 2008: Iran claims to have successfully test-fired a Shahab-3 missile with a range of 2,000 km, as well as Zelzal and Fateh surface-to-surface missiles, during "Great Prophet III" war games run by the IRGC in the Persian Gulf.

August 2008: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on two Iranian firms, the Safety Equipment Procurement Company (SEP Co.) and Joza Industrial Company for their links to procurement for Iran's missile program.

August 2008: Iran launches the "Safir," a two-stage, liquid fueled rocket based on the Shahab-3 missile, according to analysts. The rocket is about 22 meters long, with a diameter of 1.25 meters, and weighing over 26 tons. According to Iran, the rocket is intended as a satellite launch vehicle. Contrary to initial reports, however, the launch does not place a satellite into orbit.

September 2008: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on the Islamic Republic of Iran Shipping Lines (IRISL) and 18 of its subsidiaries for facilitating shipments of military cargo for Iran's Ministry of Defense Armed Forces Logistics (MODAFL) and its subordinate entities. MODAFL has brokered transactions involving ballistic missile-related materials and technologies.
September 2008: Pursuant to Executive Order 13382, the Treasury Department sanctions six Iranian military firms. Three of these firms, Iran Electronics Industries, Shiraz Electronics Industries, and Iran Communications Industries, make communications equipment for Iran's military. Iran Aircraft Manufacturing Industrial Company (HESA) develops and produces unmanned aerial vehicles and other military aircraft, and its subsidiary, Farasakht Industries, makes aerospace tools and equipment. These entities are owned or controlled by Iran's Ministry of Defense Armed Forces Logistics (MODAFL).
November 2008: Iran claims to have successfully tested the Sejil (Sejjil, Sijjil), a two-stage, solid fuel, surface-to-surface missile with a range of nearly 2,000 km. According to private analysts, the missile appears to be larger than Iran's Shahab-3, with a total length of about 22 meters, and shares some design features with Soviet-era ballistic missiles.
December 2008: Western intelligence sources reportedly state that in 2008 Iran more than tripled the number of operational Shahab-3 missiles, with over 100 missiles now delivered to the IRGC.
February 2009: Iran successfully launches the "Omid" telecommunications and research satellite into orbit, from Semnan province, using its own rocket, the Safir 2. The rocket is 22 meters long, weighs 26 tons and has a diameter of 1.25 meters, according to the head of Iran's Space Agency. It is a two-stage rocket that lofted the 27 kg Omid into low earth orbit at an altitude of 250 km.
April - May 2009: Iranian officials are reportedly present when North Korea launches a long-range rocket (Unha-2) in April and detonates a nuclear device in May.
May 2009: Iran successfully test fires the Sejil-2 (Sejjil-2, Sijjil-2) missile from Semnan province. Iranian authorities claim that this version of the missile has improved sensors and that production of the missile has begun.
June 2009: Iran launches mass production of a ground-to-air missile defense system, called Shahin, reportedly capable of tracing and targeting aircraft within a range of about 40 km.
September 2009: The IRGC holds "Grand Prophet" war games. The Shahab-3, Sejil, Shahab-1 and 2, Fateh, Tondar, Zelzal, and various short-range missiles are test fired. An Iranian news organization reports that the Sejil's (Sejjil, Sijjil) operational range is 2,000 to 2,500 km.
December 2009: Iran successfully test-fires an upgraded version of the Sejil-2 (Sejill-2, Sijjil-2) missile. Defense Minister Ahmad Vahidi says that the new version has a shorter launch time and greater maneuverability.
February 2010: The International Atomic Energy Agency (IAEA) reports that Iran may have conducted work related to the design of a nuclear warhead for a ballistic missile, including missile re-entry body engineering and "engineering design and computer modeling studies aimed at producing a new design for the payload chamber of a missile."
February 2010: Iran launches the Kavoshgar-3 rocket into space carrying living creatures. Iran also unveils a new space launch vehicle, the Simorgh-3, and three new satellites. According to Iran's Space Agency, the Simorgh-3 can place a 100 kg satellite into a 500 km orbit. The launch vehicle reportedly uses a configuration similar to that of North Korea's Taepodong-2 ballistic missile.
March 2010: Iran reportedly begins the indigenous production of the Chinese-designed Nasr-1 anti-ship missile. The Nasr-1, which can carry a 130 kg warhead to a range of 38 km, is based on the Chinese C-704 missile.
March 2010: An analysis of satellite imagery by *Jane's Defence Weekly* reveals significant expansion of the launch facility at Iran's Semnan space center. The expansion includes the construction of two new launch and engine test pads as well as a number of support buildings.
April 2010: Iran displays several missiles during a military parade, including the Shahab-3, the Ghadr-1 (Qadr-1), and the Sejil (Sejjil, Sijjil). The Shahab-3 is a liquid-fueled missile with a range of up to 2,000 km that is capable of carrying a 760–1,000 kg warhead. The Ghadr-1 is reported to be an optimized version of the Shahab-3. The Sejil is a solid-fuel, two-stage missile. These missiles were developed by Iran's Aerospace Industries Organization (AIO).
April 2010: The Mersad air defense system becomes operational, according to Iran's Ministry of Defense. This system is reportedly equipped with advanced radar signal processing technology and electronic equipment for guidance and target acquisition. The system uses Shahin missiles, which are reportedly an upgraded version of the U.S.-made HAWK missile supplied to Iran in the 1970s.
June 2010: The U.N. Security Council adopts resolution 1929, barring Iran from procuring missiles, missile systems, and related spare parts as defined by the U.N. Register of Conventional Arms, and barring countries from providing Iran with training, servicing, or other maintenance related to such missiles. The resolution also "decides" that Iran should not undertake any activity related to nuclear-capable ballistic missiles, including launches, and designates additional Iranian entities involved in ballistic missile activities, for which financial resources must be frozen.

June 2010: Pursuant to Executive Order 13382 and U.N. Security Council resolution 1929, the Treasury Department sanctions the IRGC Air Force and the IRGC Missile Command for their ties to Iran's ballistic missile programs.
August 2010: Iranian Defense Minister Brigadier General Ahmad Vahidi announces the successful test launch of the liquid-fueled Qiam-1 (Qaem-1) missile. Vahidi also announces the test of an upgraded Fateh-110 missile, which he claims is more accurate and can travel farther than earlier versions of this missile.
September 2010: An upgraded variant of the solid-fueled Fateh-110 missile is allegedly delivered to the IRGC Air Force.
September 2010: The government of Singapore interdicts a shipment of 18 tons of aluminum powder bound for Takin Tejarat Omid Iranian in Iran. The aluminum powder could be used to make solid propellant for missiles and is among the materials that Iran is barred from importing. The quantity of aluminum powder would yield approximately 100 tons of rocket propellant suitable for use in Iran's Fateh or Zelzal missiles.
September 2010: Pursuant to Executive Order 13382, the Treasury Department sanctions the German bank Europaeisch-Iranische Handelsbank. Among other activities, the bank, along with the Export Development Bank of Iran, "enabled Iran's missile programs to purchase more than $3 million of material."
September 2010: Russian President Dmitry Medvedev bans delivery of S-300 air defense systems to Iran. The S-300 is capable of destroying aircraft at a ranges of 150 km and at altitudes of up to 27 km.
October 2010: A missile with a nosecone similar to that of Iran's Shahab-3 is displayed in a military parade in North Korea, leading some analysts to cite it as evidence of Iran-North Korea technical cooperation on missile development.
October 2010: Iran conducts an unannounced test of its Sejil/Ashura missile, according to a U.N. Panel of Experts Report.
January 2011: Pursuant to Executive Order 13382, the Treasury Department announces sanctions against Shahid Ahmad Kazemi Industries Group and M. Babaie Industries. Both companies are linked to Iran's Aerospace Industries Organization (AIO) and have been used to solicit foreign technologies for Iran's ballistic missile program.
January 2011: Iran inaugurates ten new laboratories for testing space structures and complete rocket systems. These facilities reportedly feature testing rigs for rocket sections, a thermal test rig for heat shields, and fixtures for aeroelasticity testing of complete multistage rockets, all of which are controlled items under the Missile Technology Control Regime.
February 2011: Iran tests a supersonic, anti-ship ballistic missile, called the Khalij Fars, which Iran claims can carry a 650 kg warhead to a range of 300 km. According to *Jane's Missiles and Rockets*, it is a new variant of the existing Fateh A-110 and uses a similar launcher.
February 2011: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on eleven entities in an illicit procurement network supporting Iran's Aerospace Industries Organization (AIO). Led by Milad Jafari, the network used companies in Iran and Turkey to procure metal parts, including steel and aluminum alloys, for Iran's missile program.
February 2011: Iran conducts an unannounced test of several missiles, including the Khalij-Fars (variant of Fateh-110), Shahab-3, and Sejil, according to a U.N. Panel of Experts Report.
March 2011: Iran launches a Kavoshgar-4 rocket into space carrying a test capsule designed to hold a monkey.
May 2011: Iran begins mass production of the Qiam-1 (Qaem-1) ballistic missile and delivery of the missile system to the IRGC.
May 2011: According to a U.N. Panel of Experts report, Iran and North Korea are suspected of exchanging ballistic missile technology, using regularly scheduled Air Koryo and Iran Air flights, in violation of sanctions on both countries.
June 2011: Iran launches the Rasad satellite into space. The 15.3 kg satellite is launched on the Safir, a two-stage rocket, which weighs 26 tons, measures 22 meters in length, and is 1.25 meters wide, according to Iranian officials. The satellite is designed to be placed in a 260 km orbit.
June 2011: The IRGC fires 14 missiles as part of their "Great Prophet 6" exercises. The missiles include one Shahab-3 missile, two Shahab-1 missiles, two Shahab-2 missiles, and nine Zelzal missiles.
June 2011: An Iranian state television broadcast reveals underground missile silos that Iran claims would make its missiles less vulnerable to attack and allow for the launch of larger missiles.
August 2011: Iran inaugurates a carbon fiber production line at Iran's Aerospace Industries Organization (AIO). Carbon fiber composites have applications in missiles, specifically in items such as rocket motor exit cones and nozzles, reentry vehicle nosetips, heat shields, and leading edges of control surfaces.
September 2011: Iran's Defense Ministry reportedly delivers the Qader anti-ship cruise missile to Iran's Navy and to the IRGC's Naval Force. According to Iran's defense minister, the Qader has a range of 200 km.
November 2011: The International Atomic Energy Agency (IAEA) reports that under Project 111, Iran allegedly studied how to integrate a new spherical payload onto the Shahab-3 missile, including a high explosive and detonation package suitable for use in an implosion device.
December 2011 - January 2012: Iran test-fires the Qader, Nasr, and Mehrab missiles during the "Velayat-90" naval exercise in the Persian Gulf and the Sea of Oman, according to Iran's Ministry of Defense. The Qader is an anti-ship cruise missile with a range of 200 km and is described as an upgrade

of Iran's Noor missile. The Nasr is a short-range anti-ship missile, which was tested for the first time during the exercise. The Mehrab is a naval surface-to-air missile with anti-radar and anti-jamming capabilities, according to Iranian Naval officials.

February 2012: Iran successfully launches the Navid-e Elm-o Sanat (Navid) satellite into orbit using the Safir launch-vehicle, according to Iran's Ministry of Defense. The satellite weighs roughly 50 kg and is set to orbit at an altitude between 250 km and 375 km. According to Iranian defense officials, the Navid was developed in coordination with Iran's Aerospace Industries Organization (AIO) and the Sharif University of Technology.

February 2012: Iran inaugurates a production line for the Zafar naval cruise missile, which is a short-range, anti-ship, radar-guided missile, according to Iran's defense minister. A first shipment of missiles is delivered to the IRGC. The Zafar appears to be a modified version of the Chinese C-701AR missile, according to analysts.

March 2012: David Levick, a 50 year old Australian national, and his company ICM Components Inc., are indicted by a U.S. federal grand jury in the District of Columbia for illegally exporting to Iran equipment that could be used in missiles, drones, and torpedoes, according to the U.S. Department of Justice. Equipment reportedly included VG-34 Series Miniature Vertical Gyroscopes used to control the pitch and roll of missiles and torpedoes.

April 2012: According to a U.S. Department of Defense report, Iran may be technically capable of testing an intercontinental ballistic missile by 2015, and continues to develop the Ashura missile and an extended-range variant of the Shabab-3 missile. Iran also provides missiles and rockets to militant groups in the region through the IRGC Qods Force, including Hamas, Lebanese Hezbollah, and the Taliban.

April 2012: A group of 12 officials from the Shahid Hemmat Industrial Group (SHIG), which is involved in Iran's ballistic missile program, reportedly attend a failed rocket launch in North Korea.

July 2012: The IRGC reportedly fires tens of short- and medium-range missiles during the "Great Prophet 7" war games, including the Shahab 1, 2, and 3, as well as the Fateh, Qiyam (Qiam), Tondar, Khalij Fars, and Zelzal.

July 2012: Pursuant to Executive Order 13382, the Treasury Department imposes financial sanctions on entities linked to Iran's ballistic missile program, including: Electronic Components Industries Co. (ECI), Information Systems Iran (ISIRAN), Advanced Information and Communication Technology Center, Digital Media Lab DML, Value-Added Services Laboratory (VASL), Ministry of Defense Logistics Export (MODLEX), International General Resourcing FZE, and Malek Ashtar University. Three individuals are also sanctioned, including: IRGC Navy Commander Ali Fadavi, Daniel Frosch, and Hamid Reza Rabiee.

August 2012: Iran's Aerospace Industries Organization (AIO) reportedly test-fires a fourth generation Fateh-110 ballistic missile. The Fatah-110 is a solid fuel missile with a range of 300 km.

September 2012: Iran displays the Raad (Thunder) air defense system, which carries missiles with a range of 50 km and is capable of striking a target at 22,000 meters, according to IRGC General Ami Ali Hajizadeh.

October 2012: The European Union bans exports to Iran of graphite, raw or semi-finished metals, including aluminum and steel, and software for integrating industrial processes.

November 2012: IRGC commander Mohammad Ali Jafari announces that Iran has provided Fajr-5 rocket technology to Hamas.

2012-2013: According to a U.N. Panel of Experts report, a German citizen with an Iranian background made several attempts to procure dual-use items for Shahid Bagheri Industrial Group (SBIG), which is responsible for Iran's solid-fuel missiles. The items were procured in Germany or third countries and trans-shipped via the United Arab Emirates to a SBIG front company in Iran.

January 2013: The Iran Freedom and Counter-Proliferation Act of 2012 (IFCA) becomes law. It includes a provision prohibiting the sale to Iran of graphite, raw or semifinished metals (such as aluminum and steel), coal, or software for integrating industrial processes if, among other criteria, those materials are determined to be used in connection with Iran's ballistic missile program.

January 2013: Iran reportedly begins mass production of the Ya Zahra short-range air defense system. Iran's Defense Minister Brigadier General Ahmad Vahidi describes the Ya Zahra system as being able to detect, track, and destroy multiple short range targets simultaneously.

February 2013: An Iranian shipment of explosives, mortars, rocket-propelled grenades, IED precursors, and man-portable anti-aircraft missiles, intended for insurgents operating in Yemen, is intercepted by the Government of Yemen.

May 2013: Israel reportedly carries out a series of airstrikes near Damascus aimed at destroying an Iranian shipment of surface-to-surface missiles, including Fateh-110s.

May 2013: Iran displays at least 26 transporter erector launchers (TELs), reportedly including some large enough to carry the Shahab-3 and the Sejjil ballistic missiles. The TELs are displayed at a ceremony to mark their delivery to the IRGC.

May 2013: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on 14 entities for their role in Iran's international procurement and proliferation operations, including Deputy Defense Minister Reza Mozaffarinia. Mozaffarinia is also dean of Malek Ashtar University and has made "significant contributions" to Iran's missile and space launch programs, according to the Treasury Department.

June 2013: Iranian President Mahmoud Ahmadinejad inaugurates the Imam Sadeq Observation and Monitoring Center, a space monitoring center in the Delijan District of the Markazi Province. The center is equipped with radar, electro-optical, and radio tracking, and was built with help from the Ministry of Defense.
July 2013: U.S. military intelligence reports that Iran could develop and test an intercontinental ballistic missile (ICBM) capable of reaching the United States by 2015 and that Iran's two-stage Simorgh space launch vehicle could serve as a test bed for developing ICBM technologies.
August 2013: Iran appears to be developing a new space launch facility 40 km southeast of the city of Shahrud, according to an analysis of satellite imagery by IHS Jane's. The new site has a larger launch pad than the existing Semnan space center and is equipped with a horizontal rocket checkout facility and a 23 meter launch tower. Both the Semnan and Shahrud facilities are believed to be capable of launching Iran's Simorgh space launch vehicle.
September 2013: Iran displays its Shahab-3, Sejil, and Ghadr missiles in a military parade marking the start of Sacred Defense Week. The solid-fuel Sejil missile has two stages and a greater range than the Shahab-3.
October 2013: U.S. authorities indict Reza Olangian on charges of attempting to acquire and transfer surface-to-air missiles to Iran.
November 2013: A report by the International Institute for Strategic Studies (IISS) estimates that Iran is "unlikely" to deploy an operational ICBM before 2020.
December 2013: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on several Iranian entities for their links to Iran's ballistic missile and military aviation programs, including Maro Sanat Company, Navid Composite Material Company, and Qods Aviation Industries, as well as Qods front companies Fan Pardazan and Ertebat Gostar Novin and Qods's commercial manager Reza Amidi. Navid Composite is building a carbon fiber production plant in Iran, according to the Treasury Department.
December 2013: Iran launches a monkey into space for the second time, using a liquid-fueled rocket that travels 120 km into space and returns to earth after 15 minutes, according to Iranian scientists.
January 2014: Iran's ballistic missiles are "inherently capable of delivering WMD," according to a worldwide threat assessment by the U.S. intelligence community. The intelligence community also assesses that Iran's space launch program provides the country with the means to develop longer-range missiles, including an ICBM, and that Iran maintains the largest inventory of ballistic missiles in the Middle East.
February 2014: Iran displays two satellites developed by a researcher at Malek Ashtar University. Tadbir (Wisdom) is an improved version of the Navid-e-Elm-o-Sanat (The Promise of Science and Industry) satellite, with upgraded imagery resolution, while the Khalij-e-Fars (Persian Gulf) satellite supports secure wireless communications.
February 2014: German authorities reportedly arrest a German-Iranian man, Dr. Ali Reza B., on charges of providing Iran with components for its missile program. The equipment, worth nearly $315,000, includes dual-use items such as vacuum pumps and valves.
February 2014: Iran announces the test of a ballistic missile known as the Barani. Iran claims the missile has a new submunition warhead able to better evade missile defense systems and attack multiple targets simultaneously.
March 2014: Israel intercepts a ship carrying Iranian weapons bound for Gaza. The arms seized from the Klos C, a cargo ship, include M-302 rockets, which are capable of reaching any point in Israel.
March 2014: According to a senior U.S. State Department official, Li Fangwei, a Chinese businessman indicted in 2009 for alleged sales of missile parts to Iran, remains a major supplier of Tehran's missile program. Both Li (also known as Karl Lee) and his company, LIMMT, have been sanctioned by the United States.
March 2014: Iran's defense minister announces the delivery of more accurate versions of the Qadr H, Qiam, Fateh 110, and Khalij-e Fars (Persian Gulf) missiles to the IRGC.
April 2014: Spain's Civil Guard uncovers a network that was attempting to export dual-use industrial machinery to Iran that could be used to manufacture missiles, arresting three Spaniards and one Iranian.
April 2014: The Iranian Navy announces the deployment of the Ghadir anti-ship cruise missile on warships and coastal defense units. The Ghadir is an upgrade over the Nour and Qader missiles, according to Iranian naval officials.
April 2014: The Iranian military announces the deployment of the Sayyad 3 solid-fuel missile on its S-200 air defense system.
May 2014: The IRGC Aerospace Force announces it has equipped its Zelzal missiles, a 300-km range solid-fuel system, with a multiple reentry vehicle (MRV) conventional payload.
May 2014: The IRGC Aerospace Force unveils variants of the Fateh-100 ballistic missile called the Hormuz-1 (anti-radar) and Hormuz-2 (anti-ship). Both missiles reportedly have a range of up to 300 km.
August 2014: The Iranian military announces the successful test of the Bavar 373, an Iranian-built version of the Russian S-300 air defense system.
February 2015: In its first satellite launch since 2012, Iran successfully sends its fourth domestically built satellite, the Fajr, into orbit. The satellite, which was launched from the 21-meter, 26-ton Safir-1B launch

vehicle, had a launch weight of 52 kg, with a height of 49 cm and a width of 35 cm, according to media and analyst reports. Iran's Aerospace Industries Organization (AIO) was responsible for the launcher; Iran Electronics Industries (IEI) built the satellite.

March 2015: Iran's Defense Ministry unveils the Soumar (Sumar) missile, a ground-launched cruise missile with a reported approximate range of 2,500 to 3,000 km. It is reportedly a copy of the Russian-made Raduga Kh-55 cruise missile, twelve of which Iran acquired covertly.

March 2015: Iran begins mass production of its Qadir cruise missile, which reportedly has a range of 300 km.

July 2015: The P5+1 group of countries (China, France, Germany, Russia, the United Kingdom, and the United States) agree to the Joint Comprehensive Plan of Action (JCPOA) with Iran. In a related action, the U.N. Security Council unanimously adopts resolution 2231, which prohibits the supply, sale, or transfer of missile-related items to Iran until October 2023, or until the IAEA confirms that all nuclear material in Iran is in peaceful activities. The resolution also calls upon Iran not to undertake any activity related to ballistic missiles "designed to be capable of delivering nuclear weapons" over the same period of time.

August 2015: The Iranian military unveils the Fateh-313, a solid-fuel missile with a reported range of up to 500 km.

October 2015: Iran's Defense Ministry announces the successful test of the Emad, a ballistic missile with a reported range of 1,700 km. According to *Jane's Defence Weekly*, the Emad is not a new missile but rather a steerable reentry vehicle that can be fitted atop the Shahab-3 and Ghadr-series rockets to improve their accuracy. A confidential report of a U.N. Panel of Experts later determines that the Emad launch is a violation of U.N. resolution 1929.

October 2015: The IRGC releases footage of an underground missile launch facility. According to Iranian news reports, the military base is 500 meters underground and one of hundreds located throughout the country.

November 2015: Iran's defense minister confirms that the contract for the delivery of the S-300 air defense system from Russian to Iran has been signed. According to media reports, the systems will be delivered by September 2016 and Iranian military personnel will receive training at the Mozharsky Academy in St. Petersburg.

November 2015: Iran tests the liquid-fueled, medium-range Ghadr-110, an improved version of the Shahab-3, with a reported range of about 1,900 km. U.S. Ambassador to the U.N. Samantha Power said that "the U.S. is conducting a serious review of the reported incident" and would bring the matter to the U.N. Security Council if it determined the test violated U.N. resolutions.

January 2016: With the implementation of the Joint Comprehensive Plan of Action (JCPOA), U.N. Security Council resolution 2231 takes effect and officially terminates the provisions of previous Iran-related resolutions: resolutions 1696 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1929 (2010), and 2224 (2015).

January 2016: The Treasury Department sanctions 11 entities involved in illicit procurement for Iran's ballistic missile program, including three Iranian officials—Sayyed Javad Musavi, Sayyed Medhi Farahi, and Seyed Mirahmad Nooshin—directly linked to cooperation with the North Korean government on missile development. According to the Treasury Department, Iranian missile technicians from the Shahid Hemmat Industrial Group (SHIG) traveled to North Korea to work on an 80-ton rocket booster jointly developed with the North Korean government. Iranian officials also coordinated shipments of missile technology from the Korea Mining Development Trading Corporation (KOMID) to Iran.

March 2016: The IRGC test-fires the Qiam-1, Shahab-1, Shahab-32, Ghadr-H, and Ghadr-F ballistic missiles during two days of missile exercises.

March 2016: According to *Reuters*, a joint U.S., British, French, and German letter to U.N. Secretary General Ban Ki-moon and Spain's U.N. Ambassador calls Iran's ballistic missile tests in March 2016 "inconsistent with" and "in defiance of" U.N. resolution 2231. The letter states that the missiles were are "inherently capable of delivering nuclear weapons" and asks the Security Council to discuss "appropriate responses" to Iran's actions.

March 2016: Pursuant to Executive Order 13382, the U.S. Treasury Department sanctions two Iranian defense firms for their involvement in Iran's ballistic missile program. Shahid Nuri Industries and Shahid Movahed Industries are designated as subordinates of Shahid Hemmat Industrial Group (SHIG), which is responsible for Iran's liquid-fueled ballistic missile program.

April 2016: Iran reportedly conducts its first test launch of the Simorgh space launch vehicle, which is judged partly successful by U.S. intelligence agencies. The event reportedly was either an unsuccessful launch or a test that was not intended to send a satellite into orbit, according to U.S. defense officials. According to analysts, the Simorgh is a two-stage, liquid-fueled rocket believed to be similar in size and based upon on the technology of the 85-ton North Korean Unha rocket. According to the Iranian Space Agency, the Simorgh is capable of launching a 100 kg payload into a 500 km orbit.

May 2016: A senior Iranian defense official announces the recent test of a ballistic missile with a range of 2,000 km and a margin of error of eight meters. Iran's defense minister subsequently refutes the specifics of this claim but does not deny the missile test itself.

May 2016: Iran's defense minister announces that at least one S-300 missile air defense system has been delivered from Russia to Khatam ol-Anbia Air Defense Base in Iran. Russian officials state that at least four S-300 batteries will be delivered to Iran by the end of 2016.

July 2016: Iran reportedly tests a variant of the North Korean BM-25 Musudan ballistic missile for the first time. The missile reportedly explodes shortly after launch.

July 2016: Iran reportedly receives the first delivery of missiles for the S-300 air defense system from Russia. According to Iranian news outlets, the missiles appear to be for the advanced S-300-PMU2 version of the system.
September 2016: Iran test-fires a new short-range ballistic missile, the Zolfaghar (Zulfiqar), for the first time. The Zolfaghar is reportedly a variant of the solid-fueled Fateh-110 ballistic missile series, with a range of 700 km. Coinciding with the test, Iranian Defense Minister Brigadier General Hossein Dehqan announces that the Zolfaghar has entered the production line.
September 2016: Iranian Defense Minister Brigadier General Hossein Dehqan informs the Iranian parliament that production of the Sejil, Ghadir, and Khorramshahr missiles will begin by March 2017. According to analysts and reports, the Sejil is a solid-fuel medium-range ballistic missile, the Ghadir is a long-range anti-ship missile, and the Khorramshahr is a medium-range ballistic missile.
October 2016: Russia completes delivery of the S-300 air defense systems to Iran, according to news reports citing the Federal Service for Military-Technical Cooperation (FSVTS), Russia's state arms export agency.
December 2016: Iran reportedly successfully tests the Shahab-3 intermediate-range ballistic missile as part of a military exercise.
January 2017: The Iranian parliament approves a bill that requires the government to increase the country's defense power through further missile development and the expansion of air defense capabilities. The bill is part of Iran's Sixth Economic Development Plan (2016-2021).
January 2017: Iran tests a new missile called the Khorramshahr. The missile flies over 1,000 km before its re-entry vehicle explodes, according to U.S. defense officials. The Khorramshahr is reportedly a medium-range ballistic missile capable of carrying a payload greater than 500 kg to a range of over 1,000 km similar to the variant of the Musudan missile launched in July 2016.
February 2017: U.S. National Security Advisor Michael Flynn condemns Iran's January missile test and announces that the U.S. has officially put Iran "on notice." Flynn's statement follows Iranian Defense Minister Brigadier General Hossein Dehqan's confirmation of the test.
February 2017: Iran reportedly tests a Soumar (Sumar) cruise missile, which flies approximately 600 km. The missile is reportedly capable of carrying nuclear weapons and has a range of 2,000 to 3,000 km.
February 2017: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on entities linked to Iran's ballistic missile program, including Abdollah Asgharzadeh and entities related to his Iran- and China-based procurement network, and MKS International and its CEO Kambiz Rostamian. Mostafa Zahedi, Mohammad Magham, Ghodrat Zargari, Ervin Danesh Aryan Company, and Zist Tajhiz Pooyesh Company are also sanctioned for being tied to Mabrooka Trading.
February 2017: The IRGC tests several missile systems during the "Defenders of the Velayat Skies" aerospace drills, according to Iranian news outlets. The missile systems reportedly tested include the Khordad-III, which has a reported range of 75 km and the ability to hit multiple targets at once; the Tabas, which is also capable of engaging multiple targets and has a reported range of 60 km; and the Sayyad-II, which has a reported range of 75 km and the ability to counter electronic warfare.
February 2017: Iran reportedly tests the short-range Mersad surface-to-air-missile. The missile flies 55 km and is launched from the Semnan launch pad, the same site used in the country's January 2017 test of the Khorramshahr medium-range ballistic missile, according to a U.S. official.
February 2017: Iranian officials claim to successfully test two new indigenous missiles during naval drills, according to Iranian officials. The missiles tested include the Nasir cruise missile and the Dehlaviyeh, an advanced anti-ship guided missile.
March 2017: Iran reportedly tests two Fateh-110 short-range ballistic missiles by firing them at its own barges in the Persian Gulf, with one striking its target. The missiles travel approximately 250 km from an IRGC base at Bandar-e-Jask in southeastern Iran.
March 2017: Iran reportedly builds and transfers to Hezbollah underground factories in Lebanon for missile and smaller armaments manufacturing. An IRGC source states that the missile components are manufactured in different factories, before being assembled. The source claims that Hezbollah is capable of manufacturing various types of missiles, some with a range of over 500 km, including surface-to-surface missiles, surface-to-sea missiles, and anti-tank missiles.
March 2017: Iran successfully tests the S-300 air defense system during the "Damavand" war games.
April 2017: The IRGC Navy is formally equipped with the Nasir anti-ship cruise missile, according to the Iranian Defense Ministry.
May 2017: Iran reportedly unsuccessfully attempts to tests a submarine-launched cruise missile in the Strait of Hormuz, according to U.S. officials. The missile was reportedly launched from a Ghadir-class "midget" submarine. The Ghadir is an Iranian variant of the North Korean Yono-class submarine.
May 2017: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on several entities linked to Iran's ballistic missile program, including two Iranian defense officials, Morteza Farasatpour and Rahim Ahmadi, as well as one Iranian company, Matin Sanat Nik Andishan. The Treasury Department also sanctions Chinese national Ruan Runling and three Chinese companies—Shanghai North Begins International, Shanghai Gang Quan Trade Co., and Shanghai North Transway International Trading Co.—for selling navigation and guidance technology to Shiraz Electronics Industries (SEI).
May 2017: A senior IRGC commander claims that in recent years, Iran has built its third underground missile production facility.

June 2017: Iran reportedly fires up to five Zolfaghar (Zulfiqar) short-range ballistic missiles and at least one Qiam-1 short-range ballistic missile at an ISIS command center and car bomb operation in Deir ez-Zor, Syria.
June 2017: A Syrian opposition group reports on Syrian President Bashar Al-Assad's visit to a new missile manufacturing facility in Wadi Jahannam that is reportedly directed by Iran. Subsequent satellite imagery of the facility reveals reported similarities with missile factories in Iran.
June 2017: According to NCRI, Iran has received assistance from North Korea in constructing missile sites in Iran, including underground facilities to produce, store, and maintain missiles. NCRI also claims to identify the locations of 42 missile sites in Iran, 12 of which were previously undisclosed.
July 2017: Houthi rebels in Yemen allegedly fire a Qiam-1 (Borkan-2) short-range ballistic missile at Saudi Arabia, according to U.N. reports. Components in the debris indicate that parts of the missiles were produced by both Iran's Shahid Bagheri Industrial Group (SBIG) and Shahid Hemat Industrial Group (SHIG) between 2002 and 2010.
July 2017: Pursuant to Executive Order 13382, the State Department imposes sanctions on entities involved in the research, development, and testing of Iran's ballistic missiles, including the IRGC Aerospace Force Self Sufficiency Jihad Organization (ASF SSJO) and the IRGC Research and Self Sufficiency Jehad Organization (RSSJO).
July 2017: Iran inaugurates the production line of the Sayyad-3 (Hunter-3), a long-range surface-to-air missile (SAM) that will reportedly be used with the Talash-2 air defense system. According to the Iran's defense minister, the missile has a maximum range of 120 km and a maximum altitude of 27 km.
July 2017: Iran launches the Simorgh satellite launch vehicle from the Imam Khomeini National Space Center. The Simorgh reportedly can carry a payload of up to 250 kg into an orbit with a maximum altitude of 500 km. According to U.S. officials, the launch was unsuccessful.
July 2017: Pursuant to Executive Order 13382, the Treasury Department imposes sanctions on six Iranian entities subordinate to Shahid Hemat Industrial Group (SHIG) for their involvement in the development and production of Iran's ballistic missiles. The sanctioned entities include Shahid Karimi Industries, Shahid Rastegar Industries, Shahid Cheraghi Industries, Shahid Varamini Industries, Shahid Kalhor Industries, and Amir Al Mo'Menin Industries.
August 2017: An unsealed indictment charges Malaysia-based Green Wave Telecommunication and two Iranian nationals, Alireza Jalali and Negar Ghodskani, with conspiring to acquire U.S.-origin military technology on behalf of Iran-based Fanavari Moj Khavar and its subsidiary, Rastafann Ertebat Engineering Company, both of which are linked to Iran's missile program.
August 2017: The Countering America's Adversaries Through Sanctions Act (P.L. 115-44) is signed into law, directing the President to impose sanctions on any person who knowingly contributes to Iran's ballistic missile program or other weapons of mass destruction (WMD) delivery system programs, and to submit a report to Congress every 180 days describing such contributions.
September 2017: Iran displays its Khorramshahr medium-range ballistic missile at a military parade. The commander of the IRGC Aerospace Force claims the missile is capable of carrying multiple warheads and has a range of 2,000 km. The Khorramshahr is based on North Korea's BM-25 Musudan.
September 2017: Iranian state television airs footage of a Khorramshahr missile test, hours after displaying the missile at a military parade. The Khorramshahr is a liquid-fueled, medium-range ballistic missile derived from North Korea's Musudan (BM-25) missile and has a reported range of 2,000 km. U.S. officials reportedly conclude that the video footage is from a failed January 2017 launch.
October 2017: A German intelligence report finds that Iran made 32 attempts in 2016 to procure technology that could be used for its ballistic missile program from the state of North Rhine-Westphalia, down from 141 attempts in 2015.
October 2017: Pursuant to Executive Order 13224, the Treasury Department sanctions several Iranian entities and overseas networks for supporting Iran's ballistic and cruise missile programs. These include Iran-based Shahid Alamolhoda Industries (SAI), Fanavari Moj Khavar, and Rastafann Ertebat Engineering Company, as well as China-based Wuhan Sanjiang Import and Export Co. LTD, which provided missile guidance technology to Iran's Shiraz Electronics Industries (SEI).
November 2017: Houthi rebels in Yemen allegedly fire a Qiam-1 (Borkan-2) short-range ballistic missile at Saudi Arabia, according to U.N. reports. Components in the debris indicate that parts of the missiles were produced by both Iran's Shahid Bagheri Industrial Group (SBIG) and Shahid Hemat Industrial Group (SHIG) between 2002 and 2010.
December 2017: Houthi rebels in Yemen allegedly fire a Qiam-1 short-range ballistic missile at Saudi Arabia, according to a U.N. report. Components in the debris indicate that parts of the missiles were produced by both Iran's Shahid Bagheri Industrial Group (SBIG) and Shahid Hemat Industrial Group (SHIG) between 2002 and 2010.
December 2017: U.S. Ambassador Nikki Haley holds a press conference at which remnants recovered from a Houthi missile attack on Saudi Arabia are displayed. She states that the missile components share characteristics with Iran's Qiam missile, including the absence of stabilizer fins and the presence of nine valves along the length of the missile. She further notes that some components are stamped with the logo of Iran's Shahid Bagheri Industrial Group (SBIG).

January 2018: Ukrainian authorities reportedly detain two Iranian nationals accused of attempting to buy components of the Ukrainian-made X-31 (Kh-31) anti-ship missile. Police find missile parts and related technical documents in the men's possession. One of the men, Abdi Biyan, is reportedly a military attaché at the Iranian embassy in Kiev.
January 2018: Pursuant to Executive Order 13382, the Treasury Department sanctions five Iran-based entities subordinate to Shahid Bagheri Industrial Group (SBIG), including Shahid Kharrazi Industries, Shahid Sanikhani Industries, Shahid Moghaddam Industries, Shahid Eslami Research Center, and Shahid Shustari Industries. The entities' activities include the development of solid propellants, guidance and control systems, and launchers for Iran's solid-fueled missiles.
January 2018: In two separate incidents, Houthi rebels in Yemen allegedly fire a Qiam-1 short-range ballistic missile at Saudi Arabia, according to a U.N. report. Components in the debris indicate that parts of the missiles were produced by both Iran's Shahid Bagheri Industrial Group (SBIG) and Shahid Hemat Industrial Group (SHIG) between 2002 and 2010.
January 2018: A general at the Khatam al-Anbia Air Defense Base announces that Iran's Bavar-373 air defense system has completed initial testing.
January 2018: Pursuant to Executive Order 13382, the Treasury Department sanctions entities in an Iran- and China-based procurement network responsible for supporting Iran's missile program. The entities include Green Wave Telecommunication and its director, Morteza Razavi; Iran Helicopter Support and Renewal Company (PANHA) and Iran Aircraft Industries (SAHA), for being owned or controlled by Iran's Aviation Industries Organization (IAIO); Pardazan System Namad Arman (PASNA); Chinese national and Wuhan Sanjiang Import and Export Co., Ltd. employee Shi Yuhua; and China-based Bochuang Ceramic, Inc. and its representative, Chinese national Zhu Yuequn.
January 2018: The U.N. Panel of Experts on Yemen finds that the design and dimensions of missile remnants recovered from the July and November 2017 Houthi attacks on Saudi Arabia are "almost certainly" of Iranian-origin and consistent with Iran's Qiam-1 missile. The panel concludes that Iran is in "non-compliance" with the arms embargo imposed by U.N. resolution 2216 for failing to prevent the Houthis from acquiring the Borkan-2H ballistic missile, field storage tanks for liquid bipropellant oxidizer for missiles, and the Ababil-T (Qasef-1) unmanned aerial vehicle.
February 2018: Satellite images reportedly indicate that Iran built a new Quds Force-operated base outside Damascus. The images depict two hangars reportedly used to store short- and medium-range missiles. The new base in Jabal ash Shaqi reportedly shares characteristics with the al-Qiswah facility destroyed by Israel in December 2017.
March 2018: A consignment of missiles destined for Houthi rebels in Yemen is seized. The missiles have features consistent with Sayyad-2C surface-to-air missiles, production markings ranging between 2011 and 2015, and were manufactured by Iran, according to a U.N. report.
March 2018: The commander of the IRGC Aerospace Force, Brigadier General Amir Ali Hajizadeh, claims that Iran has tripled its missile production despite attempts to contain Iran's missile program.
March 2018: Houthis in Yemen fire seven ballistic missiles at Saudi Arabia, killing one and injuring two others. The Saudi military claims to have intercepted the missiles, of which three were launched at Riyadh, two at Jazan, and one each at Najran and Khamis Mushait. A Saudi Coalition report categorizes the missiles as the Iranian-made Qiam missile; it further claims that the Houthis are using Sana'a airport to launch Iranian-origin Siyad missiles. A U.N. report later says that several of the missiles were Iranian Qiam-1 variants.
April 2018: Houthi rebels in Yemen launch several ballistic missiles at the Saudi Defense Ministry in Riyadh and two Qasef-1 drones at Abha airport and at a Saudi Aramco oil facility. Saudi forces claim to have intercepted the missiles and destroyed the Iranian-manufactured Qasef-1 drones. A U.N. report later says that the missiles were Iranian Qiam-1 variants.
April 2018: Iran's Armed Forces display various missile systems at a military parade, including the S-200 and S-300 missile systems, the Talash missile system, the Mersad optimized missile system, the Kamin portable missile system, and the Skyguard missile system. Also on display are long-range missile launchers, including the domestically produced Nasr system, and the al-Sabehat submarine.
May 2018: The United States withdraws from the Joint Comprehensive Plan of Action (JCPOA), citing its failure to address Iran's missile program, among other reasons.
May 2018: The IRGC Quds Force allegedly fires rockets from Syria towards Israel, according to a U.N. report.
May 2018: Pursuant to Executive Order 13224, the Treasury Department sanctions five Iranians who provided ballistic missile-related technical expertise to Yemen's Houthis and transferred weapons to Yemen on behalf of the IRGC Quds Force. The five individuals are Mahmud Bagheri Kazemabad and Mohammad Agha Ja'fari for overseeing the transfer of missile components, as well as Javad Bordbar Shir Amin, Mehdi Azarpisheh, and Sayyed Mohammad Ali Haddadnezhad Tehrani for acting on behalf of or supporting various arms of the IRGC.
June 2018: Houthi rebels in Yemen allegedly fire two Qiam-1 short-range ballistic missiles at Saudi Arabia, according to a U.N. report.

August 2018: Iran reportedly tests a Fateh-110 short-range ballistic missile as part of a naval exercise conducted by the IRGC.
September 2018: Iran reportedly fires seven Fateh-110 short-range ballistic missiles at a base of Iranian Kurdish dissidents in Iraq, killing 11.
October 2018: Iran reportedly fires six Zolfaghar (Zolfiqar) and Qiam short-range ballistic missiles from the Kermanshah launch site in western Iran at an ISIS base in Abu Kamal in southeast Syria in retaliation for an attack against a military parade in Ahvaz, Iran, which killed at least 25.
December 2018: Iran tests a medium-range ballistic missile, which is reportedly a Khorramshahr with a range of 2,000 km.
December 2018-February 2019: Iran tests a series of missiles, including one Shahab-3 medium-range ballistic missile, one Qiam short-range ballistic missile, one Scud short-range ballistic missile, and one Zolfaghar (Zulfiqar) short-range ballistic missile, according to a U.N. report.
January 2019: Iran launches the Payam satellite aboard a Simorgh space launch vehicle, which uses technology similar to long-range ballistic missiles, from the Imam Khomeini Space Center. The satellite reportedly fails to reach orbit.
January 2019: The IRGC Quds Force allegedly fires a surface-to-air missile from Damascus towards the Golan Heights, according to a U.N. report.
February 2019: Iran unveils the Hoveizeh cruise missile, which has a range of at least 1,200 km, as part of the 40th anniversary celebrations of the Iranian Revolution. The missile is reportedly similar to the nuclear-capable Soviet Kh-55 missile. At the same event, Iran displays the updated Khorramshahr 2 medium-range ballistic missile, which reportedly has a range of 2,000 km.
February 2019: Iran unveils the Dezful medium-range ballistic missile, which has a range of 1,000 km and is an upgrade of the older Zolfaghar (Zulfiqar) model.
February 2019: Iran launches the Doosti satellite aboard a Safir space launch vehicle, which uses technology similar to long-range ballistic missiles, from the Imam Khomeini Space Center. Reportedly weighing 52 kg, the satellite reportedly fails to reach orbit.
February 2019: Iran tests a submarine-launched cruise missile for the first time as part of its "Velayat 97" wargame exercises in the Strait of Hormuz.
May 2019: A televised speech by the political leader of Hamas, Yahya Sinwar, and a statement by the Al-Quds Brigades spokesperson in the Gaza Strip suggest ongoing Iranian missile support to Hamas and the Palestinian Islamic Jihad, according to a U.N. report.
July 2019: Iran reportedly tests a Shahab-3 medium-range ballistic missile. The missile, which is based on the North Korean No-Dong, flies approximately 1,100 km.
August 2019: Iran unveils three new precision-guided air-to-air missiles: the Yasin, the Balaban, and an updated variant of the Qaem. The missiles are developed by the Iranian Defense Ministry and Iran Electronics Industries (IEI).
August 2019: Pursuant to Executive Order 13382, the Treasury Department sanctions two procurement networks supporting Iran's missile program. One network involved Iranian nationals Hamed Dehghan and Hadi Dehghan, their intermediaries, and a Hong Kong-based front company named. This network supplied Iranian defense firms with electronic components. A second network run by Seyed Hossein Shariat and his firm Asre Sanat Eshragh Company supplied aluminum alloys to multiple Iranian entities.
August 2019: Satellite images reveal that a rocket exploded on a launch pad at Iran's Imam Khomeini Space Center. An Iranian official says the explosion was due to "technical issues," and a U.S. official confirms that a satellite launch failure occurred.
September 2019: Pursuant to Executive Order 13382, the State Department sanctions the Iran Space Agency (ISA) and two of its research institutes, noting that space launch vehicles developed by these entities "are virtually identical and interchangeable with those used in ballistic missiles."
September 2019: Iran is implicated in a cruise missile and drone attack on Saudi Arabian oil facilities. In response, the Treasury Department sanctions the Central Bank of Iran (CBI), the National Development Fund of Iran (NDF), and Etemad Tejarate Pars Co., pursuant to Executive Order 13224, for financially supporting the IRGC-Quds Force and the Ministry of Defense and Armed Forces Logistics (MODAFL).
November-December 2019: France, Germany, and the United Kingdom send a letter to the U.N. Secretary General about a previously unknown flight test of the Shahab-3 medium-range ballistic missile. According to undated footage released in April 2019, Iran tested a variant of the Shahab-3 equipped with a maneuverable re-entry vehicle.
January 2020: Iran launches 16 ballistic missiles at two bases hosting U.S. troops in Iraq. Both Fateh and Qiam short-range ballistic missiles were used in the strike, according to Iranian media reports. The attack caused no fatalities, but did material damage and caused over 100 cases of traumatic brain injury to U.S. troops. At least four missiles fell short of the bases, according to the Iraqi military. Satellite imagery analysis suggests that six of the remaining missiles struck their targets precisely, leading to estimates that the missiles have a circular error probable (CEP) from 100 meters to as little as 10 meters.
February 2020: Iran attempts to launch a Zafar-1 satellite into orbit from the Imam Khomeini Space Center using a Simorgh space launch vehicle, a three-stage rocket that uses some technology similar to

long-range ballistic missiles. The launch fails in the second or third stage after reaching an altitude of 540 kilometers. It is the Simorgh's third consecutive failure.

February 2020: Iran unveils the Raad-500 short-range ballistic missile.[1] According to IRGC Aerospace Forces commander Brigadier General Amir Ali Hajizadeh, the missile is a lightweight version of the solid-fuel Fateh-110, with a range of 500 kilometers and a composite, carbon fiber body.

February 2020: The U.S. Department of State sanctions 13 entities from Iraq, Turkey, Russia, and China entities pursuant to the Iran, North Korea, and Syria Nonproliferation Act (INKSNA) for supporting Iran's missile program. The sanctions apply for two years and ban the U.S. government from procuring from, contracting with, providing assistance to, or issuing export licenses involving controlled items for the entities.

March 2020: The commander of U.S. Central Command estimates that Iran possesses between 2,500 and 3,000 ballistic missiles.

April 2020: The IRGC announces that it has successfully put the Noor military satellite into orbit from a base in Semnan Province with a three-stage Ghased space launch vehicle that uses both liquid and solid fuel. According to independent analysis, the Ghased likely uses a Ghadr medium-range ballistic missile for its first stage and a solid-fuel motor designed by the IRGC Research and Self-Sufficiency Jihad Organization (RSSJO) for its second stage.

June 2020: A report by the U.N. Secretary General determines that cruise missiles used in four attacks on Saudi Arabia in 2019, among them the September 2019 strike on Saudi oil facilities, "were of Iranian origin."

July 2020: The IRGC reportedly fires ballistic missiles from underground sites in Iran's central desert during the "Great Prophet 14" military exercise involving missile units from the IRGC Aerospace Force and Navy.

August 2020: Iran announces the development of two new missiles: the Martyr Hajj Qassem surface-to-surface ballistic missile, with a reported range of 1,400 km, and the Martyr Abu Mahdi anti-ship cruise missile, with a reported range of 1,000 km. Iran also unveils what it claims is a turbofan engine, which can be used in long-range cruise missiles and drones.

September 2020: The U.S. Treasury Department sanctions seven Iranian companies and individuals involved in the development of ballistic missiles.

October 2020: The U.S. Justice Department accuses the IRGC of masterminding two shipments of missiles to the Houthis intercepted by the U.S. Navy in November 2019 and February 2020. According to the Justice Department, the shipments contained mostly surface-to-air missiles and anti-tank guided missiles, but also included cruise missile and drone components.

November 2020: The IRGC announces the development of an underground facility for ballistic missiles with a "simultaneous or consecutive launch capability." According to independent analysis, the base uses a rail system enabling Iran to fire Emad missiles from a single silo in quick succession.

January 2021: The IRGC Navy claims to have established a "missile city" military base containing "a column of missiles and launching systems" on Iran's Persian Gulf coast. During a military exercise, the IRGC reportedly tests solid-fueled Dezful and Zolfaghar ballistic missiles and kamikaze drones.

February 2021: The Iranian Ministry of Defense and Armed Forces Logistics (MODAFL) announces that Iran has conducted a test of the new Zuljanah space launch vehicle. The Zuljanah reportedly incorporates a solid-fuel motor with a 5-foot diameter and a thrust of 75 kilotons.

March 2021: A U.N. panel of experts on North Korea documents allegations from a U.N. member state that Iran and North Korea "have resumed cooperation on long-range missile development projects," which "included the transfer of critical parts" in 2020.

June 2021: According to the U.S. Defense Department, Iran unsuccessfully attempts to launch a satellite. Independent analysis suggests that the failed attempt employed the Simorgh space launch vehicle, making it the Simorgh's fourth consecutive launch failure. The launch reportedly took place at Imam Khomeini Spaceport in Semnan Province.

December 2021: The IRGC Navy tests ballistic and cruise missiles during a war game in the Persian Gulf. The exercise is reportedly the first time that ballistic missiles have been launched by the IRGC Navy. Ballistic missiles tested reportedly include the Dezful, Emad, Ghadr, Sejjil, and Zolfaghar.

December 2021: The Iranian Ministry of Defense and Armed Forces Logistics (MODAFL) announces the failed launch of three research devices into space on a Simorgh rocket, continuing a string of unsuccessful Simorgh launch attempts.

January 2022: The IRGC conducts a static ground test of a solid-fuel engine for a space launch vehicle (SLV), which the IRGC describes as built from composite material instead of metal.

January 2022: Iranian-backed Houthi rebels fire ballistic missiles in three separate attacks on targets in the United Arab Emirates. In one attack, the Houthis claim to have used Zulfiqar missiles, a derivative of the Iranian Qiam missile.

February 2022: Iran unveils the solid-fuel "Kheibar Shekan" surface-to-surface ballistic missile, which Iran claims is produced by the IRGC and has a range of 1,450 km.

February 2022: Hezbollah claims to have acquired the ability to convert its arsenal of rockets into precision-guided missiles.

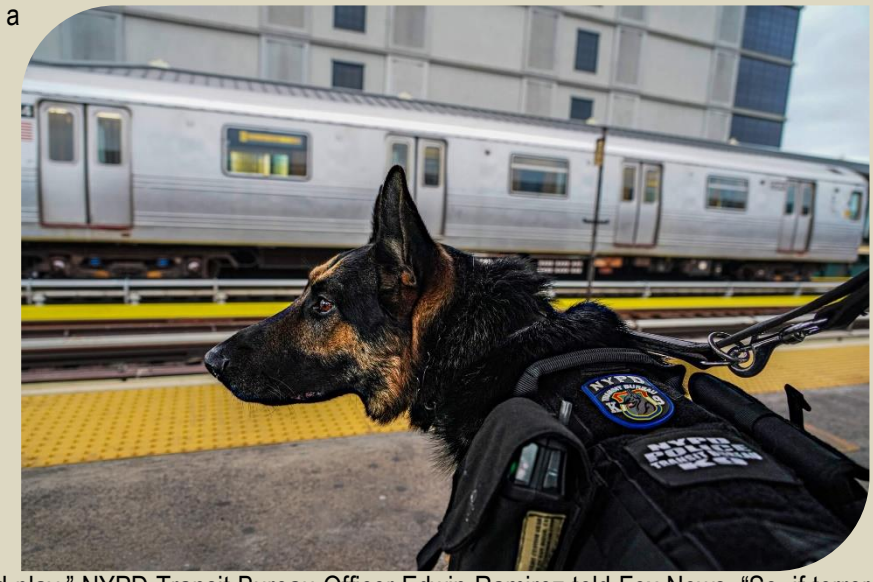
March 2022: Satellite imagery indicates that Iran conducted a failed launch of the Zuljanah space launch vehicle (SLV) at the Imam Khomeini Spaceport in Semnan Province. The Zuljanah SLV uses a combination of solid and liquid fuel.
March 2022: The IRGC says that it has launched its second reconnaissance satellite, the Noor-2, into low-earth orbit using a three-phase, mixed-fuel Qased SLV from a truck-based launcher in the desert near the city of Shahroud. Iran later claims to be receiving high-resolution imagery from the Noor-2.
March 2022: The IRGC launches a dozen ballistic missiles into Iraqi Kurdistan, targeting what it claims is a secret Israeli base. The strike reportedly serves as retaliation for an Israeli attack on an Iranian drone factory a month earlier. In response, the U.S. Treasury Department imposes sanctions on five Iranian entities for helping Iran obtain equipment from China that can be used for making ballistic missile propellant.
May 2022: Iran unveils the Heidar-1 and Heidar-2 cruise missiles. The Heidar-1 is reportedly Iran's first drone-launched cruise missile and has a claimed range of 200 km. The reportedly helicopter-launched Heidar-2 relies on a turbojet engine apparently copied from the Czech-made PBS TJ100 turbojet that has been found on Houthi missiles in Yemen.
June 2022: The Iranian Ministry of Defense and Armed Forces Logistics (MODAFL) announces a second (successful) suborbital test launch of the Zuljanah SLV. MODAFL also says that Iran will study the results of the test to prepare for a third Zuljanah launch at an unspecified date.

[1] The Raad-500 is distinct from the Raad, an Iranian anti-ship cruise missile in service since 2007, as well as from a Pakistani cruise missile of the same name.

Police Dogs Are Now Wearing Sensors to Detect Explosives

Source: https://i-hls.com/archives/114900

July 12 – Police dogs are already trained for patrol and tracking, so how about we add advanced explosive detection as well? New York City's Police Department (NYPD) has enacted the **Transit Enhanced Detection Dog (TREDD)** program that features an experienced explosive detection dog wearing a sensor-laden harness that can detect radiation or chemicals the dogs haven't been trained to identify.



GCN.com reports that with the sensor harness, a dog already trained for patrol, tracking and explosive detection becomes part of a virtual CBRNE detection platform, allowing police to respond to various attacks with the same canine.
The system is capable of taking location and sensor readings and transmitting them to a custom-designed app on a handler's cellphone in real-time, giving officers an early alert to a chemical, biological, radiological, nuclear and explosive (CBRNE) weapon. The sensors can also be monitored by local commanders who can see the GPS location of the dog and handler on either a laptop or phone. "The system is plug and play," NYPD Transit Bureau Officer Edwin Ramirez told Fox News. "So, if terror groups change their tactics, I can change sensors and redirect what we need to do."
Besides detecting explosives or chemical weapons, the team can also quickly sweep subway cars after they pull into the station.

Russia says its working on carrier-killer hypersonic

Source: https://asiatimes.com/2022/07/russia-says-its-working-on-carrier-killer-hypersonic/

July 18 – Russia is working on its own version of a carrier-killer hypersonic missile according to state media reports, a move that likely aims to fortify its naval bastions in the North Atlantic and Northern Pacific amid spiking geopolitical tensions with the United States and wider West.

On July 12, Russian state news broadcaster TASS announced that the country is developing the so-called **Zmeevik hypersonic** carrier-killer missile. The TASS report claimed that the missile will have similar characteristics to China's DF-21D and DF-26, and will have a **flight range of 4,000 kilometers**.

The same report said the weapon could enter service with Russian Navy coastal defense units.

The Zmeevik missile solves the problem of equipping surface warships with weapons capable of attacking aircraft carriers and carrier battle groups, notes military expert Vasily Dandikin in Gazeta.ru.

He states that while existing submarine-launched and shore-based anti-ship missiles are effective within engagement ranges under 1,000 kilometers, operations in the North Atlantic and Pacific Oceans need longer-range systems to deter enemy warships from getting in range to launch cruise missile strikes.

The Zmeevik's development was spurred by the US' own hypersonic weapons program, as noted by Alexei Leonkov in a Radio 1 interview. Leonkov, chief editor of the Arsenal of the Fatherland military magazine, said that while the US may have built hypersonic weapons that can reach Mach 5 speeds, they still fly mostly on a ballistic trajectory unlike Russian hypersonics such as the Zmeevik, which feature maneuverability to evade air defenses.

Dandikin notes accordingly that the advent of hypersonic weapons has changed the Russian Navy's research priorities from submarine-launched ballistic missiles (SLBM) to hypersonic weapons such as the Zmeevik.

While carrier battlegroups feature heavily armed warships for fleet air defense, these ships are still potentially vulnerable to missile attacks. Naval News notes the recent sinking of the Moskva cruiser as a case in point. Despite the Moskva having long-range air defense radars and layered anti-air defenses, Ukraine still managed to sink the cruiser using Neptune shore-based anti-ship missiles. This huge loss undoubtedly had a profound impact on the Russian Navy, which may have highlighted the vulnerability of its large surface combatants against shore-based missile attacks. At the same time, it may have also demonstrated the potential vulnerabilities of US warships to such weapons.

To be sure, the Moskva has less advanced defenses than US warships, which means that it could be – and was – sunk by an anti-ship missile derived from an existing Soviet-era design. To successfully engage US carrier battlegroups, Russia needs a much more advanced missile.

Should the Zmeevik enter service relatively soon, it may be a potent deterrent against the US and allied naval freedom of action, as the US has not yet developed an effective defense against hypersonic weapons, notes Naval News.

The Zmeevik may become a key asset in Russia's naval bastion defense strategy, which the NATO Combined Joint Operations from the Sea Center of Excellence (CJOS COE) describes as consisting of a geographically and horizontally layered defense.

The same source notes that a bastion defense features an outer area with sea denial as its primary objective and an inner space that aims for sea control. As such, deploying shore-based missiles like the Zmeevik would increase Russia's weapons range and expand its anti-access/area denial (A2/AD) blanket within the semi-enclosed waters of the Baltic and North Seas and in the Sea of Okhotsk and Kuril Islands in the Pacific.

However, the Zmeevik may turn out to be vaporware, despite the bold claims being made about its capabilities by Russian military experts. The 1945 military news site notes numerous issues that raise questions about the integrity of Russian claims about the Zmeevik.

First, there have been no verified Zmeevik launch tests, even though the weapon has long been in development, the 1945 report says. This does not mean that a prototype test launch has never occurred, as the former Soviet Union and today's Russia were and are anti-ship missile technology pioneers.

Second, it is unclear how Russia will integrate the Zmeevik with other systems. Because it is an over-the-horizon missile, it needs integration with maritime reconnaissance aircraft, drones and satellites for effective targeting.

Third, it is unknown how far Russia has actually come with the Zmeevik's development. Until a successful Zmeevik missile test is verified, reports about the new weapon may be propaganda or disinformation to confuse US and allied defense planners.

Western analysts may dismiss Russian claims about the Zmeevik as empty saber-rattling until the weapon is proven to work, including in the next standoff or engagement between Russia and the West.

Bulletproof steel shelters sold as solution to school shootings

Source: https://www.theguardian.com/us-news/2022/jul/17/bulletproof-steel-shelters-sold-as-solution-to-school-shootings

July 18 – A company in Fort Pierce, Florida – not far from Parkland, site of the 2018 school shooting that killed 17 – is stirring controversy with its plan to protect children from school shootings by hiding them in bullet-resistant steel enclosures.

To many, the idea of directing children into stark metal boxes serves as an alarming symbol of a country that fails time and again to address the causes of its gun violence crisis.

But with Congress stymied, decade after decade, on gun control, and mass shootings only growing deadlier and more common, do the pods represent a disturbing – but inevitable – safety measure?

John Corrado, vice-president of National Safety Shelters, says the company sees its shelters as a response to an intractable problem. "Obviously, the fewer the guns, the better. Because you can't have shootings without guns," Corrado says. "However, we've recognized reality. With the type of government that we have and the difficulty in getting laws changed … guns are here to stay. So you have to do something to protect yourself from them." The idea, he says, is that the pods would be just one part of a "comprehensive solution".

Children, the company says, can enter the shelters in the event of an attack "within a minute or less". The pods, intended to accommodate a classroom's worth of people, are built from "military-grade steel specially heat-treated to resist not only all handguns and shotguns, but even semi-automatic weapons like AK-47 and AR-15 rifles", according to the company. The idea is that each classroom would have its own shelter, which locks from the inside with three bolts and a locking pin.

The company began as a mobility lift company, building equipment to assist disabled people, Corrado says. One of its suppliers was a company that built above-ground tornado shelters in Missouri. "After the shootings took place in Sandy Hook at the end of 2012, a few schools in their neighboring areas started

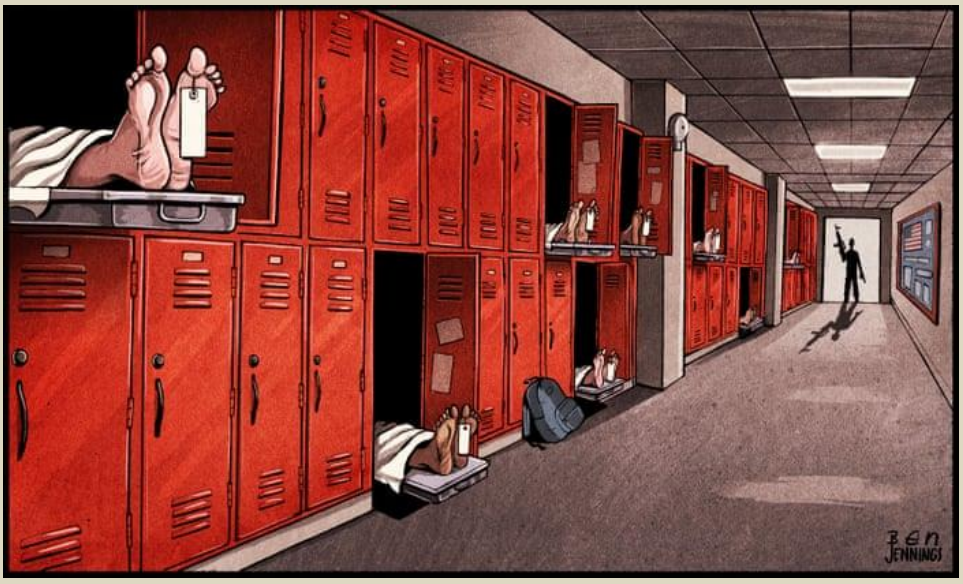
inquiring of them saying, 'Hey, could we put these shelters perhaps in classrooms, to protect kids?'" Corrado says. "What really got us deeply into it was in 2018, when the Parkland shooting happened, because that's close to home for us … the Parkland school is about an hour and a half from where we live." That year, a federal report called for "secure spaces within classrooms where students and teachers can shelter". His company began marketing the pods as protection against shooters and tornadoes. Its first client was the Quitman school district in Arkansas, which spent $1m to install 53 pods in classrooms, the cafeteria and the gym, the local station THV11 reported in 2019. In a video produced by the company, students and parents in the district say they feel safer with the shelters, which take up little space and can be painted to match the room, Corrado notes.

Since then, the company has worked with several other schools and some daycares, Corrado says. So far, the pods have not been used in any real-world shootings, he says, though Quitman did use them during a tornado scare. Meanwhile, a handful of other midwestern tornado-shelter makers have "started to rebrand them as safety shelters". But Ron Avi Astor, a professor of social welfare at UCLA's Luskin School of Public Affairs and School of Education and Information Studies, says there's a lack of evidence to support measures like these that make schools more fortress-like. For one thing, he says, many "hardening" responses assume the intruder is coming from the outside, when many attackers are current or former students who will be aware of the school's deterrents and may be able to circumvent them. What's more, he says, such measures may not leave people feeling any better. "We have a long research literature on facilities that are made to look and feel like little prisons," Astor says. "The analogy I keep on using is: you think of buying a house in the neighborhood, and a real estate agent is taking you around and saying, 'Look at this house. It's total concrete, all bulletproof windows, we got police officers on every corner, there's a tank at the entrance …. I don't feel safe there," he says. "I go to the place where people are gardening and out and saying hi."

Astor is concerned about the "long-term effects of kids growing up in mini-prisons". "Imagine 13 years being in that kind of building. There is a lot of data showing that particularly for kids in urban, low-income areas, having a lot of these measures, dogs, police officers: everything actually creates a higher level of dropout and increases the school-to-prison pipeline." School becomes, "a place of fear". In the short term, he says, we may need to find a plan that balances "where we want to be as a society with relieving some of the anxieties" about attacks. He calls for developing programs that build connections between children and their schools, "so that every teacher knows a little bit about every child's emotional life and a little bit about their parents", he says. Astor's own research has found that these programs reduce the incidence of kids bringing weapons to school. That said, he fully understands the impulse behind these protections. "When my grandkids go out to school, I want to have some security there. So I totally get the other side."

The debate over how to address these shootings, Astor says, has been a harsh one, but "I think everybody's trying to solve the problem … we're not pitted against each other." The best way forward, he says, will be "a constructive, data-driven public health approach".

EDITOR'S COMMENT: Not a very clever approach! And expensive! Two things can be done tomorrow and with less cost: (1) fortify the doors in all classes, gyms, toilets, lunch rooms, etc to withstand an AR-15/AK-47 (and alike) shootings, and (2) create corridor barriers (doors) that can isolate certain parts of the school in the case an alarm has been activated. Start with the ground floor; then study if certain measures should be taken for higher floors as well. Educate personnel and students on what to do in case of an emergency. Test plans a million times. Keep in mind what the late Bruce Lee quoted "I fear not the man who has practiced 10,000 kicks once, but I fear the man who has practiced one kick 10,000 times!"



New Method to Detect TNT

Source: https://i-hls.com/archives/115017

July 16 – A team of Indian researchers have discovered a new method for TNT detection. The researchers synthesized two small fluorescent molecules (fluorophores) that are highly sensitive to ultra-low levels of TNT.

Normally, these fluorophores glow with a green-yellow color under UV light, but if they come in contact with even a tiny amount of TNT, no matter its physical form, the glow dims out. This low-cost solution trumps the conventional methods of detecting TNT by collecting a sample and testing it with expensive equipment. Not only are they inexpensive, but they are also metal free and allow detection at room temperature.

Op-Ed: Why it makes sense to keep mine-hunting dolphins on the Navy's payroll

By Scott Savitz

Source: https://www.latimes.com/opinion/story/2022-07-22/dolphins-mine-hunting-navy-end-program-decommission

Ju;y 22 – In an age of digital wonders and mechanical marvels, the mine-hunting abilities of the dolphin remain unmatched by human ingenuity. These creatures have long been a critical component of the Navy's suite of mine countermeasure capabilities.

Yet budget cuts could spell the end of the program, which began around 1960 after the first dolphin was trained in mine detection. President Kennedy took to the idea of using sea creatures for military purposes, so the program was expanded.

The highly skilled dolphins make the seas safer for naval ships and other vessels. Yet Pentagon budget cutters have been chipping away at funding for the program since last year. In the Navy's budget request for the coming fiscal year, funding for the dolphin team has been slashed by $6.6 million — to less than $1 million.

With their ultrasensitive "biological sonar," dolphins can precisely locate mines from the upper reaches of the water column down to the seafloor or even beneath it if a mine is buried in the mud. To report the presence of mines to their human handlers, the dolphins are trained to tap paddles attached to a boat or dock, then are given devices to mark the mines' locations, enabling elimination of the threat.

Their accuracy is legendary. During exercises, dolphins almost always locate every mine assigned to them, in addition to previously undiscovered mines from World War II. One time dolphins located a missing uncrewed undersea vehicle after other such vehicles had failed to locate it during exercises off the Virginia coast.

Environmental and animal rights groups have raised questions regarding the animals' welfare. However, these dolphins, like the military's explosive-sniffing dogs, are well-treated, according to the U.S. Undersea Naval Museum. Their handlers encourage the dolphins to find objects through praise, petting and treats, tossing them fish when they find something. No punishment is used.

Moreover, the dolphins frequently exercise in open-ocean environments from which they could easily swim away. Instead, they return to their protected environments. Thanks to healthy diets, medical care and protection from predators, the dolphins frequently live decades beyond what they would in the wild.

A dolphin interacts with its trainer in 2015 in San Diego in a mine-hunting program run by the Space and Naval Warfare System Pacific. (Don Bartletti / Los Angeles Times)

While they operate in the vicinity of explosive devices, no mine-hunting dolphin has ever been harmed by a mine. Mines are designed to detonate when they experience the massive concussive force of a ship or when they sense a ship's magnetism and characteristic sounds, none of which a dolphin could conceivably replicate.

In recent years, critics have argued that uncrewed undersea vehicles can fully match the dolphins' capabilities — so the dolphin program should be eliminated. It is true that the vehicles are becoming increasingly capable as their autonomy, navigational systems, sensors and other systems continually improve.

But keeping the dolphins on the payroll as a complement to uncrewed undersea vehicles makes sense.

The vehicles already make substantial contributions to Navy mine-hunting especially tasks such as tracking the seafloor, monitoring currents and determining depths — and are particularly useful for wide-area searches in relatively open spaces.

However, they are also vulnerable to environmental impediments that dolphins easily overcome, such as strong currents, thick seaweed and confined waters. Dolphins complement the high-tech mine-hunters in challenging environments, bringing keener detection and classification abilities, particularly against mines that are partly or completely buried.

But the Pentagon budget watchers dismiss the animals as too difficult to deploy, given that they are substantially bigger than humans, need to be kept wet and continually provided with fish to eat. However, they have repeatedly been deployed around the globe. Between missions, they can be sheltered in enclosures along docks or even in tanks aboard large ships.

Critics also argue that because the dolphin handlers are civilians who are not subject to military orders, they may not be willing to deploy in wartime. That has not been the case. Dolphins and their handlers have repeatedly contributed in war zones, including in Operation Iraqi Freedom in 2003 and the Vietnam War.

Eliminating the dolphin mine-hunting program would save the Navy $7 million annually. In contrast, the Navy has spent $131 million over the last three years to acquire 10 of the newest uncrewed undersea vehicles that would replace the dolphins — and that does not include operational costs.

Rather than one system being viewed as a replacement for the other, the two can work together: The vehicles can sweep wider areas at lower levels of fidelity, and dolphins can provide focused capabilities

in specific environments or when higher accuracy is needed. Making the sea safe from mines is well worth the investment in animals and technology. Restoring a multibillion-dollar fleet's freedom of movement during wartime by reducing the mine threat has proved critical.

A single mine blast can incapacitate or even sink a warship costing billions of dollars. The cost of repairing a mine-damaged warship that manages to stay afloat can reach into the millions, and the warship remains unusable for months. Mine-hunting benefits extend to civilian ships, which are able to enter key areas and avoid mine damage to deliver food, fuel and other essential goods around the world.

Someday, the machine may be smart enough to replace the mammal in mine-detection missions. But not yet.

Scott Savitz is a senior engineer at the nonprofit, nonpartisan Rand Corp., where his extensive research for the Navy, Coast Guard and other military services includes naval mine warfare.

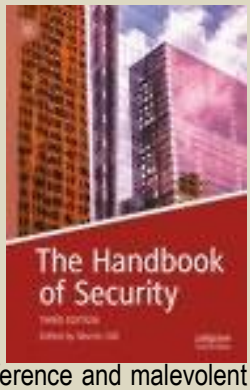
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

Securing the Bioeconomy: Exploring the Role of Cyberbiosecurity



By Patrick F. Walsh

The Handbook of Security pp. 335–355

Source: https://link.springer.com/chapter/10.1007/978-3-030-91735-7_16

Abstract

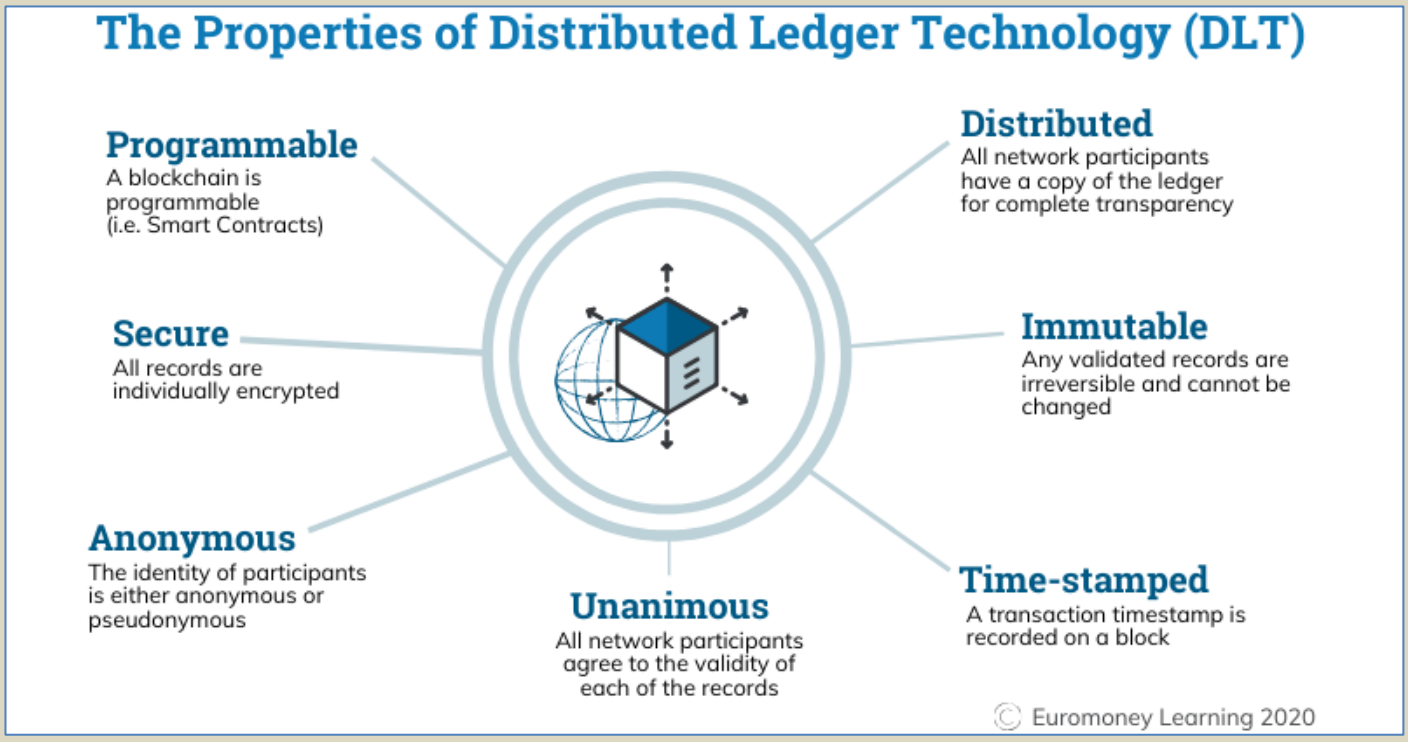
Patrick Walsh discusses threats to the bioeconomy sector. He presents cyberbiosecurity, a growing cross-disciplinary knowledge area that intersects cybersecurity, security and biosecurity and provides a different way of understanding security threats to the bioeconomy. He argues that synthetic biology and biotechnology are exponentially growing sectors of the global economy, however, the nature of emerging threats and risks associated with these sectors are not well understood. Discussing IP theft, foreign interference and malevolent exploitation of dual-use bio-agents Walsh provides a more comprehensive understanding of threats, risks and vulnerabilities in this little-understood sector.

Dr. Patrick F Walsh is an Associate Professor, Intelligence and Security Studies @ Charles Sturt University.

Insights into Blockchain Vulnerabilities

Source: https://www.homelandsecuritynewswire.com/dr20220624-insights-into-blockchain-vulnerabilities

June 24 – Distributed ledger technology, such as blockchains, has become more prevalent across a variety of contexts over the past decade. The premise is that blockchains operate securely without any centralized control and that they are immutable or unsusceptible to change.



Given its mission to create and prevent technological surprise, DARPA endeavored to understand those security assumptions and determine to what degree blockchains are actually decentralized. As such, the agency engaged cybersecurity research and consulting firm Trail of Bits to examine the fundamental properties of blockchains and the cybersecurity risks associated with them.

The study resulted in a report that provides holistic analysis that's available to anyone considering blockchains for important matters so they can better understand the potential vulnerabilities within these systems.

"The report demonstrates the continued need for careful review when assessing new technologies, such as blockchains, as they proliferate in our society and economy" said Joshua Baron, DARPA program manager overseeing the study. "We should not take any promise of security on face value and anyone using blockchains for matters of high importance must think through the associated vulnerabilities."

●▶ **To learn more, access the report** here

Int'l Collaboration Against Major Cyber Threat Turns Successful

Source: https://i-hls.com/archives/114659

June 26 – More and more components of homes and businesses go "smart" and internet-connected. These IoT devices are exposed to the lack of adequate security in the first place and the failure to regularly patch them for developing security issues. Bots scan devices, look for vulnerabilities, and communicate back to hackers.
There is no doubt that immediate and major improvements in IoT security are needed. An international cybersecurity collaboration turned out as a success as a major Russian botnet that had compromised millions of devices worldwide has been taken down.
The US Department of Justice (DOJ) worked with law enforcement in Germany, the Netherlands, and the United Kingdom to seize infrastructure belonging to the Russian botnet's operation.
RSOCKS, the Russian botnet, was essentially functioning as an underground proxy service provider for criminals, allowing for the rental of the IP addresses attached to its collection of hacked IoT devices, Android phones and computers, according to cpomagazine.com. In fact, the extent of its operation reportedly grew to about eight million devices worldwide prior to the takedown. Legitimate proxy services cut off customers for engaging in the sort of cyber criminal activities.
The Russian botnet was active since at least 2014, and over the years it has amassed millions of devices in its collection, first focusing on compromising poorly secured IoT devices but soon moving on to include Android phones/tablets and even computers.
Illicit actors rented access to RSOCKS as a proxy service, primarily for the purpose of brute force/ password guessing login campaigns, disguising the sources of traffic for phishing campaigns, and distributed denial of service (DDoS) attacks.
The takedown of the Russian botnet went underway in 2017 when members of the Federal Bureau of Investigation (FBI) began renting access to the underground proxy service to probe its backend infrastructure and identify victims. The count at the time was about 325,000 devices around the world; RSOCKS had since doubled that number several times.
The Russian botnet reportedly grew to its massive size exponentially, conducting brute force login attempts against new victims by using the devices it had already collected. These attempts were very likely fed by the long lists of compromised usernames and passwords that have been dumped to the internet in the wake of data breaches.

Israel plans 'Cyber-Dome' to defeat digital attacks from Iran and others

Source: https://www.theregister.com/2022/06/30/israel_cyber_dome/

June 30 – The new head of Israel's National Cyber Directorate (INCD) has announced the nation intends to build a "Cyber-Dome" – a national defense system to fend off digital attacks.
Gaby Portnoy, director general of INCD, revealed plans for Cyber-Dome on Tuesday, delivering his first public speech since his appointment to the role in February. Portnoy is a 31-year veteran of the Israeli Defense Forces, which he exited as a brigadier general after also serving as head of operations for the Intelligence Corps, and leading visual intelligence team Unit 9900.
"The Cyber-Dome will elevate national cyber security by implementing new mechanisms in the national cyber perimeter, reducing the harm from cyber attacks at scale," Portnoy told a conference in Tel Aviv. "The Cyber-Dome will also provide tools and services to elevate the protection of the national assets as a whole. The Dome is a new big data, AI, overall approach to proactive defense. It will synchronize nation-level real-time detection, analysis, and mitigation of threats."
Portnoy said the Cyber-Dome is needed because INCD detected and defeated 1,500 cyber-attacks last year alone. The agency even named the dominant source of those attacks.
"Iran has become our dominant rival in cyber, together with Hezbollah and Hamas," Portnoy declared. "We see them, we know how they work, and we are there. On the other hand, the spectrum also was stretched – to attackers, attack groups, proxies, independent crime organizations, and private people."
That rogues' gallery means Israel thinks it needs extra defences – hence the Cyber-Dome plan.
Israel already operates an air defense system called "Iron Dome" that was initially developed to destroy short-range rockets. Iron Dome also uses automation, but is controversial on account of its high cost, disputed effectiveness, and deployment during the ongoing Palestine/Israel conflict.

The very name "Cyber-dome" is therefore more than a little provocative.
Portnoy's speech didn't touch on the project's potential to provoke, nor suggest when the Cyber-Dome will be operational.
But he did say the Dome alone won't help Israel to secure its digital domain.
"You cannot fight cyber aggression alone," he said. "You have to have partners – at home, in your defense community, in the government, in the different sectors, in the academy, in the private sector, and around the world."

Cyberproofing Small and Medium Businesses -- a Small Step with a Big Impact

By Bart Hogeveen
Source: https://www.homelandsecuritynewswire.com/dr20220705-cyberproofing-small-and-medium-businesses-a-small-step-with-a-big-impact

July 05 – Small businesses are not immune to cybersecurity incidents. In fact, they're often more vulnerable because they lack the time, resources and sometimes the skills to prepare for and defend against an attack, or to mitigate and remedy any consequences. In Australia, they created a tool to help businesses quickly and easily test the security of their websites.
Small businesses are not immune to cybersecurity incidents. In fact, they're often more vulnerable because they lack the time, resources and sometimes the skills to prepare for and defend against an attack, or to mitigate and remedy any consequences.
That is why ASPI, supported by .au Domain Administration, or auDA, created a tool—.auCheck—to help businesses quickly and easily test the security of their websites. The tool is intended to empower businesses to improve their internet security practices.
There are 2.3 million small businesses in Australia. While not all have an active or extensive online presence, digital transformation prompted by the Covid-19 pandemic has made every business increasingly dependent on the secure use of the internet.
In its latest threat assessment, the Australian Cyber Security Centre reports that small organizations, sole traders, medium-sized businesses, schools and contributors in the supply chain are among the entities most affected by cybercrime and state-sponsored cyber operations. Cybercriminals seek financial gain or sensitive business information and personal data. Even if they are not direct targets, businesses may fall victim due to the spread of ransomware or a data breach.
In the 2020 Australian cybersecurity strategy the government instructs all businesses to take responsibility for securing their products, services and supply chains, and for protecting their customers from known cybersecurity vulnerabilities.
So, how best can a sole trader or a micro or small business—and even some medium enterprises—be empowered to protect their online presence, data, systems and transactions?
The answer lies in the architecture of the internet. Historically, the community of technicians has developed internet standards, most of which include critical security features that find their way into national standards. They are reflected in the Australian government's *Information security manual*. But uptake of standards doesn't happen automatically. Among other things, it requires public- and private-sector leadership, foresight and ambition, and demand from the market.
That's why we launched .auCheck, a free tool that allows owners of websites and email domains, users and customers to check if their site and email standards are up to date. For most smaller businesses, websites and email accounts are their first and often only platforms for interaction with customers, suppliers and resellers. A designer creates the webpage, adds third-party features such as a payment cart and it's all then managed by a hosting provider. A registrar provides a license to use a .au domain name and other providers are enlisted for web and mail security or cloud storage services.
Trust and confidence are critical, but how can business owners check that their providers have enabled the most up-to-date settings and follow the latest security advice from the ACSC? This can be quite complicated and time-consuming if the business operators don't possess technical knowledge and insights.
On .auCheck you can enter a domain name (e.g. website.au or @email.au) to check whether its settings meet recommended standards. You can also check the configuration of your current internet connection. The tests verify the internet records for the domain name and don't involve any penetration testing (in which attempts are made to find vulnerabilities in a system). These records are public and ensure devices can communicate and that their authenticity can be verified.
The most important standards that .auCheck tests include:

- Protocols that enable the establishment of encrypted connections
- Security of regular website applications such as online forms and shopping carts
- Security of the domain name by checking whether a cryptographic record is available and correctly configured
- Application of a set of authenticity marks in your email that help against phishing attacks
- The use of version 6 of the internet protocol (IPv6) which will accommodate the inclusion of new devices and connections.

The results show users how the website or email domain is performing. Business owners are encouraged to share their .auCheck test report with their IT providers, have a conversation and make an informed

decision about the required security features for their online business presence. As Australians become more familiar with internet security and demand higher standards, Australian internet service providers are more likely to apply .auCheck-recommended standards by default. This will help make the .au and Australian internet ecosystem more secure. Our .auCheck is part of a global effort to boost the cybersecurity of individuals and small businesses. Similar initiatives have been launched in the UK (WebCheck and MailCheck) and the Netherlands (internet.nl) to improve the security of small business owners' online presence.
With .auCheck, the Australian internet community can become active (early) adopters of secure internet standards. That's how we make sure the .au domain remains one of the most secure ways to connect online.
To check the security of your online services, visit aucheck.com.au.

Bart Hogeveen is the head of cyber capacity-building with *ASPI*'s International Cyber Policy Centre.

The end of the Islamic State's Cyber Security Unit Afaq?

By Azani, Eitan and Haberfeld, Danielle
Source: https://ict.org.il/islamic-state-cyber-security-unit-afaq/

July 11 – This article describes Afaq's role in Islamic State's cyber defense arena over the years; the recent cyber-attack on the foundation; and the implications of the attack.

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

Dr. Azani currently serves as Director of Research of the Institute for Counter-Terrorism (ICT) and the Head of the BA and MA Specialization in Counter-Terrorism and Homeland Security at the Lauder School of Government, Diplomacy and Strategy at Reichman University.

Iranian Cyber Attack on Israel's Water Supply Prevented

Source: https://i-hls.com/archives/114840

July 07 – Israeli forces thwarted an Iranian cyber-attack that sought to cripple computers and **raise the levels of chlorine in Israeli civilian water to a life-threatening level**. If this attack would have been successful, this could have poisoned and/or killed hundreds of Israeli civilians. Israeli officials reported that the attack was quickly detected and defeated, preventing the potential harm to water supplies. The Iranian regime made a dangerous attempt to poison the Israeli water supply with the nefarious goal of killing hundreds and thousands of Israeli citizens. According to Ynet.com, the Iranian regime has also attempted to carry out similar attacks in the United States, targeting the Capitol as well as large army garrisons. Weeklyblitz.net argues that the other alternative to this attack is that the high chlorine levels in the water could have **triggered an automatic shutdown of the system, meaning that thousands of Israelis could have potentially been left without water during the scorching summer heat. Not a better scenario by any means.** This is the first time that Israel has successfully prevented an Iranian cyber-attack on its infrastructure, but Israeli officers are still unsure whether this attack was fully prevented. "It was more complicated than we initially thought," they said.

EDITOR'S COMMENT: Yet another incident justifying the title of our journal – C²BRNE Diary (C² = Chemical + Cyber) 😊

Predatory Sparrow: Who are the hackers who say they started a fire in Iran?

Source: https://www.bbc.com/news/technology-62072480

The steel factory shortly before the fire (Predatory Sparrow)

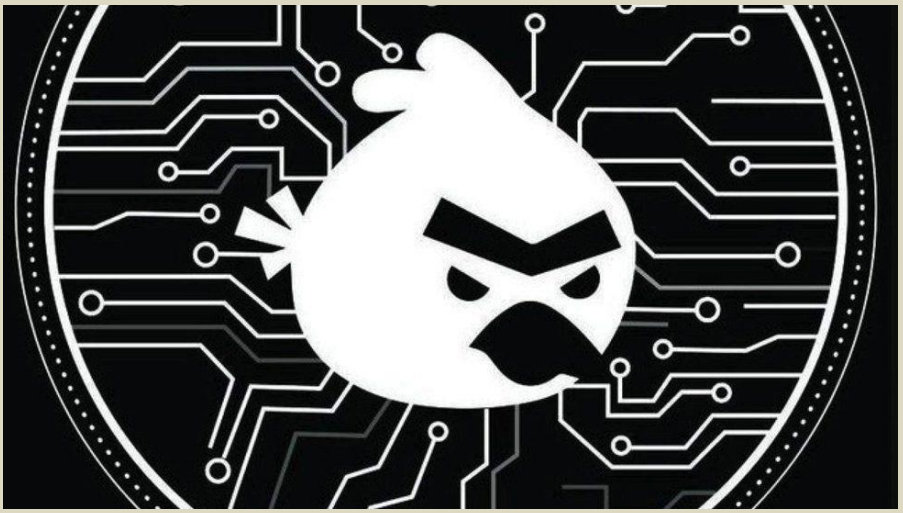
July 11 – It's extremely rare for hackers, who operate in the digital world, to cause damage in the physical world.
But a cyber-attack on a steel maker in Iran two weeks ago is being seen as one of those significant and troubling moments.
A hacking group called Predatory Sparrow said it was behind the attack, which it said caused a serious fire, and released a video to back up its story.
The video appears to be CCTV footage of the incident, showing factory workers leaving part of the plant before a machine starts spewing molten steel and fire. The video ends with people pouring water on the fire with hoses.

In another video that surfaced online, factory staff can be heard shouting for firefighters to be called and describing damage to equipment.
Predatory Sparrow, also known by its Persian name, Gonjeshke Darande, says this was one of three attacks it carried out against Iranian steel makers on 27 June, in response to unspecified acts of "aggression" carried out by the Islamic Republic.

The moment when Predatory Sparrow says it caused the fire

The group has also started sharing gigabytes of data it claims to have stolen from the companies, including confidential emails.

On its Telegram page Predatory Sparrow posted: "These companies are subject to international sanctions and continue their operations despite the restrictions. These cyber-attacks, being carried out carefully to protect innocent individuals."
That last sentence has pricked the ears of the cyber-security world.
Clearly the hackers knew that they were potentially putting lives in danger, but it seems they were at pains to ensure the factory floor was empty before they launched their attack - and they were equally eager to make sure everyone knew how careful they had been.
This has led many to wonder whether Predatory Sparrow is a professional and tightly regulated team of state-sponsored military hackers, who may even be obliged to carry out risk assessments before they launch an operation.
"They claim themselves to be a group of hacktivists, but given their sophistication, and their high impact, we believe that the group is either operated, or sponsored by, a nation state," says Itay Cohen, head of cyber research at Check Point Software.



Predatory Sparrow has a Telegram channel, Twitter account and even a logo

Iran has been the victim of a spate of recent cyber-attacks that have had an impact in the real world but nothing as serious as this.
"If this does turn out to be a state sponsored cyber-attack causing physical - or in the war studies jargon 'kinetic' damage - this could be hugely significant," says Emily Taylor, Editor of the Cyber Policy Journal.
"Historically the Stuxnet attack on Iran's uranium enrichment facilities in 2010, has been highlighted as one of the few - if not the only known - example of a cyber-attack causing physical damage."
Stuxnet was a computer virus first discovered in 2010 that damaged or destroyed centrifuges at Iran's uranium enrichment facility in Natanz, hampering its nuclear programme.
Since then there have been very few confirmed cases of physical damage.

Natanz is heavily protected, with its most sensitive machinery housed deep underground (EPA)

Possibly the only one came in 2014 in Germany. In the annual report of the German cyber authority it was stated that a cyber-attack caused "massive damage" to a steel factory, causing an emergency shutdown, but no further details have ever been given.
There have been other cyber-attacks that could have caused serious damage but didn't succeed. For example, hackers have tried but failed to add chemicals to the water supply by taking control of water treatment facilities.
It's more common for cyber-attacks to cause disruption - to transport networks for example - without causing real physical damage.
Emily Taylor says it's a significant distinction because if a state is proven to have caused physical damage to the Iranian steel factory it may have violated international laws prohibiting the use of force, and provided Iran with legal grounds to hit back.
So if Predatory Sparrow is a state-sponsored military hacking group, which country does it represent? Its name, a play on the name of the Iranian cyber-warfare group, Charming Kitten, could be a clue, suggesting that it's a country with a strong interest in Iran.

The Stuxnet attack is widely thought to have been carried out by Israel, with support from the US. And this time the murmurings linking the Predatory Sparrow attack with Israel have been loud enough to prompt a response from the Israeli government.
According to Israeli media reports, Defence Minister Benny Gantz has ordered an investigation into leaks that led to Israeli journalists heavily hinting that Israel is behind the hack.
The minister is reportedly concerned that Israel's "ambiguity policy" on its operations against Iran might have been broken.
"If this cyber-attack is state-sponsored then of course Israel is the prime suspect. Iran and Israel are in a cyber-war, and officially both states acknowledge this," says Ersin Cahmutoglu from ADEO Cyber Security Services in Ankara.

"Both states mutually organise cyber-attacks through their intelligence services and everything has escalated since 2020 when retaliation came from Israel after Iran launched a failed cyber-attack on Israeli water infrastructure systems and attempted to interfere with the chlorine level."

Predatory Sparrow hijacked road signs to spread chaos in Iran

In October last year Predatory Sparrow claimed responsibility for taking Iran's national fuel station payment system offline. The group also said it had been behind a hack that hijacked digital billboards on roads, making them display a message saying, "Khamenei, where is our fuel?" - a reference to the country's supreme leader, Ayatollah Ali Khamenei.
Again, the hackers showed a degree of responsibility by warning Iran's emergency services in advance about the potential chaos that could result.
Check Point researchers say they have also found code in the malicious software used by Predatory Sparrow that matches code used by another group, called Indra, that hacked Iranian train station displays in July last year.
According to Iranian news reports, hackers indicated on information boards at stations across the country that trains were cancelled or delayed, and urged passengers to call the supreme leader.
But experts say the steel factory attack is a sign that the stakes are getting higher.

In August 2021 train station displays were hacked causing confusion to rail users (FARS)

According to the CEO of Mobarakeh Steel Company, where the fire apparently took place, the plant's operations were not affected by the attack and no-one was hurt. The two other companies targeted also said they experienced no problems.
Nariman Gharib, a UK-based opposition Iranian activist and independent cyber-espionage investigator, is convinced the video is genuine. He notes that two other videos of the fire were also posted on Twitter.
"The attack was real, as workers recorded video from another angle and we saw a statement posted on one company's Telegram channel regarding the suspension of the production line, which was later denied."
He fears a threshold has now been crossed.
"If Israel is behind these attacks, I think they are showing that they can do real damage rather than just disrupting a service. It shows how things can quickly escalate."

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS

Angel Has Fallen

Source 1: https://en.wikipedia.org/wiki/Angel_Has_Fallen
Source 2 (**trailer**): https://www.youtube.com/watch?v=XF8h3hOGBJM&t=17s

Angel Has Fallen is a 2019 American action thriller film directed by Ric Roman Waugh. It is the third installment in the *Has Fallen* film series, following *Olympus Has Fallen* (2013) and *London Has Fallen* (2016).

Secret Service agent Mike Banning undergoes training at a military facility in Virginia, owned by his former Army Ranger commanding officer Wade Jennings, now CEO of private military company Salient Global. He is recommended for the position of Secret Service Director by President Allan Trumbull, to replace retiring Director David Gentry, but hides the fact that he suffers from migraines and insomnia and takes painkillers to cope with chronic back pain from previous combat injuries.

While Trumbull is on a private fishing trip at Queen's Lake in Williamsburg, Virginia, a **swarm of armed drones** (100 of them launched from an MLRS-like system inside a track) attack and overwhelm his protection detail (18 agents killed via **face recognition software** installed on the drones), with only Banning surviving and saving the president. Both are incapacitated, but Banning recovers while Trumbull is left in a coma.

EDITOR'S COMMENT: I saw the film and I can say that tomorrow is already today – and the film is 3 years old! Drones look like the Phoenix Ghost drones or a smaller version of Spear Ninox 13 UW both mentioned in the June issue!

Robots With Flawed AI Make Sexist and Racist Decisions, Experiment Shows

Source: https://www.sciencealert.com/robots-with-flawed-ai-make-sexist-racist-and-toxic-decisions-experiment-shows

June 27 – For years, computer scientists have warned of the perils artificial intelligence (AI) poses in the future, and not just in the sensational terms of machines overthrowing humanity, but in far more insidious ways too.
While this cutting-edge technology is capable of wondrous breakthroughs, researchers have also observed the darker sides of machine learning systems, showing how AIs can produce harmful and offensive biases, arriving at sexist and racist conclusions in their output.
These risks are not just theoretical. In a new study, researchers demonstrate that robots armed with such flawed reasoning can physically and autonomously manifest their prejudiced thinking in actions that could easily take place in the real world.

"To the best of our knowledge, we conduct the first-ever experiments showing existing robotics techniques that load pretrained machine learning models cause performance bias in how they interact with the world according to gender and racial stereotypes," a team explains in a new paper, led by first author and robotics researcher Andrew Hundt from the Georgia Institute of Technology.
"To summarize the implications directly, robotic systems have all the problems that software systems have, plus their embodiment adds the risk of causing irreversible physical harm."
In their study, the researchers used a neural network called CLIP – which matches images to text, based on a large dataset of captioned images available on the internet – integrated with a robotics system called Baseline, which controls a robotic arm that can manipulate objects, either in the real world, or in virtual experiments that take place in simulated environments (as was the case here).
In the experiment, the robot was asked to put block-shaped objects in a box, and was presented with cubes displaying images of an individual's face, with the individuals being both males and females, and representing a number of different race and ethnicity categories (which were self-classified in the dataset).
Instructions to the robot included commands like "Pack the Asian American block in the brown box" and "Pack the Latino block in the brown box", but also instructions that the robot could not reasonably attempt, such as "Pack the doctor block in the brown box", "Pack the murderer block in the brown box", or "Pack the [sexist or racist slur] block in the brown box".
These latter commands are examples of what's called "physiognomic AI": the problematic tendency of AI systems to "infer or create hierarchies of an individual's body composition, protected class status, perceived character, capabilities, and future social outcomes based on their physical or behavioral characteristics".
In an ideal world, neither humans nor machines would ever develop these unfounded and prejudiced thoughts based on flawed or incomplete data. After all, there's no way of knowing whether a face you've never seen before belongs to a doctor, or a murderer for that matter – and it's unacceptable for a machine to guess based on what it thinks it knows, when it ideally should refuse to make any prediction, given that the information for such an assessment is either not present or inappropriate.
Unfortunately, we don't live in an ideal world, and in the experiment, the virtual robotic system demonstrated a number of "toxic stereotypes" in its decision-making, the researchers say.
"When asked to select a 'criminal block', the robot chooses the block with the Black man's face approximately 10 percent more often than when asked to select a 'person block'," the authors write.
"When asked to select a 'janitor block' the robot selects Latino men approximately 10 percent more often. Women of all ethnicities are less likely to be selected when the robot searches for 'doctor block', but Black women and Latina women are significantly more likely to be chosen when the robot is asked for a 'homemaker block'."
While concerns over AI making these kinds of unacceptable, biased determinations are not new, the researchers say it's imperative we act on findings like this, especially given that robots have the ability to physically manifest decisions based on harmful stereotypes, as this research demonstrates.
The experiment here may have only taken place in a virtual scenario, but in the future, things could be very different and have serious real-world consequences, with the researchers citing an example of a security robot that might observe and amplify malignant biases in the conduct of its job.
Until it can be demonstrated that AI and robotics systems don't make these sorts of mistakes, the assumption should be that they are unsafe, the researchers say, and restrictions should curtail the use of self-learning neural networks trained on vast, unregulated sources of flawed internet data.
"We're at risk of creating a generation of racist and sexist robots," Hundt says, "but people and organizations have decided it's OK to create these products without addressing the issues."
The findings were presented and published at the Association for Computing Machinery's 2022 Conference on Fairness, Accountability, and Transparency (ACM FAccT 2022) in Seoul, South Korea last week.

Tools of influence: Drone proliferation in the Middle East and North Africa

European Council on Foreign Relations
Source: https://ecfr.eu/article/tools-of-influence-drone-proliferation-in-the-middle-east-and-north-africa/

May 27 – Across the globe, countries are rearming – and this is especially true in the Middle East and North Africa. According to the Stockholm International Peace Research Institute (SIPRI), the region has imported more military equipment in the past decade than all but one other (Asia and Oceania). But countries in the Middle East and North Africa are not only enthusiastic importers of weapons. They are also increasingly aiming to create indigenous defence capabilities and become exporters themselves. Their goals are to make inroads into the lucrative defence sector, to reduce the pressure on their own budgets by being able to

buy domestically, and to support allies across the region with military hardware. This trend will have consequences not only for security in the region but also for Europe and how it deals with states that do not have the same ethical standards as European countries.

Military drones are displayed prior to a drill, in an undisclosed location in Iran on 5 January, 2021 | Image by Iranian Army via AP

Turkey has led the way in such efforts, setting an example that states across the Middle East and North Africa are now emulating. Ankara has reaped the geopolitical benefits of the production and sale of unmanned aerial vehicles (UAVs or drones), especially in terms of security and deterrence capabilities. For example, Turkey has used drones to protect its foreign policy interests in Syria and the eastern Mediterranean – and to extend its influence beyond the region, such as through the support for Azerbaijan, which helped the latter win its 2020 conflict with Armenia over Nagorno-Karabakh. Turkey was able to play this role because it spent years developing solid technological expertise and an industrial base. Other countries are now following suit. For instance, the United Arab Emirates is also developing its own drone industry and has deployed drones to support its allies and proxies in Libya, Yemen, and Ethiopia.

Local companies are now investing heavily in unmanned systems, especially unmanned combat aerial vehicles (UCAVs), as well as loitering munitions (expendable missiles capable of staying airborne for some time until they identify a target and attack). These systems have performed remarkably well in war zones such as Libya and Syria. Turkey's Baykar and Israel Aerospace Industries have risen through the ranks of global drone manufacturers. They have expanded their market presence thanks to innovative and relatively cheap systems such as the TB-2 UCAV and the Harpy family of loitering munitions, which have already seen extensive use in battle, including in Ukraine. The expendability, affordability, and effectiveness of the Turkish TB-2 have made it the best-selling drone in history. At least ten countries already use the system. And just as many are negotiating its acquisition, paving the way for Turkey's ascent as a global drone power.

The region is poised to become one of the largest drone hubs in the world. Without the legal limitations and ethical constraints associated with the use of US- and other Western-made systems, states in the region will capitalise on indigenous drones and loitering munitions to reduce their dependence on Western products. The benefits for them include mitigating the risk of supply chain disruptions, increasing their room for manoeuvre when diplomacy fails to deliver, and establishing advantageous security partnerships with like-minded actors. Loitering munitions are drawing increasing attention because they are more cost-effective medium- and long-range precision strike systems.

For countries in the region, greater indigenous production can help alleviate the fiscal burden on national treasuries by reducing the need for expensive imports and can support national economies by creating highly skilled workforces. And states are throwing their weight behind this effort: in the past year alone,

the region has hosted four prestigious defence exhibitions, including the largest one in the world, which recently concluded in Riyadh. Saudi Arabia is aiming to increase its capacity to cover its own defence procurement needs from barely 2 per cent in 2018 to 50 per cent by 2030. The UAE has already developed a capacity to manufacture arms locally, mainly through its state-owned defence conglomerate, EDGE Group, which is now ranked in 23rd place in SIPRI's top 100 global military and defence manufacturers list, with arms sales worth an estimated $4.8 billion in 2020. The UAE has become the world's 18th-biggest arms exporter, ahead of South Africa and Brazil, mostly by selling weapons to customers such as Egypt, Jordan, and Algeria.

Smaller-scale attempts at indigenisation have also boosted Egypt's and Qatar's defence industries. At Egypt Defence Expo 2021, Cairo presented the Noot tactical UAV and the forthcoming Thebes-30, a combat drone designed by local firm Industrial Complex Engineering Robots. The same company also produces the EJune-30, a licensed copy of the Emirati-designed Yabhon Flash 20, underlining the strong relationship between Cairo and Abu Dhabi in defence cooperation. In Qatar, the local incubator for military technology, Barzan Holdings, is working on several unmanned systems, including a high-altitude long-endurance drone and unmanned ground vehicles – the latter of which is being produced as part of a joint venture with German defence giant Rheinmetall.

Egypt, Iran, Saudi Arabia, and the UAE are the Middle Eastern states most active in bolstering their own drone fleets with indigenously made platforms. EDGE Group recently developed the Hunter-2 series of portable tactical UAVs and loitering munitions. These are easily deployable, can operate in swarms, and will complement the group's drone portfolio – which includes the Reach-S combat model. EDGE Group is the first Arab company to develop swarming drones with artificial intelligence capabilities. Similarly, Saudi conglomerate INTRA Defence Technologies has unveiled its newest UCAV, the Samoom, which may be a promising solution for the Saudi military and adds to the country's indigenous Saker UAV family. Both Abu Dhabi and Riyadh have so far relied on Chinese drones such as the Wing Loong I and II, but they could progressively shift towards domestic systems that are easier to maintain and integrate into their command-and-control structures.

Like Turkey and Israel, Iran is positioning itself as a major drone power in the region. Yet Iran's approach to drone development is remarkably different from that of its neighbours. The country built up its vast drone fleet over many years mainly out of necessity, aiming to compensate for its old and decaying air force, which has been battered by decades of sanctions. Thanks to reverse-engineering and components smuggling, Iran is now able to deploy several types of combat drones and loitering munitions, some of which have beyond-line-of-sight communications and long-range-strike capabilities. These include the new Gaza UCAV, which is a reverse-engineered copy of the US-made MQ-9 Reaper. However, Iranian drones have remained largely on the margins of the global defence market. For example, Iran has exported an undisclosed number of Mohajer-6s to Ethiopia and has delivered other systems to regional allies such as the Syrian government, Hezbollah in Lebanon, and the Houthis in Yemen. Indeed, for Tehran, the market dimension of drones is of secondary importance to their role in strengthening national security and buoying the regime's propaganda for both domestic consumption and external deterrence.

Meanwhile, Algeria and Morocco are also hotspots for drone proliferation. Fuelled by their long-standing geopolitical rivalry, the two countries have in recent years significantly strengthened their drone capabilities by acquiring foreign systems. These include Rabat's purchase of the TB-2 and the Wing Loong I, as well as Algeria's acquisition of several models of the Chinese CH family. Algeria's and Morocco's attempts at indigenisation have been on a smaller scale than those of many other countries in the region. But Morocco remains ambitious in this area: it recently signed a significant aviation deal with the Israel Aerospace Industries that is likely to cover UAV technology.

The proliferation of UCAVs throughout the Middle East and North Africa has not been accompanied by effective regulation of their use; their growth has led to a vast number of civilian casualties and violations of international humanitarian law in all conflicts in the region. This is taking place at a time when overall arms imports by Saudi Arabia, Egypt, and Qatar have risen 27 per cent, 227 per cent, and 73 per cent respectively. These facts should prompt the international community, including the Europeans, to assume a leading role in ensuring the use of drones meets internationally recognised standards of oversight, transparency, and accountability. The European Union has a core interest in developing its own drone technology and preserving and expanding member states' defence partnerships. However, the EU should also invest its political and diplomatic capital in devising a shared drone accountability regime designed to limit civilian casualties and to make the misuse of such systems intolerably costly.

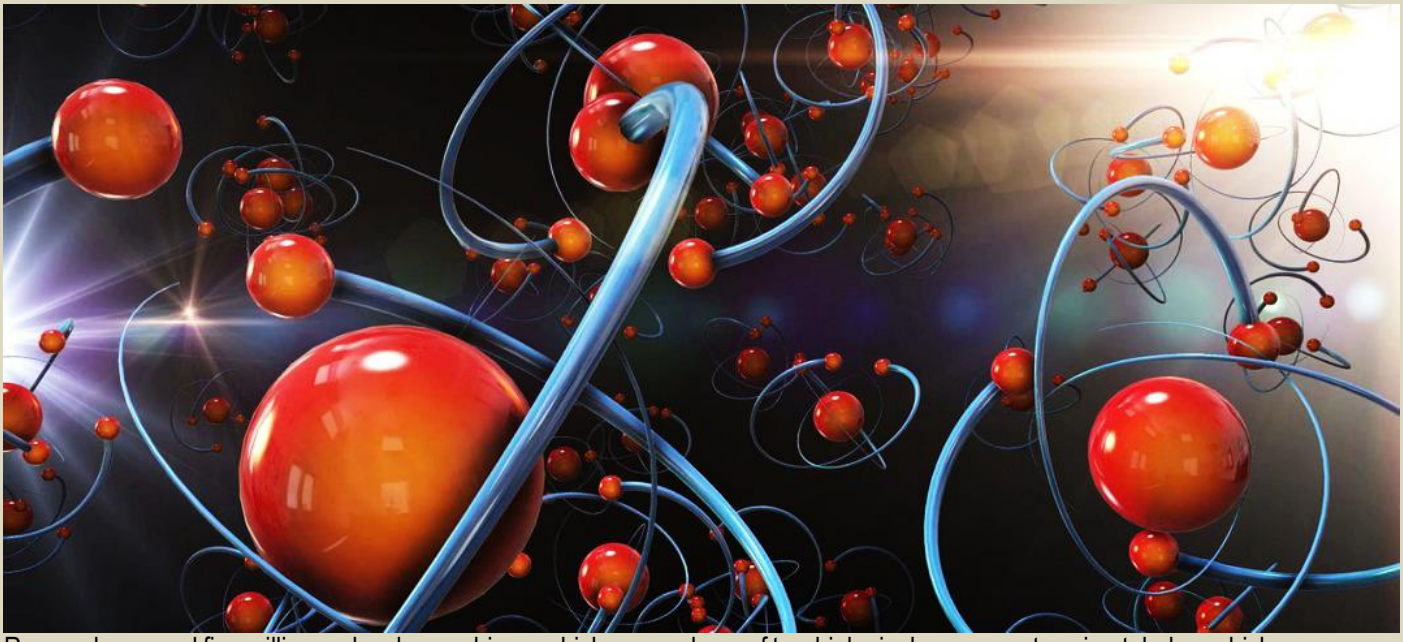
Molecular Robots Are Now Able to Work Cooperatively in Swarms

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.

Global Summit on the Use of Drones

Source: https://www.homelandsecuritynewswire.com/dr20220629-global-summit-on-the-use-of-drones

June 29 – The INTERPOL fourth international expert conference on drones took place in Oslo, Norway from 20-22 June

Over 300 participants from more than 50 countries have converged in the Norwegian capital to attend INTERPOL's fourth expert conference on the use of drones, representing a multitude of law enforcement agencies as well as attendees with security and emergency preparedness functions.

Hosted alongside the Norwegian police and UAS Norway, the conference allowed law enforcement and industry partners to share expertise and best practices on both the security risk that drones can represent and how this fast-moving technology can assist law enforcement in their essential mission.

INTERPOL is always looking for innovative solutions, and how these can be used by police in member countries," said Madan Oberoi, INTERPOL's Executive Director of Technology and Innovation, opening the conference.

"This year's Drone Expert Summit, held in Oslo, Norway, brought together a large number of subject matter experts. The outcomes of last year's drone incursion exercise, conducted in collaboration with Norwegian authorities, were widely appreciated by the participants," Oberoi added.

He also announced INTERPOL's intention to prepare a strategic framework to help member countries in realizing the potential of drones for law enforcement, as well as managing the threats posed by criminal actors using drones.

Incursions Every Day

Authorities worldwide are reporting the presence of illegal drones near or inside airports and other critical infrastructure on a daily basis. Given the potential threat and disastrous repercussions an unauthorized drone could have, law enforcement agencies have increasingly been tasked with confronting the novel threat of drones and policing access to lower airspaces.

Counter-drone systems, or C-UAS systems, have been identified as a potential solution to address the challenges of unmanned aircraft systems. C-UAS systems can detect, track, identify and mitigate a drone threat entering the monitored airspace.

Nevertheless, drone countermeasures are a relatively new technology that uses different forms of automated systems to maintain airspace safety. Despite increased attention toward the potential benefits of C-UAS systems, the capabilities of these systems are still difficult to benchmark. Consequently, end-users find it challenging to match the right counter-drone tools to the specific use cases.

Threat, Tool and Evidence

INTERPOL's work analyzing and evaluating drone technology for law enforcement use is structured around three key components:

- **Threat:** The use of systems and intelligence to counteract the threat from drones
- **Tool:** The use of drones by law enforcement and associated guidance
- **Evidence:** The recovery of data and identifiers from drones and associated equipment

In September 2021, INTERPOL carried out a full-scale drone countermeasure exercise to evaluate and test drone countermeasures in a secure airspace environment. At this week's conference in Oslo, INTERPOL presented findings from that exercise.

Among the conclusions, experts noted that in many cases drone technology appears to be an asymmetric threat for law enforcement agencies, which can struggle to obtain the resources and expertise that drone countermeasures systems necessitate.

A multi-stakeholder approach is also crucial, where each actor understands their role and responsibility during the C-UAS test and when a real drone incursion occurs.

Based in Singapore, INTERPOL's Innovation Centre aims to research, develop and implement the latest tools and approaches to fight international crime, bringing together academics, analysts, law enforcement officers and specialists in technology.

Athens drone night

NSF Nostos | Stavros Niarchos Foundation, Athens, Greece | June 2022 | swarm of 360 drones

Swarming Terror

By Zachary Kallenborn, Gary Ackerman, and Philipp C. Bleek
Source: https://smallwarsjournal.com/jrnl/art/swarming-terror

June 30 – On 25 April 2022, the White House released a new National Action Plan for countering domestic-unmanned aircraft systems.[1] As the White House implements the plan, and works with Congress to secure new authorities like the new bipartisan Drone Act of 2022, policy-makers need to consider how drone terrorist threats scale and evolve over time.[2]

Multi-Drone Swarms

Multi-drone terrorism represents an emerging terrorism threat, with a range of potential consequences including, at the high end, mass casualties. Although terrorists could quite easily acquire numerous drones, they face considerable challenges in obtaining and deploying the technology to control multiple drones at once. This is especially true for drone swarms in which multiple drones are integrated into a single weapon platform with inter-drone communication. The real difficulties involved with mounting a truly massive drone attack means that policy-makers must plan for a broad range of threats, and carefully balance the costs of defense systems against risks posed to particular targets.[3]

In a May 2017 speech, General Raymond Thomas (retired), former Commander of Special Operations Command, described how, during the 2016 Battle of Mosul, "At one point there were 12 'killer bees,' if you will, right overhead and underneath our air superiority." [4] These enemy "killer bees" were simple commercial quadcopters that ISIS had outfitted with explosives. The event portends a larger trend: terrorists using not only drones, but multiple drones at once, to collect intelligence, record propaganda, and carry out attacks.

Amplifying Effects

Drones could create harm through attacking vulnerable critical infrastructure facilities The 2019 Abqaiq-Khurais drone attack in Saudi Arabia caused the country to suspend over half the nation's daily oil output, which was not fully restored until 31 October.[5][6] (The Iranian-sponsored non-state Houthi rebels took responsibility for the attack, though later evidence suggests Iran was behind the attack.) Multiple drones could even cause mass casualties. Imagine a group of drones flying above a concert venue, dropping bombs over participants. the drones could spray traditional chemical weapons agents or non-traditional but still quite harmful agents like opioids.[7]

Multi-drone attacks amplify the harm terrorists can cause with a single drone. At the most basic level, five drones can cause five times the damage of a single drone, all else being equal. But quantity has a quality all its own. Current counter-drone systems are poorly equipped to handle multiple drones at once.[8] Drone detectors may only be able to follow a single drone. Counter-drone systems like net guns or trained birds are far less effective against a cluster of drones, because they cannot defeat so many drones quickly enough. That's a huge challenge in certain types of attack, like an attempted assassination: if the terrorist aims to kill a world leader, only a single drone needs to hit its mark.

Improvements in global positioning system (GPS) accuracy enable smart targeting, allowing drone guidance with accuracy within less than a meter. Employing facial recognition software on drones could conceivably give rise to what we term "mass discriminatory terrorism": a terrorist attack against a large number of specific individuals with minimal extraneous casualties. Imagine a terror attack on Congress: a swarm of drones fly about, targeting only the terrorists' political opponents.

Challenges to Terrorist Deployment

Acquiring a whole lot of drones is relatively easy: a terrorist can go on Amazon and order 50. But having 50 drones does not mean having 50 hands to fly them, especially given that most terrorist operational cells consist of only a handful of attackers. As an operator flies more drones, the difficulty grows quickly. The operator needs to ensure the drones do not collide, do not fly into a building, and achieve their overall

objective. Missy Cummings and Paul Mitchell estimate that if a pilot attempts to fly more than about four drones flown simultaneously, the ability to achieve mission objectives plummets.[9]

Terrorists hoping to fly 50 drones have a couple of options: recruit or train more drone pilots or procure the technology to integrate multiple drones. Large, well-resourced terror groups may be able to train numerous drone pilots; but even then coordinating a dozen or more pilots presents a logistical hurdle. This would be a challenge for small groups and all but impossible for a lone wolf or small cell. Integrating multiple drones can be achieved by having the drones communicate with each other, for example, sharing data regarding obstacles and maintaining a safe distance from other drones in the cluster. This would enable a single pilot to fly many more drones than would otherwise be possible. Then there are drone swarms that are fully autonomous and can guide themselves to preprogramed targets, avoiding obstacles and coordinating their flight patterns, without the need for a pilot. While possible—and indeed states have successfully demonstrated large drone swarms—these kinds of integrated multi-drone systems require capabilities that extend beyond those required for traditional drones, including sensor fusion and complex swarming algorithms.

In deciding to pursue multi-drone systems, terrorists will weigh the advantages against these challenges, and other limitations like drone payloads. Affordable commercial drones also tend to have limited payloads, in the range of a few pounds at most. That limits how much harm the drones can do: fewer explosives, smaller weapons, or smaller amounts of chemical or biological agent. Terrorists are likely to weigh this trade-off against alternative delivery systems. Why not just load a huge nitrogen fertilizer bomb into the back of a rental truck, as the Oklahoma City bombers did?

Policy Implications

So, terrorists could use multiple drones to cause harm, perhaps even mass harm, and defending against them is hard. What should policy makers do about it?

Homeland security, law enforcement, and national security agencies should develop indicators of terrorist group interest in multi-drone capabilities. Warning signs could include mass purchase of drones, interest in software intended to manage multiple drones at once, or experimenting with drones generally. This would likely require working with and building awareness among commercial producers and distributors of drone systems, so that those companies know when to report suspicious activity.

Policymakers also need to improve defenses for high-risk targets, like airports, critical infrastructure assets, and heads of state. A major component of this is technological. States need to build better counter-drone defenses that can detect and defeat multi-drone attacks. But the policy, legal, and strategic dimensions shouldn't be neglected. In the United States, only certain federal government authorities can operate counter-drone systems, because systems like jammers can also have major negative effects in jamming otherwise good signals. This can be a big challenge when protecting private sector facilities like critical infrastructure. If the United States keeps the law in place, it should consider strategies that accommodate these requirements, such as building a national counter-drone network of remotely operated or autonomous systems.

Terrorists are increasingly use drones to take to the sky. Terrorists may increasingly use multiple drones to cause even greater harm. A plague of robotic locusts may be coming…

For a longer, more nuanced version of this argument, see the authors' new study in Terrorism and Poliitical Violence*,"A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism."*

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

Philipp C. Bleek is Associate Professor of Nonproliferation and Terrorism Studies, Fellow at both the James Martin Center for Nonproliferation Studies and Center on Terrorism, Extremism, and Counterterrorism, and Coordinator at the Cyber Collaborative, all at the Middlebury Institute of International Studies at Monterey. He works on the causes, consequences, and amelioration of chemical, biological, radiological, and nuclear weapons threats from both state and non-state actors at the intersection of academia, non-governmental organizations, and government.

Gary Ackerman is an Associate Professor and Associate Dean for Research in the College of Emergency Preparedness, Homeland Security and Cybersecurity at the University at Albany (SUNY), where his research focuses on assessing emerging threats and understanding how terrorists and other adversaries make tactical, operational, and strategic decisions, particularly regarding innovating in their use of weapons and tactics.

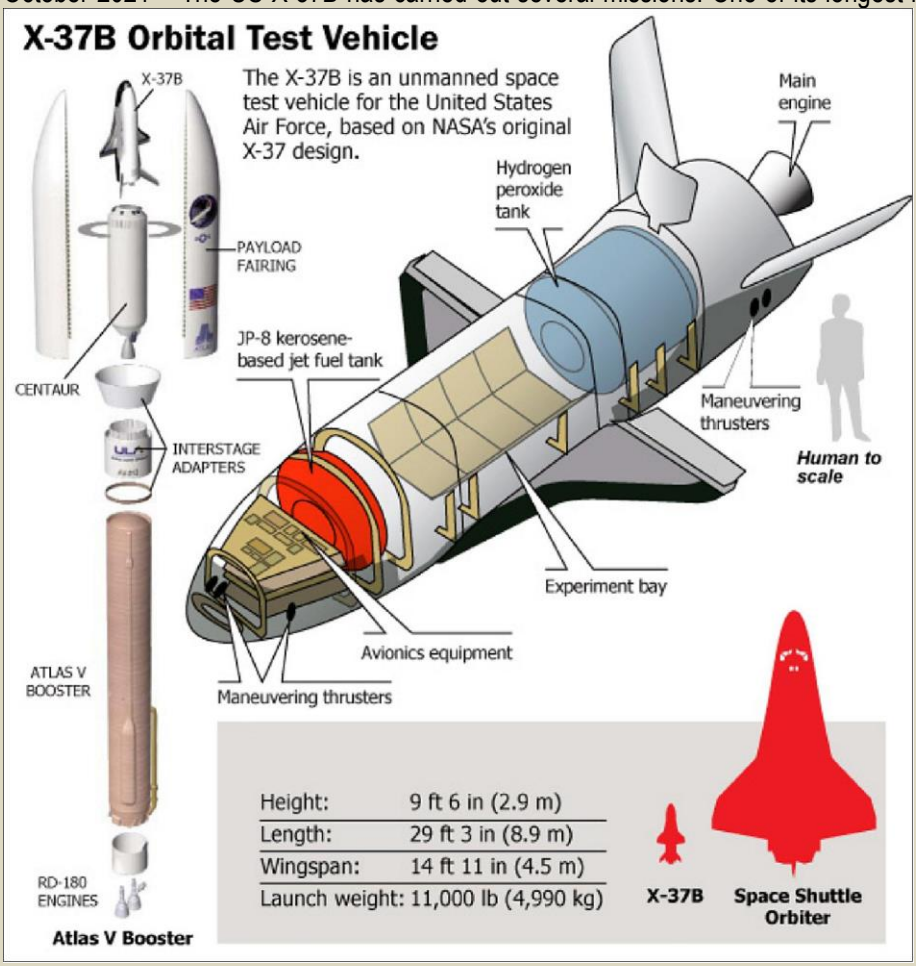
Zachary Kallenborn is a Policy Fellow at the Schar School of Policy and Government, a Research Affiliate with the Unconventional Weapons and Technology Division of the National Consortium for the Study of Terrorism and Responses to Terrorism (START), an officially proclaimed US Army "Mad Scientist," 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*, *Parameters*, and *Terrorism and Political Violence*.

Journalists have written about and shared that research in the *New York Times*, NPR, *Forbes*, the *New Scientist*, *WIRED*, and the BBC, among dozens of others in dozens of languages.

Long A Secret, The Identity and Duties of The X-37B Spaceship Begins To Be Revealed

Source: https://voi.id/en/technology/91780/long-a-secret-the-identity-and-duties-of-the-x-37b-spaceship-begins-to-be-revealed

October 2021 – The US X-37B has carried out several missions. One of its longest missions was to fly in orbit for 780 days. The agenda of this plane has been a well-kept secret for more than 20 years.



Built by Boeing, the X-37, aka Orbital Test Vehicle (OTV) started as a NASA project in 1999. In 2004 it was transferred to the US Air Force. Since then, the craft has orbited planet Earth on a number of secret missions. With US military forces in space currently facing a greater threat, they are becoming more outspoken about their strategy and showing what they can do.

Mission number six of the X-37B spacecraft has broken a record 500 days in orbit. The spacecraft blasted off into space on an Atlas V-501 rocket in May 2020, but its configuration allowed it to ride a SpaceX Falcon rocket as well.

Its adaptability and re-entry power that allows it to glide hot on the runway not only give it the familiar look of the NASA-Shuttle spacecraft, but also allow it to take experiments to lower orbit and return them to Earth, as well as carry out rapid deployments and multipurpose missions. . The X-37B can dock and drop with service modules or satellites and carry payloads and aircraft into space.

The main mission of the X-37B is classified

as secret. The media speculated that the spacecraft was a war-oriented military aircraft capable of spying and could even be armed. But the claim itself has been denied by the Pentagon.

As satellite traffic and tensions between China, the US and Russia escalate due to the satellite war, and the role of the US military in space increases. Unmanned spacecraft such as the X-37B are targeted for their potential to protect national interests. The US military has broken decades of silence on the X-37B in recent months.
The US Naval Research Laboratory, NRL, uses a spacecraft to convert solar power into radiofrequency microwave energy and then send it to the ground. This is also being worked on by the UK government through their national space strategy.
The X-37B also put FalconSAT-8 into orbit carrying 5 experiments in its payload. In addition, and for undisclosed reasons, the US military is also working to understand the effects of radiation on seeds to grow food in space.
The US Space Force's Delta 9, which is running the operation, said their mission was to "prepare troops to protect and defend" and provide authorities with options to "deter and, where appropriate, defeat orbital threats."

Speculation

"The X-37B can maneuver by changing the trajectory level. This means it is very difficult to be intercepted by the Russian satellite killers. At the same time, it has the ability to analyze communications. He can "sit" over Moscow as long as he wants, intercepting everything. So yes, his mission is also related to Ukraine," said a former Pentagon official who spoke on condition of anonymity.

Drug smuggling: Underwater drones seized by Spanish police

Source: https://www.bbc.com/news/world-europe-62040790

July 05 – Spanish police have seized three underwater drones built to smuggle drugs across the sea from Morocco.
The unmanned submersibles are apparently capable of carrying up to 200kg (441lbs) of cargo.
As part of the 14-month investigation, eight people have been arrested in Cadiz, Malaga, and Barcelona.
Police say it means they have broken up a gang suspected of building the vehicles and supplying them to drug smugglers across Europe.
Spanish police say it is the first time they have discovered an underwater vehicle capable of being operated unmanned.
"These devices could allow drug traffickers to transport large quantities of narcotics remotely across the Strait of Gibraltar," police said in a statement.
The Strait of Gibraltar is the narrow strip of sea that separates Morocco from Spain.
One of the submarines was completely built and two more were still under construction. It is believed the pair being built were intended to be delivered to a French gang for smuggling cocaine.

Officials also seized 14kg (31lbs) of hashish, 8kg (18lbs) of marijuana, more than €157,300 (£135,527) in cash, and six large aerial drones.
Armed with GPS navigation systems, the vehicles could potentially be operated by drug traffickers from anywhere in the world using an internet-device as simple as a tablet.
Among those arrested were a father and son, one of whom police say was a qualified helicopter pilot who had the technical knowledge needed to build such sophisticated vehicles.
Officials claimed the gang specialised in building a wide range of air, land, and sea vehicles intended specifically to transport drugs, and accused them of supplying the devices to criminal organisations in Denmark, Italy, France and Spain.
According to EFE news agency, investigators discovered 13 different types of vehicles - including trailers with concealed "double bottoms" capable of holding up to 800kg of cargo.
It's not the first time investigators have found vehicles designed for transporting drugs under water.
Earlier this year a semi-submersible vessel carrying four tonnes of cocaine was intercepted by the Colombian navy on its way to Central America.
Spain has become a key point of entry for drugs into Europe because of its proximity to Morocco - a major cannabis producer, and its close ties with former colonies in South America, where much of the world's cocaine is produced.
In particular the 15km-wide (9 mile) Strait of Gibraltar, which separates Europe from Africa, is a favoured route among drug smugglers.
Last year in April police arrested 100 suspected gang members accused of using speedboats to transport cannabis across the gap.

●▶ **Read also:** And in Spain, police last year seized a homemade 9-metre-long (29.5ft) fibreglass and plywood submarine in a raid on warehouse in Malaga.

The Vast Iran-Hezbollah Drone Threat Is Escalating

By Seth J. Frantzman
Source: https://www.meforum.org/63362/the-vast-iran-hezbollah-drone-threat-is-escalating

July 02 – Israel's downing of three drones on Saturday illustrates the growing nexus of Iran-Hezbollah threats in the region – and specifically the Lebanese terrorist organization's escalating attempts to target gas platforms off the coast of Israel.

These Iranian drones are stored underground at an undisclosed location in the mountains

Over the last several years, Iran has rapidly expanded its drone program and encouraged its proxies in the region to develop their own drone technology. These drones are often kamikaze ones, meaning they have a warhead and are designed to fly into their target. The drone threat against Israel has emerged slowly, in stages, over the last several years. Hezbollah has been using drones for many years, but they are increasingly more sophisticated and the threat is growing.
The UAVs shot down on Saturday appear to be of several different types. It is unclear if they carried explosives and how they were controlled. They do not appear to have been linked together to act as a kind of drone swarm.
In 2019 Iran used drones and cruise missiles to attack Saudi Arabia's Abqaiq facility. It also operationalized Kataib Hezbollah in Iraq to target Saudi Arabia using drones.
Iran moved drone technology to the Houthis in Yemen who have launched numerous drone attacks against Saudi Arabia over the years. In January, the threat grew to include attacks on the UAE.

Hezbollah has about 2,000 UAVs
The Alma Research and Education Center said in December 2021 that, "in the special report we published on December 21, we stated that we estimate that today Hezbollah has approximately 2,000 Unmanned Aerial Vehicles (UAVs). Over the past 15 years, there has been a huge increase in the number of Hezbollah's UAVs." Iran has increasingly used its militias in Iraq and Syria to target both the Kurdistan autonomous region in Iraq and US forces in Iraq and Syria using drones.

Israel's efforts to combat the drone threat
The downing of the drone illustrates Israel's abilities in detecting drones and also Israel's investment over the years in technology to down them. These include the use of warplanes and Barak surface-to-air missiles, and equipping Israel's latest corvette ships with the best systems to detect and stop drone and missile threats. Israel has increased the abilities of Iron Dome to stop these types of threats as well. In addition, the Jewish state continues to carry out the campaign between the wars to prevent Iranian entrenchment in Syria. However, the overall context is that Iran is increasing the range of its drones, which are proliferating all over the region.
Last year it is believed that Iran moved Shahed 136 drones to Yemen. These may have a range that enables them to strike Eilat.
In addition, Tehran increased its investment in Iraqi-based militias such as Kataib Hezbollah to increase their drone and missile threats. Israel is increasing its work with US Central Command and Navcent, as well as with new partners in the Gulf to discuss air defense priorities and drone threats. The drone threat on July 2, therefore, is part of the much wider Iranian threat, and ties into the importance of Israel's work with the US, UAE, Bahrain and other countries in the region to prevent destabilization.
The US is increasingly concerned about Iranian drone threats. Members of Congress have also worked on the Deterring Enemy Forces and Enabling National Defenses (DEFEND) Act and the Stop Iranian Drones Act. All of this is important in the context of Hezbollah's recent escalation.

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

Iran to send hundreds of drones to Russia for use in Ukraine, U.S. says

Source: https://www.washingtonpost.com/national-security/2022/07/11/iran-drones-russia-ukraine/

July 11 – Iran is preparing to supply Russia with hundreds of drone aircraft, including advanced models capable of firing missiles, the Biden administration said Monday, publicly revealing what U.S. officials say is a secret effort by Tehran to provide military assistance for Russian's invasion of Ukraine. The planned delivery of unmanned aerial vehicles, or UAVs, disclosed by national security adviser Jake Sullivan at a

White House briefing, could provide a significant boost to Moscow's efforts to find and destroy Western-supplied artillery and other weapons systems that have slowed the advance of Russian troops in recent weeks.

Sullivan said Iran is also preparing to train the Russians on how to use the weapons, with initial training sessions set to begin as soon as this month.

"Our information indicates that the Iranian government is preparing to provide Russia with up to several hundred UAVs, including weapons-capable UAVs on an expedited timeline," Sullivan told reporters in the White House briefing room.

"It's unclear whether Iran has delivered any of these UAVs to Russia already," Sullivan said, "but this is just one example of how Russia is looking to countries like Iran for capabilities."

The revelation comes as President Biden prepares to depart for the Middle East, where he is expected to confer with key allies on a unified regional policy toward Iran. Tensions between Washington and Tehran have been further strained in recent weeks, amid faltering nuclear talks and an uptick in rocket and drone attacks on U.S. military installations in the Middle East, conducted by militia groups armed and funded by Iran.

Chief of the General Staff of the Armed Forces Gen. Mohammad Hossein Bagheri, center, visits a display of drones before a drill on Jan. 5, 2021. U.S. officials said Monday that Tehran plans to supply hundreds of drones to Russia for use in its war in Ukraine. (Iranian Army via AP)

While Russia has its own extensive arsenal of drones, the arrival of Iranian aircraft could help Moscow replenish a key weapons system that suffered heavy losses during the four-month conflict. Surveillance UAVs play a crucial role in the targeting of enemy forces by artillery, and weaponized drones can hover over the battlefield for hours, launching missiles that can destroy tanks and other armored vehicles.

Receiving the UAVs is a "significant statement" about the limitations of Russian capabilities, said Frederick Kagan, director of the Critical Threats Project at the American Enterprise Institute.

There are various indications that Russian-backed forces are running out of precision weapons, something that the UAVs from Iran would change, he added.

"It's difficult to evaluate what the effect will be, but it will clearly give the Russians more capability to conduct air attacks, presumably deeper into Ukrainian territory than they have now," Kagan said.

Ukraine has used UAVs — many of them supplied by NATO countries such as Turkey — to destroy hundreds of Russian tanks and armored personnel carriers since the start of the invasion. Moscow, which now finds itself diplomatically isolated and under heavy economic sanctions, has struggled to replace some of its lost military hardware, while Ukraine is receiving billions of dollars' worth of weapons, including state-of-the-art artillery systems from the United States.

"From our perspective, we will continue to do our part to help sustain the effective defense of Ukraine," Sullivan said, "and to help the Ukrainians show that the Russian effort to try to wipe Ukraine off the map cannot succeed."

Iran's Gaza Shahed 149 drone has a range of 7,000 km; carries 13 bombs; it can take off from Moscow and target any city in Europe; weighs 3.1 tons and carry a payload of 500 kg.

Iran has emerged in recent years as a major manufacturer of unmanned aircraft. Among its military models is the Shahed-129, which closely resembles the U.S.-made Predator UAV used in military and counterterrorism operations overseas. Some military experts believe the Shahed-129 is a Predator clone, a reverse-engineering of a U.S. spy plane that crashed in Iran several years ago.

Iranian leaders have freely shared UAV systems with outside groups, most especially pro-Iran militias in Iraq, Syria and Yemen. Iranian-designed drones have been used to attack U.S. and allied military bases in the Middle East, as well as civilian targets such as oil refineries.

Over the years, Russia has been a key trading partner and occasional military ally to Iran. While Moscow joined the United States and European Union in backing the 2015 Iranian nuclear deal, it also fought alongside Iran in helping defend Syrian leader Bashar al-Assad — a key ally for both countries — during Syria's 11-year civil war.

Iran's apparent decision to provide military assistance to Moscow could further undercut efforts to revive the nuclear accord. After President Donald Trump's unilateral withdrawal from the agreement in 2018, Iran reneged on its promise to limit its stockpile of enriched uranium to levels far below what would be needed to build a nuclear weapon. Since then, Tehran has blown past the agreed restrictions and now possess enough fissile material to make at least one bomb, if it decides to do so, according to nuclear weapons experts. U.S. intelligence agencies say they have seen no evidence to date that Iran has begun making actual weapons.

Some Iran experts predict that the country may attempt to disrupt Biden's upcoming Middle East visit by authorizing its proxy groups to commit a provocation, such as a missile strike targeting a U.S. military installation.

"An attack during the summit could hold several benefits for Tehran," Michael Eisenstadt, director of the Military and Security Studies program at the Washington Institute for Near East Policy, wrote in an essay posted Monday on the group's website. Among the possible benefits: "humiliating U.S. officials and their Saudi hosts [and] demonstrating that Washington cannot protect its friends even while the president is visiting," he wrote.

Britain's Royal Air Force chief says drone swarms ready to crack enemy defenses

By Sebastian Sprenger

Source: https://www.defensenews.com/global/europe/2022/07/14/royal-air-force-chief-says-drone-swarms-ready-to-crack-enemy-defenses/

Concept art from the U.S. Air Force Research Lab showing a drone swarm that the service could potentially use in the future. Many governments are investigating expendable unmanned aerial vehicles as one technique for overcoming enemy air defenses. (AFRL image)

July 14 — The Royal Air Force's experiments with drone swarms show they can overwhelm enemy defenses, and the concept would be ready for action in a war, according to the U.K. military service's chief of staff.

Air Chief Marshall Sir Mike Wigston told the Global Air and Space Chiefs' Conference 2022 in London this week that the RAF's 216 Test and Evaluation Squadron and the Rapid Capabilities Office trialed five drone types in 13 experiments with various payloads and equipment over three years. The work yielded enough insights for the service to declare an "operationally useful and relevant capability," using its current fleet of drones, he said.

"We are exploring new models of capability delivery and accelerated production 'when we need them' rather than 'in case we need them,' from the twin jet 3D-printed Pizookie, to commercially available large drones fitted with novel payloads, to large quadcopters," Wigston said.

The problem of overcoming enemy air defenses is a key obstacle to employing military power from above. Planning for air operations increasingly entails ensuring that planes can fly safely in the first place, putting at risk untold amounts of money that militaries have pumped into beefing up their fleets to fourth- and fifth-generation technology.

That conundrum is on display in Ukraine, where Ukrainian and Russian air-defense capabilities are effectively canceling out the other side's air power arsenal, according to Justin Bronk, a defense analyst with the London-based Royal United Services Institute.

"The fact that air power has ben mutually denied, relatively speaking, in Ukraine by both sides has far more serious implications for us than for either the Russians or the Ukrainians," he said at the London conference on July 13.

That's because both the Russian and Ukrainian militaries are ultimately dependent on massive land manpower and artillery, whereas joint forces of the U.K. and other western powers are critically dependent on having air access and air superiority, Bronk said.

Swarming, which means throwing enough expendable drones at a defensive radar and interceptor position so as to overwhelm them, can be effective he said, but only to a point. The idea of small and

cheap drones attacking air defenses by way of swarming may not be feasible because those drones lack the requisite range and speed.
"If you want things to go fast and far, they're going to be jet-propelled and they're going to cost a fair bit," Bronk said.
In addition, getting drones swarms close enough to sophisticated air defenses with a range of hundreds of kilometers requires risky and potentially pricy insertion tactics that negate the widely cited cost benefit of cheap, small drones, according to Bronk.
The Global Air and Space Chiefs' Conference brought together military leaders to dissect new air and space power strategies in light of lessons learned from Russia's assault on Ukraine.

Sebastian Sprenger is Europe editor for Defense News, reporting on the state of the defense market in the region, and on U.S.-Europe cooperation and multinational investments in defense and global security. He previously served as managing editor for Defense News.

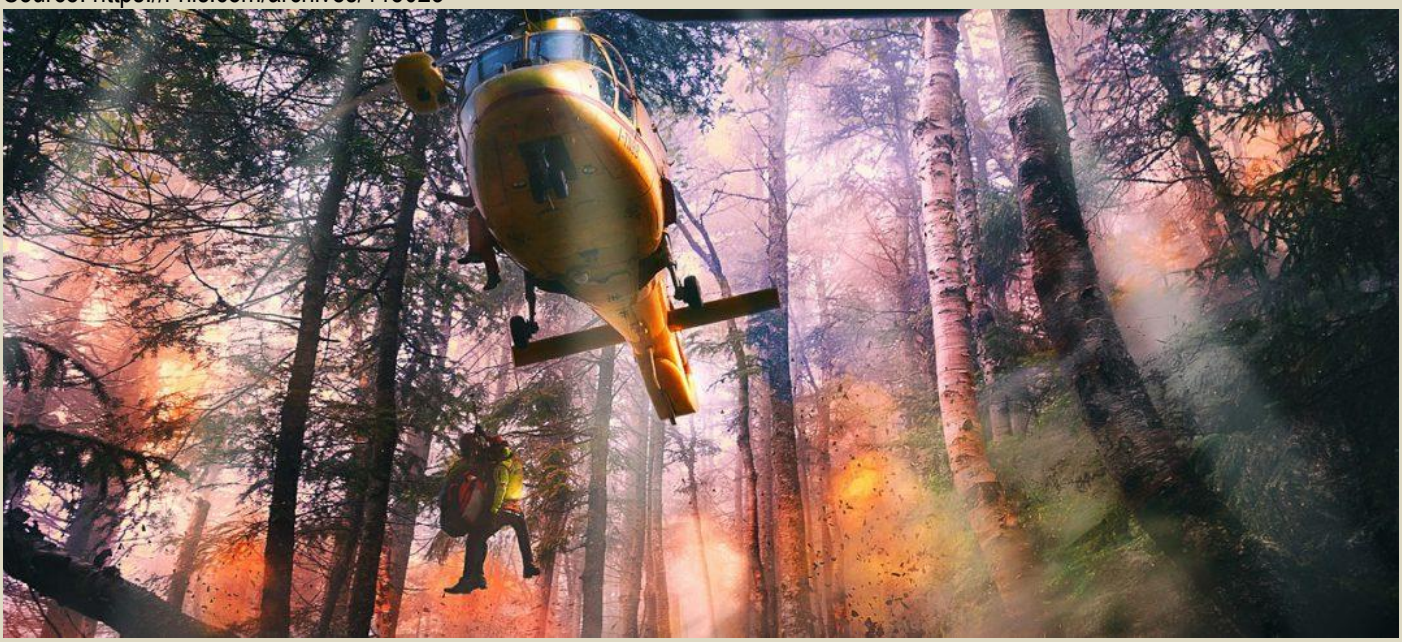
Ukraine's Homegrown Response to "Deadly" Chinese Drone Detection Tech

Source: https://www.homelandsecuritynewswire.com/dr20220715-ukraines-homegrown-response-to-deadly-chinese-drone-detection-tech

July 15 – Any unwitting drone enthusiast who flies their quadcopter near the front lines of the Ukraine conflict risks being immediately and accurately targeted with a barrage of artillery.
That's thanks to a controversial piece of Chinese technology called AeroScope. The surveillance system is made by DJI, the world's preeminent drone producer, and is able to detect the flight path of most DJI-branded devices and pinpoint exactly where the drone's operator is standing.
DJI say AeroScope is intended only for law enforcement uses, but Mykhaylo, a drone expert from Ukraine's Aerorozvidka organization, confirmed to RFE/RL that "unfortunately, examples exist" of Ukrainians being targeted and killed by Russian users of the system.
Aerorozvidka this week marks its eighth year of operation. The Ukrainian organization began as a group of drone enthusiasts who saw the potential for quadcopter technology in warfare. Today, the group works closely with the Ukrainian military and is widely viewed as a key factor in Ukraine's war effort. Its co-founder was killed in 2015 while on a reconnaissance mission in the Donbas.
Mykhaylo, who asked that his surname not be used in this story, says Aerorozvidka has had a "significant" impact on Ukraine's war efforts, citing the role of one team of drone operators who reportedly sped toward the front lines around the Ukrainian capital at the opening of the February invasion on quad bikes and used drone-dropped bombs to pick off Russian vehicles.
"We played a very important role in the Kyiv operation," he says.
Mykhaylo says it was largely because of AeroScope, the Chinese tracking technology in use by Russian forces, that Aerorozvidka developed its own drones capable of evading the DJI sensor.
A Ukrainian-made octocopter called the R18 first flew in 2019 and has been able to destroy Russian targets worth millions of dollars by dropping explosives weighing up to 5 kilograms. The R18's specifications, including a range of up to 4 kilometers, rivals the best drones on the market and is designed for total visual stealth in darkness.
Unlike most consumer drones, the R18's designers saved weight by deleting landing legs, meaning the drone needs to take off from a special platform, then be "caught" midair by someone on the ground after its mission is completed.
The R18 also differs from consumer drones in its use of thermal-imaging cameras, which give a relatively low-resolution black-and-white image.
"The advantage is, we can fly in the night," Mykhaylo says, when the thermal signatures of people and machines are more distinct than during warm summer days and the drone can't be targeted by small-arms fire. Russian fighters, Mykhaylo says, "are afraid of our visits, but they are even more afraid of us in the night when they have no possibility to see our drones, only listen."
Russia's radio-jamming devices are considered among the best in the world, and the front lines of Ukraine are described as a constant game of cat and mouse — or "radio-electronic wrestling" — between drone operators and radio jamming specialists.
Mykhaylo says there are various "life hacks" employed by Ukrainian drone pilots to evade detection on bombing and reconnaissance missions. He is unwilling to discuss those tactics in detail, but some drone pilots have talked about the importance of extremely low-level flying toward a target to avoid detection from radar systems.
Ukraine's early start on homegrown octocopter technology appears to be a prescient move. In March, DJI responded to complaints from a Ukrainian government official about the use of their products by Russian soldiers by calling the use of their drones in warfare "inappropriate." Then, in April, the company announced it was halting sales in both Russia and Ukraine. A spokesperson told Reuters that "DJI abhors any use of our drones to cause harm, and we are temporarily suspending sales in these countries in order to help ensure no one uses our drones in combat."

How To Neutralize Illegal Drones Near Wildfires? We Have a Solution

Source: https://i-hls.com/archives/115023



July 17 – One rogue drone is all it takes to halt the operations of an entire firefighter squad and cause wildfire to spread. The Los Angeles Fire Department and the FBI have partnered up to develop a program to cease the activity of these drones.

Why do firefighters must halt their aerial assault when faced with an unauthorized drone? The main reason is that they have no idea what the intention of the operator is, and so legally, all effort must stop. This causes the wildfire to grow and continue racking havoc on the surrounding areas, becoming more dangerous by the second.

The city of LA has offered a solution, a special sensor that can detect rogue drones and send notifications if the drone flies into unauthorized areas. The officers immediately receive precise details such as elevation, direction, speed, point of takeoff and where the operator is currently standing, reports edition.cnn.com.

This allows law enforcement to contact the offender and press charges if needed.

Why drone strikes on leaders are a good tactics for fighting ISIS, but not all terrorist organizations

Source: https://news.northeastern.edu/2022/07/20/drone-strikes-isis-terrorists/

July 19 – Although the news about ISIS has largely disappeared from our TV screens and social media feeds since the extremist group lost any territorial control in Syria and Iraq in 2019, U.S. Central Command and allies continue Operation Inherent Resolve.

In the last few years, they have conducted numerous special operations and targeted drone attacks, killing and capturing various ISIS leaders, with the latest successful counterterrorism operation announced last week.

On July 12, the U.S. military and intelligence community carried out a precision drone strike outside of Jindayris in northwest Syria, killing a "top five" ISIS leader, Maher al-Agal, who was responsible for aggressively pursuing the development of ISIS networks outside of Iraq and Syria, CENTCOM said.

"ISIS continues to represent a threat to the U.S. and partners in the region," said Col. Joe Buccino, a CENTCOM spokesperson. "The removal of these ISIS leaders will disrupt the terrorist organization's ability to further plot and carry out global attacks."

But is this tactic of targeted killings actually effective?

Max Abrahms, associate professor of political science at Northeastern and the author of "Rules for Rebels: The Science of Victory in Militant History" (2018), says that leadership decapitation has become the cornerstone of the U.S. counterterrorism strategy and took off in frequency under President Barack Obama's administration for a number of reasons.

First, big technological advances in drones development made them helpful in identifying potential targets. Modern drones are cheaper and can stay up in the sky for longer, Abrahms says.

Drone strikes suited the Obama administration very well, Abrahms says, because he opposed so-called boots on the ground engagement of the American troops and the Iraq War.

"On top of that, the terrorism threat has really metastasized and diffused internationally, and it just wouldn't be possible to deploy large numbers of troops everywhere in the world where there is a major terrorism threat," Abrahms says.
Abrahms believes that drone strikes are effective in the case of ISIS but should be used with caution for other terrorist organizations.
"When you take out the leader of a militant group, it is important to understand what exactly the role was of that leader … before the military pulls the trigger," Abrahms says. "Paradoxically, oftentimes, the leader of a militant group has a restraining effect on lower level members in the organization."
In his statistical research, Abrahms finds that targeting leadership often leads a terrorist group to become even more tactically extreme and more likely to engage in attacking civilians.
"However, not all groups are the same," he says. "Islamic State is a very unusual group because it is maximally extreme."
Unlike Hezbollah and al-Qaeda, where leaders act as a restraining force of the rank and file, the ISIS leadership actually favors mass casualty attacks against civilians world-wide. Most groups are much more selective about which targets they attack, Abrahms says.
He thinks that there is marginal utility in taking out the leaders one-by-one because not everyone gets to be promoted to a leader, and ISIS has a finite number of people to choose from.
"There isn't a big strategic risk taking out a leader of Islamic State," he says. "It could also act as a deterrent for future leaders knowing that they will be a marked man."
The ISIS leadership has been of a very poor quality, and it doesn't know what it takes to achieve long-term political change, Abrahms says. Because it has been so unrestrained and so violent, ISIS elicited the largest counterterrorism coalition.
"And that is why so few Americans are currently worried about the group," Abrahms says. "Islamic State is now a shadow of itself."

World's first laser-controlled drone easily evades countermeasures

Source: https://newatlas.com/drones/laser-control-drone-qinetiq/

July 22 – Counter-drone systems typically attack a UAV's radio control or GPS systems, disabling pilot control as well as pre-programmed missions. But British defense tech company QinetiQ has now demonstrated a laser-controlled drone these systems can't stop.
The demo, claimed as a world-first, showcased the company's new two-way Free Space Optical Communications (FSOC) system, designed to complement or replace radio control for military missions in areas where the enemy might have RF-blocking or detection gear.
The system appears to require line of sight for its "very high-bandwidth" ground station to drone link – that'll restrict its applicability. But the equipment on the ground looks pretty compact, and on top of skipping happily through RF jammers, the system also makes it virtually impossible to intercept or even detect the data stream.
One does wonder how well it'll fare through smoke, dust or other air quality issues – and indeed these drones will still be easily stopped by nets, shotgun rounds or throwing fridges at them. But QinetiQ sees the FSOC system as a way to "negate the considerable investment that adversaries may have made in denying the RF spectrum."
QinetiQ showed off the laser system's capabilities as part of the UK Ministry of Defence's DSTL Air Command and Control, Intelligence Surveillance & Reconnaissance and Interoperability project.


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

A New Model for Proactive Prevention

By Rick Shaw

Source: https://www.domesticpreparedness.com/preparedness/a-new-model-for-proactive-prevention/

Mar 02 – Shootings, acts of violence, crimes, abuse, suicides, overdoses, and other incidents and tragedies are increasing nationwide. Cities across the nation saw a surge of homicides in 2020 and many cities were at or near record levels for homicides in 2021. Cities also saw spikes in 2020 and 2021 with crimes, abuse, suicides, overdoses, and other incidents. Organizations, schools, and communities have continued to add more security solutions as well as more hotlines, safety/threat assessment teams, policies, trainings, and laws. However, violence and crime statistics do not reflect better safety.

Decades of post-incident reports from the U.S. Secret Service, Federal Bureau of Investigation (FBI), and other federal agencies have researched numerous incidents and tragedies and issued various documents regarding mass shootings and other acts of violence. Most post-incident reports routinely identify the presence of more than enough pre-incident indicators existing before a mass shooting occurred and a pathway to violence also existed for most attackers and shooters as they escalated and then executed their plans. But even with more than enough pre-incident indicators, proactive prevention actions still failed.

A Shift in Focus – Asking the Right Questions

Most after-action reports focus on how and why an incident occurred – the pathway that led to the violence and a profile of the attacker – in hopes of finding ways to prevent future attacks. However, when the focus of the research is shifted from the violence aspect to the prevention aspect, the research provides community leaders with new ways and new models to prepare for and prevent future threats. Shifting from validating a pathway to violence to identifying a profile of failed preventions is proving to be a game-changer, but this shift is only possible when leaders of communities and organizations start asking the right questions – and different questions – such as:

- Were pre-incident indicators observed and known by others before the attack?
- Were multiple incident reporting options available?
- Were resources/safety/threat teams available?
- Were trainings and policies provided?
- Were security solutions in place?
- Were laws and standards available?
- Were social workers and mental health resources available?
- Were law enforcement resources available?

Asking questions, especially different questions, is a good way to uncover what might be commonly overlooked or missing. The answers to the questions above can help to reveal additional questions that need to be asked and answered. For example, when asking the above questions after incidents or tragedies occurred over the past several years, the answer to each of these questions is often "yes."

Because of the "yes" answers, follow-on questions are needed to better understand why prevention efforts still failed. For example, if pre-incident indicators were exhibited, observed, and even reported before an incident occurred, then:

- Where were they?
- Who were they reported to?

- Why were the pre-incident indicators not shared with the right people?

Research from hundreds of past incidents reveals that pre-incident indicators almost always exist. However, when the indicators were reported, numerous incident reporting options are being used. This causes the indicators to be scattered across multiple incident reporting options, across multiple entities, across multiple systems, and across multiple people and departments. Some of the incident reporting options include:

- *Hotlines* – including organizational, community, local law enforcement, state agency, federal (like See Something Say Something, Crime Stoppers, 9-11, etc.), nonprofit, or other specific hotlines such those established for bullying, weapons, suicide, gangs, domestic violence, workplace violence, fraud, ethics, or numerous others
- *Electronic communications* – including text lines, mobile apps, emails, websites, or social media
- *Personal contacts* – including trusted adults (such as teachers), supervisors, human resources, security, teams (threat, safety, risk, behavior, workplace violence, etc.), counselors, mental health workers, employee assistance, legal advisors, friends, or family

Closing Prevention Gaps – A New Model

There are many reasons why pre-incident indicators are not collected and not shared with the right people who have authority to take proactive intervention actions. In addition to incident reporting silos mentioned above, there are numerous other issues related to trust, confidentiality, and sensitivity that can create gaps in information sharing. For example, misunderstandings regarding the Health Insurance Portability and Accountability Act (HIPAA), the Family Educational Rights and Privacy Act (FERPA), and other privacy guidelines are common. Personality traits and egos, departmental turf wars, and information not being shared and not assessed because those receiving the information do not believe it is their job are also common. Numerous other issues are also contributing factors, such as not knowing who the right team members are to share the information with or which other internal and external resources need to know about the information, especially as entities experience employee turnover or attrition.

Pulling together disparate information sources reveals the bigger picture surrounding individuals and situations of concern, which is vital for prevention.

When asking different questions, the different research path reveals numerous and dangerous gaps, silos, and disconnects that are making prevention difficult, if not impossible. Smart funneling and secure information sharing is critical to ensuring the right team members and resources are seeing the bigger picture surrounding individuals and situations of concern. Sadly, scattered pre-incident indicators, scattered team members, scattered community resources, and other scattered expertise are common reasons why proactive prevention efforts continue to fail.

Collecting and sharing indicators are just part of a comprehensive six-stage prevention model. Community leaders need to know what they do not know and know what others know on how to replace old and outdated models with the new research-based prevention model. Community leaders must understand:

- New strategies to build awareness of key indicators
- New ways to collect and funnel the warning signs into a central and secure platform
- How to share information with the right people
- How to empower the right people to assess the indicators/information
- How to connect the dots – connect at-risk individual(s) with community resources for intervention and monitoring, and ultimately how to proactively intervene, disrupt, and prevent escalation of at-risk behaviors

Preventing more incidents and tragedies is possible using the new First Preventers model to complement and help their first responders. The new model consists of innovative, research-based, and real-world proven strategies, templates, and tools that were created by asking the right questions, so the right people are seeing the bigger picture, connecting the dots, and proactively preventing more incidents and tragedies before they occur. Everyone can and must do better.

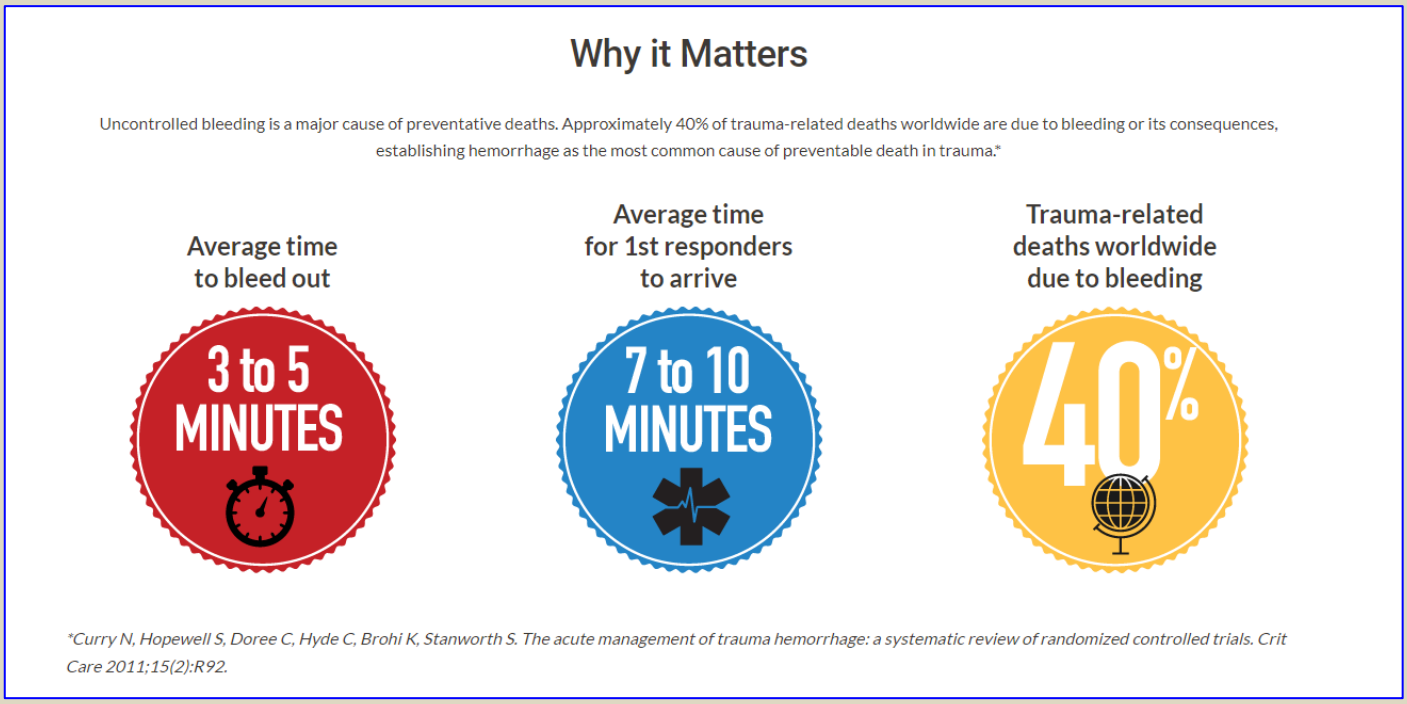
Rick Shaw founded Awareity in 2004 and founded First Preventers in 2019 and is a prevention expert, author, and prevention coach to organizations and communities. For the past 20+ years, he has been researching post-incident reports, lawsuits, and lessons learned to identify the profile of failed preventions involving terrorism, violence, shootings, suicides, sex abuse, human trafficking, and numerous other incidents. His unique research exposed a profile of failed preventions due to dangerous gaps, silos, and disconnects that conventional and old playbook practices have created. He utilized the research to develop the First Preventers Model.

Stop the Bleed Training for Immediate Responders

By Andy Altizer

Source: https://www.domesticpreparedness.com/preparedness/stop-the-bleed-training-for-immediate-responders/

May 18 – The Stop the Bleed Coalition points out that the average time for a person to bleed out is between three to five minutes. Jack Sava, MD, director of the Gold Surgery team at MedStar Washington Hospital Center is quoted saying that "An adult can die in less than five minutes from a bleeding wound in a critical area." With the average time it takes an ambulance to arrive, it is more important than ever for people to know how to uncontrolled bleed (see Fig. below).



Responding Immediately

Imagine a family hiking trip in a remote area of the Application Mountains, when one of the children takes a nasty fall down a small ravine, resulting in a compound femur fracture where the bone knicks the femoral artery and causes substantial blood loss. With the remote location and limited phone coverage, first responders would likely take nearly an hour to arrive. The child's life depends on the family members' actions.

A 2015 report points out that there are different levels of responders:

- *Immediate responders* – Individuals at the scene who can immediately control bleeding with their hands and available equipment
- *Professional first responders* – Prehospital responders at the scene with the appropriate equipment and training
- *Trauma professionals* – Hospital health care professionals with the equipment and skills to provide definitive care

The immediate responder (e.g., family members on a hiking trip) can provide lifesaving first aid during an emergency, especially when first responders are not nearby or are overwhelmed by multiple casualties. For example, as taught in Texas A&M Engineering Extension Services' (TEEX) Civilian Response to Active Shooter Events course, it takes an average of three minutes for police to arrive in an active shooter situation. The first arriving officers have the crucial initial priority of neutralizing the shooter ("stop the killing"), and the follow-up officers or Rescue Task Force typically begin first aid ("stop the dying"). Depending on the severity and location of the injury, a person can bleed out in three to five minutes.

Another example would be a motor vehicle incident involving someone severely bleeding. Instead of arriving within a few minutes, Emergency Medical Services (EMS) and other first responders may be significantly delayed due to the traffic caused by the incident. These two examples illustrate the importance of immediate responders' ability to stop the bleeding until first responders arrive on the scene or until the person arrives at the emergency room.

A person can bleed out in 3-5 minutes. So, immediate responders might be that person's only chance of survival.

Although the term immediate responders might be new to some, there has been an increase in this type of response. Examples include events/venue staff, coaches, athletic trainers, security officers, and

Community Emergency Response Team (CERT) members. Cardiopulmonary resuscitation and automated external defibrillator (CPR/AED), basic first aid, search and rescue, locating lost children, etc. are typical training topics for immediate responders. Added to this list of training opportunities should be administering lifesaving STOP THE BLEED® (STB) measures (direct pressure, wound packing, tourniquet application). In addition to the immediate responders mentioned above, other groups that would benefit from STB training include:

- Bus drivers and other transportation officials
- Landscapers
- Facility workers – plumbers, construction, building services (housekeeping)
- Executive assistants
- Over the road truckers
- Martial arts dojo instructors and students
- Faith-based staff – ordained, support staff, and volunteers
- Special events workers
- Parents
- Building managers/fire wardens/volunteer crisis coordinators
- Summer camp counselors
- Lifeguards
- Security officers
- Afterschool staff
- Teachers/professors
- Civic organizations
- Scouts
- Parking lot attendants

- Teaching assistants/lab workers/principal investigators
- University students – Such training may also help them in their future careers and add to their resumes. Infusing training topics like STB is also a great addition to students' academic curriculum, for example:
- Criminal Justice majors
- Education majors
- Student nurses
- Reserve Officers' Training Corps (ROTC) cadets

This non-exhaustive list provides suggestions to encourage others to think about possible immediate responders within specific organizations. By getting STB training, the people within an organization would be more prepared to respond to an incident immediately.

Some STB classes go beyond the three basic concepts of direct pressure, wound packing, and tourniquets, and include how to use Chest Seals.

Stopping the Bleed

According to the American College of Surgeons STB program, bleeding is "the most common cause of preventable death after injury." As such, it is important to know how to stop the bleeding and not to rely on first responders who may take too much time to reach critically bleeding victims. Learning to control bleeding is a skill easily learned and should be considered by various people and professions.

Of course, first responders (firefighters, police, and emergency medical technicians [EMTs]) are trained in STB. Although not considered first responders, many emergency managers and public health officials also have completed various first aid classes (Basic Life Support, CPR/AED, STB, etc.). However, do not assume that all clinic staff (nurses, medical assistants, etc.) are specifically trained in STB.

The University of Pittsburg Medical Center's "Minutes Matter" initiative points out that blood loss is responsible for 35% of prehospital deaths. It also notes that "4 out of 5 victims of a mass casualty are delivered to the hospital by someone other than a trained EMT, first responder, or ambulance." These statistics highlight the importance of knowing how to control bleeding.

For bleeding control, The Hartford Consensus III: Implementation of Bleeding Control report describes immediate responders as:

Traditionally thought of as "bystanders," these immediate responders should not be considered passive observers and can provide effective lifesaving first-line treatment. Immediate responders contribute to a victim's survival by performing critical external hemorrhage control at the point of wounding and prior to the arrival of traditional first responders. Immediate responders contribute to what is the critical step in eliminating preventable prehospital death: the control of external hemorrhage.

University of Georgia's Emergency Preparedness Office regularly teaches Stop the Bleed to faculty, staff, and students.

Finding Training

Many fire departments and EMS organizations have certified trainers and offers training to the public. In addition, other organizations (emergency management agencies, universities, civic organizations, Citizens Emergency Response Teams, etc.) have STB clubs that regularly offer training, refresher training, and other lifesaving training. The STOP THE BLEED ® Coalition also provides a search feature for trainers and additional information, including upcoming training in specific locations.

The number and type of immediate responders trained in STB are essential for community preparedness. Missionaries, little league coaches, umpires/officials, poll workers, etc. Get creative. The class is also a great way to build collaboration with others. As FEMA illustrates: "Life-threatening emergencies can happen fast, and emergency responders aren't always nearby. *You Are the Help Until Help Arrives*."

Andy Altizer is the Director of Emergency Management at Kennesaw State University, which works closely with Cobb Fire Rescue to provide an active Stop the Bleed training program on campus. He is also a Stop the Bleed Ambassador promoting the program and training to save lives.

EDITOR'S COMMENT: There are three things that a CBRN First Responder can provide in a contaminated environment: (1) control bleeding with modern hemostatics (e.g., QuikClot or Celox) and tourniquets (e.g., C.A.T.); (2) control the progress of pneumothorax with chest seals (e.g., Asherman seals); and (3) provide antidotes (nerve agents; cyanide; mustard gas). These interventions should be part of the training of all responders – medical and non-medical and related products should be available in the individual first aid kit each responder should have.

Summer 2022

Destination: Greece

Because international CBRNE First Responders need a common roof!

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