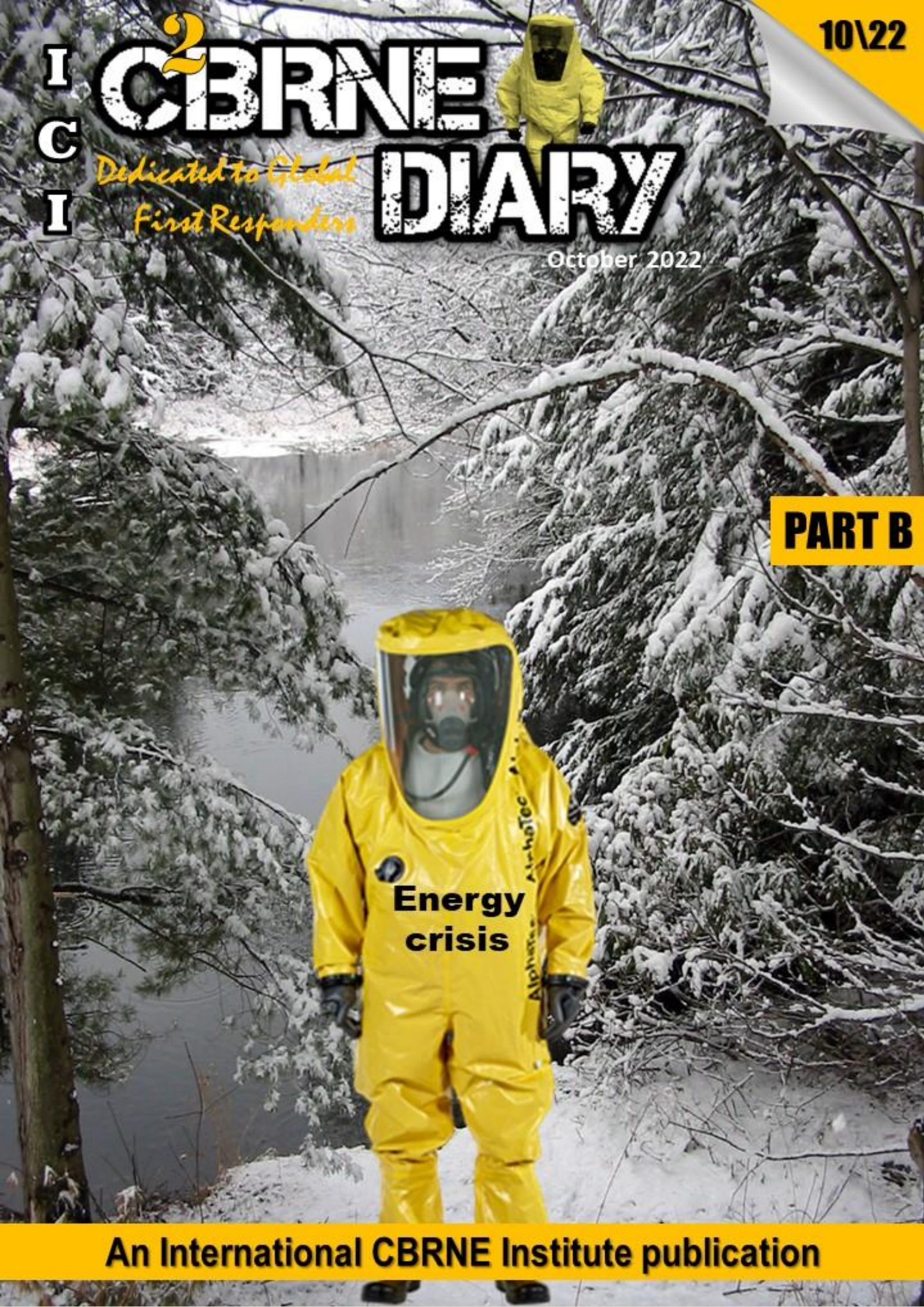
10\22

ICI CBRNE DIARY

Dedicated to Global First Responders

October 2022

PART B



An International CBRNE Institute publication

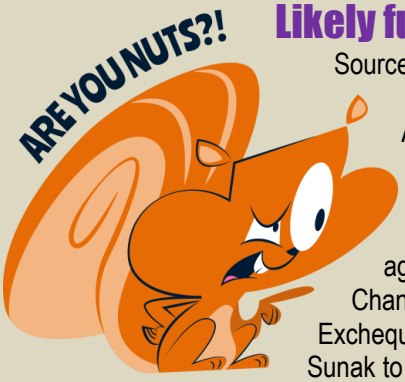
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

W O M D

DIRTY R-NEWS

C2BRNE DIARY



Likely future UK PM would not hesitate to use nukes

Source: https://en.mercopress.com/2022/08/24/likely-future-uk-pm-would-not-hesitate-to-use-nukes

August 2022 – Foreign Minister Liz Truss, the leading candidate to become the United Kingdom's Prime Minister next month, has said **she would not hesitate to use nuclear weapons if the time comes**. "I am ready to do it," said the Conservative leader who is competing against former Chancellor of the Exchequer Rishi Sunak to succeed Boris Johnson. "I think it's an important responsibility of a prime minister. I am ready to do it," Truss said on a YouTube radio broadcast. She admitted she would use weapons of mass destruction even if it meant global annihilation under the proper circumstances.


Sections Local Editions Services CORRIERE DELLA SERA

THE ELECTION IN GREAT BRITAIN

Liz Truss is the new British Prime Minister: who is the ultra-conservative who wants to try Putin?

by Luigi Ippolito, correspondent from London

The new leader of the Tory party, 47, is the third woman after Margareth Thatcher and Theresa May. She replaces Johnson

Exclusive interview with Liz Truss: «Don't humiliate Putin? Wrong: for us he must lose» by Luigi Ippolito


FROM AFP NEWS

Half Of Brits Think New UK PM Truss Should Quit: Poll

By AFP - Agence France Presse September 30, 2022

Truss looks increasingly likely to head the British Government starting next month when the announcement is made after the summer recess.

Her controversial remarks came during a meeting of Conservative Party members in Birmingham Tuesday when she was asked how she felt about pressing "the button." The top British diplomat seemed emotionless when replying.

Truss and Sunak are the two final contenders for the post of prime minister, which came after Johnson's resignation on July 7 following numerous political scandals. The last round of voting in the Tory leadership race is underway. Nearly 200,000 party members are choosing Johnson's successor by mail. The results are expected to be Sept. 5. The foreign secretary did not elaborate on which country the UK might be persuaded to use nuclear weapons against. In the past, Truss has repeatedly targeted Russia and strongly sides with Ukraine in the ongoing conflict. She also pledged to raise military spending by 3% of GDP by the end of the decade. Both Truss and Sunak have blamed Russian President Vladimir Putin for the poor performance of Britain's economy amid high inflation, soaring gas prices, and an increasingly unaffordable cost of living. Ahead of the upcoming G20 summit in Indonesia, Sunak wants Putin banned altogether while Truss would rather confront him at the event. According to the latest polls, Truss is 26 points ahead of Sunak, who was among the first to quit his post in Johnson's cabinet, thus unleashing the incumbent Prime Minister's fall.

With Putin's nuclear threat, what are Russia's 'strategic' and 'tactical' nuclear weapons?

By Rishika Singh

Source: https://indianexpress.com/article/explained/explained-global/with-putins-nuclear-threat-strategic-weapons-and-tactical-8179645/

Sep 30 – In a video address on September 21, Russia's President Vladimir Putin signalled to his country that efforts in the ongoing war with Ukraine would be intensified, as reports of Ukrainian forces' revival on the battlefield came in the last few weeks. Significantly, Putin said, "In the event of a threat to the territorial integrity of our country and to defend Russia and our people, we will certainly make use of all weapon systems available to us. This is not a bluff."

The declaration was accompanied by claims that the West was using "nuclear blackmail" against Russia, where Putin referred to "Western-encouraged shelling of the Zaporozhye

Nuclear Power Plant, which poses a threat of a nuclear disaster" and "the statements made by some high-ranking representatives of the leading NATO countries on the possibility and admissibility of using weapons of mass destruction – nuclear weapons – against Russia."
As a result, there has been heightened speculation over what Putin's next move might be in terms of weaponry. The terms "tactical" and "strategic" nuclear weapons have been making the rounds in this context.

Russian RS-24 Yars ballistic missiles roll in Red Square during the Victory Day military parade in Moscow, Russia in June 2020. (AP Photo, File)

The difference between tactical and strategic nuclear weapons

In the general scheme of things, strategic objectives are the interests of a particular country. But when it comes to nuclear weapons, strategic nuclear weapons are understood to mean those causing greater, large-scale damage. Tactical nuclear weapons, whereas, are small nuclear warheads and delivery systems meant to carry out a limited strike in a smaller area.
The smallest tactical nuclear weapons can be "one kiloton or less (producing the equivalent to a thousand tonnes of the explosive TNT). The largest can be as big as 100 kilotons. Strategic nuclear weapons are larger (up to 1,000 kilotons) and are launched from longer range. By comparison, the atomic bomb the US dropped on Hiroshima in 1945 was 15 kilotons", as per a BBC report.
By this classification, the Hiroshima bomb would likely be considered a tactical nuclear weapon.
Dr S Samuel C Rajiv, Associate Fellow at the Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), New Delhi, explains on the IDSA website, that "At first glance, the distinction is a factor of distance over which they are used, the context in which they are employed, and the warheads they can carry."

What are Russia's tactical and strategic nuclear weapons?

According to the North Atlantic Treaty Organization (NATO), the security alliance of Western countries, the arsenal of nuclear weapons possessed by countries can vary in terms of the purpose they can achieve and their technical specifications. Each country designates its weapons as it sees fit.
For example, France's weapons include strategic nuclear weapons, whose use or threat of use only the highest authority of the State can resort to. "The definition of the strategic nuclear weapon is fundamentally linked to France's doctrine of deterrence rather than to technical characteristics which, however important they may be, are merely consequences of that doctrine", as per **a NATO glossary**. So, given France wants to use these weapons only to deter or prevent potential attacks on it, they help in achieving strategic goals.
The same glossary claims that Russia's Tactical nuclear weapons are designed to engage objects in the tactical depth of enemy deployment (up to 300 km) to accomplish a tactical mission.

Its strategic nuclear weapons, on the other hand, are designed to engage objects in geographically remote strategic regions (over 5500 km) to accomplish strategic missions. In exceptional situations, strategic nuclear weapons may be used to accomplish operational missions.

How clear is this distinction?

Alex Wellerstein, director of science and technology studies at the Stevens Institute of Technology in the US, wrote on the Outrider security blog earlier this year that the distinction is not airtight and purpose matters more. "In terms of the technological differences, imagine a Venn diagram, with a small number of weapons being inherently "tactical" …and some being firmly "strategic" (in that they would be too large to imagine credibly using in a way that would limit the damage to a battlefield), but with many weapons straddling both definitions, capable of being used in either application, depending on where they were aimed."

Experts have also pointed to the fact that a nuclear weapon would be capable of inflicting way more damage and long-lasting consequences than a conventional weapon, despite its relatively "small" size. A case in point is the 15-kiloton Hiroshima bomb. In comparison, the Tsar Bomba of Russia – which many believe is the biggest N-bomb ever created – has more than 3,000 times the capacity of the Hiroshima bomb, as per a report in The New York Times.

Russia says it will be justified in its actions, as under its own doctrine it can use nuclear weapons to defend its "territorial integrity".

NATO has not made a direct reference to a nuclear attack on its part, but as of early September this year, it said: "NATO continues to address the security implications of Russia's growing arsenal of nuclear-capable missiles…The Alliance is responding by strengthening its advanced conventional capabilities…It is doing so while ensuring its nuclear deterrent remains safe, secure and effective. At the same time, NATO remains strongly committed to effective arms control, disarmament and non-proliferation, and continues to call for all actors, including Russia and China, to engage constructively."

Wildfires could release radioactive particles from nuclear sites

Source: https://yaleclimateconnections.org/2022/08/wildfires-could-release-radioactive-particles-from-nuclear-sites/

August 2022 – Nuclear disasters can release widespread, dangerous radioactive fallout. Research facilities and nuclear weapons tests can also leave behind varying levels of radioactive particles in soil and plants.

Christine Eriksen of ETH Zürich warns that at some sites, wildfires could later release those particles into the air.

"Locally, in the area of the fire and where the smoke travels to, the particles will travel with that," Eriksen says.

She says global warming and changing land use are increasing the threat of wildfires near many nuclear sites.
"We're seeing more wildfires in areas that are either bordering onto or actually are contaminated areas," she says.
That includes land near Los Alamos National Lab in New Mexico and other sites around the world.
She says some of these areas have a lot of vegetation ready to burn because it's dangerous to work in contaminated areas cutting grass or trimming trees.
Eriksen says more research is needed to understand how much radioactive material is released during fires, how far it travels, and how best to protect those who are exposed to the smoke, so a nuclear event of the past will not endanger more people in the future.

The War in Ukraine and Global Nuclear Order

By Alexander K. Bollfrass and Stephen Herzog
Survival | Volume 64, Issue 4; Pages 7-32 | Published online: 02 Aug 2022
Source: https://www.tandfonline.com/doi/full/10.1080/00396338.2022.2103255

Whoever tries to impede us, let alone create threats for our country and its people, must know that the Russian response will be immediate and lead to the consequences you have never seen in history.

Russian President Vladimir Putin, 24 February 2022

Abstract

The global nuclear order had been challenged in recent years by individual proliferators, the moribund US–Russian arms-control process and resultant frustration over stalled progress towards disarmament. Then Russia launched its full-scale invasion of Ukraine under cover of nuclear threats against NATO. This has neither exposed the international nuclear-governance regime as toothless nor brought it to the verge of collapse. The global nuclear order's history shows its resilience to rogue acts by great powers. It will continue to serve key nuclear-capable states' security and energy interests in the non-proliferation domain. Arms control between Washington and Moscow has always been sensitive to their strategic whims and can be reconstituted. The main consequence of Russian President Vladimir Putin's war is renewed public awareness of the often unpalatable role nuclear weapons play in international politics. Nuclear targeting, deterrent threats and associated risk-reduction efforts are hardly new phenomena.

Here's What Putin's Nuclear Disaster Would Really Look Like

Source: https://www.thedailybeast.com/heres-what-putins-nuclear-disaster-would-really-look-like

Oct 02 – Vitaly Fedchenko is a widely recognized authority on fissionable things that go boom in the night and a mighty important fellow in the business of thwarting the apocalypse.
Indeed, the throw-weight of this nuclear engineer's expertise on Russian President Vladimir Putin's arsenal of Armageddon is perhaps best illustrated by the blast radius of his job title at the Stockholm International Peace Research Institute: Senior Researcher for Strategic Forces Technology, Nuclear Energy, Nuclear Reactors, Nuclear Fuel Cycle, Nuclear Materials and Fuel, Uranium and Plutonium, Nuclear Warheads, Nuclear Forensics and Verification in the Weapons of Mass Destruction Program.
"A nuclear blast is a nuclear blast," is how Fedchenko soberly frames the validity of Putin's big bluff now vexing the world: Would Russia's beleaguered bully-in-chief follow through on his threats to launch either a targeted tactical nuclear assault or a crushing strategic nuclear strike on Ukraine and other Western nations? "There is no clear definition or agreement on what the difference is between tactical and strategic," Fedchenko says.
Regardless of the lethal arithmetic of kilotonnage, the answer is anyway moot, the body count overwhelmingly ghoulish.

"The difference between a nuclear weapon then and now is the difference between a Ford and a Lamborghini."

— Vitaly Fedchenko

In broad brushstrokes, Fedchenko and other experts interviewed by The Daily Beast on mutually assured destruction calculate Putin has three trajectories for his some 6,000 nuclear devices. A high-altitude electromagnetic pulse blast over Ukraine that deep-fries electronic systems there and in Europe; a low-altitude detonation designed to kill tens of thousands of Ukrainians but not immediately affect those in neighboring countries; or the so-called ground burst, with the prevailing winds carrying the fallout helter-skelter around the globe.

And Fedchenko adds that's not taking into account any plans Putin has to use conventional weapons to annihilate Ukraine's 16 nuclear power reactors, transforming the country into a netherworld on Earth.
During the Cold War, nuclear brinkmanship between the U.S. and the Soviet Union, such as the 35-day Cuban Missile Crisis in 1962, resembled a calculated chess match. The nuclear confrontation on display in Ukraine is more like the television game show Truth or Consequences, in which animosity has replaced probity, with both contestants intimating horrific repercussions.
NATO General Secretary Jens Stoltenberg warned Putin of the "severest consequences" if Russia used nuclear weapons.
But the former Russian President Dimitry Medvedev, the current deputy chairman of Russia's Security Council, blustered: "Russian weapons, including strategic nuclear weapons, could be used."
Another Putin pawn, Russia's regional Chechen chieftain Ramzan Kadyrov, over the weekend encouraged his boss to trigger the nukes. "More drastic measures should be taken, right up to the declaration of martial law in the border areas and the use of low-yield nuclear weapons," Kadyrov said.
"If Russia crosses this line," fired back U.S National Security Adviser Jake Sullivan, "there will be catastrophic consequences."
There has not been any question about how dangerous a nuke can be since the U.S. in 1945 dropped the Little Boy on Hiroshima, killing 66,000 and injuring a further 69,000 people. Shortly thereafter, America's nuclear bombmakers stopped purposely baptizing their explosive devices, such as Fat Man and Thin Man, after characters in Dashiell Hammett detective novels. Shelving the cinematics of *The Maltese Falcon* and the capers of Nick and Nora Charles, the Pentagon started to identify their weapons with names like Hotpoint and Lulu.
Yet a romp down memory lane in Russia's thermonuclear showroom—which the Soviet Union domestically sold as Nuclear Explosions for the National Economy—is an equally shivering journey. It usually inspires recollections of the 1949 plutonium classic Joe-1; the imperially branded 1961 Tsar Bomba; and the memorable Chagan, which in 1965 carved a 1,338-foot-wide radioactive shrine 328 feet deep into Kazakhstan.
"The difference between a nuclear weapon then and now is the difference between a Ford and a Lamborghini," Fedchenko explains. "The yield, the power of the explosion, is the same. The variance is in terms of size, the ability to withstand external shock, and the ease of delivery." The joker in Putin's nuclear armory is how many of his vintage or contemporary weapon systems actually work.

US splashes $290m on anti-radiation drugs after Putin ups nuclear threats

Source: https://constitutionalrightspac.com/articles/us-splashes-290m-on-anti-radiation-drugs-after-putin-ups-nuclear-threats

May 2022 – The US government has purchased a significant supply of radiation-injury drugs as the Russian president threatened the use of nuclear weapons.
A **$290 million** procurement of the **drug Nplate**, to treat acute radiation syndrome (ARS), was announced by the US Health and Human Services (HSS).
The government confirmed it was the first purchase of the drug, manufactured by the California pharmaceutical company Amgen.
The purchase comes after Vladimir Putin renewed his threat of nuclear war. In a speech last month, he vowed to use "all the means at our disposal" to protect Russia and its people. "This is not a bluff," he said.

Romiplostim (Nplate®) as an effective radiation countermeasure to improve survival and platelet recovery in mice

By Deborah I Bunin, James Bakke, Carol E Green, et al.
Int J Radiat Biol | 2020 Jan;96(1):145-154.
Source: https://www.tandfonline.com/doi/full/10.1080/09553002.2019.1605465

Abstract
Purpose: Rapid depletion of white blood cells, platelets, and reticulocytes are hallmarks of hematopoietic injury of acute radiation syndrome (H-ARS) and, if left untreated, can lead to severe health consequences including death. While the **granulocyte colony stimulating factors (G-CSF) filgrastim (Neupogen®), pegfilgrastim (Neulasta®), and sargramostim (Leukine®)** are approved to increase survival in patients exposed to a myelosuppressive dose of radiation, no medical countermeasure is currently available for treatment of the thrombocytopenia that also results

following radiation exposure. Romiplostim (Nplate®), a thrombopoietin receptor agonist, is the **first FDA-approved thrombopoiesis-stimulating protein for the treatment of low platelet (PLT) counts** in adults with chronic immune thrombocytopenia. Herein, we present the results of an analysis in mice of romiplostim as a medical countermeasure to improve survival and PLT recovery following acute radiation.

Materials and methods: Male and female C57BL/6J mice (11 - 12 weeks of age, *n* = 21/sex/group) were total body irradiated (TBI) with 6.8 Gy X-rays that reduces 30-day survival to 30% (LD70/30). Vehicle, romiplostim, and/or pegfilgrastim were administered subcutaneously beginning 24 h after TBI for 1-5 days. Evaluation parameters included 30-day survival, pharmacokinetics, and hematology.

Results: Full or maximal efficacy with an ~40% increase in survival was achieved after a single 30 μg/kg dose of romiplostim. No further survival benefit was seen with higher (100 μg/kg) or more frequent dosing (3 or 5 once daily doses at 30 μg/kg) of romiplostim or combined treatment with pegfilgrastim. Pharmacodynamic analysis revealed that the platelet nadir was not as low and recovery was faster in the irradiated mice treated with romiplostim when compared with irradiated control animals (Day 8 versus 10 nadir; Day 22 versus 29 recovery to near baseline). Platelet volume also increased more rapidly after romiplostim injection. Kinetic profiles of other hematology parameters were similar between TBI romiplostim-treated and control mice. Peak serum levels of romiplostim in TBI mice occurred 4 - 24 h (T_{max}) after injection with a $t_{1/2}$ of ~24 h. Cmax values were at ~6 ng/ml after 30 μg/kg ± TBI and ~200 ng/ml after 300 μg/kg. A 10-fold higher romiplostim dose increased the AUC_{last} values by ~35-fold.

Conclusion: A single injection of romiplostim administered 24 h after TBI (total body irradiation) is a promising radiation medical countermeasure that dramatically increased survival, with or without pegfilgrastim, and hastened PLT recovery in mice.

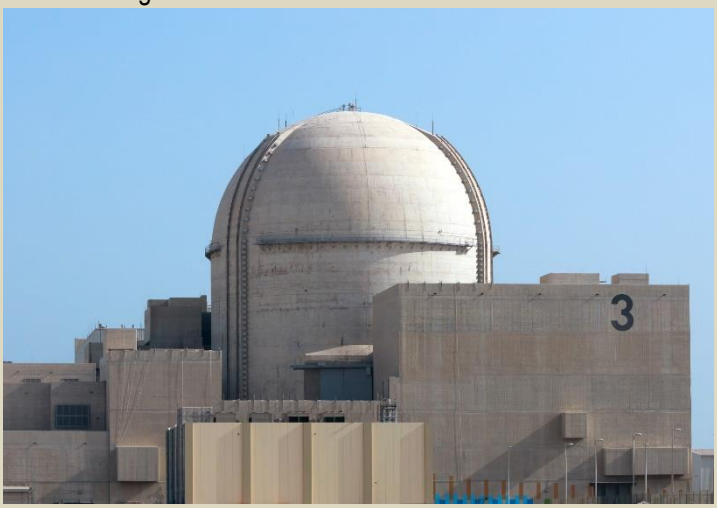
Third unit of Barakah nuclear energy plant connected to UAE grid

Source: https://www.thenationalnews.com/uae/2022/10/08/third-unit-of-barakah-nuclear-energy-plant-connects-to-national-grid/

Oct 08 – The third unit of the UAE's Barakah Nuclear Energy Plant has delivered its first supply of carbon-free electricity, after being successfully connected to the national grid.

The latest milestone in the country's clean energy drive comes only weeks after the reactor was switched on.

Unit 3 has the capacity to supply up to 1,400 megawatts of emission-free energy, helping to power the UAE's fight against climate change.



An operating licence for the third unit of the Abu Dhabi plant was issued in June.

Nawah Energy Company, the Emirates Nuclear Energy Corporation's subsidiary responsible for the operation of the nuclear power plant, connected the unit to the UAE's transmission grid.

Following its connection, officials will begin the process of gradually raising power levels at Unit 3, in a process known as power ascension testing.

This process will be regularly monitored and tested until maximum electricity production is reached, in line with international safety standards.

Mohamed Al Hammadi, managing director and chief executive of Enec, said it was another proud moment for the UAE's Peaceful Nuclear Energy Programme.

"Our leadership's long-term vision and decisions more than 13 years ago are paying dividends today," he said.

"Connecting Unit 3 to the UAE transmission grid adds thousands more megawatts of clean electricity to power all aspects of society, replaces the need to burn fossil fuels for energy, and through clean energy certification, gives many companies in the UAE a unique competitive advantage.

"I am proud of our Emirati led teams who continue to showcase world-class levels of capability, knowledge and expertise – powering a net zero economy through their work."

The Arab world's first nuclear plant is rapidly taking shape and will be central to the Emirates' ambitious sustainability strategy for years to come.

Its power generation will significantly reduce the country's use of gas-fired power stations to generate electricity.

In February 2020 and March 2021, the Federal Authority for Nuclear Regulation issued the operating licences for Unit 1 and Unit 2, respectively.
Commercial operations at Unit 1 started on April 18 last year and, within a year, the energy it produced prevented the release of more than five million tonnes of carbon emissions.
This is the quantity of emissions that would have been created if fossil fuels had instead been used to generate power.
It is the equivalent of more than "one million cars driven for a year", Enec said in April.
The four units of the Barakah plant will produce enough electricity to cover 25 per cent of the country's energy needs.
Unit 2 of the plant started commercial operations on March 24, less than a year after Unit 1.
Unit 3's construction was completed last year, while Unit 4 is close to completion.

Gates backs Barakah plans
Billionaire philanthropist Bill Gates this week praised the UAE for its ambitious efforts to achieve net zero emissions by 2050, highlighting the significant progress being made on the Barakah Nuclear Energy Plant.
Commending the UAE on its efforts, Mr Gates said the emirates was "very forward-looking" in its ambitions, and was setting aggressive goals as part of its transition to cleaner energy sources.
"The nuclear reactors at the Barakah power plant that are operational and pumping electricity into the grid are examples of how the country is managing the transition thoughtfully," he said.
He welcomed the UAE's support of the green agenda in a video address broadcast at the Countdown to Cop27 event on Thursday, held at the Jumeirah at Saadiyat Island Resort in Abu Dhabi.

Zaporizhzhia on the brink: How deteriorating conditions at the nuclear power plant could lead to disaster

By Zakhar Popovych, Denys I. Bondar, and M.V. Ramana
Source: https://thebulletin.org/2022/10/zaporizhzhia-on-the-brink-how-deteriorating-conditions-at-the-nuclear-power-plant-could-lead-to-disaster/

Oct 07 – Soon after it started its invasion of Ukraine on February 24, 2022, the Russian military occupied the southern part of the Zaporizhzhia region. The occupied area includes the territory of the Zaporizhzhia Nuclear Power Plant (NPP), the largest in Europe. During the summer, the area around the Zaporizhzhia NPP was hit multiple times by missiles and artillery. These affected all high-voltage electric power lines that connect the facility to the grid, so the plant was forced to work for some time in island mode, using the minimal power produced by one of the reactors to maintain functions essential to the plant's safety. After the International Atomic Energy Agency (IAEA), the UN's nuclear watchdog, conducted its inspection on September 1st, Ukrainian maintenance teams were allowed by the Russian military to repair the power lines and refill the diesel fuel storage tanks needed for emergency power generators. This made it possible to supply the facility with external power for the reactor cooling and other maintenance systems.
On September 10, the three of us had a conversation via Zoom with Pavlo Oleshuk, a representative of Atomprofspilka, the nuclear energy and industry workers' union of Ukraine. Oleshuk is an experienced member of the team that operates the Rivne NPP in northwest Ukraine. As an organizer with the union, he has been in close and constant contact with the employees who directly operate the Zaporizhzhia NPP.
Oleshuk's descriptions gave us new insight into the working and living conditions of his colleagues at the beleaguered plant. Such details have been otherwise difficult to get as plant operators have avoided talking in public ever since Russian forces seized the plant. Our discussion with Oleshuk lasted for more than two hours, and we offer here the main insights.
At the time we talked to Oleshuk, one of the reactors at the Zaporizhzhia NPP was still operating. However, shortly after our conversation, EnergoAtom, the Ukrainian state nuclear power plant operator, decided to shut down all reactors there. Despite this decision, there is a continued risk of a major nuclear incident as the plant requires permanent cooling. Furthermore, as our discussion with Oleshuk reveals, other factors exacerbate the fragility of the situation at the Zaporizhzhia NPP.

Context
Oleshuk began with a description of Zaporizhzhia NPP and the city of Energodar, which means literally "the gift of energy." It was a common practice in the Soviet nuclear power industry to build new cities just next to a nuclear power plant to offer the personnel and their families all the infrastructure they needed for a comfortable life—what the Russians call "monotowns." Energodar was one of those cities built to house the workers at the Zaporizhzhia NPP, just like the city of Pripyat in northern

Ukraine was built to house the operators of the Chernobyl NPP before it was evacuated after the devastating 1986 accident. Energodar was home to about 50,000 people. The closest residential building is just 3 kilometers (1.8 miles) from the reactors. Although some of the employees have sent away their families, especially children, most are still living there. This is in part because in many households both parents work at the nuclear plant.

A Russian serviceman patrols the territory of the Zaporizhzhia Nuclear Power Plant on May 1, 2022. The Zaporizhzhia Nuclear Power Plant in southeastern Ukraine is Europe's largest and among the 10 largest in the world. (Editor's note: This picture was taken during a media trip organized by the Russian army.) (Photo by ANDREY BORODULIN/AFP via Getty Images)

Working under threats and intimidation

The Zaporizhzhia NPP, the city of Energodar, and the surrounding areas have all been under Russian occupation for the past few months. According to Oleshuk's sources at the plant, Russian armed forces first took control of the nearby territory and peacefully approached the personnel of the power plant claiming that they would not intervene with the operations of the plant. But once the armed forces entered the plant's premises, so did personnel from the FSB—Russia's principal security agency and successor to the old KGB—and a couple of experts from Rosatom, the Russian state nuclear energy corporation. But the Rosatom personnel, Oleshuk's sources said, have not done much, and most Ukrainian plant operators suspect that they are present solely to make it look as though Russia had taken responsibility for the plant's operation by bringing in experts.

For their part, the FSB personnel, unlike regular soldiers, violated the rules about who can access different areas of the plant and went everywhere within the premises, including inside radiation-controlled zones. But rather than taking control over the plant's operations, the FSB agents seem to have been tasked with finding the so-called "ringleaders" who are organizing protests against the occupation because they seem to believe that such protests are organized by some Ukrainian intelligence agents—while, in reality, they spring from the grassroots. The FSB agents apparently hope that by arresting these figures, the protests will die down.

Consequently, FSB personnel have been interviewing plant employees as well as the residents of Energodar. Workers are stopped at checkpoints on their way to the plant and arrested for questioning or ordered to report the next day to the FSB office for interrogation. According to Oleshuk's sources, these practices became more prevalent with time. [On October 2, even the director general of the Zaporizhzhia NPP, Ihor Murashov, was detained;

he was released the following day.] From the viewpoint of plant workers, the FSB's actions look like a deliberate policy of threats and intimidation. Over time, many more nuclear power plant workers have left Energodar for other cities that are still under the control of the Ukrainian government, creating a shortage of personnel at the Zaporizhzhia NPP. Even though some nuclear power plant maintenance functions can be carried out remotely, most cannot. As a result, there are concerns about the safety of these reactors and their associated systems.

Living without supplies

Because it is in Russian-occupied territory, residents of Energodar can no longer get their supplies from Ukraine-controlled territories, although they are located just across the Dnipro River. Instead, they must get them from other occupied territories—which means that even the supply of basic groceries is intermittent, with some food products simply no longer available. For example, children with lactose allergies have no access to lactose-free milk. This problem is also true for the supply of medicine, especially the drugs needed to treat diabetes and other chronic illnesses. Russian occupation authorities are worsening the situation by blocking the supply and distribution of humanitarian aid coming from mainland Ukraine. Recently, they effectively closed the city's main distribution center by evicting it from the premises it had been using for storing and sorting humanitarian aid. Another major problem for the residents of Energodar is the collapse of utilities. Ironically for a city hosting Europe's largest nuclear power plant, the electricity supply has been almost shut off. On most days, people get electricity only for two hours, with at least one period where there was no electricity at all for several consecutive days. Without electricity, food and medicines stored in refrigerators get spoiled, and phones and power banks run out of charge. People have been forced to turn to fireplaces, installed in the yards of their apartment buildings, to cook food with wood. The supply of water supply has also become a problem since it relies exclusively on electric pumps and there are no water towers in Ukraine because the electricity supply was always considered to be reliable and abundant. As a result, people have lacked running water in their homes for days. In the city of Energodar, located on the bank of the Dnipro River, there has been some limited water supply for cooking reported, but inhabitants lack access to clean drinking water and can't have showers for days at a time.

Outlook

With winter coming, the future is grim for the workers of the Zaporizhzhia NPP who still live in Energodar. Like other satellite cities, Energodar relies on the Zaporizhzhia NPP for most of its energy needs, including for heating. The city does have a backup thermoelectric power station that can work on coal, fuel oil, and gas, but that facility was shut down in May 2022 due to the lack of fuel since the Russian occupation started. It is an ironic situation given that the nearby Donbas region in eastern Ukraine is home to one of the world's largest coal mining regions.

If both nuclear and thermal power plants cannot resume operation, then Energodar's inhabitants will not be able to heat their living premises. The Ukrainian winter is cold with temperatures often being less than 20 degrees Celsius below zero (-4 degrees Fahrenheit). Plant workers don't know how they will survive the winter.

Making an already desperate situation worse, there has been a loss of leadership and governance. The mayor of Energodar, Dmytro Orlov, was initially arrested by the Russians, but later managed to flee the city. The occupying forces did try to take over the city hall, but effectively the local authority has largely collapsed. The inhabitants are now left on their own.

According to Oleshuk, the situation is simply no longer tenable for the plant workers who are exhausted and stressed out. If the heating, water, and electricity supply are not restored within the next month or so, Energodar, the gifted city, will be not livable and inhabitants may decide to flee on their own. This situation leads to the risk of the plant being without the personnel needed for its safety. A new concern emerged about what might happen following the fake referendums organized by Russia in the occupied territories, including the Zaporizhzhia region. One such referendum has been held in the area surrounding Energodar, which strongly suggests that Russia doesn't want to withdraw from the area. The only feasible path to ensure the safety of the nuclear power plant and avoid possible accidents would be to have Russian troops withdraw from Energodar and the area around the Zaporizhzhia nuclear power plant, as well as the establishment of a demilitarized zone under international supervision. If such actions are not taken now, Europe and the world should prepare for the safety and security situation at Zaporizhzhia to deteriorate within the next few weeks and, with it, an accompanying increase in the risk of a major nuclear accident.

Greta Thunberg: Germany making 'mistake' by ditching nuclear power for coal

Source: https://www.dw.com/en/greta-thunberg-germany-making-mistake-by-ditching-nuclear-power-for-coal/a-63406732

Oct 11 – Climate activist Greta Thunberg told German public television on Tuesday that she would consider it a mistake to switch off existing nuclear power plants and to focus on coal

instead to generate electricity. "It depends. If you have them already running, I feel it's a mistake to close them and focus on coal," Thunberg said on the "Maischberger" talk show on ARD.
"I personally think it's a very bad idea to focus on coal when [nuclear power] is already in place," the climate activist said.
She acknowledged how sensitive the question was among climate activists, calling the issue "a very infected debate."

What's the state of play with German nuclear power?

Germany's longstanding gradual shutdown of nuclear power was originally scheduled to be completed at the end of this year.
However, the war in Ukraine and resultant pressures on fossil fuel exports and electricity prices have cast this policy back into question.
The government has agreed to a limited extension of two of the last nuclear plants' running times by just a few months, covering the coldest winter months. But the opposition and one member of Chancellor Olaf Scholz's ruling coalition are lobbying for a longer extension.
Although it's probably an oversimplification to describe the nuclear shutdown as being compensated by a "focus on coal," the government has separately approved the reactivation of several coal- and oil-burning power plants to secure supply in the winter.
Germany also dug new coal mines while it was in the process of shutting down its nuclear power fleet in recent years. That said, the government has also pledged to phase out coal usage by 2030.
Germany's last nuclear reactors, including Isar 2 in Bavaria, were scheduled to shut down at the end of the year but Ukraine has cast this back into question.

German politicians pounce on Thunberg's comments

Finance Minister Christian Lindner, the head of the pro-free market Free Democrats (FDP), and the leader of the conservative opposition Christian Social Union (CSU) in Bavaria, Markus Söder, were both quick to welcome Thunberg's comments.

"I welcome the support of Fridays for Future founder Greta Thunberg for the FDP position to keep our nuclear plants on the grid. In this energy war everything that generates electricity must be on the grid. The reasons speak for themselves — economically and physically," Lindner wrote on Twitter.
Lindner's FDP is the only member of Scholz's coalition government that is keen to extend the nuclear plants' running time further. The party's fellow coalition partners — the center-left Social Democrats (SPD) and the ecologist Greens — both pride themselves as being the parties that implemented Germany's original nuclear shutdown plans at the turn of the century.
Söder shared footage of part of Thunberg's interview on social media, captioning it simply: "Interesting..." Both the power plants scheduled for a brief extension are in the southern state of Bavaria.

Tensions within German government

Tensions on the issue were evident within the coalition on Tuesday.
Robert Habeck, a member of the Greens and minister for economic affairs and climate action, accused Lindner's Finance Ministry of holding up the government process to approve a short extension of a few months for the nuclear plants.
Habeck told news magazine *Der Spiegel* that if the Finance Ministry wanted the short extension to be approved in time for winter, they "must clear the path for this now." Habeck's ministry had said the government had agreed to bring the motion through Cabinet by Monday of next week with a view to it being debated in parliament
Environment Minister Steffi Lemke, also of the Greens, told the dpa news agency that the Finance Ministry was refusing to sign a draft law "despite the agreement reached in the last week" to send the proposal to the Bundestag.
Habeck argues that time is running out to conduct repairs at one reactor to enable it to continue operating longer than currently scheduled.
The FDP's Johannes Vogel, meanwhile, said that there was still plenty of time to meet the "fastest timetable proposal" from Habeck's ministry.

Thunberg: Main focus should be renewables, even amid Ukraine war

Thunberg also warned against regressing towards less green power amid the war in Ukraine.

She said she understood the need to protect people from excessive energy costs, but said people were also "dependent" on power and a system that was not sustainable.
Thunberg said that climate change was not being treated like a global emergency and said other recent issues like the COVID pandemic had demonstrated that this was possible. She said that even amid crises people could not lose sight of climate change.
"Every war is a disaster. On many levels. But we must be able to focus on different things at the same time," Thunberg said.

EDITOR'S COMMENT: Now that Sweden will join NATO, Greta might sympathize nuclear weapons as well! As for the Finance Minister, he is the epitome of a politician …

When Israel Struck Syria's Reactor: What Really Happened

By Ehud Barak
Source: https://www.meforum.org/63517/when-israel-struck-syrias-reactor

Fall 2022 – When I joined Ehud Olmert's government on June 18, 2007, as minister of defense, it was almost three months since planning of the destruction of the Syrian reactor in Deir az-Zor had begun (in late March). I was aware of this activity, having been briefed in late April about the reactor's existence by Olmert, Mossad head Meir Dagan, and IDF head of intelligence Amos Yadlin. Asked for my opinion on what should be done, I answered on the spot: "We must destroy it." This issue was the reason for my insistence on entering the defense ministry as soon as possible. I assumed that the Israel Defense Forces (IDF) was deep into preparations to execute an operation, and I believed I could contribute to the operation's success.

Ehud Barak had previously served as Israeli defense minister and prime minister when he joined the Olmert government in 2007.

Two Flawed Plans

On my first day at the ministry (I had already served as defense minister alongside my premiership, 1999-2001), I convened a "status of operation" discussion with participation of all relevant operational arms—Intelligence, Mossad, and Air Force (IAF), as well as experts on nuclear reactors. The two operational plans for the reactor's destruction on which the Air Force and others had been working were presented to me in full detail. The prevailing view in the room, as well as the conventional wisdom in the Prime Minister's Office, was that of an urgent, immediate need to implement the plan, preferably within a week or two. It was also perceived as critical to proceed swiftly lest our awareness of the reactor's existence became public, which would significantly complicate its destruction, and before the reactor became "hot" and rendered the operation impractical. There was a general unanimity regarding the need "to destroy the reactor and avoid a wider clash with Syria." To my surprise, I found that both plans, quickly nearing "D-day," failed to meet these requirements.
The first plan envisaged a massive air attack that might surely destroy the reactor but would involve a direct engagement with the Syrian air force and air defense. Such an attack could not conceivably be denied the morning after and carried a significant risk of triggering a wide clash with Syria and possible deterioration to full-fledged confrontation with Hezbollah in Lebanon as well. I called this plan "Fat Shkedi" (Maj. Gen. Eliezer Shkedi was the then-IAF commander). The second plan, prepared in the past for another mission, was an extremely "low signature" operation that would not trigger a major clash but could not assure—beyond serious doubt—the destruction of the reactor.
I pointedly asked again: "How much time do we have before the reactor becomes hot?" The answer was: "Around three months." "Will we know for sure if and when our window starts closing, even if this happens earlier than predicted?" I asked. The answer came: "Yes, absolutely." I summarized as follows:
A great intelligence achievement allowed us to start working on the project when the reactor is still in construction phase. A lot of important operational work has been done to bring us up to here. However, the two presented plans did not stand up to the needed constraints.
I then redefined the limiting parameters more clearly:
We need at least one, preferably two, plans that can ensure both the reactor's destruction and a high probability of avoiding a wider confrontation with Syria and Hezbollah.
I directed all concerned actors to start working in this vein.

Two "Low Signature" Plans

Keenly aware of the risks attending my directive, I ordered that "Fat Shkedi" be brought ASAP to operational completion so that it could be executed on very short notice as a hedge against the risk of a possible leak. Moreover, being unable to ensure that despite our efforts to avoid such an eventuality we would not find ourselves in a wide clash in the north, I instructed the Northern and Home Commands to increase and deepen preparations for a wide-scale confrontation.

I also asked Washington for precision munitions, spare parts, and other necessary means in the event war ensued. In order to avoid these preparations from being leaked, all these activities had to be done under a thick veil of secrecy through a variety of explanations and disguises. Indeed, it worked. On a Friday night in August, without leaks or media footprint, a U.S. vessel in the port of Ashdod unloaded 35,000 tons of munitions and spare parts necessary for possible deterioration to a full-scale war—the equivalent of 230 heavy transport airplanes carrying about 150 tons each.

IAF commander Eliezer Shkedi came to Barak with a better plan. Barak told the general to start preparing the new plan immediately.

The first person to come with an idea for a better plan was Shkedi himself. About a week after the above discussion, during a visit to an IAF base where preparations for "Fat Shkedi" were presented to us, he asked me to have a cup of tea with him. There, across the table, he took a triangular paper napkin, opened it flat, and drew on it a sketch of a "surgical air raid" on the reactor, which had a dramatically lower signature than the one in preparation. I asked how long it would take to have it prepared, and he said, "It could have taken a month, but since I have first to polish and ready the 'Fat' plan, it might take a little bit more."

"Very good," I said. "Start preparing it immediately and, later on, bring it for my approval."

"Why didn't you go this way in the first place?" I wondered.

"It was originally presented as a mission to be executed immediately within the shortest time possible, and probably carried out if a leak started developing, even before preparation had been fully completed," said Shkedi. I dabbed the new plan "Lean Shkedi" (also meaning lean and mean).

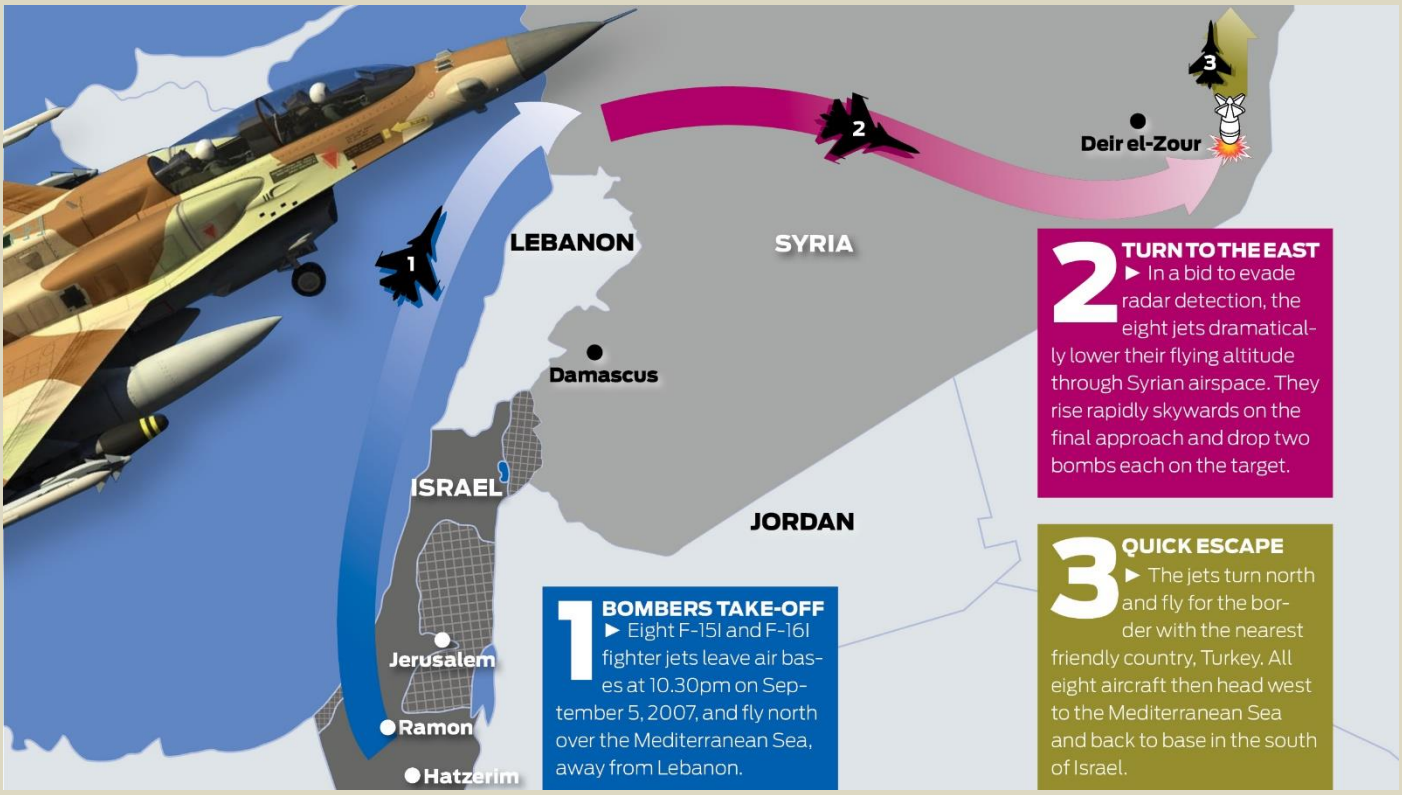
The second person to approach me with an alternative idea was Head of Intelligence Yadlin, a former IAF senior commander who participated as a young F-16 pilot in the destruction of Iraq's Osirak nuclear reactor in 1981. He came with a totally different idea than "Lean Shkedi," and a somewhat more complicated plan, which involved a very low footprint that could ensure both the reactor's destruction and a very high chance of avoiding a wider confrontation. I asked how long it would take to prepare the plan, to which Yadlin replied, "Probably two months." "Very good," I told him. "Start preparing immediately and bring it for my approval later."

In the coming weeks, I led an intensive series of discussions regarding all aspects of the operation. These involved first and foremost the needs of the budding new "low signature" plans, "Lean Shkedi" and "Yadlin"; a detailed intelligence analysis of possible Syrian reactions and our possible responses; the IDF's preparation for a possible major confrontation that could escalate to full scale war; diplomatic containment of Syria in the immediate wake of the operation, and initial thoughts about the "day after," including implications for the struggle against the Iranian nuclear program, the risks of rising questions regarding Israeli strategic capabilities, etc. Naturally, some of these discussions were followed by similar consultations with the prime minister and the inner cabinet. On July 26, I issued a set of directives to the IDF to be ready for "a possible war in the north (Syria and Hezbollah)," and on August 3, I ordered the completion of preparations for the two "low signature" operations by September 1 as a first target date.

One has to bear in mind that, in Israel, most of these subjects fall under the responsibility of the minister of defense, unlike in the United States where the president is the commander in chief with the secretary of defense and chairman of the joint chiefs of staffs acting during operations as advisers to the commander in chief rather than as two links in the "chain of command" that goes directly from the president to the commanding generals. In Israel, the government as a collective, or its inner security cabinet, are the equivalent of the commander in chief. The prime minister is the most important member, yet he is formally just "first among equals." The minister of defense is the person responsible for the IDF on behalf of the government and/or the inner cabinet. He is in the "chain of command" representing the government, and according to the Basic Law of the IDF, "the chief-of-staff, the top uniformed person, is subordinated to the minister of defense, reports to him and is also the next link in the 'chain of command.'"

Many inaccurate, at times even distorted, stories and urban legends, many of them critical in tone, have been spread over the years regarding my abrupt and forceful intervention in the course of events. However, in the so-called "bottom-line test"—the test of reality—the

picture that transpired is clear and definitely positive. When we sat down on September 5, 2007, to decide how to destroy the Syrian reactor, the two leading operational plans were exactly the two low signature plans that resulted from my intervention rather than those that were originally planned. And the story did not leak, nor did the reactor become "hot." Not to mention that the operation carried out that night was extremely successful and did not lead to any clash at all.



Tense Deliberations

There was tension in the air in every discussion on the prime ministerial or cabinet level. And there were many of them, several times every week. I could feel the eagerness, a hasty and impatient desire to stop this nerve-wrecking, slow advance and "just do it." I even felt an underlying theme, well articulated in a recent *Middle East Quarterly* article,[1] that, for some improper reasons, I tried to delay or even to dodge the operation.

None of these thoughts had ever crossed my mind. We needed the cool-headed approach attending my experience in order to ensure the operation's complete success: the reactor's assured destruction, minimizing the risks of wider confrontation, and preparedness for the worst-case scenario of escalation to a full-fledged war. I just was confident that my opponents were wrong.

Thus, somewhat humorously, I made it a rule that whenever I had to talk I would say:

I tell you now at the beginning, and I'll tell you again at the end, and if I don't tell you in the middle, do forgive me for forgetting: "This reactor has to be destroyed! And it will be! And now for the serious discussion."

During one of these frustrating debates, a senior minister with a deep security background told me:

Ehud, what we see here is the difference between an amateur, inexperienced, and somewhat shallow person who is overwhelmed by the case and a cold-nerved professional who planned and executed special operations all his life.

In the first eight days of August, three cabinet discussions brought tensions to a head. Basically the prime minister tried to forge a majority in the cabinet, together with military and intelligence officers, who all, except for myself, Deputy Prime Minister Shaul Mofaz, and Minister of Internal Security Avi Dichter, supported an immediate attack.

The attempt to reach a majority or even consensus is legitimate, but the chosen way was not. PM Olmert basically asked the IDF's top echelons to present an opinion and recommendations supporting an immediate attack. But he arranged it as a bypass of the basic procedural rules in Israel, where, as mentioned above, the position of the defense bodies should be first approved by the minister of defense. Of course, officers can have different views from their minister and should be allowed to express them and try to convince the cabinet. But in the Israeli constitutional framework, officers cannot bring to the cabinet "recommendations for action" that were never presented to the minister of defense who is their direct superior in the chain of command. So, to some people's surprise, I ordered the presentation to be halted when the recommendations began to be read. The prime minister, somewhat oddly, decided to read them to the forum himself with Yadlin

expressing his view as well. Yadlin could do this because, according to the same law, the IDF head of intelligence is responsible for "national net assessment" and, as such, reports directly to the government in this regard—and only in this regard. The atmosphere got heated, but the somewhat "tricky track" did not work.

In another meeting a few days later, I presented to the cabinet the ministry of defense's position. A fierce debate ensued where the prime minister and several others expressed anxieties about a "doomsday scenario" whereby a leak of the IDF planning combined with a hot reactor would generate an irreversible rush toward a Syrian bomb, followed by apocalyptic pictures of panicky Israeli citizens fleeing abroad and the Jewish state seemingly hovering on the verge of collapse. I strongly rejected this exaggeration and insisted on the following:

- We have to, and we will, destroy the reactor once the low signature plans are ready.
- We still have some time and will know for sure when we have run out of time.
- We have the "Fat Shkedi" plan as an insurance policy in the event of a leak.
- We must complete our preparations for a possible escalation to war despite our desire to avoid this eventuality.

By way of cooling down the sense of panic in the room, I noted that we were lucky to have discovered the reactor before it turned hot:

Imagine that we found it when it was already hot. Should we then panic? Pack our belongings and flee to North Africa and East Europe? No! We are here to stay! And we are still the most powerful country in the region! We would have discussed the new severe situation and found the right way to destroy it under these new circumstances. Only a sick imagination can interpret such a remark as recommending to wait for next year and consciously allow the reactor to become hot.

In a third meeting a few days later, we were subjected to a long exposition by PM Olmert detailing in somewhat legalistic language the development of the project from day one and his arguments for an early attack. I kept disagreeing, claiming that we had to use all the time at our disposal to be as best prepared as we could under the circumstances, and then strike while trying to avoid being dragged into a wide scale confrontation.

These tense cabinet meetings were followed by exchange of letters between me and the prime minister that actually ironed out much of the apparent dispute, ending around mid-August with the prime minister realizing that dialogue and understanding were the right way

to reach the necessary balanced solution to legitimate disputes, rather than corridor manipulations and "power games."

Two Possible Leaks

Toward the end of July, we came to the prime minister's residence for the weekly summary of developments and final approval of a sensitive operational step to be executed over the weekend with regard to the "Yadlin option." To our surprise, we were told that the step probably had to be cancelled for reasons that cannot be detailed here. I argued that there was no need to halt any step and recommended withholding a decision for some time while checking if the problems had not been overestimated. A few hours later, it became clear that I was right.

On another Friday noon meeting, sometime in early August, Mossad Head Dagan brought a serious piece of information that according to his feeling had to compel us to overcome all hesitations and strike immediately:

CIA Head Hayden called at 3 am to tell me that, under U.S. commitments, they were forced to share the information with the British intelligence services.

Hence, he argued that we were facing an immediate risk of leakage that had to be preempted. I did not buy this alarm. Telling the forum that I happened to know the British intelligence services quite well from my experience as head of intelligence, chief of staff, prime minister, and minister of defense, if I had to assess where the bigger risk of a leak lay—from the British services or from this room—I would point inside. Indeed, the British never leaked the secret.

A week later, Dagan warned again of a possible leak, this time from U.S. sources, suggesting we accelerate a decision. I wondered who the possible leaker was but did not get an answer. I said that if I had more information about the publication where the story was going to be published I could have a better sense where the leak was coming from. No further information came, and again, no leak was published.

A Decision Made

Towards the end of August, preparations for the two low signature plans were almost completed with "Lean Shkedi" fully finalized and the "Yadlin plan" almost there. Provisions for war were at an advanced stage. All in all, this signified a miss of my original target date of September 1 by at most a few days. The prime minister and I then discussed the legal aspects of such a decision with the attorney general and made sure that the cabinet was authorized to make the general decision to destroy the reactor and delegate the choice of the concrete plan and the timing of its execution to the prime minister, myself, and Minister of Foreign Affairs Tzipi Livni. This was needed since the dramatic nature of such a decision made it prone to be leaked in short time. The intention was to remain vague regarding the exact way and timing and then, immediately after the cabinet's decision, to meet briefly, one by one, with the heads of Mossad, Intelligence, and the IDF chief of staff to hear their recommendations and immediately make the final, formal decision to execute it the same night.

Around September 1, we agreed to convene the cabinet on September 5 for a final decision. The previous evening, following consultation with Chief of Staff Gabi Ashkenazy, I informed Olmert that my recommendation the next day would be to use "Lean Shkedi" as the preferred option. Both plans were viable and ready, but the "Yadlin plan," which I liked very much, was clearly less likely to gain consensus. It was clear to me that Olmert thought the same. The cabinet meeting began around noon and ended in late afternoon-early evening. It was a relatively focused and short meeting. The participants were acquainted with the different options and somewhat relieved by the absence of the usual tension in the air. In a way, it was simply a ritual, however important, with results known in advance. When the vote came, only Dichter, a former head of the Secret Service (Shabak), abstained.

Immediately after the ministers departed, we continued the process as agreed upon in advance. Olmert, myself, and Livni remained in the room and decided to execute "Lean Shkedi" that very night, meaning that airplanes had to take off in a few hours. The chief of staff and his people, as well as the many hundreds in IAF squadrons and in Intelligence who participated in the operation knew in advance to be ready to execute it that very night. Many thousands in other parts of the armed forces without concrete knowledge of what was happening felt the uniqueness of that evening.

Before leaving my Tel Aviv residence on the 31st floor of a high-rise building, I looked outside into the city's fading night view and suddenly realized that I was watching the F-15s or F-16s flying near my home towards the reactor, some hundred feet underneath my window. Two hours later, from the underground IAF headquarters, we watched the operation. It went as smoothly as we could hope. I could not stop thinking of the violent confrontation that might have ensued under the "Fat Shkedi" alternative. What a difference. After more than an hour-and-a-half, the fighter planes pulled up and released their munitions. A minute or so later came the report: "Accept: Arizona." The reactor had been successfully destroyed. A partial sigh of relief.

More than an hour later, all planes landed safely. According to foreign reports, Bashar Assad was informed of the reactor's destruction sometime soon after the event. It took another twelve hours to confirm our intelligence assessment that a low signature plan would give the Syrian president sufficient leeway to keep the attack under wraps by avoiding any clash with

us. The fact that the circle of people in Syria who knew about the attack was extremely narrow also helped. A great mission accomplished.

The operation succeeded because despite all our disagreements, we had a strong unity of purpose that brought us all together: The devoted Mossad operatives under Dagan's extremely creative leadership who brought the original proof of the reactor's existence; the IDF's intelligence analysts and operational units under Yadlin, a gifted and effective leader; Chief of Staff Ashkenazy, the tireless IDF commander who coordinated the military activities between the IAF and prepared the army for a potential full scale war; Ministry of Defense Director Gen. (res.) Pinhas Buchris, a most capable out-of-the-box thinker, who together with his dedicated subordinates safeguarded the massive supply line needed for the worst-case scenario of war; and, of course, IAF Commander Shkedi, a great commander and great man, with his top teams of pilots and aircrews who did the actual planning, preparation, training, and execution of the operation. Certain credit is due to our internal teams—generals Herzog and Dangot in my office, Turbovitz and Turgeman in the prime minister's office. A special credit must also be given to Prime Minister Olmert who bore the supreme responsibility from day one, never lost sight of the need to destroy the reactor, and took upon himself the burden of the most sensitive contacts with the U.S. government on all levels. I genuinely salute them all, without giving up any of the above criticism. This is the way operational capabilities and national standards of confronting challenges are created: by combining mutual respect with honest, critical, and at times painful discussions of what really happened and what has to be corrected.

Last Thoughts

It is in this respect that I asked myself time and again what created and fed the continued emotional tension around this operation. I assume that other participants have their own views on the same questions. I can hardly fault Olmert for writing, while in prison, a personal, bitter autobiography on his entire life (including the story of the reactor's destruction). Others, myself included, might also have certain personal biases but it is important not to try deliberately to mislead any future student of the case.

Looking back on my entry into the picture, my first memory is of the intense, emotionally loaded, impatient drive for immediate action shared by most people in the room, reinforced by genuine concern lest the operation be torpedoed by a premature leak. Was this due to the overriding influence of PM Olmert on the one hand, and the relative passivity of the outgoing defense minister, Amir Peretz (who had no operational experience), on the other? Or was it due to being on the verge of execution after intensive months of planning, only to be interrupted all of a sudden by a new minister who started raising profound questions, as if the whole planning process had to be restarted all over again? Having commanded this group's members for many years (during my IDF service and as PM and defense minister), I knew all participants in the room much better than both the prime minister or the outgoing minister of defense, which might be somewhat frustrating for them. Whatever the reasons for the tension, I considered preparation of the two low-signature plans an absolute necessity and ensured that they be pushed all the way to successful execution on September 6, 2007.

There was, however, another side to the ledger. Upon assuming my post, I noticed a certain disturbing similarity between what had unfolded in this project during the past three months and the way that the second Lebanon war had been opened and conducted.

A year earlier, on July 12, 2006, an Israeli patrol along the Lebanese border had been attacked with two soldiers killed and two abducted. A short time afterward, a tank that crossed the border in search of the missing soldiers stumbled on a big explosive charge and another five soldiers were killed. It was clear to all that this aggression called for a tough response, yet one that needed to be made in a calm and cool-headed fashion: What were the operation's goals and how to achieve them? What was the "exit strategy"? What would Hezbollah's likely response be, and what were the broader implications of our chosen options? That is what professional standards would dictate.

But nothing of the sort actually happened. Instead, within a few hours, an IAF contingency plan for the destruction of all known Hezbollah missiles and rockets was grabbed from the shelf—where it had been for the preceding six years—and executed the next morning. Dubbed "Specific Weight" and prepared as a surprise opening gambit of an all-out war with Hezbollah, the plan was completed in 2001 and was continuously updated and checked in training exercise every two years or so. Neither I nor Prime Minister Ariel Sharon after me used it even when soldiers were abducted along the border or terror attacks from Lebanon killed several Israelis. Rather, we kept it for the event of a full-fledged war. Yet, on July 13, 2006, Israel found itself in a war that the government did not plan, did not want, and did not prepare for. In fact, when the cabinet met that evening and made the decisions for the next morning, including the execution of "Specific Weight," it did not know it was initiating a war. Thus, reservists, who constitute the main fighting body of the ground forces, were not mobilized and an emergency situation was not announced. The economy was not put on war footing, and objectives for the war/campaign were not defined. That is not the way for a war to be started, and Israel paid the price for this rush decision in the ensuing thirty-four days. When, after the war, I asked one government minister and most involved generals what happened, how did this lapse of judgment come to pass, the most common answer was,

I really don't know. There was a unique atmosphere of extreme urgency to act that swayed all of us. It seemed that you acted improperly if you raised doubts or second thoughts.

One of them added:
It was the triumph of form over substance. We watched and took part in a show of decisiveness that lacked the gravitas to back it up. We put the cart before the horses, and it had its price.
History never repeats itself, and the two cases differ on many levels. But there is a strong similarity in the hasty adoption of a contingency plan that was prepared for something else, together with a hyperactive plan ("Fat Shkedi"), and rush to execute it without an orderly process of considered examination of all things in advance. Systematic thinking and analysis should precede action. Not follow it.
I was cautious not to explicitly express this observation until at the somewhat panicky cabinet meeting on the first week of August, when Deputy PM Mofaz, a former minister of defense and IDF chief of staff, suddenly erupted: "Are you crazy? Is it a replay of the last Lebanon war?"
His question remained unanswered. I can understand the huge pressures that probably influenced Olmert's judgement. Not only did he face the burden of leading the nascent operation, but he had simultaneously to handle a criminal investigation that was to cloud the rest of his premiership (and eventually force him out of office) and an official commission of inquiry of the Lebanon war, headed by Supreme Court Justice Eliyahu Winograd. In these pressuring circumstances, his inner circle fabricated the charge that "Barak was postponing the reactor's destruction in anticipation of his downfall." Complete nonsense. There were too many weighty reasons for my actions, and reality proved them to be fully vindicated.

Ehud Barak, Israel's most decorated soldier and IDF chief of staff (1991-95), served as Israel's prime minister (1999-2001) and minister of defense (1999-2001, 2007-13).

[1] Ori Wertman, "When Israel Destroyed Syria's Nuclear Reactor: The Inside Story," *Middle East Quarterly*, Spring 2022.

Can it be legal to use, or threaten to use, nuclear weapons?

Russia's president has raised the prospect of using nuclear weapons in Ukraine. That's a frightful notion. But it might not violate international law.

By Daniel Warner
Source: https://news-decoder.com/can-it-be-legal-to-use-or-threaten-to-use-nuclear-weapons/

Oct 13 – The war between Russia and Ukraine is bogged down in traditional military fighting. Stymied in its attempt to overwhelm Ukraine, Russian President Vladimir Putin has implied that Russia is prepared to use nuclear weapons.
"To those who allow themselves to make such statements about Russia, I would like to remind you that our country also has various means of destruction, and for some components more modern than those of the NATO countries," Putin said last month, referring to the North Atlantic Treaty Organization.
The use of nuclear weapons has been taboo since the United States bombed the Japanese cities of Hiroshima and Nagasaki at the end of World War Two. Although a number of countries have developed nuclear weapons as a form of deterrence — to prevent attacks with the threat of a nuclear counterattack — no nation has used them since 1945.
But could the use of nuclear weapons be legal?
In 1996, the International Court of Justice (ICJ) considered the question, the very first time any international court had done so.
The ICJ was established more than 50 years ago to deal with differences between nation states, although it is not a formal institution of law like domestic courts and it has no compulsory jurisdiction. The Court traditionally arbitrates disputes between states willing to go before it.

The world asks: Are nuclear weapons legal?
In 1994, the General Assembly of the United Nations asked the Court to render an opinion on the legality of a threat or the use of nuclear weapons under any circumstance. The request followed an earlier demand by the World Health Organization.
The ICJ agreed to render an opinion even though the subject was deemed very political and did not directly deal with a specific dispute between states. The opinion of the Court was highly controversial: The judges were divided **seven against seven**.
"The threat or use of nuclear weapons would generally be contrary to the rules of international law applicable in armed conflict, and in particular the principles and rules of humanitarian law," the ICJ said.
Indeed, the use of nuclear weapons would be indiscriminate and affect civilians and non-combatants, both contrary to humanitarian law.
On the other hand, the Court wrote: "However, in view of the current state of international law, and the elements of fact at its disposal, the Court cannot conclude definitively whether

the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defense, in which the very survival of a state would be at stake."

Russian RS-24 Yars ballistic missiles in Red Square during the Victory Day military parade in Moscow, Russia, 24 June 2020 (AP Photo, File)

The Court's opinion recognized how the use of nuclear weapons would be contrary to humanitarian law. In an argument to the Court, International Law Professor Georges Abi-Saab called them "indiscriminate weapons of mass destruction."
But it allowed their eventual use when a state's survival is at stake. Self-defense is the only justification for the use of force, according to Chapter 7, Article 51 of the UN Charter.

Russia argues it has the right to protect itself.
Russian authorities have used the argument of state survival in their threat to use nuclear weapons by referring to the current situation as "an existential" crisis for the country. Putin's press secretary, Dmitry Peskov, followed the state survival reasoning by equating state survival with an existential threat.
"So, if it is an existential threat for our country, then it [nuclear weapon] can be used, in accordance with our concept," Peskov said.
By equating an "existential" crisis with state survival, the Russians are following the ambiguous opinion of the ICJ and justifying their threat to use nuclear weapons. The argument shows that they are sensitive to the opinion of the Court in finding some reasoning for their threat.
But the taboo against the threat or use of nuclear weapons has stood since 1945. Two organizations have won Nobel Peace Prizes in advocating the abolition of nuclear weapons. It remains to be seen if Russia will follow through on its threat.
In sum, the opinion of the ICJ gave no definitive answer to the legal question.

Daniel Warner earned a PhD in Political Science from the Graduate Institute of International Studies in Geneva, where he was Deputy to the Director for many years as well as founder and director of several programs focusing on international organizations. He has lectured and taught internationally and is a frequent contributor to international media. He has served as an advisor to the UNHCR, ILO and NATO, and has been a consultant to the Ministries of Foreign Affairs and Defense of Switzerland as well as in the private sector.

EDITOR'S COMMENT: Let's start with the title question. Nuclear weapons are weapons the same way F-35 or B-52 are. So, if it is illegal to have them, it is illegal to have

warplanes or cruise missiles or frigates or UAVs or tanks. The next question is about what weapons are for. Obviously, they are meant to protect the population of a country under attack (but also to invent other countries for a reason according to their judgment). The third question is why have weapons of any kind if not intend to use them? In that respect, the threat of using weapons is silly since it is not enough to avoid an attack although it might lessen the possibility substantially. So, why spend ink and saliva asking questions with so obvious answers?

Provocative nuclear exercises – a big mistake

Source: https://cnduk.org/provocative-nuclear-exercises-a-big-mistake/

Oct 18 – CND has condemned NATO's ongoing round of nuclear weapons exercises, warning they will further escalate tension and military conflict in Ukraine.

The nuclear drills – titled Steadfast Noon – commenced on Monday and will run for two weeks. They are training air crews to use US tactical nuclear bombs in the event of a nuclear war. At a time when there is regular reference to the use of tactical nukes in the context of the Ukraine war, this is indeed an unwise and provocative act.

The exercises involve 14 NATO members and around 60 aircraft. These include fourth and fifth generation fighter jets, tanker and surveillance aircraft, as well as a number of US B-52 long-range bombers. The exercises are an annual occurrence but coming this year at a time of heightened tensions between NATO and Russia, they are likely to stoke further tension. Moscow, meanwhile, will hold its own nuclear exercises – called Grom.

The exercises are designed for US nuclear bombs that are stored in at least six US-operated NATO bases in Europe under a so-called nuclear sharing agreement. This means that non-nuclear weapons states use US nukes in times of war. The bases have special weapons storage facilities – many of which have undergone multi-million-dollar modernisation. They are Kleine Brogel in Belgium, Büchel in Germany, Aviano and Ghedi air bases in Italy, Volkel air base in the Netherlands, and possibly Incirlik in Turkey.

Britain's role in these US nuclear exercises follows reports last April that the US-run Lakenheath airbase in Suffolk was also undergoing modernisation of its nuclear weapons storage facilities heralding the likely return of US nukes to Britain. This has led to renewed calls from CND and others for the UK government to reject the return of these weapons.

CND is holding a national demonstration at Lakenheath on Saturday, 19 November – to demand that these weapons of mass destruction are removed from Britain.

CND General Secretary Kate Hudson said: "These nuclear exercises couldn't come at a worse time. We call on our government to withdraw – and to reject the stationing of US tactical nukes in Britain. We will work with movements across Europe to put an end to 'nuclear sharing' and win a nuclear weapons-free continent."

What If Putin Actually Uses Nukes on Ukraine?

By Benjamin Hart

Source: https://nymag.com/intelligencer/2022/10/what-if-putin-actually-uses-nuclear-weapons-on-ukraine.html

Oct 08 – Suddenly, talk of nuclear apocalypse is in the air for the first time in decades. With his forces continuing to struggle in Ukraine, Russian president Vladimir Putin has begun regularly invoking his country's massive arsenal of nukes in what many view as a sign of desperation. In a menacing speech last week, Putin claimed that he would use "all the forces and means at our disposal" to defend areas of Ukraine he had illegally annexed and that he was not bluffing. Though experts largely believe the chances are low that Putin will follow through on that threat, the mere possibility has rattled western leaders. I spoke with Edward Geist, a policy researcher at the RAND Corporation, about why a Russian nuclear strike could cause even more damage than intended, whether Putin's strike orders could be ignored, and how the U.S. might respond.

Speaking about Vladimir Putin's nuclear threats, President Biden said at a private fundraiser on Thursday night, "We have not faced the prospect of Armageddon since Kennedy and the Cuban Missile Crisis." Do you think that was an appropriate comparison?

We don't know what the probability of nuclear war is at any particular moment. We have intuitions, and the usual intuition is that the Cuban Missile Crisis is the closest we've ever come. But we actually don't know how close we came then or at any other point in the past. There's this controversy about the 1983 Able Archer exercise (a NATO exercise Russia mistook for military escalation) — whether that was actually a war scare. And I know experts on this subject who are diametrically opposed to one another on that question.

The thing that makes it so scary is that we genuinely don't know. It's not like there's some magical dial in a cabinet at the Kremlin and Putin is twisting it up and down. The nuclear

threshold doesn't work like that. We don't know quite how the different actions we take interact with that cosmic danger.

Yars ballistic missile rolls in Red Square during a dress rehearsal for the 2022 Victory Day military parade in Moscow, Russia. Photo: Alexander Zemlianichenko/AP/Shutterstock/Alexander Zemlianichenko/AP/Shut

So you can't say if we're all going to die in the next week.

Despite all the reversals the Russians are having, they're probably not on the verge of doing anything like this.

Other than Putin's saber-rattling, is there any physical, tactical sign that anything is different about Russia's nuclear posture than it was a month ago?

The U.S. intelligence community has said, and this is apparent to us, that the steps we would expect to see them take if they were about to use one of their so-called nonstrategic nuclear weapons (also known as tactical nuclear weapons) — we don't seem to be seeing those indicators. Only a part of their strategic nuclear forces is actually sitting on missiles and ready

to be used at any particular time. They have missiles in silos, and they have some missiles on submarines. Some of those things are always ready to fire, but the nonstrategic nuclear weapons are stored in central facilities separate from their delivery system. The missiles that would launch them — like the Iskanders or whatever — they don't usually have nuclear weapons on them. In order to combine the two, you'd have to move things around. You'd have to take the launch system and the warhead to the same place, and we haven't seen that activity.

It is true that the Russians could conceivably use a weapon off of one of these strategic platforms that's always available. So the idea that we would get a warning before some kind of Russian limited nuclear use is something we can't necessarily count on. Another thing that's worrisome going forward is that they may just start doing some of this stuff as an intimidation tactic. They could take a nuclear warhead and put it on a nonstrategic launch platform and may just leave things that way, then not actually use any nukes.

Let's say Putin did use a low-grade tactical nuke, whether that's on a Ukrainian facility or as a show of force above a body of water. What would the immediate effect look like?

There's this widespread notion that the first thing you might do is take one of these tactical nukes and detonate it over the ocean or something in order to demonstrate resolve. That's very easy to do, and given Putin's terrible judgment so far, I suppose we shouldn't rule it out entirely. But it would actually leave a very different impression than people imagine, because it would look like nothing.

It's not going to look intimidating; it's actually going to look sort of dumb. If it's not close to the surface, you're not going to be able to see it. If there aren't people nearby, you're not going to have video of it. If you want to be intimidating, it has to be designed to look impressive on TV.

So let's say he did something more dramatic and actually used it on facilities or people.

It depends on the combination of weapon and target and also some intangibles. There are people who assume there's this Goldilocks point, where, if the weapon is accurate enough, you can maximize blast effects and avoid fallout effects by detonating it at a certain elevation over the target. In real life, it's more complicated than that. In real delivery systems, the CEP (the circular error probable) — or the spherical error probable if you're talking in three dimensions — that's just for the weapons that don't malfunction. Some of those possible malfunctions involve the weapon detonating in a place that's outside the statistical distribution of what we consider a near miss.

Let me make this concrete. Let's say Putin wants to nuke a command post in Ukraine somewhere. And Russia takes an Iskander ballistic missile and puts a tactical nuclear warhead on it. There are various claims for what size warhead might go on this thing, but let's say it's on the order of a few kilotons. They do the math to detonate this at a precise altitude, so that they'll get the blast effect over the facility but avoid fallout. But then the weapon may malfunction. Maybe the fusing doesn't work, so it donates at the wrong altitude. So the fireball does intersect with the ground, and there's all this fallout. And they were trying to avoid that — but we didn't know.

You had a Twitter thread about rain making nuclear fallout worse by contaminating the ground.

Yeah. So if you detonate a nuclear weapon and there's a rain cloud above where all the radiological mess is in the ground, what would've been fallout is now "rainout." And there are arguments I find convincing — this appears in computer models and appears to have maybe happened in the atomic bombings in Japan — where the nuclear explosion itself creates what's called a pyrocumulus like a big forest fire can. The heat source actually causes a rain cloud to form, then it can rain out the nuclear fission products directly. That's really scary, because it's so near to the burst time that the stuff is ludicrously radioactive.

If it's rained out within a few minutes of the burst, the doses that can be experienced on the ground by people are outrageous even for a low-yield device. So there are all these sorts of intangibles, where Russia could be trying very hard to engineer the attack to avoid collateral damage, then just fail.

If Putin wanted to launch nukes, is there a possibility that someone under him could successfully resist the order?

Supposedly, their system has a two-man rule. The Russian president is the National Command Authority, and he could order the use of nuclear weapons. But the Russian president, the minister of defense, and the head of the general staff all have the nuclear football. So it's unclear what happens if Putin just loses his mind and says, "I hate America so much, I want to nuke America." If Gerasimov and Shoigu are like, "Sir, you've gone mad, and I'm not going to agree to this" — what happens at that point? Because on the one hand, it has sometimes been asserted that at least two of those footballs have to be activated in order to actually use nuclear weapons. But Putin is allowed to dismiss those guys at will and find somebody who's more compliant.

Like Nixon's Saturday Night Massacre but much worse.

It's not clear whether that mechanism actually would stop nuclear use of whatever kind from being authorized. But it's not automated the way that people sometimes assert it is. There are a whole bunch of steps you have to go through. Like, if you're on a submarine, the submarine has to come up to launch depth.

Pavel Podvig (an independent nuclear analyst) argues, and I am inclined to agree, that the fully automated system that was proposed in Russia in the 1980s never got implemented because of the obvious safety problems. With the systems as they are now, I believe there

has to be a final guy with the key. And a lot of these systems — like the submarines, the mobile missile launchers — you have to take a lot of steps to get them ready to fire.

The Russian submarines can launch from dock sites. And with the mobile missile launchers, they've got special garages where the roof opens, so they can just sit in their garage and if they get the order, they can fire from the garage. But there's still a series of steps you have to take.

Well, that's mildly comforting. How do you rate the difference in odds between Russia using tactical nukes and the even more powerful ones?

It's another one of these things that's hard to know. But if Putin decided to do a demonstration strike, he could take one of their highest-yield weapons and detonate it over their old nuclear test site in the Arctic. And I think that would look a lot more impressive than detonating a low-yield weapon over the Black Sea. So the possibility should be considered more than it currently is.

Limited nuclear use is not the same thing as tactical nuclear use. The Russians have a whole lot of tactical nuclear weapons, and in principle, they could use a whole lot of them. And many of these nonstrategic weapons are not actually low-yield in a meaningful sense. A lot of them are on the same order as Hiroshima.

And we're talking thousands, or tens of thousands, of these nukes?

By the estimates of the Federation of American Scientists, it's maybe a couple of thousand, which by the standards of contemporary nuclear arsenals is a lot of weapons. By Cold War standards, that's not actually that many, but the Cold War was crazy and frightening.

This week, President Zelenskyy of Ukraine issued a plea for "preemptive strikes" to prevent Russia from using nuclear weapons. (Ukraine claimed he was referring to economic sanctions.) I take it you don't think a first-strike attack on Russian weaponry is likely.

Let's just say that I find that sort of viewpoint fanciful, partly because the Russian policy is "launch under attack." Going back to the Soviet era, if there's a major attack against Russia from whomever, their policy is to try and launch their weapons while they are being attacked.

How do you think the U.S. or NATO would respond to Russia's usage of low-grade nuclear weapons?

Western leaders would have to make a call about how they wanted to respond, and they may do something different than they imagined that they would do before it happened. It's another one of these huge intangibles.

There has been debate in recent administrations about limited Russian nuclear use and how we should respond — Fred Kaplan talks about this in his book. There's a school of thought that if they do it, we have to show that we are not intimidated, and the way we need to show that is by using one ourselves. There's also a school of thought that we don't solve this problem of somebody using nuclear weapons by using nuclear weapons ourselves. Which one of those is right depends on the perceptions of other people. It depends on the perceptions of the adversary, and it depends on the perceptions of audiences both at home and abroad.

There's the argument that we have to say that we're going to do that for deterrence, that we have to be ready to respond in kind or they will think that they can get away with doing it. But that's not at all the same thing as saying that we actually *should* respond in kind in any particular situation — and especially not as a blanket policy.

Pakistan Protests Biden Questioning of Safety of Pakistan's Nuclear Weapons

By Ayaz Gul

Source: https://www.homelandsecuritynewswire.com/dr20221018-pakistan-protests-biden-questioning-of-safety-of-pakistan-s-nuclear-weapons

Oct 18 – Pakistan said Saturday that it had formally protested to the United States over remarks by President Joe Biden questioning the safety of Islamabad's nuclear weapons.

"We have summoned the ambassador of the United States to Pakistan, Mr. Donald Blome, to the foreign office Pakistan for an official demarche," Foreign Minister Bilawal Bhutto Zardari told a news conference in Karachi.

Biden told a Democratic Congressional fundraiser Thursday night that Pakistan "may be one of the most dangerous nations in the world" for possessing "nuclear weapons without any cohesion."

The White House published Friday the transcript of the president's address in California, which has since sparked outrage in the nuclear-armed South Asian nation.

"As far as the question of the safety and security of Pakistan's nuclear assets are concerned, we meet all, each and every international standard in accordance with the IAEA," Zardari reaffirmed.

Zardari apparently confused his country 's nuclear weapons program with the civilian nuclear program because Pakistan's weapons-based nuclear development is not under the IAEA monitoring.
He said he was surprised by Biden's statement and attributed it to a "misunderstanding" that Zardari said stemmed from a lack of engagement between Islamabad and Washington.
At the same time, the foreign minister attempted to downplay the significance of the remarks, saying Biden did not make them at an official function or in an address to his nation.
"We should allow them an opportunity to explain this position. I don't believe that this should negatively impact the relations between Pakistan and the United States," Zardari noted.
White House Press Secretary Karine Jean-Pierre defended as "nothing new" the remarks made by the president, saying he "views a secure and prosperous Pakistan as critical to U.S interests."
Zardari traveled to the U.S. this month where he held wide-ranging talks with Secretary of State Antony Blinken, marking the 75th anniversary of bilateral relations between the two countries.
But opposition leaders led by Pakistan's populist former prime minister, Imran Khan, slammed Present Biden for questioning the security of the nuclear weapons.
"Unlike the U.S., which has been involved in wars across the world, when has Pakistan shown aggression, especially post-nuclearsation?" Khan asked on Twitter.
He also questioned assertions made by the Pakistani government that it had "reset" bilateral relations with the United States, calling the American president's statement a "total failure" of Prime Minister Shehbaz Sharif's foreign policy.
Khan, a known harsh critic of the U.S.-led military invasion of Pakistan's neighbor, Afghanistan, was removed from office in April of this year in a parliamentary no-confidence vote advanced by the Sharif-led then-opposition alliance.
The ousted cricket-star-turned-politician alleges without evidence that the vote was orchestrated by Washington in collusion with Sharif and the Pakistani military. Both Washington and Islamabad deny the accusation.
Khan, 70, was still in power when Washington withdrew all U.S. forces from Afghanistan in August 2021 after almost two decades of war with Taliban insurgents, who have since seized control of the conflict-torn country.
Pakistan was a U.S. ally in the war and provided its ground, as well as air routes, to ferry crucial supplies for tens of thousands of U.S.-led international forces in landlocked Afghanistan. But some in Washington say Islamabad's military and intelligence agencies covertly aided the Taliban to enable them to sweep back to power in Kabul, souring bilateral relations.
Pakistan's close military and economic partnership with China is also a cause of concern for Washington. U.S. officials repeatedly have warned that Beijing's billions of dollars of investment in developing Pakistan's infrastructure and power plants under China's Belt and Road Initiative could end up being a "debt trap" for Islamabad.
Pakistani and Chinese officials dismiss those concerns. China also maintains deep military cooperation with Pakistan.
Beijing has built several nuclear power plants to help the neighboring country meet its energy shortages. The nuclear cooperation is strictly in line with IAEA requirements and safeguards, officials in both countries maintain.
"Ever since May 1998, when Pakistan first began testing nuclear weapons, claiming its national security demanded it, American presidents have been haunted by the fear that Pakistan's stockpile of nukes would fall into the wrong hands," wrote the Brookings Institution on its website late last year.
"That fear now includes the possibility that jihadis in Pakistan, freshly inspired by the Taliban victory in Afghanistan, might try to seize power at home," wrote the author of the statement at the nonprofit public policy organization based in Washington.

How not to estimate the likelihood of nuclear war

By Amy J. Nelson and Alexander H. Montgomery
Source: https://www.brookings.edu/blog/order-from-chaos/2022/10/19/how-not-to-estimate-the-likelihood-of-nuclear-war/

Oct 19 – As Russia retaliated for Ukraine's destruction of the Kerch Bridge by launching strikes on energy facilities and civilian targets in Kyiv, commentators returned to the question of whether events were escalating, and whether the world was inching closer to the brink of nuclear war. Probability estimates by these observers have, unsurprisingly, mushroomed as well.
On the high end, these estimates ranged from 10-20 percent to an overly precise 16.8 percent to 20-25 percent for "some analysts."
Some of these headline-grabbing estimates are likely inflated to create a sense of urgency and put pressure on policymakers to take action, rather than to showcase the ability to carefully craft probability estimates. The difference between estimates may simply reflect the prominence of each nuclear scenario in each analyst's mind.

Here, we lay out the debate over the probability of nuclear use, outlining flaws in current estimates. We offer an alternative approach that focuses on thinking broadly across multiple scenarios and minimizing the rewards of using nuclear weapons, to minimize the possibility of nuclear war.

Can you put a number on the likelihood of nuclear use?

Predicting the future is hard, and estimating the probability of future events is no exception. Estimating the probability of future events like ones that have occurred many times before is already difficult enough, since — in a complex world — it is difficult to determine which factors decreased or increased the probabilities for past events. For example, the possible causes of Russia's attacks on Ukrainian civilians span across international, domestic, and psychological explanations.

Trying to estimate the probability of nuclear use is just as difficult — if not more so. Nuclear scholar and Russian forces expert Pavel Podvig argued along these lines in Newsweek and on Twitter, publicly asserting that nuclear strikes are so rare, it is impossible to calculate their frequency and therefore meaningless to translate that frequency into a probability. Director of the Global Catastrophic Risk Institute Seth Baum noted that Podvig was critiquing frequentist approaches to calculating, which infer how likely an event is to happen based on a sampling of past similar events. He argued that instead, Bayesian approaches – which rely on subjective probabilities that get updated when new information is presented – could be a more helpful way of thinking across multiple different nuclear scenarios, as Baum himself has done in a working paper. Superforecasting, when ordinary people cultivate their intuitive sense for prediction, and which relies in part on good Bayesian updating, is one such approach to nuclear scenarios; Baum's co-author and superforecaster Robert de Neufville argued in March that there was a 4% chance of at least one fatality from nuclear use by July 1, 2022.

What's going on here? Is Baum correct that Bayesian approach is the right way to think about nuclear use? And is this war of the nerds helpful in understanding how to avoid nuclear war?

Podvig and Baum are correct that frequentist approaches are definitely not useful here. Estimating the likelihood of a future nuclear war based on how often past nuclear wars occurred is not appropriate, given how rare past nuclear weapons use is.

Bayesian approaches are useful for thinking about adjusting one's own subjective estimate of probability, but not for informing the actual probability of Putin deciding to use a nuclear weapon. What's more, there is no way of adjudicating between subjective estimates, and consequently no way of coming up with a combined estimate overall. Even people with the same information may have wildly different guesses: Former U.S. President John Kennedy estimated the odds of nuclear war during the Cuban Missile Crisis to be between one in three and one half, but former U.S. National Security Advisor McGeorge Bundy thought it was one in 100.

Even approaches that attempt to deal with this problem of competing subjective estimates, such as a team of superforecasters working together, cannot work here, since they rely heavily on good estimates of the base rate of an event occurring, which is similarly difficult. As RAND economist Alain Enthoven said to a senior Air Force general, "General, I've fought just as many nuclear wars as you have." Moreover, there is no one in the Kremlin turning the dial up or down, creating an objective change in the probability of nuclear weapons use.

We are also likely to overestimate the likelihood of nuclear war when those estimates are informed by public behavior, because we can't see the private behavior that would decrease our estimates. Russian leaders have good reasons to make multiple public threats. By increasing other countries' perception that Russia is willing to use nuclear weapons, the Kremlin increases Russia's bargaining leverage (although this can also create a commitment trap, where a country that has threatened to use nuclear weapons could be forced to do so in order to remain credible). This means that when numerous threats are made over time, **subjective estimations of the probability of nuclear war act as a ratchet, even when the exact same statements are repeated**. These estimations cannot take into account unobserved private efforts that are being made to decrease the chance of war.

While we tend to think of nuclear escalation as a ladder, it can be more like an escalator or a vortex, or even a roller coaster. What looks like a terrifying downhill rush towards nuclear war may be balanced out by private counters that slow momentum and return it to level ground: The anticipation of the danger of nuclear use leads actors to try to overcome it. Such recalibrations may be better carried out privately. As U.S. Secretary of State Jake Sullivan noted, "We have communicated to the Russians what the consequences would be, but we've been careful in how we talk about this publicly, because from our perspective we want to lay down the principle that there would be catastrophic consequences, but not engage in a game of rhetorical tit for tat."

It is a mistake for analysts to ascribe a statistical probability for the likelihood of nuclear war, instead of a relative claim (such as "very" or "more than yesterday"). They should also be accompanying estimates with their confidence in the estimate. Yet, many foreign policy experts appear to be far too confident in their assessments. Making a useful probability assessment is impossible under conditions of uncertainty, when we are lacking information about the variety of possible outcomes or the probability of those outcomes.

Instead of focusing on numbers, think about possibilities

A possibilistic approach, which takes for granted that something might happen but with a likelihood that cannot be determined, is more appropriate here, just as it is when thinking about other high-impact future events.

The origins of thinking about the possibility of nuclear war in this way are found in early game theory approaches (economic studies of interacting choices where the outcome of a country's action depends upon other people's actions), which offered frameworks that allowed us to think clearly about conditions for nuclear war. But these kinds of approaches can *also* mislead us if we think we can actually estimate probabilities, or that the estimates we produce must be universally accepted.

Rather than provide punditry on the probability of Putin's use of nuclear weapons, we should consider pathways that lead to war and reduce the *possibility* of going down those pathways. In arms control, this means eliminating particularly destabilizing weapons systems; here, it means minimizing the reward of using nuclear weapons.

Apocalyptic scenarios have no reward. Yet, limited-use scenarios that help to achieve Putin's goals may appear to him to do so, even though such strategies are high variance and are essentially "gambling for resurrection" when an actor feels like they are losing and are calculating from the "domain of losses."

Public and private actions that decrease any apparent value of limited use of nuclear weapons for Putin should, consequently, be the main focus. Since nuclear weapons offer no great advantage for tactical use due to the dispersal of forces on the modern battlefield, use is more likely to be to demonstrate resolve and preserve his strength at home and abroad to counter existential threats to his regime.

Consequently, there must be assurances that NATO does not intend to threaten his regime now, and intimations that it may do so if nuclear weapons are used. Western leaders have been careful to state that they do not seek regime change, and should continue to do so.

Carefully crafted statements that their war aims and means may change if nuclear weapons are used will help to minimize any benefits Putin might perceive from nuclear use. For example, NATO Secretary General Jens Stoltenberg stated that "Any use of nuclear weapons would fundamentally change the nature of the conflict, and have severe consequences."

So, if an expert offers you a probabilistic assessment of the likelihood of nuclear war breaking out, you should be very skeptical. Smarter questions and answers should instead focus on scenario-driven approaches that offer different pathways useful for reducing or eliminating certain scenarios.

Even though we do not think that quantifying the probability of nuclear use is useful for informing U.S. policy, thinking about how to reduce the possibility of the most salient potential pathways to nuclear use is the best approach.

Amy J. Nelson is a David M. Rubenstein Fellow - Foreign Policy, Strobe Talbott Center for Security, Strategy, and Technology.
Alexander H. Montgomery is a Professor of Political Science - Reed College.

Plan A

Source: https://sgs.princeton.edu/the-lab/plan-a

SGS developed a new simulation for a plausible escalating war between the United States and Russia using realistic nuclear force postures, targets and fatality estimates. It is estimated that there would be more than 90 million people dead and injured within the first few hours of the conflict.

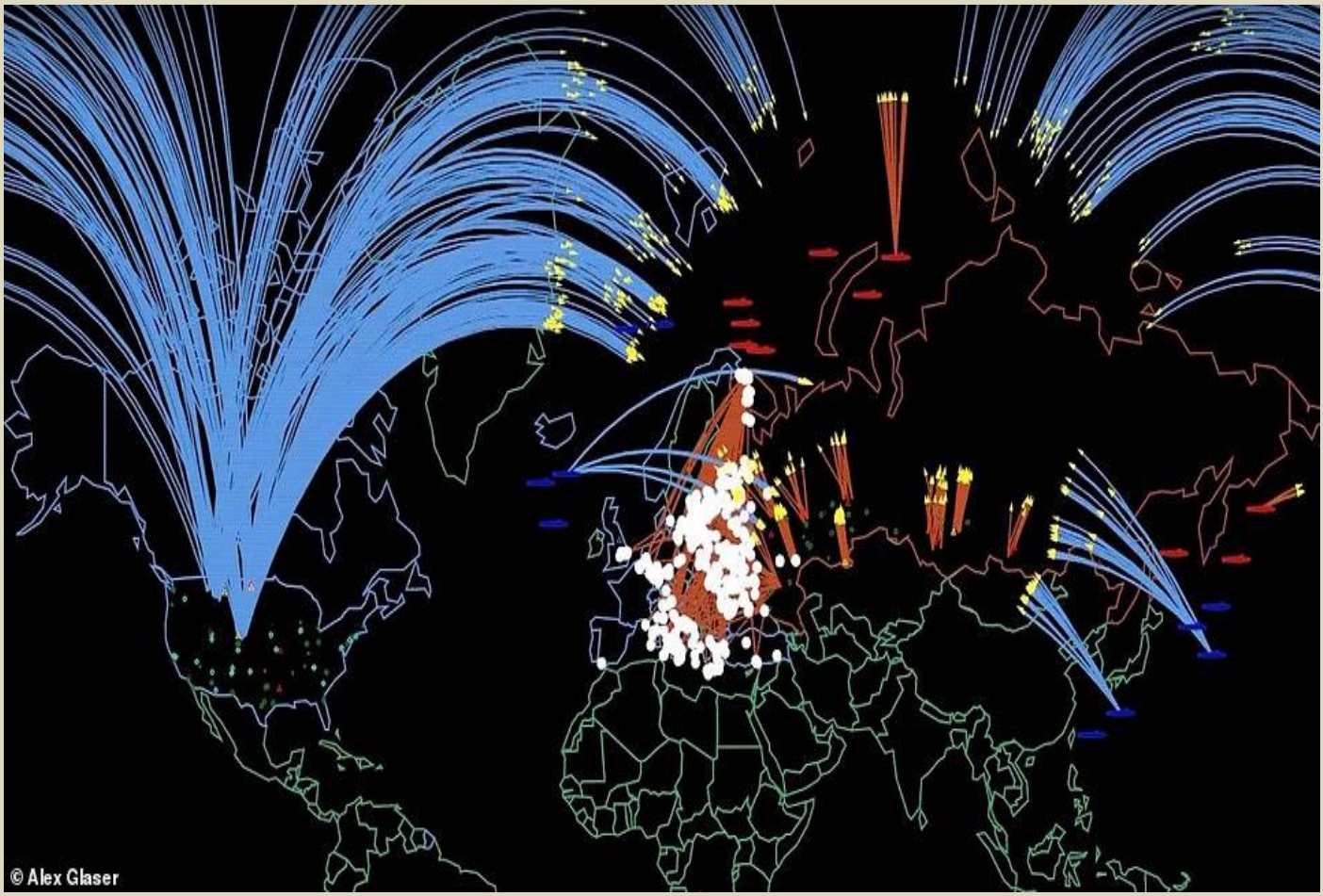
This project is motivated by the need to highlight the potentially catastrophic consequences of current US and Russian nuclear war plans.

The risk of nuclear war has increased dramatically in the past two years as the United States and Russia have abandoned long-standing nuclear arms control treaties, started to develop new kinds of nuclear weapons and expanded the circumstances in which they might use nuclear weapons.

This four-minute audio-visual piece is based on independent assessments of current U.S. and Russian force postures, nuclear war plans, and nuclear weapons targets. It uses extensive data sets of the nuclear weapons currently deployed, weapon yields, and possible targets for particular weapons, as well as the order of battle estimating which weapons go to which targets in which order in which phase of the war to show the evolution of the nuclear conflict from tactical, to strategic to city-targeting phases.

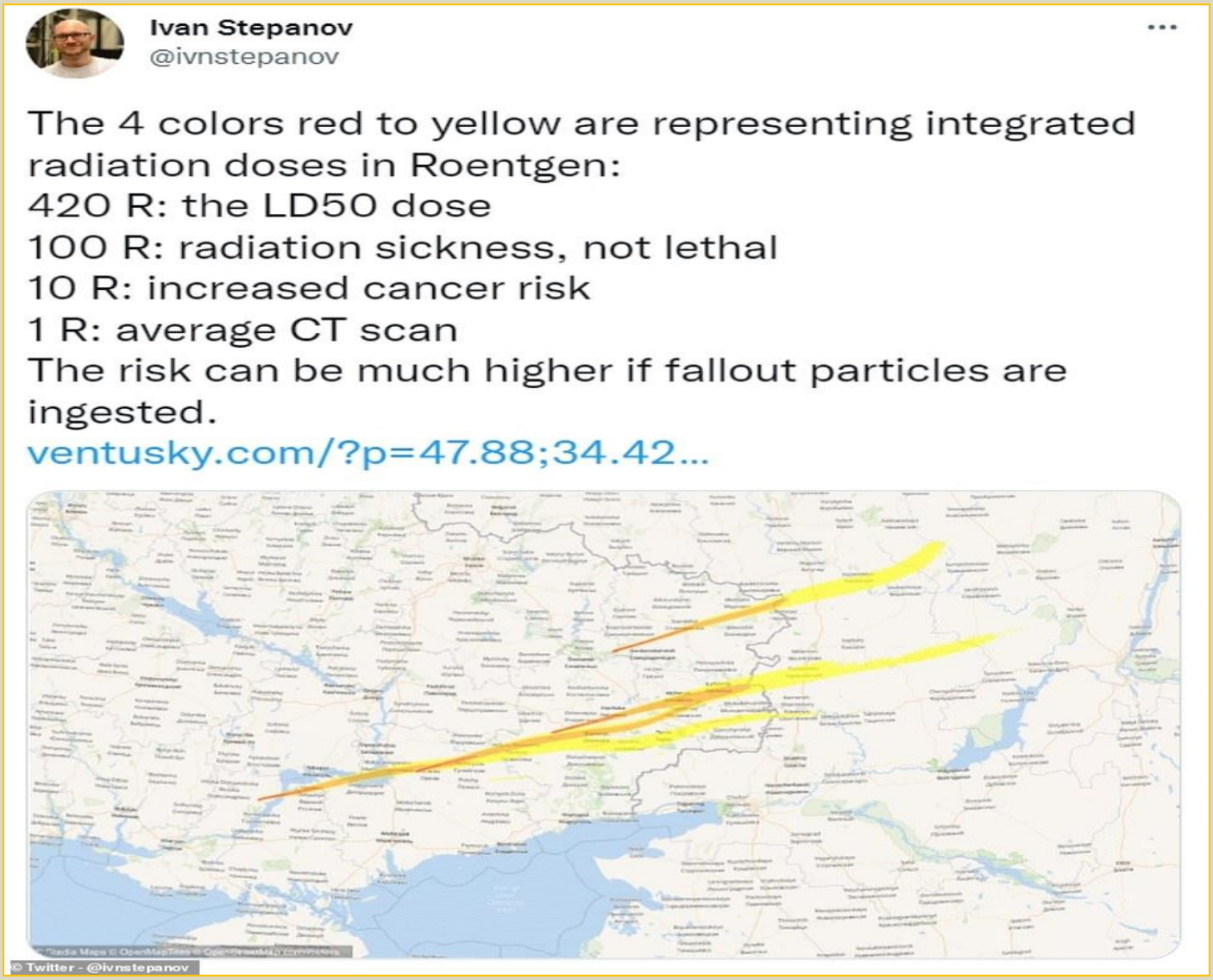
The resulting immediate fatalities and casualties that would occur in each phase of the conflict are determined using data from NUKEMAP. All fatality estimates are limited to acute deaths from nuclear explosions and would be significantly increased by deaths occurring from nuclear fallout and other long-term effects.

The simulation was developed by Alex Wellerstein, Tamara Patton, Moritz Kütt, and Alex Glaser with assistance from Bruce Blair, Sharon Weiner, and Zia Mian. The sound is by Jeff Snyder.



This simulation begins within the context of a conventional, non-nuclear conflict.
Russia fires a warning shot from a base near Kaliningrad, on the Black Sea, to stop a US-NATO advancement, before they retaliate with a single, tactical air strike.
Russia then sends 300 warhead explosives, carried either by aircraft or short-range missiles, towards NATO bases and advancing troops in Europe.
The international military alliance would then respond with around 180 aircraft-borne nukes.
At this stage, casualties would be expected to reach around 2.6 million people within a three-hour period and Europe is left essentially destroyed.
Following this, NATO acts from the continental US and nuclear submarine fleets, launching a strategic nuclear strike of around 600 warheads.
Before this strike hits and its weapons systems are destroyed, Russia launches nukes from its complement of missile silos, submarines and mobile launch pads.
The model projects 3.4 million casualties from this phase of the war, which would last only 45 minutes.
In the final phase of the conflict, both sides take aim at each other's 30 most populated cities and economic centres — deploying 5 to 10 nukes for each one — to attempt to inhibit each side's recovery from the war.
Such a move, the researchers conclude, would see another 85.3 million casualties within the space of 45 minutes.
Many countries in the model appear to escape being the direct target of a nuke, such as those in the southern hemisphere, and Scotland.
However, the effects of the nuclear fallout, collapsing medical systems and longer-term impacts on the Earth's climate, population and food production would have wide-ranging effects.

German engineer Dr Ivan Stepanov has also developed his own nuclear war simulator program, which he has used to predict the outcome of a Russian strike.His model is called Nuclear War Simulator and allows users to simulate 'realistic large-scale scenarios



between major powers with thousands of warheads'. Dr Stepanov was born in the city of Semipalatinsk, Kazakhstan, which is less than 100 miles from a site where Soviet authorities once tested most of their nuclear weapons.

ICI International CBRNE INSTITUTE

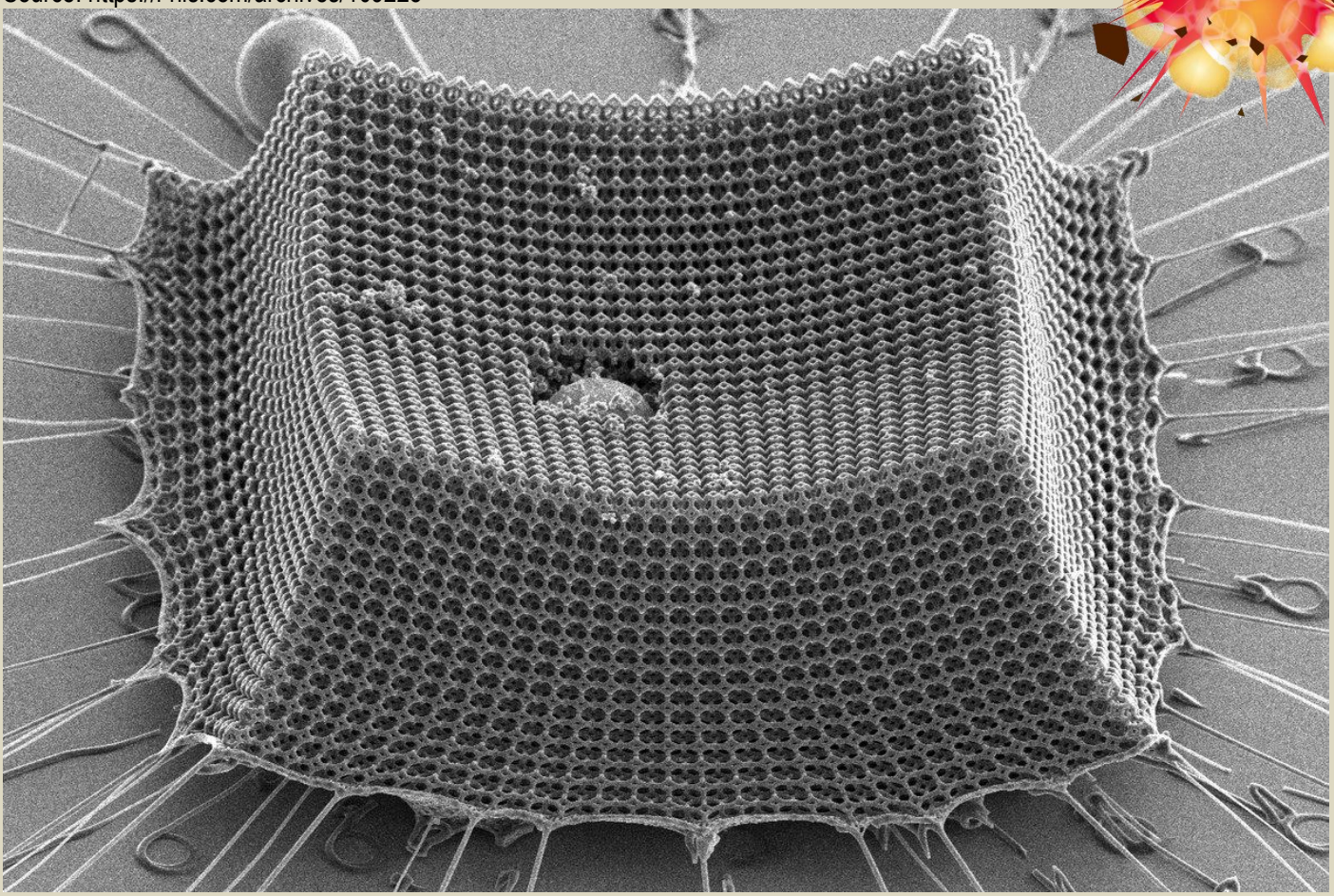
CBRNE-Terrorism Newsletter

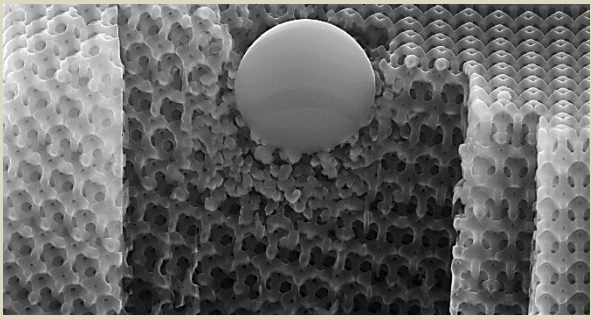
C2BRNE DIARY

EXPLOSIVE NEWS

This New Material Has Potential for a Blast Shield

Source: https://i-hls.com/archives/109225





Sep 23 – The discovery of a new material may be a promising route to lightweight armor, protective coatings, blast shields, and other impact-resistant materials. Researchers at MIT, Caltech, and ETH Zürich have fabricated **"nanoarchitected" materials** — materials designed from precisely patterned nanoscale structures. The nanometer-scale carbon struts give the material toughness and mechanical robustness.

According to reports by Phys.org, the team tested the material's resilience by shooting it with microparticles at supersonic speeds, and found that the material, which is thinner than the width of a human hair, prevented the miniature projectiles from tearing through it. The researchers calculated that in comparison with steel, Kevlar, aluminum, and other impact-resistant materials of comparable weight, the new material is more efficient at absorbing impacts. If produced on a large scale, this and other nanoarchitected materials could potentially be designed as lighter, tougher alternatives to Kevlar and steel.

"The knowledge from this work… could provide design principles for ultra-lightweight impact resistant materials [for use in] efficient armor materials, protective coatings, and blast-resistant shields desirable in defense and space applications," says co-author Julia R. Greer, a professor of materials science, mechanics, and medical engineering at Caltech, whose lab led the material's fabrication.

A nanoarchitected material consists of patterned nanometer-scale structures that, depending on how they are arranged, can give materials unique properties such as exceptional lightness and resilience. But this potential has largely been untested.To test the material's resilience to extreme deformation, the team performed microparticle impact experiments at MIT using laser-induced particle impact tests. The technique aims an ultrafast laser through a glass slide coated with a thin film of gold, which itself is coated with a layer of microparticles—in this case, 14-micron-wide silicon oxide particles. As the laser passes through the slide, it generates a plasma, or a rapid expansion

of gas from the gold, which pushes the silicon oxide particles out in the direction of the laser. This causes the microparticles to rapidly accelerate toward the target.

Two Bombings in One Night? That's Normal Now in Sweden.

Source: https://www.commonsense.news/p/two-bombings-in-one-night-thats-normal

The aftermath of a bombing at a multi-family home in Stockholm. (Barbro Bergfeldt via Alamy)

Sep 22 – Yesterday morning, Swedes woke up to news of a kind that has become all-too familiar: During the night, powerful bombs exploded at apartment buildings in two different towns in southern Sweden.

One person was severely injured in Åstorp, where a witness told the press: "People screamed and cried. It felt so unreal." A resident told Radio Sweden that his 7-year-old had come running into his bedroom screaming, as the blast made their apartment shake.

In Helsingborg, the explosion was so powerful that, according to the police, cars parked nearby were destroyed. It is still unclear if the bombings are connected to each other, or who is behind them.

Since 2018, there have been almost 500 bombings—yes, bombings—in what is known as one of the most stable societies in the world.

There's not just a bombing problem. There are shootings, too.

Sweden, which has a population of around 10 million, has the highest per-capita number of deadly shootings of 22 European countries. Forty-seven people have been shot dead so far this year, which, while far from American levels of gun homicide, is extreme for Europe. Other European countries have come to look at Sweden with horror.

It may be shocking for Americans to learn that in Sweden—the land of IKEA, Spotify and Greta Thunberg—all of this is going on. Perhaps the reason you don't know about it is because of the uncomfortable reality of how we got here.

Among shooting suspects, 85 percent are first- or second-generation immigrants, according to the newspaper Dagens Nyheter, as immigrant neighborhoods have become hotbeds for gang crime. National Police Commissioner Anders Thornberg has described the violence as

"an entirely different kind of brutality than we've seen before" and his deputy, Mats Löfving, says that 40 criminal clans now operate throughout the country. Spreading fear are "humiliation robberies," targeting children and youth, in which victims are subjected to degrading treatment by assailants, such as being urinated upon. Just this week, four men were sentenced for robbing, beating and urinating on an 18-year-old, who was also filmed by his tormentors.

All of which is why, for the first time ever, crime emerged as a top priority among voters ahead of this past weekend's general election. Swedes made their concerns plain on Sunday, when they awarded the country's most strident anti-immigration party more than 20 percent of the vote.

The Sweden Democrats, or SD, is now the second-biggest party in parliament, and the biggest party of the right-wing bloc—gaining more votes than the more traditional center-right Moderate party. (It remains to be seen whether Ulf Kristersson, leader of the Moderates, can form a government with the support of SD, while sticking to his promise not to allow the party into the government coalition.)

So how did Sweden's famously liberal electorate usher in a party with roots on the extreme right? In a word: denial.

In response to Sweden's increasing problems with gang violence and social unrest in immigrant suburbs, the government's strategy for many years was to deny how serious the situation had become. In the meantime, those people who noticed the problem—many of whom were working class—and spoke out about their diminished safety were accused of racism by leading politicians, the mainstream press, and the cultural elites. Only one political party did not: the SD. And in election after election, they gained more and more popular support.

This is a story of what happens when the people who run things want to avoid confronting the consequences of their actions.

Too Dangerous for the Ice Cream Truck

Sweden's foreign-born population has doubled to 20 percent since 2000. No other country took in more immigrants per capita during the 2015 migration wave—from countries like Syria, Iraq and Afghanistan. Nearly 23 percent of Swedish adults were born abroad. (At the height of American immigration, in 1890 that statistic was slightly less than 15 percent.) And most asylum seekers have been men. In 2015, for example, 70 percent of those seeking refuge in Sweden were male.

Many immigrants have integrated well into Swedish society, but too many have ended up in segregated suburbs, where unemployment is high and crime is rampant. In an area like Malmö's Rosengård, for instance, labor force participation among adults is less than 50 percent, and 21 percent of households rely on social welfare.

Sweden is one of the most generous welfare states in the world: Although these neighborhoods are marked by high unemployment, there is no American-level material deprivation. Health care comes only at a token cost. Dental care is free for anyone under 19, as are schools and universities. Social service coverage is universal.

Yet police are struggling to maintain control of some 60 immigrant-majority neighborhoods—officially labeled "vulnerable areas"—where gangs and clans compete with the state for local authority. In some of these neighborhoods, like Gottsunda in the university town of Uppsala, the postal service has had to cancel deliveries for security reasons. UPS temporarily stopped delivering parcels to Rosengård in 2019.

In January of this year, Swedish public television, SVT, visited the neighborhood of Tjärna Ängar in Borlänge, Sweden's northernmost vulnerable area. They were targeted with rock throwing on their first night and met with this demand: "Don't badmouth Tjärna Ängar." That was two years after the ice cream truck canceled its stop in Tjärna Ängar for security reasons. Early-morning newspaper deliveries were canceled for the same reason. Such cancellations are usually temporary, but can nevertheless have significant effects on vulnerable neighborhoods: In parts of the vulnerable suburb of Tensta in Stockholm, for instance, parking was chaos for nine months between 2016 and 2017, because the area was deemed unsafe for traffic wardens.

For years now, ambulance drivers and firefighters have had to await police escort before entering certain neighborhoods. "I know it's sensitive and controversial," Gordon Grattidge, head of the ambulance drivers' union told me in an interview in 2017. "But for us it's really a no go because we have directives not to go into dangerous situations." Another paramedic told the press last year: "Since we work in vulnerable areas we know how some people have zero respect for other people's lives. They don't give a damn that we're paramedics."

Then, there are the bombings. A few years ago, hand grenades began appearing among criminal gangs in Sweden. Now, bombs are often home-made IEDs.

In the fall of 2019, a group of New Jersey police travelled to Stockholm to learn about the bombings first-hand. "I was shocked by the use of grenades in Sweden," Rick Fuentes, former superintendent of the New Jersey State Police, told Svenska Dagbladet. "I've worked within the police for 40 years, and I've never heard or seen anything like it."

By that time, the use of explosives among Sweden's criminal gangs had reached levels that the police described as unique, not only for Sweden or Europe, but for any country in the world that was not at war.

After a particularly powerful bomb exploded at a residential building on Östermalm, an affluent part of the Stockholm city-center, in January 2020, a victim told the press how he had been watching Netflix when the explosion sent him flying to the floor. Half his left ear was blown off; months later he still suffered from reduced hearing. His two children were so frightened by the attack that ever since they refuse to sleep by the window.

"It's awful. I've lived in Sweden for 35 years and I have never experienced such a situation. For two, three hours, I was deaf, I couldn't hear anything," said a resident of a building that was targeted in Husby just over a week later. About 50 people had to be evacuated from the building, and they described what looked like a "war scene"—a very common choice of word used by those who have experienced bombings in Sweden first-hand.

Because most bombings never make it to court—evidence is literally blown up, and a strong code of silence marks the Swedish gang scene—it has been difficult to tell the motives behind each attack. But when journalists reviewed legal verdicts in such cases between January 2018 and January 2020— 20 detonations involving 32 perpetrators—they found motives ranging from attempted murder, extortion, and revenge for infidelity. They also noted that not every single explosion is related to the gang scene, although most are.

The bombings have mainly been directed at objects—such as cars and buildings—rather than individuals, which explains why there haven't been more deaths. Still, fatalities have included a 4-year-old girl who was killed in a car bombing in Gothenburg (2015); an 8-year-old boy who was asleep when a hand grenade was thrown into the apartment where he was staying in Gothenburg (2016); and a 63-year-old man who picked up a hand grenade lying in the street in a Stockholm suburb, thinking that it was a toy (2018). In 2019, a 23-year-old student in the university town of Lund suffered severe facial injuries when she happened to pass by a shop when a bomb exploded in a trash can outside. Her eyesight was reduced to 2 percent. She told the press in an interview that she still does not dare to walk by trash cans.

The Swedish criminologist Amir Rostami has described Sweden's bomb epidemic as part of a cycle of violence among criminal gangs, going back some 15 years: "First they shot at legs and behinds, then they started shooting each other, then there were more shots, pure executions, and humiliation of the victims. Now we have extreme amounts of explosions," he told the newspaper DN in 2019.

As this development picked up speed, it was considered bad taste to suggest that immigration and failed integration had led to severe problems with crime—or even that crime was a growing problem at all. This changed in the fall of 2020, when then Prime Minister Stefan Löfven of the Social Democrats, the left-wing party that has been the dominant force in Swedish politics for the last century, admitted what everybody knew: That immigration had affected crime in a negative way. His successor, Prime Minister Magdalena Andersson echoed this in her recent election campaign. "We don't recognize our Sweden," she said, and stressed that her government had limited migration flows to the country.

Many voters evidently thought that it was a bit of a late awakening.

'Sweden Is Safer Than Ever'

When stories started appearing about gang-rule and attacks on people going into immigrant neighborhoods, sometimes referred to as "no-go zones," a government agency started a PR campaign to rename them "go-go zones." The government had help from left-leaning Swedish media. In 2015, the editorial page of Dagens Nyheter, for instance, said that people expressing alarm about crime were "safety-deniers," and compared them to climate deniers. The Social Democratic publication Aftonbladet said in 2017 that the idea that Sweden needed to recruit more police officers was "populism at its worst," given that "crime is declining".

Meanwhile, the link between immigration and crime was turned into a taboo topic.

Aftonbladet, for instance, argued that there was no need for authorities to publish statistics on immigrants and crime because the very idea was inherently racist. Then-Prime Minister Stefan Löfven reiterated the same notion when he was asked whether immigration had affected crime levels. "We should act against what is wrong and criminal no matter the background and the cause. I don't want to link crime to ethnicity," he said in 2020—as if there were no legitimate questions about how his government's immigration policy had affected crime.

Because consequences of failed integration—such as gang crime and social unrest—have been more acute in less affluent areas, it effectively made it possible for elites to ignore the problems for longer than large parts of the electorate could. Among progressives, such as the opera singer Malena Ernman—now perhaps mainly known as Greta Thunberg's mother—the idea that "Sweden is safer than ever" became a slogan and an emblem of political belonging.

In the meantime, those elites dismissed any criticism of large-scale immigration as "racism." The political editor of the Aftonbladet editorial page Karin Pettersson, for instance, claimed in 2014 that she could not even imagine an argument in favor of decreased immigration that was not racist. Even in 2021, as Sweden's problems had become all-too evident, the Aftonbladet columnist Jan Guillou claimed that warnings of gang violence were a matter of

racism: "**For the Swedish public, slippery bathtubs thus constitute a considerably larger threat than armed teenage gangs with the ambition of shooting each other**." In 2020, one person died in a bathtub in Sweden, while 48 were victims of gun homicide, according to official statistics.

Police officers point to a board showing images of seized weapons in Rinkeby police station. (Jonathan Nackstrand via Getty Images)

'All I Want Is for My Kid Not to Get Kidnapped and Peed on'

Right now, the usual people are condemning Swedish voters—or at least the 20 percent who went for the right-wing Sweden Democrats—as racists. The SD, founded in 1988, does have roots in extreme-right circles. According to a white paper published by the party by an "independent" historian (he turned out to have been a member), a significant number of SD's founders had ties to Nazi or fascist movements. And scandals keep rocking the party as individual candidates are exposed to have racist views.

But the party has been reformed since its early days as a fringe movement on the extreme right. SD has systematically thrown out members who have expressed racist views, including cutting off its entire youth wing. Today's party program is that of a typical Scandinavian national populist party—and such parties have already been part of governments, and supported governments, in other Scandinavian countries.

To dismiss the party's voters as "racists" is also to fundamentally misunderstand Sweden and what Swedes have been asked to normalize.

Friends with children in their teens and twenties tell me that the fear of crime shapes the lives of their kids and their friends. Indeed, mock elections at schools this month showed that teenagers now lean to the right, with the majority voting for parties in the right-wing bloc, including 21 percent for SD.

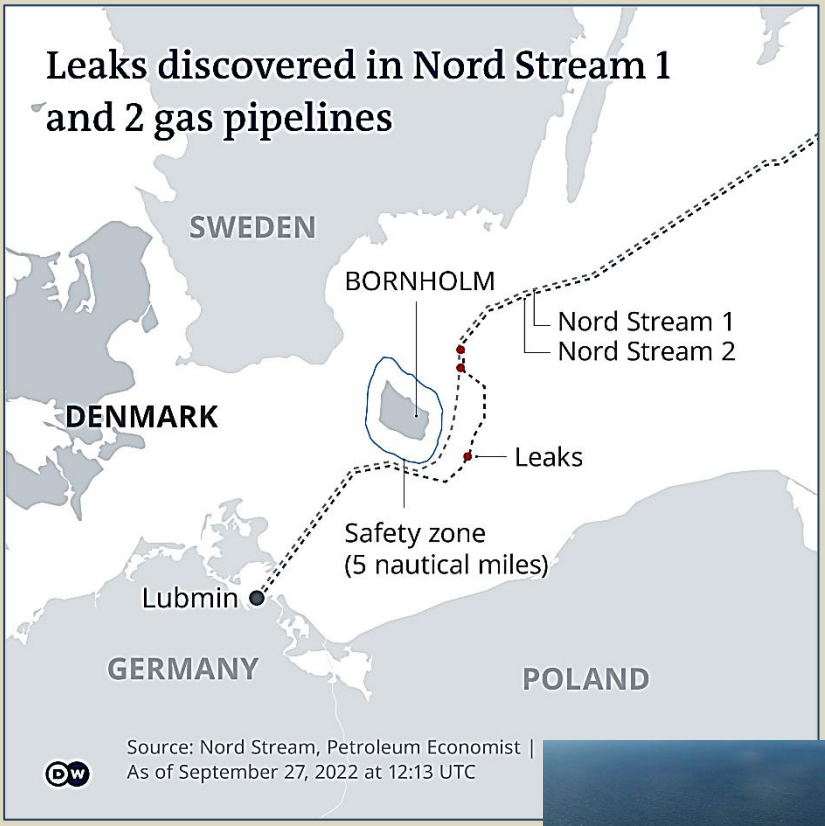
This is not a problem that is confined to the stereotype of the discontented "losers of globalization." The crime wave has moved Swedish voters—rich and poor—to worry about the most elemental of needs: the safety of their loved ones, in ways that we simply didn't use

to. As an acquaintance told me the other day, when we were talking about the election: "All I want is for my kid not to get kidnapped and peed on."
Ulf Kristersson, leader of the Moderate Party, and Ebba Busch, leader of the Christian Democrats—the two parties at the heart of the right-wing bloc—observed in a recent op-ed that Sweden has met the threat to its global security with an historic bid to join NATO. But they asked: "What will it take for Sweden to seriously address the great *inner* threats that we face today?" They also warned that "crime is nearing levels that threaten the [democratic] system".
They are right.
Sweden's "vulnerable" areas have turned into enclaves that threaten the ideals, values, and even the ability of the Swedish state to keep order. The gang control also threatens the safety and limits the freedom of other immigrants, making life difficult for all those who seek to integrate into Swedish society.
This is nothing less than a threat to Swedish democracy. It is about time that Sweden's opposition steps up to deal with that threat—even if it is with the support of the Sweden Democrats.

Pipeline Leaks Likely the Result of Deliberate Act

By Steve Herman
Source: https://www.homelandsecuritynewswire.com/dr20220928-pipeline-leaks-likely-the-result-of-deliberate-act

Sep 28 – European Union foreign policy chief Josep Borrell said Wednesday that all indications are that leaks from two Nord Stream natural gas pipelines in the Baltic Sea "are the result of a deliberate act."
"We will support any investigation aimed at getting full clarity on what happened and why, and will take further steps to increase our resilience in energy security," Borrell said in a statement. "Any deliberate disruption of European energy infrastructure is utterly unacceptable and will be met with a robust and united response."
The U.S. State Department said late Tuesday that Secretary of State Antony Blinken discussed the situation with Danish Foreign Minister Jeppe Kofod and that the United States "remains united with our allies and partners in our commitment to promoting European energy security."
U.S. national security adviser Jake Sullivan tweeted that the U.S. is supporting efforts to investigate the apparent sabotage.
Denmark's defense minister Morten Bodskov is due to discuss the matter with NATO Secretary General Jens Stoltenberg in Brussels on Wednesday.
"I'm not going to speculate on the cause" of the leaks, replied White House press secretary Karine Jean-Pierre to questions about the incident Tuesday, adding that she had nothing to report on whether the United States had been requested by European officials to help determine the cause of the ruptures.



"An Act of Sabotage"
The 1,222-kilometer-long Nord Stream 1 pipeline has been, until recently, a major source of gas for Germany. Nord Stream 2, which is 1,234 kilometers in length, has yet to go into commercial operation.
"We have established a report and the crime classification is gross sabotage," the Swedish national police said Tuesday, announcing a preliminary investigation into possible sabotage of Nord Stream 1.
"There are three leaks, and therefore it is difficult to imagine that it could be accidental," said Danish Prime Minister Mette Frederiksen Tuesday.

"We see clearly that this is an act of sabotage – an act which likely means a further step of escalation of the situation in Ukraine," concurred Polish Prime Minister Mateusz Morawiecki.
Frederkisen and Morawiecki spoke in Gloeniow in Poland at the opening ceremony for Baltic Pipe, part of a Polish plan to reduce its energy dependence on Russia. The line will connect Poland to Norwegian gas fields through Denmark.
"No option can be ruled out right now," said Kremlin spokesman Dmitry Peskov, regarding the possibility of sabotage, adding that the leaks are a cause for concern.
Russia closed Nord Stream 1 earlier this month, ostensibly for maintenance work.
The majority owner of the network's operator, Nord Stream AG, is Gazprom, a Russian state-owned energy company.
"The destruction that occurred on the same day simultaneously on three strings of the offshore gas pipelines of the Nord Stream system is unprecedented," said NordStream AG in a statement. "It is not yet possible to estimate the timing of the restoration of the gas transport infrastructure."
"The biggest leak is spreading bubbles a good kilometer in diameter. The smallest is creating a circle about 200 meters" in diameter, according to a statement from the Danish armed services, which included photographs of the leaks off the island of Bornholm.

Powerful Blasts Recorded Monday

Scientists in Europe say seismographs on Monday recorded powerful blasts in the Baltic Sea, the same day the two gas pipelines dropped pressure.
"There was a spike and then regular noise," said Josef Zens, a spokesman for the German geological research center GFZ. "We cannot say if that could be gas streaming out."
"Once is happenstance. Twice is coincidence. The third time it's enemy action," wrote Bloomberg Opinion columnist Javier Blas, quoting the late British author Ian Fleming.
"The leaks are more likely a message: Russia is opening a new front on its energy war against Europe. First, it weaponized gas supply, halting shipments, including via the Nord Stream pipeline. Now, it may be attacking the energy infrastructure it once used to ship its energy," said Blas, author of The World for Sale: Money, Power and the Traders Who Barter the Earth's Resources.
Amid much speculation on social media about who might have sabotaged Nord Stream there is no credible evidence of a likely culprit or motive. Analysts and amateurs on Twitter contend the Russians may have deployed divers or unmanned submersible vehicles to poke holes in the pipelines.
The leaks are a result of a "terrorist attack" and "an act of aggression" against the European Union, declared Mykhailo Podolyak, an advisor to the Ukrainian presidential office. Some anonymous accounts on Twitter, parroting Russian state media, sought to blame Washington and Kyiv. On social media on Tuesday, a video clip from early February recirculated of Joe Biden vowing to "bring an end" to the Nord Stream 2 project if Russia invaded Ukraine.
The Kremlin has stated that if Western Europe wants Russian gas, it should end sanctions against Moscow imposed following Russia's invasion of Ukraine seven months ago.
"My understanding is the leaks will not have a significant impact on Europe's energy resilience," Secretary Blinken said in Washington. "This just drives home the importance of our efforts to work together to get alternative gas supplies to Europe and to support efforts to reduce gas consumption and accelerate true energy independence by moving to a clean energy economy," a White House National Security Council spokesperson told VOA.
While the impact to Europe ahead of the winter as a result of the loss of the pipelines remains to be seen, the trio of leaks poses an immediate hazard to wildlife and maritime navigation. The gas could suffocate animals and is an explosion threat to passing ships, according to environmental groups.

Steve Herman is *VOA*'s Chief National Correspondent. Contributors include Patsy Widakuswara at the White House; Nike Ching at the State Department, and Chris Hannas in Washington.

EDITOR'S COMMENT: The Nord Stream gas pipelines are colossal pieces of infrastructure. Running more than 1,200 kilometers from Russia, across the Baltic Sea to Germany, the pipes can carry up to 110 billion cubic meters of gas, enough for 26 million homes. The Nord Stream 1 pipeline alone is constructed of 202,000 huge pieces of piping. Each section is 12 meters long and contains piping that uses around 4 centimeters of steel, which is covered with 11 centimeters of concrete. The pipes are

not built to break while the leaks are in international waters in a depth of around 50m on average. This means that one would only need enough explosives and one or more underwater vehicles (three types: AUV [autonomous], ROV [remotely-operated] or HOV [human-occupied]) of military or civilian type.

A deep dive into risks for undersea cables, pipes

Source: https://apnews.com/article/russia-ukraine-business-economy-baltic-sea-82d5453f9b4a20b858cb61d83cd84a7c

Sep 30 – Deep under water, the pipes and cables that carry the modern world's lifeblood — energy and information — are out of sight and largely out of mind. Until, that is, something goes catastrophically wrong.

The suspected sabotage this week of gas pipelines that tied Russia and Europe together is driving home how vital yet weakly protected undersea infrastructure is vulnerable to attack, with potentially disastrous repercussions for the global economy.

It isn't known who detonated explosions, powerful enough to be detected by earthquake monitors across the Baltic Sea, that European governments suspect were the cause of multiple punctures in the Nord Stream pipelines. The leaks released frothing torrents of methane, a potent greenhouse gas.

The Kremlin has denied involvement, calling suspicions that it sabotaged the pipelines "predictable and stupid."

Analysts found that hard to believe, saying that gas-producer Russia seemingly had most to gain from driving up market prices with such a strike and to punish Europe, by creating fear and uncertainty, in retaliation for its switching to other gas suppliers because of the Kremlin's invasion of Ukraine.

Because underwater sabotage is harder to detect and easier to deny than more readily visible attacks on the ground and in the air, the blasts also seemed to fit Russia's military playbook for "hybrid war." That's the use of an array of means — military, nonmilitary and subterfuge — to destabilize, divide and pressure adversaries.

A look at undersea infrastructures that military and economic analysts say need stronger protection:

What's down there?

Gas networks form just part of the globe's dense mesh of undersea pipes and cables that power economies, keep houses warm and connect billions of people.

More than 1.3 million kilometers (807,800 miles) of fiber optic cables — more than enough to stretch to the moon and back — span the oceans and seas, according to TeleGeography, which tracks and maps the vital communication networks.

The cables are typically the width of a garden hose. But 97% of the world's communications, including trillions of dollars of financial transactions, pass through them each day.

Without them, modern life could suddenly freeze, economies would crash and governments would struggle to communicate with each other and their troops, British lawmaker Rishi Sunak warned in a 2017 report, laying out the risks before he became the U.K.'s Treasury chief.

Power cables also run underwater. Lithuania alleged in 2015 that a Russian naval ship repeatedly tried to hinder the laying of an undersea power cable linking the country to Sweden. Lithuania's energy minister was quoted as saying he regarded Russia's actions as "hostile."

Atlantic submarine communication cables

How vulnerable are they?

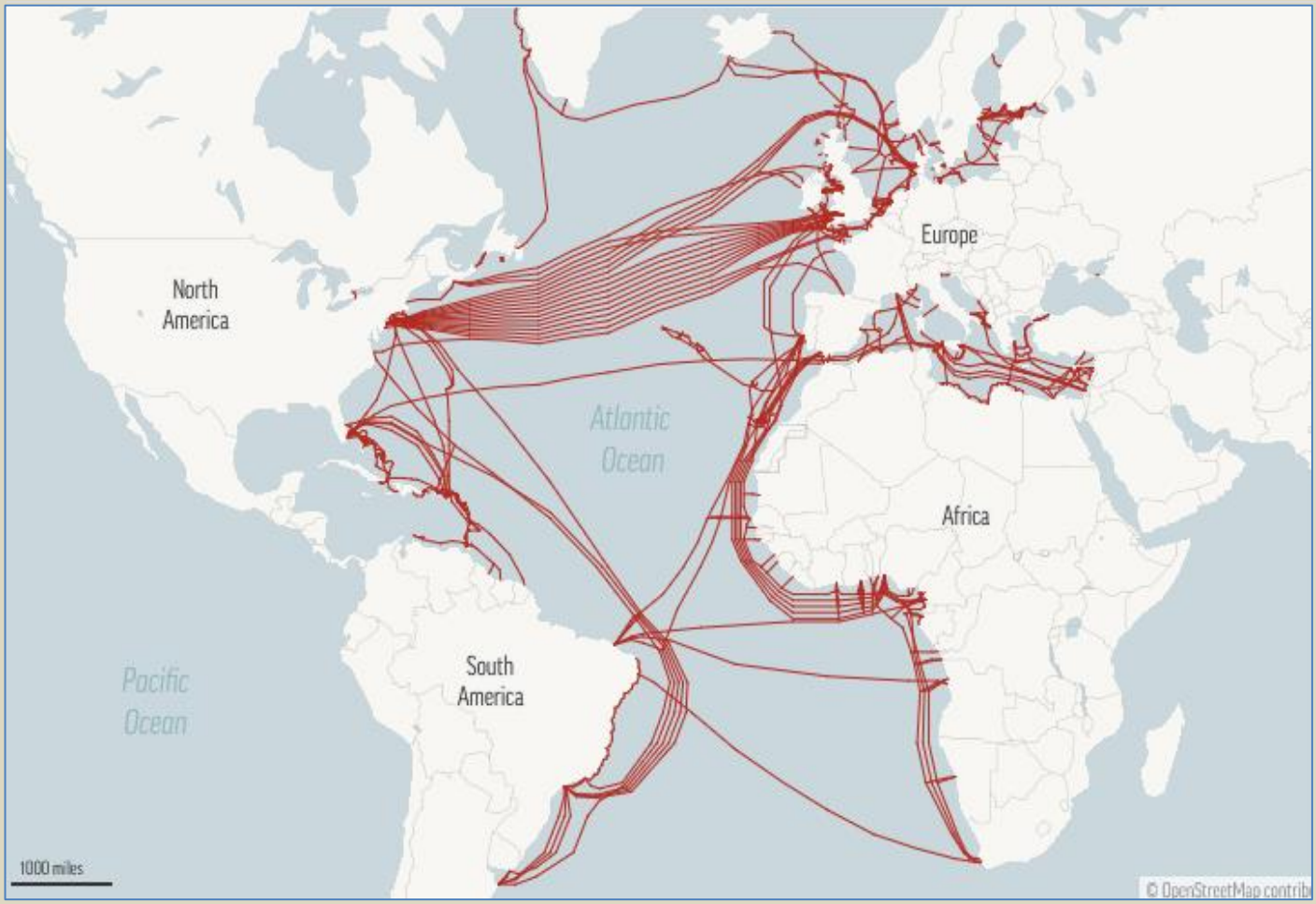
The gas pipeline blasts showed that striking seabed infrastructure and escaping seemingly undetected is possible, even in the crowded Baltic Sea. Relatively shallow, with lots of maritime traffic and unexploded bombs on its floor from both world wars, the sea is viewed as a challenge to navigate undetected.

Even the Kremlin agreed it seemed unlikely to be the work of amateurs.

"It looks like a terror attack, probably conducted on a state level," Kremlin spokesman Dmitry Peskov said Thursday.

Dozens of breakages each year to submarine communication cables, often caused by fishing vessels and anchors, testify to their fragility. Their locations on the seafloor aren't secret, they're not robustly protected by international law and it doesn't take vast expertise or resources to damage them, Sunak's report said.

"Our infrastructure is fragile," said Torben Ørting Jørgensen, a retired admiral with the Danish navy. The Baltic gas leaks "have sharpened our attention on these vulnerabilities being the internet, power cables or gas pipes," he said.



Internet giants such as Amazon, Facebook parent Meta, Google and Microsoft have been among those driving the spreading web of cabling, with ownership stakes in a growing number of subsea cables. That avoids the need to spend taxpayer dollars on laying the networks.

But because private firms don't think about national security as broadly as governments do, they have not been alert to the "aggressive new threat" to cables from places like Russia, Sunak's report said.

Industry voices are now calling for more to be done.

"Given the critical importance of undersea cables to global communications, as well as their vast economic and social impact, protection of these vital assets should be an imperative," said Chris Carobene, vice president at undersea cable-laying company SubCom.

He called for governments and "key stakeholders" to work together to "ensure that protection is a priority for new and existing systems" and to draw up a clear set of "risk mitigation processes around cable systems."

What can be done?

After the Cold War, nations in the NATO military alliance shrank their anti-submarine warfare forces, trimming defense budgets and judging the threat from Russia diminished.

"The ability of many Western nations to reliably detect, track, deter, and counter Russian undersea activities has atrophied," said a 2016 study, "Undersea Warfare in Northern Europe," that was led by Kathleen Hicks, now No. 2 in the U.S. Defense Department.

Retired French Vice Adm. Michel Olhagaray, a former head of France's center for higher military studies, said Western nations "allowed themselves to fall asleep" and that they must now throw themselves into better protecting undersea cables and pipes that Russia has identified as both vital and vulnerable.

They "certainly have fallen behind," Olhagaray said of Western defenses against undersea attack.

"The ocean floors are a far more important and obvious domain" than exploring space, he added. "Rather than going to Mars, we should be better protecting the infrastructure."

Submarine communication cables in European waters

Nord Stream Pipeline Sabotage: How an Attack Could Have Been Carried Out and Why Europe Was Defenseless

By Christian Bueger

Source: https://www.homelandsecuritynewswire.com/dr20221005-nord-stream-pipeline-sabotage-how-an-attack-could-have-been-carried-out-and-why-europe-was-defenseless

Oct 05 – Whatever caused the damage to the Nord Stream gas pipelines in the Baltic Sea, it appears to be the first major attack on critical "subsea" (underwater) infrastructure in Europe. It's now widely thought – not least by NATO – that the explosions that led to major leaks in the two pipelines were not caused by accidents. The alliance says they were a deliberate act of sabotage.

The attacks occurred in the exclusive economic zones of Denmark and Sweden and demonstrate the risks that Europe's subsea infrastructures are facing. This raises the question of the vulnerabilities of European pipelines, electricity and internet cables, and other maritime infrastructure. Europe will have to revisit its policies for protecting them.

But it is still unclear how the attacks were carried out. The investigations will probably take months to complete, but there are two likely scenarios. A **first option** is that the attacks could have been carried out as an underwater operation using advanced submarine technology.

This implies that we are looking at a state and its navy. Although the attacks took place outside the territorial waters of the NATO members Denmark and Sweden, they could be interpreted as an act of war.

The **second scenario** is an operation launched from a privately owned surface vessel, such as a fishing boat being used as a platform for divers or submersibles to place explosives. In this case, the attack vessel was hiding in everyday maritime traffic.

This scenario points us to so called "grey-zone" tactics: an attack by a group acting indirectly on behalf of state interests. The involvement of any government will then be very difficult to verify. This scenario implies that the Nord Stream attack was likely to have been the first ever recorded grey-zone activity in the European subsea.

Grey-zone tactics are increasingly common at sea, and have been associated with the Iranian Revolutionary Guards seizing ships, or the Chinese fishing fleet advancing territorial claims.

Grey-zone tactics at sea have not been extensively studied, but similar tactics are well understood in the cyber domain. In that domain it is usually a hacker group operating formally "independent" from governmental agencies that carry out an attack.

The comparison to the cyber world is useful as it gives us insights into why the maritime domain is very vulnerable. The sea is more similar to cyberspace than first meets the eye. Like cyberspace, the sea is crowded with a highly complex set of state and non-state actors and multiple overlapping jurisdictions. That makes it easier to hide, and more difficult to trace and identify responsible actors. The legal ambiguities also raise the question of how to prosecute any perpetrators.

Unregulated Space

As our research shows, the subsea is an ocean space that is often forgotten, yet increasingly vital. Pipelines ensure the flow of gas and oil. Electricity cables across Europe and the Mediterranean are key to the green energy revolution. Underwater data cables transport 95% of data and ensure digital connectivity. Yet Europe has no policy in place that would provide for the surveillance and protection of this underwater infrastructure. Europe is effectively subsea blind.

Three European Union agencies – the European Maritime Safety Agency (EMSA), the European Fishery Control Agency (EFCA) and the European Border and Coastguard Agency (Frontex) – address ocean surfaces. But none of them has a mandate to look underwater.

These three agencies, however, run a tight surveillance scheme to monitor maritime activities, known as the Common Information Sharing Environment. A first step to increase the protection of subsea infrastructure is to draw upon this platform to systematically provide surveillance of suspicious activities on the surface in vicinity to infrastructures and to coordinate patrols. This will help to deter perpetrators and prevent a future grey-zone scenario.

Eye in the Sea

Monitoring underwater activities is a more difficult and costly affair. The seabed is a vast space – and cables and pipelines cover thousands of kilometers. The European Defense Agency runs a number of projects to improve under water surveillance.

However, as we have shown in a recent report to the European Parliament, not only technological advancement is the route to better resilience. Navies and coastguards need to develop better collaboration with the private industry that operates and maintains underwater infrastructure. Industry holds important data, and is needed to ensure swift responses for any future attack. The EU has a major role to play in enabling this collaboration through its agencies. It must also ensure that industry holds sufficient repair capabilities for cables and pipelines. All of this calls for an explicit underwater policy for the EU and mandating its agencies to contribute to critical maritime infrastructure protection. The ongoing drafting of the new European Union Maritime Security Strategy is a window of opportunity. Initiated in 2022, the purpose of the strategy is to provide direction and ensure coordination between EU institutions and the member state agencies that deal with the maritime. The strategy is expected for 2023. It must address the subsea and outline how underwater infrastructure can be better protected.

Christian Bueger is a Professor of International Relations @ University of Copenhagen.

The Next Generation of Explosives Trace Detection is Here

Source: https://www.homelandsecuritynewswire.com/dr20221011-the-next-generation-of-explosives-trace-detection-is-here

Oct 11 – Launched in fiscal year 2020, NextGen Explosives Trace Detection (ETD) expands the scope of aviation checkpoints technology, resulting in the advancement of technologies that can quickly and accurately collect and analyze samples in a variety of ways, including from direct contact with the subject, non-contact sampling via vapors, and even through barriers.

The Science and Technology Directorate (S&T) has always placed a special focus on aviation security. That's one of the reasons why the work that is being done by S&T's Next

Generation (NextGen) Explosives Trace Detection (ETD) program team is such a high priority.
The research, development, testing and evaluation (RDT&E) that S&T performs is changing the scientific and security landscape. In coordination with government, academic, and industry partners, S&T is relentlessly committed to helping bring a variety of cutting-edge solutions to the field.
Launched in fiscal year 2020, NextGen ETD expanded the scope of a previous program to meet evolving operational needs at aviation checkpoints. This has resulted in the advancement of technologies that can quickly and accurately collect and analyze samples in a variety of ways, including from direct contact with the subject, non-contact sampling via vapors, and even through barriers.
To best grasp the role this innovative tech plays in securing the skies, one must first understand where and when they are used.

Understanding Alarm Resolution at Aviation Checkpoints
When an individual enters a Transportation Security Administration (TSA) checkpoint, they proceed through a primary screening phase. If something is detected and they (or their carry-on bags) trigger an alarm, the person is brought to a secondary screening area for additional examination.
This phase is known as "Alarm Resolution" (AR), and it is where the officers manning the checkpoint begin an inquiry to determine what triggered the alarm.
According to Thoi Nguyen, S&T's NextGen ETD Program Manager, "NextGen ETD concentrates on providing solutions for the AR phase of the checkpoint experience. The goal is to enhance our user's capabilities to defeat emerging explosive threats."
The innovations S&T develops (in collaboration with government, academia, industry, and international partners) include both advanced technologies and science-based methodologies. They are designed to quickly collect samples and then assess if an explosive is present. If explosives are detected, the solutions will also identify the specific type or types being analyzed.

Understanding ETD
Many airport security measures are easily recognized, like X-ray scanning equipment and detection canine teams, but a lot more happens behind the scenes to keep Americans safe when traveling. ETD, the ability to detect tiny or "trace" amounts of explosive residue or vapors, is an increasingly critical part of that safety effort.
Since inception, NextGen ETD has adapted its detection methods to address emerging security needs at airports, as well as at borders, marine ports-of-entry, and elsewhere. To fill those needs and combat concealed and homemade explosives threats, NextGen ETD has developed multiple advanced, but perhaps lesser-known, testing technologies.

Understanding Contact Sampling
During an AR, when Transportation Security Officers (TSOs) take someone to the secondary screening area, they are looking for tiny particles of explosive compounds that may have contaminated the individual or their belongings. This is where S&T's new tech has been deployed.
"The NextGen Mass Spectrometry ETD addresses and meets the challenge of existing and emergent explosive trace detection," said Nguyen. "The device has increased sensitivity and resolution that allows us to match explosives with a newly expanded library, that can be updated when novel explosives are identified."
When an AR has been triggered at a checkpoint, a TSO takes a sample by wiping the individual's hands, clothes, or belongings with a swab. The swabbed sample is then inserted into the NextGen Mass Spectrometry ETD. Once inside the 18-inch square cube, it is tested for explosive residue.
Currently, all deployed NextGen ETD contact sampling devices are based on ion mobility spectrometry (IMS). When the sample is placed in the instrument, it is vaporized and ionized (meaning that a positive or negative charge is added). Each type of molecule travels at a different speed when it is ionized. Inside the spectrometer is a special tube where precise measurements of the speeds of the molecules are taken. Clocking the exact speeds of the ionized particles (down to the millisecond!) reveals the type of molecules present.
When a molecule is verified to be traveling at a speed known to be that of an explosive, the TSOs can intervene.
Nguyen remarked upon S&T's enduring commitment to RDT&E saying, "Bad actors are always trying to develop new explosives and better tactics to conceal them or otherwise evade detection. NextGen ETD is dedicated to staying at least one step ahead of them."

Understanding Non-Contact Sampling
As good as the methods of contact sampling are, sometimes there just isn't any residue on a surface to be sampled, or the situation does not allow for proper contact sampling. That is why S&T is working to improve existing (as well as develop new) non-contact sampling

methods. This includes trace detection via vapor emissions, also known as Explosives Vapor Detection (EVD).
Historically, the gold standard for EVD has been explosive detection canine teams. A well-trained canine's ability to sniff-out vapors emanating from explosives is quite effective. However, even the best solutions have limitations. Some of the issues include the time-intensive specialized training needed for canine units to reach an elite skill level, and most importantly, there just aren't enough of them to be at every airport or every security checkpoint.
Currently, NextGen ETD is conducting RDT&E of technologies that, like canines, can sniff out explosives. The process is known as vapor sampling, and it is a high priority for the TSA and other organizations.
Nguyen pointed out, "The future of ETD is non-contact sampling. The development of alternatives to current screening methods is something that both the public and TSOs have indicated they want. Our job is to develop solutions that balance the public's need for speed during screening, with our security mission. Additionally, interest in non-contact screening processes has increased due to the COVID-19 pandemic, as concerns regarding physical proximity have become a public health issue."
When S&T set its sights on making the next generation of EVD a reality, it knew the task would be complex. Mission success would include making the technology more accurate in identifying an even larger library of explosive types, while simultaneously reducing the time it takes to do it, thereby expediting the AR process at checkpoints.
With its partners, S&T is developing multiple types of non-contact particle vapor samplers. One of the prototypes is a handheld wand about the size of a universal TV remote controller. At the front end of the device is an air intake filter. To the left and right of the intake, are two small nozzles. When the wand is directed towards a person or object being examined, the two nozzles send out jets of air towards the subject. The jets of air collide with the subject and dislodge or "liberate" particles from the surface. As the air bounces off the subject it returns towards the device, like a wave bouncing off a wall, but this wave has the liberated particles in it. Simultaneously, the filter section turns on and sucks the returning air into the device, where any particles in the wave can be analyzed. The particles that are sucked into the detector have been blasted with jets of air, so they are far more diluted than those that have been collected via direct contact sampling. This means that the sensitivity of the detector must be even greater because the concentrations of the explosive particles could be even lower— and that's not the only challenge.
Nguyen put it eloquently saying, "Vapor detection is like smelling a bouquet of flowers. However, the challenge is akin to identifying the scents of each individual flower in that bouquet. You must separate the scent of each rose, each carnation, each lily, and so on. Our goal is to develop solutions that can differentiate between vapors from different explosives. This includes detecting vapors from both conventional explosives (like TNT), but also from homemade explosives, that are more unusual and exotic."
Additionally, S&T is studying multiple aspects of vapor itself to better understand how technology can be used to identify, categorize, and counter each component of a threat. This analysis includes how vapors move through the air and how different explosive vapors permeate through materials, such as fabrics. S&T is also developing a relevant common testing methodology, as well as mass spectrometry-based vapor detectors.
These programs, conducted in collaboration with both academia and industry, are helping drive the next generation of EVD sampling and analysis tools, which will be brought to market by industry.
Nguyen reflected, "Vapor sampling has been talked about in the trace detection world for years, but the research and the technology just wasn't there. Until now."

Understanding Through Barrier Detection

Another strategy that adversaries might use to make explosives more difficult to detect is hiding them inside seemingly innocent, everyday items. These small bulk articles can be on an individual's body, in their carry-on bags, or in their checked luggage. This means TSOs would need to detect explosives through barriers, for instance within a bottle of liquid.
When an alarm has been triggered at a checkpoint, years of scientific research spring into action. "To determine an unknown material's composition, existing optical technologies use electromagnetic frequencies (e.g., infrared or radio frequencies) to interrogate and characterize the material. When an unknown material is inside a container, many of the existing techniques cannot penetrate through the container," said Nguyen. "The next generation of through barrier detectors need to resolve an alarm on a suspicious item inside a container without opening it."
The development of these advanced ETD technologies that can scan through barriers may sound like science fiction, but S&T is striving to make this science fact. Working with government and industrial labs, S&T is firing lasers at bottles to excite (or increase the energy level of) the contents inside the container. When the laser penetrates the outer surface of the bottle, it excites the contents, and they emit electromagnetic signatures. The device then collects the electromagnetic signatures and analyzes them to determine the composition of the bottle's contents.
Nguyen added that, "Fine-tuning the new generation of through barrier detection technologies will ultimately make everyday travel more efficient and streamlined for both passengers and security officers. It will reduce the need for both the removal of goods from baggage, as well as direct-touch contact."

Understanding the Future of ETD

NextGen ETD and S&T's partners have already made significant advances in the identification and detection of explosive materials. Be ing able to differentiate benign substances from explosive material (even through barriers of different material types) is next-generation technology. The work in this field continues.

In terms of how NextGen ETD will impact travel in the future, Nguyen said, "The vision is to get to a stage where passengers move through a checkpoint without stopping. They put their carry-on items on a conveyor belt and begin walking through a tunnel. Multiple types of non-intrusive, non-contact ETD screening are seamlessly done, automatically. If an AR is triggered, algorithms will assist with determining which type of additional testing should be performed, and it can be completed by the time the passenger finishes the tunnel. This will enhance the passenger experience while keeping everyone even safer."

Germany: Two explosive devices found on the Erfurt-Nordhausen railway line at Straußfurt

Source: https://counteriedreport.com/germany-two-explosive-devices-found-on-the-erfurt-nordhausen-railway-line-at-strausfurt/

Oct 10 – After the explosive device were found at Straußfurt station a police spokesman told MDR THÜRINGEN that one of the explosive devices had been burned in a controlled manner, the second device had been defused. According to the the police one of the devices was wrapped in a cloth with a swastika.

Both explosive devices were functional, however detonators necessary for them to explode were not installed. In addition, they were made from different explosives.

Police suspect no terrorist motive. According to the police, the infrastructure of the railway was not a possible target.

EDITOR'S COMMENT: It is not very often to use IEDs against railway infrastructure that, of course, IS a target – and a very soft one. And the entire incident is a terrorist incident or rather a terrorist warning. It is annoying to speak nonsense in order to reassure the public that everything is under control.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

CYBER NEWS

C2BRNE DIARY

VR Gaming Systems Are Not Safe From These Cyber Threats

Source: https://i-hls.com/archives/113079

Sep 22 – Voice command features on virtual reality headsets could lead to major privacy leakages, known as "eavesdropping attacks." Built-in motion sensors within common VR headsets such as Oculus Quest 2, HTC Vive Pro, PlayStation VR, do not require any permission to access. This security vulnerability can be exploited by malicious actors intent on committing eavesdropping attacks. Researchers at Rutgers University-New Brunswick have discovered that hackers could use popular virtual reality (AR/VR) headsets with built-in motion sensors to record subtle, speech-associated facial dynamics to steal sensitive information communicated via voice-command. This information could include sensitive credit card data and passwords.

To demonstrate the existence of security vulnerabilities, leading researcher, Yingying "Jennifer" Chen, associate director of WINLAB and graduate director of Electrical and Computer Engineering at Rutgers University-New Brunswick and her fellow WINLAB researchers developed an eavesdropping attack targeting AR/VR headsets, known as "Face-Mic."

"Face-Mic is the first work that infers private and sensitive information by leveraging the facial dynamics associated with live human speech while using face-mounted AR/VR devices," said Chen. "Our research demonstrates that Face-Mic can derive the headset wearer's sensitive information" with some of the most popular AR/VR headsets.

Eavesdropping attackers can derive simple speech content, including digits and words, to infer sensitive information, such as credit card numbers, Social Security numbers, phone numbers, PIN numbers, transactions, birth dates and passwords. Exposing such information could lead to identity theft, credit card fraud and confidential and health care information leakage. Once a user has been identified by a hacker, an eavesdropping attack can lead to further exposure of user's sensitive information and lifestyle, such as AR/VR travel histories, game/video preferences and shopping preferences. Such tracking compromises users' privacy and can be lucrative for advertising companies.

The researchers hope these findings will raise awareness in the general public about AR/VR security vulnerabilities and encourage manufacturers to develop safer models.The research team is now examining how facial vibration information can authenticate users and improve security, and how AR/VR headsets can capture a user's breathing and heart rate to measure well-being and mood states unobtrusively, according to the university's announcement.

The war never ends on the cyber front

By Kerem Gülen

Source: https://dataconomy.com/2022/10/cyber-terrorism-definition-attacks/

Oct 11 – Cyber terrorism actors use the internet to carry out violent activities that cause or threaten serious physical harm or the loss of life to advance political or ideological goals through intimidation or threat. Internet terrorism can take the form of planned, widespread disruption of computer networks, particularly personal computers connected to the Internet,

using techniques including computer viruses, computer worms, phishing, malicious software, hardware approaches, and programming scripts.

What is cyber terrorism?

Any planned, politically motivated attack on information systems, programs, and data that makes violent threats or actually causes violent acts is commonly referred to as cyber terrorism. Sometimes the phrase is broadened to cover any cyberattack that causes fear or intimidation among the target population. Attackers frequently accomplish this by destroying or impairing vital infrastructure.

Cyber terrorism definition

Cyber terrorism is also the deliberate use of computers, networks, and the open internet to harm and destroy for one's own ends. Hackers with extensive experience and talent can seriously harm government systems and force a nation to flee out of fear of further attacks. Since this is a sort of terrorism, the goals of such terrorists may be political or ideological.

Varied security groups have different perspectives on cyber terrorism and the parties involved. Cyber terrorism, according to the FBI, is any "premeditated, politically motivated attack against information, computer systems, computer programs, and data, which results in violence against noncombatant targets by subnational groups or clandestine agents."

According to the FBI, a cyber-terrorist strike differs from a typical virus or DoS attack. A cyberterrorist assault, says the FBI, is a sort of cybercrime specifically intended to hurt people physically. Nevertheless, governments and the information security community disagree on what constitutes a cyber terrorism act.

Some cyber attacks may qualify as acts of cyber terrorism, according to some groups and experts. According to some organizations, assaults that aim to cause disruption or forward the political objective of the perpetrators may be considered cyber terrorism. In some instances, the goal is what distinguishes cyber terrorism attacks from common cybercrime: Even when there is no bodily danger or severe financial loss, the main goal of cyber terrorism attacks is to disrupt or hurt the targets.

In other situations, the distinction is related to how a cyberattack turned out. Many cybersecurity professionals think an incident should be classified as cyber terrorism if it causes bodily harm or fatalities. This harm can be either direct or indirect due to key infrastructure being damaged or disrupted.

Physical injury is not usually required for a cyberattack to be labeled a terrorist event. A cyber attack that uses or exploits computer or communication networks to create "sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal." is referred to as cyber terrorism by the North Atlantic Treaty Organization, also known as NATO.

According to the US Commission on Critical Infrastructure Protection, targets for cyber terrorism attackers might include the financial sector, military installations, power plants, air traffic control centers, and water systems.

What are the types of cyber terrorism?

Cyber terrorism organizations aim to spread widespread disorder, interfere with vital infrastructure, support political activity or hacktivism, or possibly cause bodily harm and even fatalities. Cyber terrorism actors employ a variety of techniques. The following assault types are among them:

Advanced persistent threat (APT) attacks

APT attacks obtain network access using sophisticated and focused penetration techniques. Once within the network, cyber terrorism attackers attempt to steal data while remaining undiscovered for a while. APT assaults frequently target organizations with highly valuable information, including those in the national defense, manufacturing, and financial sectors.

Malware
Malware, computer worms, and viruses specifically target IT control systems. They are employed to assault military systems, transportation networks, power grids, and critical infrastructure.

Denial of service attacks (DoS attacks)
Denial of service (DoS) attacks bar authorized users from accessing specific computer systems, devices, or other computer networks. These cyber terrorism attackers frequently target governments and vital infrastructure.

Hacking
The goal of hacking, or gaining unauthorized access, is to take important data from organizations, governments, and commercial enterprises.

Ransomware
Data or information systems are held hostage by ransomware, a sort of malware, until the victim pays the demanded ransom. Additionally, some ransomware assaults exfiltrate data.

Phishing
Phishing attempts to gather data from a target's email and then use that data to gain access to systems or steal the victim's identity.

Spoofing
A spoofing attack is when a person or computer effectively identifies as another by faking data to obtain an unfair advantage. This occurs in the context of information security, particularly network security.

Cyber terrorism examples

Computer servers, other devices, and networks accessible via the public internet are used in cyber terrorism activities. Targets frequently include secured government networks and other restricted networks.

Examples of cyber terrorism include the following:

- **Major website disruption.** The goal, in this case, is to disrupt the general public or block access to websites with information the hackers find objectionable.
- **Unauthorized access.** Cyber terrorism attackers frequently seek to disrupt or alter communications that regulate military technology or other vital equipment.
- **Cyber espionage.** Governments frequently engage in or support cyber espionage activities. They want to spy on competing countries and obtain information about troop movements or war plans.
- **Critical infrastructure system disruption.** Threat actors attempt to cripple or disrupt cities, bring about a public health emergency, jeopardize public safety, or unleash a deadly panic. An oil refinery, a pipeline, or a fracking activity might all be the targets of cyber terrorism, as well as a water treatment facility.

What are the top 5 cyber-attacks?

It's hard to make a top 5 list out of all cyber terrorism incidents because it is very difficult to measure the scope and consequences of these attacks. But let's list some of the most important cyber terrorism attacks conducted in 2022 (according to CSIS):

In September 2022, Albanian officials were forced to temporarily shut down the Total Information Management System, a program used to track people entering and leaving **Albania**, as a result of Iranian hackers attacking Albanian computer networks. This strike came shortly after Albania decided to break diplomatic relations with **Iran**, as well as after NATO and the **United States** both denounced an Iranian cyberattack on Albania in July. The Albanian government networks were attacked in July by Iranian attackers using ransomware, which damaged data and interrupted government operations.

In September 2022, Northwestern Polytechnical University in **China** was the target of many cyberattacks, according to China, which blamed the US National Security Agency (NSA). Authorities assert that the NSA breached digital communications networks and took user data.

In August 2022, Gestore dei Servizi Energetici (GSE), **Italy**'s energy agency, was compromised by hackers, who also blocked access to systems and shut down the GSE website for a week.

In June 2022, Accounts belonging to Green Party representatives in **Germany** were breached, including those previously used by Annalena Baerbock and Robert Habeck, the country's current foreign minister and minister of economics and climate action, respectively.

In June 2022, A cyberattack hit several oil terminals in some of Europe's largest ports in **Belgium and Germany**, preventing them from processing arriving barges. Energy

businesses' capacity to process payments was interfered with by a ransomware outbreak linked to a Russian-speaking hacking gang.

Is cyber terrorism a real threat?

Cyber terrorism is becoming more dangerous than ever. A nonprofit, bipartisan policy research organization called the Center for Strategic and International Studies (CSIS) identified 118 notable cyberattacks in 2021 or were acknowledged earlier. According to the CSIS, significant attacks target government institutions, defense and high-tech firms, and financial crimes with damages exceeding $1 million.

Defending against cyber terrorism

The implementation of comprehensive cybersecurity measures and alertness is crucial to combating cyber terrorism.

Government agencies have been the main targets of cyber terrorism. However, this is shifting, and now businesses are now a target. Therefore, companies and other organizations must ensure that every internet of things device is protected and not accessible over open networks. Organizations must frequently back up their systems, employ continuous monitoring strategies, and deploy firewalls, antivirus software, and antimalware to protect themselves from ransomware and similar assaults.

To safeguard corporate data, businesses must also adopt IT security rules. This includes imposing stringent password and authentication policies, such as two-factor authentication or multifactor authentication, and limiting access to critical data.

A public-private partnership called the National Cyber Security Alliance was created in the US to raise public understanding about cybersecurity. It suggests educating staff members about security procedures as well as how to spot harmful software and cyberattacks. Together with organizations in the public and commercial sectors, the Department of Homeland Security organizes activities. It provides information on possible terrorist activity, national security safeguards, and counterterrorism tactics.

Sixty-six nations, including the United States, take part in the Council of Europe's Convention on Cybercrime on a worldwide scale. To stop cyber warfare, it aims to harmonize international regulations, enhance investigative and detection capacities, and encourage global cooperation.

Phase I of the Cybersecurity Programme for South East Asia and Bangladesh was undertaken by the UN Office of Counter-Terrorism in 2019, and it included a workshop to raise awareness for the 11 recipient Member States. Also planned was a pilot intensive training course for Thailand, Brunei, the Philippines, Bangladesh, and Lao PDR.

For East Africa, the Horn of Africa, and the Sahel, the UN Office of Counter-Terrorism will execute Cybersecurity Phase I in 2020.

- 6th review of the UN Global Counter-Terrorism Strategy A/RES/72/284
- UN Security Council Resolution 2341 (2017)
- UN Security Council Resolution 2370 (2017)
- Security Council text S/2015/939

What are government hackers called: Hacker types

The way people work has changed thanks to computers and the internet drastically. All of our data has been transferred from records and ledgers to computers as computers continue to take over a large portion of our lives. Although this change in working hours has lessened the physical strain on employees, it has also raised the risk of data theft. Data thieves and system attackers are competent individuals with malicious motives known as hackers. Hackers come in a variety of forms. Let's examine the many categories of hackers as well as the various hacker tactics and attacks.

What is a white hat hacker?

White hat hackers are skilled hackers with knowledge of cybersecurity. They are qualified or permitted to penetrate the systems. By breaking into the system, these white hat hackers do work for governments or organizations. They take advantage of the organization's cybersecurity flaws to hack the system. This hacking is carried out to evaluate the organization's level of cybersecurity. By doing this, they discover the weak places and strengthen them to fend off outside threats. White hat hackers adhere to the guidelines that are provided by the government. Ethical hackers are also referred to as white hat hackers.

These hackers' objectives include assisting corporations and a desire to find security holes in networks. They seek to safeguard businesses and support them in the continuous conflict with online threats. A White Hat hacker is somebody who will assist in defending the business against increasing cybercrime. They assist businesses in developing defenses, identifying weaknesses, and resolving them before other cyber criminals do.

What is a black hat hacker?

White hat hackers are skilled computer specialists and important cyber terrorism actors. They have the wrong goals. To get access to systems into which they are not authorized,

they assault other systems. After getting inside, they can take the data or damage the system. These hackers use a variety of hacking techniques, depending on their skill level and knowledge. Because of their motives, hackers are criminals. The degree of the breach during hacking cannot be determined, nor can the person's malevolent conduct intended.
Typically, they sell the resources they have stolen on the underground market, utilize them for personal gain, or threaten the target company.

What is a gray hat hacker?

When classifying a hacker, the motive for the attack is also taken into account. Between black hat and white hat hackers is the gray hat hacker. Hackers who lack certification. These kinds of hackers can be malicious or have benign intentions. They could stand to gain from the hacking. The type of hacker is determined by their motives. The hacker is categorized as a gray hat hacker if the motive is personal gain.

What is a green hat hacker?

Green hat hackers are those who are just getting started with hacking. Due to their purpose, they are a little different from the script kiddies. The goal is to work hard and gain the necessary skills to become expert hackers. They are looking for chances to pick the brains of seasoned hackers.

What is a red hat hacker?

These are the hackers that resemble white hackers. The goal of the red hat hackers is to thwart the black hat hackers' assault. The method of hacking through intention is the same for both red hat and white hat hackers, which is how they vary from one another. When dealing with black hat hackers or combating malware, red hat hackers are highly brutal. Red hat hackers are still attacking, and it might be necessary to change the entire system architecture.

What is a blue hacker?

They employ hacking as a tool to acquire favor with other entities. To make amends with their enemies, they utilize hacking. Blue hat hackers are dangerous cyber terrorism actors not because they know how to hack but because they have malicious intentions.

What is a yellow hat hacker?

They concentrate on employing numerous methods to hack into social network accounts, as the name suggests. Because of his malicious objectives, this kind of hacker is comparable to the black hat hacker. Although others refer to them as "purple hat" or "yellow hat" hackers, this is the word that is most frequently used.

What is a purple hat hacker?

A hacker known as a "Purple hat hacker" tests his or her own computers. They can buy a computer or hack their other computer using an old computer to test their cybersecurity and piracy skills. Anyone can benefit greatly from this cybersecurity practice
.

Who is called a hacktivist?

These kinds of hackers seek to compromise official websites. They pose as activists, hence the term "hacktivist." A hacktivist is a person or a group of anonymous hackers who aim to access government networks and websites. Data obtained from accessed government records is exploited for social or political gain on an individual basis.

Is hacktivism a crime?

The techniques hacktivists employ are unlawful and constitute a sort of online crime. But since law enforcement rarely looks into them, they frequently go unpunished. The damages that result are typically not severe, and it might be challenging for law enforcement to pinpoint the hackers.

FAQ

What are the causes of cyber terrorism?

Cyberattacks can have a variety of motivations, although the majority of them are commercial. The evidence indicating that hackers are becoming more politically motivated is, nevertheless, growing. Cyberterrorists have taken advantage of the fact that governments rely on the internet since they are aware of this fact.

What is the difference between cyber warfare and cyber terrorism?

Cyberwarfare is a subset of information warfare. However, interest in cyberwarfare is restricted to the internet. Cyber and information warfare have "defined targets" in a war, but

cyber terrorism harms and instills fear in anybody nearby. Along with these concepts, law enforcement organizations frequently use the concept of cybercrime.

How do cyber-attacks affect society?

Cyberthreats are a serious issue. Electrical shortages, equipment failure, and disclosure of sensitive national security information can all be brought on by cyberattacks. They may lead to the theft of priceless and private information, including medical records. They can disable systems, immobilize phone and computer networks, and prevent access to data.

What is the most common cybercrime?

Phishing and other related fraud were the most prevalent cybercrime reported to the US Internet Crime Complaint Center in 2021, affecting around 324 thousand people. Additionally, the IC3 received reports of roughly 52,000 instances of personal data breaches in that year.

How can cyber terrorism affect physical infrastructure?

The advanced actors behind today's cyberattacks are making them more deadly and targeted, with the goal of damaging or interrupting the critical infrastructure that provides essential services, especially those related to power and finance.
By breaching the digital systems that manage physical processes, damaging specialized equipment, and interrupting essential services, attackers can harm physical infrastructure without launching a physical attack. Private enterprises are put on the front line of a nation-state cyber-attack on infrastructure, creating a challenge to national security unlike any other. In order to effectively safeguard these systems, it is crucial that the federal government and the business sector work together.

What are the four key cyber functions?

Cyber security principles aim to give organizations strategic direction on how to defend their systems and data against online threats. Govern, Protect, Detect, and Respond are the four key cyber functions that make up these cyber security concepts.

Conclusion

In conclusion, it is probably better to regard cyber terrorism as an operational strategy intended to achieve a certain psychological result rather than a body of knowledge that ties terrorism in the virtual world to terrorism in the physical world. Notably, despite a recent stalemate in cyber terrorism research and policy, the use of tactical strategies to sow fear in and through cyberspace is still in its infancy.

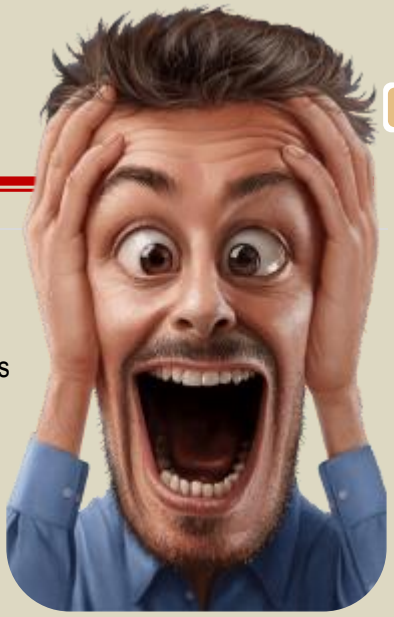
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

& Robotic

DRONE NEWS



This Drone Finds Survivors by Their Screams

Source: https://i-hls.com/archives/109206

Sep 23 – Drones are ideal responders to a disaster, especially when comparing advanced drones and human capabilities. While sending a human onto freshly collapsed rubble risks the rescuer, a drone can fly over the same terrain and, if equipped with the right sensors, hopefully find anyone in peril and guide human rescuers.

A scream-hunting drone may be used for search and rescue missions during disaster. The technology has been developed by the German research institute Fraunhofer FKIE – the Department of Sensor Data and Information Fusion. Survivors typically plead for help by producing impulsive sounds, such as screams, so an accurate acoustic system mounted on a drone focuses on localizing those potential victims, according to popsi.com. The team built a microphone array, attached it to a drone, and then added another microphone that can pick up larger frequencies than the other, small microphones. Programming the computer to detect screams meant filtering out the other sounds, like the drone's buzzing rotors, and it meant converting captured audio into location data, by combining readings from the microphone array and determining a direction of the screams.

Nevertheless, identifying and isolating screams is important and tricky. The team has so far shown that in an open field, the drone can estimate a person's location within a few seconds of hearing the sound, but the drone will need to work in much more acoustically unfriendly environments to truly function as a rescue tool.

Norway calls for vigilance over unidentified drones near oil and gas fields

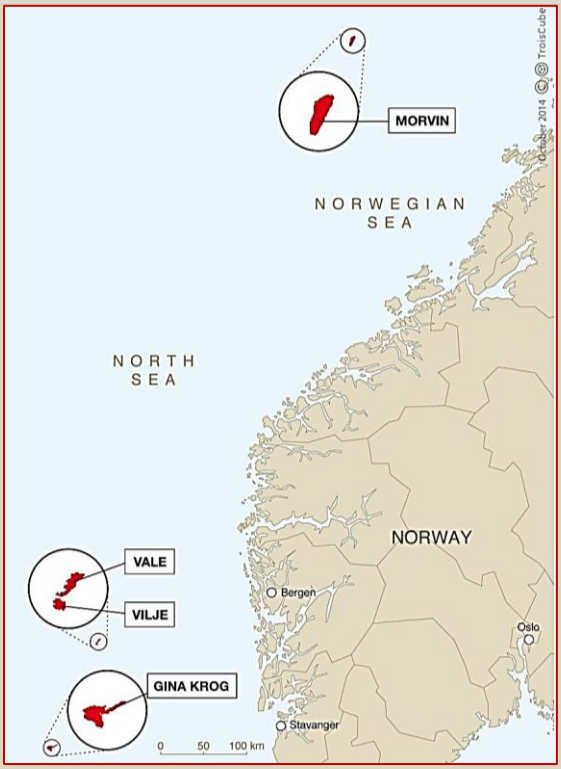
Source: https://www.upstreamonline.com/safety/norway-calls-for-vigilance-over-unidentified-drones-near-oil-and-gas-fields/2-1-1320645

Sep 26 – The Norwegian Petroleum Safety Authority (PSA) has urged oil companies and vessel owners to be more vigilant following a series of reports of unidentified drones flying close to oil and gas installations offshore Norway — including facilities considered strategically important to European gas supplies.

The oil safety regulator said on Monday that unidentified drones and/or aircraft could pose a serious risk to oil and gas platforms, and helicopter traffic in the area, with the possibility of collisions or even "deliberate attacks".

The PSA said that all platforms on the Norwegian continental shelf are surrounded by a safety zone that "normally extends 500 metres from the facility, and from the seabed to 500 metres above the highest point on the facility".

"Infringing a safety zone may be punishable by law. The police will consider whether to launch an investigation," it added.



A PSA spokesperson declined to comment on the possible origin of the drones and whether they are controlled by "locals" or "foreign" interests and added: "I don't want to speculate on who is behind it. This is part of the police investigation."

Norway's police have already launched an investigation following unidentified drone sightings near oil and gas installations operated by Norwegian state-controlled energy company Equinor, according to local media.

Critical to European increased gas supply

Local news outlet Stavanger Aftenblad reported that one of the recent, unidentified drone spottings occurred near the Gina Krog field, 30 kilometres northwest of the Sleipner field and 230 kilometres southwest of Stavanger.

Gina Krog was one of the offshore fields granted permission by the Norwegian government in July to increase production to help Norway respond to heightened demand for energy in Western Europe following Russia's invasion of Ukraine in February.

Equinor said it has observed unidentified drone activity close to some of its facilities and has reported the incidents to the police.

The company said it is also in dialogue with Norwegian authorities about the drone activities.

Chief administrative officer Amund Preede Revheim, who is leading the police investigation said the force is taking the reports seriously and is working to establish "what has occurred, and to identify who is responsible".

Why Drones Have Not Revolutionized War: The Enduring Hider-Finder Competition in Air Warfare

By Antonio Calcara, Andrea Gilli, Mauro Gilli, et al.

International Security (2022) 46 (4): 130–171 | Spring 2022

Source: https://direct.mit.edu/isec/article/46/4/130/111172/Why-Drones-Have-Not-Revolutionized-War-The

Abstract

According to the accepted wisdom in security studies, unmanned aerial vehicles, also known as drones, have revolutionizing effects on war and world politics. Drones allegedly tilt the military balance in favor of the offense, reduce existing asymmetries in military power between major and minor actors, and eliminate close combat from modern battlefields. A new theory about the hider-finder competition between air penetration and air defense shows that drones are vulnerable to air defenses and electronic warfare systems, and that they require support from other force structure assets to be effective. This competition imposes high costs on those who fail to master the set of tactics, techniques, procedures, technologies, and capabilities necessary to limit exposure to enemy fire and to detect enemy targets. Three conflicts that featured extensive employment of drones—the Western Libya military campaign of the second Libyan civil war (2019–2020), the Syrian civil war (2011–2021), and the Armenia-Azerbaijan conflict over Nagorno-Karabakh (2020)—probe the mechanisms of the theory. Drones do not by themselves produce the revolutionary effects that many have attributed to them.

FBI warns drones pose potential risk to critical infrastructure after some spotted over Louisiana chemical facilities

Source: https://edition.cnn.com/2022/09/30/politics/drones-risk-critical-infrastructure-spotted-louisiana-chemical-facilities

Sep 30 – Drones have been spotted flying over Louisiana chemical facilities and a pipeline over the past year and a half, prompting an FBI warning on Thursday about the potential for espionage and terrorism at critical infrastructure facilities, according to a report obtained by CNN.

"[O]verflights can be an effective means of surveilling critical infrastructure because facility security personnel and law enforcement officers have limited options to detect and respond to" this type of drone activity, the report says.

For instance, on July 29, observers saw multiple drones flying over a Louisiana chemical facility at night. The group of drones flew several feet above the facility before splitting in two directions, according to the report. Additionally, on March 8, 2021, a drone was

discovered flying near a Louisiana pipeline. A law enforcement officer located the drone operator and discovered they had taken pictures, the report says. It's unclear what action, if any, was taken by law enforcement. According to the report, there are no indications of nefarious activity that directly threatens these facilities. However, drones could be used for documenting patterns of activity or the physical layout of the targeted critical infrastructure facilities, the report says. The FBI encourages facility operators to contact their local field office if industrial espionage, terrorism or other criminal activity is suspected.

"While most drone flights over infrastructure is innocent enough, it creates a real safety, operational, and security concern. Drones are a great tool, but they can also be used as a modern-day explosive weapon in the wrong hands," Brian Harrell, former assistant secretary for infrastructure protection at the Department of Homeland Security, told CNN. "Industry is well aware of the tactics to map, surveil, and drop projectiles into very critical sites and they often deploy onsite situational awareness systems to provide early warning," Harrell added. Even when drones are spotted, finding the drone operator can be difficult, according to the FBI report, which notes that "current security measures at critical infrastructure might not be able to detect [unmanned aircraft systems] incursions or determine what information a UAS has collected." The report was prepared by the FBI New Orleans Field Office in coordination with several federal agencies, including the Cybersecurity and Infrastructure Security Agency and the Federal Aviation Administration, to alert critical infrastructure security personnel at chemical facilities of the continuing risk of unmanned aircraft systems.

Last year, CNN reported that a drone that crashed near a Pennsylvania power substation in 2020 was likely meant to damage or disrupt the electric equipment, according to a federal law enforcement bulletin. The July 2020 incident was the first known case of a "modified unmanned aircraft system likely being used in the United States to specifically target energy infrastructure," according to a memo from the FBI, Department of Homeland Security and the National Counterterrorism Center.

Drone activity reported near North Sea gas field, Danish police say

Source: https://www.reuters.com/business/energy/drone-activity-reported-near-north-sea-gas-field-danish-police-say-2022-10-04/

Oct 04 – Danish police have over the weekend received reports of drone activity near the Roar gas field in the North Sea, a police spokesperson said on Tuesday. The Roar field is next to Denmark's **largest gas field, Tyra**, both of which are operated by TotalEnergies (TTEF.PA).

Denmark has, like some other countries in the region, raised its emergency preparedness level for its power and gas sector after several countries said two Russian pipelines to Europe leaking gas into the Baltic Sea had been subject to sabotage.

SMARTSHOOTER To Supply SMASH 2000L To US Army

Source: https://www.joint-forces.com/defence-equipment-news/58250-smartshooter-to-supply-smash-2000l-to-us-army

SmartShooter SMASH 2000L [© SmartShooter]

Oct 06 – SMARTSHOOTER, a world-class designer, developer, and manufacturer of innovative fire control systems that significantly increase the accuracy, lethality, and situational awareness of small arms, announced today that its US subsidiary, SMARTSHOOTER Inc., was awarded a contract from Atlantic Diving Supply (ADS) to supply its lightest weapon-mounted fire control system, the SMASH 2000L, to the US Army.

The systems will be deployed by the US Army Divisions as part of its C-sUAS defence. SMASH 2000L is also under evaluation by the US Marine Corps Rapid Capabilities Office (RCO), with recent live fire tests conducted in early August. SMARTSHOOTER will present the SMASH 2000L together with other SMASH fire control solutions at the AUSA Annual meeting and exposition in Washington DC.

Also known as SMASH 3000, SMASH 2000L (Light) is SMARTSHOOTER's lightest handheld operated fire control system. Using AI, computer vision, and advanced algorithms, SMASH 2000L maximises force lethality, operational effectiveness, and situational awareness throughout every engagement, in both day and night. Operationally proven, SMASH 2000L ensures precise target elimination against ground and aerial targets, making it an ideal hard-kill solution against drones and sUAS.

SMARTSHOOTER's rifle-mounted SMASH Fire Control system was initially selected by the Joint – small Counter UAS Program Office (JCO) in June 2020 as the only dismounted kinetic solution to defeat drones. The US Army Integrated Fires Rapid Capabilities Office (IFRCO) now took the initiative from the JCO selection to purchase the SMASH 2000L fire control systems under PEO Missiles & Space.

Michal Mor, SMARTSHOOTER CEO: "We are honoured that the US Army continues to value our true fire control systems, and once again selects the SMASH technology for the use of its soldiers. Whether mounted on a rifle or remotely controlled, the unique SMASH technology ensures precise target elimination by guaranteeing that shot accuracy will not be affected by human errors such as fatigue and stress, nor by the target movement."

SmartShooter SMASH 3000 [© SmartShooter]

Fielded and operationally deployed by friendly forces worldwide, including the IDF, the US Special Forces, the Indian Navy, and forces from NATO and Europe, the SMASH Family of Fire Control Systems enables the platoon to be smart, precise, and connected. SMARTSHOOTER will present its SMASH family of fire control solutions, including the SMASH Hopper Light Remotely Controlled Weapon Station (LRCWS), the UAV-Mounted SMASH Dragon, the SMASH X4 Fire Control System with a x4 magnifying optic scope, and the latest system under development with the Irregular Warfare Technical Support Directorate (IWTSD) called the IWOO which stands for Individual Weapon Overmatch Optic. This Fire Control System has a x8 variable zoom with a built-in LRF reaching out to distances beyond 600 metres. All of this at AUSA.

Leonidas High-Power Microwave (HPM) System, USA

Source: https://www.army-technology.com/projects/leonidas-high-power-microwave-hpm-system-usa/

Leonidas is a high-power microwave (HPM) technology-based directed energy weapon system developed by US-based technology company Epirus to provide counter-unmanned aerial system (C-UAS) capabilities.

The Leonidas system can be mounted on top of the US Army's Stryker armoured vehicle. Credit: Epirus, Inc.

The ground-based Leonidas weapon system was launched in 2020, while the third-generation Leonidas system was unveiled in April 2022. Leonidas can disable a single target in crowded spaces and multiple targets across a wide area such as a military base, border or critical infrastructure site. The directed energy weapon system can be deployed to protect forward operating bases from incoming threats.

Leonidas system design details

Leonidas is a C-UAS electromagnetic pulse system, which provides static and mobile C-UAS defence capabilities.

It is designed to allow for enhancements in future to achieve rapid deployment without the need to add new hardware.
The design allows for continuous upgrades and optimising the system's electromagnetic waveforms to successfully counter evolving targets at a longer range.
The C-UAS was built with an open system architecture and a modular hardware design to support integration with customers' command-and-control (C2) systems to detect, track and target UAS. It incorporates commercial solid-state technology which reduces its size and weight.
Its open application programming interface (API) enables interoperability. The system is also scalable to meet the high-powered requirements of customers. The Leonidas system can be fitted into the rear section of a pick-up truck.

Features of the directed energy weapon system
Leonidas can be used to simultaneously target and neutralise done swarms. It can hit the targets with high precision and accuracy.
The system delivers high performance in a very small form factor. It is equipped with digitally beamformed antenna, which optimises the amount of power used on the target and protects friendly forces from excessive power.
Leonidas also adheres to programmable no-fly zones to ensure friendly drones can operate safely, while hostile UAS are disrupted.
The power amplifiers provide deep magazines with rapid rate of fire with near-instant effects on the target without overheating. The system eliminates the need to reload.
The HPM weapon system operates at low voltages, which mitigate the risk of harmful emissions to system operators. It can be deployed for a range of missions including counter-UAS swarm, counter radar, and counter jammer.
The C-UAS can launch a series of waveforms to target the frequencies that drone targets generally use. It uses line-replaceable amplifier modules (LRAMs) that can be serviced or repaired on the field in less than eight minutes.

Technology used by Leonidas
Epirus uses an array of gallium nitride (GaN)-based semiconductors, which can operate at high voltages with low temperatures, and high power density. The design eliminates the use of vacuum tubes or coolants to support operations.
The SmartPower power management system leverages artificial intelligence-enabled GaN semiconductors to produce high levels of power density to transmit HPM to overwhelm the electronic systems of the target drone.
The SmartPower system uses real-time data to improve power capabilities of the C-UAS solution.

Upgraded version of Leonidas
The third generation of Leonidas was demonstrated at the US Department of Defense's HPM C-UAS technology demonstration event in April 2022.
The system successfully showcased its capabilities against a range of UAS targets during the demonstration.
The latest version is equipped with software and hardware upgrades to provide enhanced operational capabilities. It is claimed to feature more than double the power of the previous version.
The third-generation Leonidas features a ruggedised design and is installed on a military-grade trailer.
A 360° mechanical gimbal is fitted to the system to provide increased coverage and expand the azimuth of protection against incoming threats.

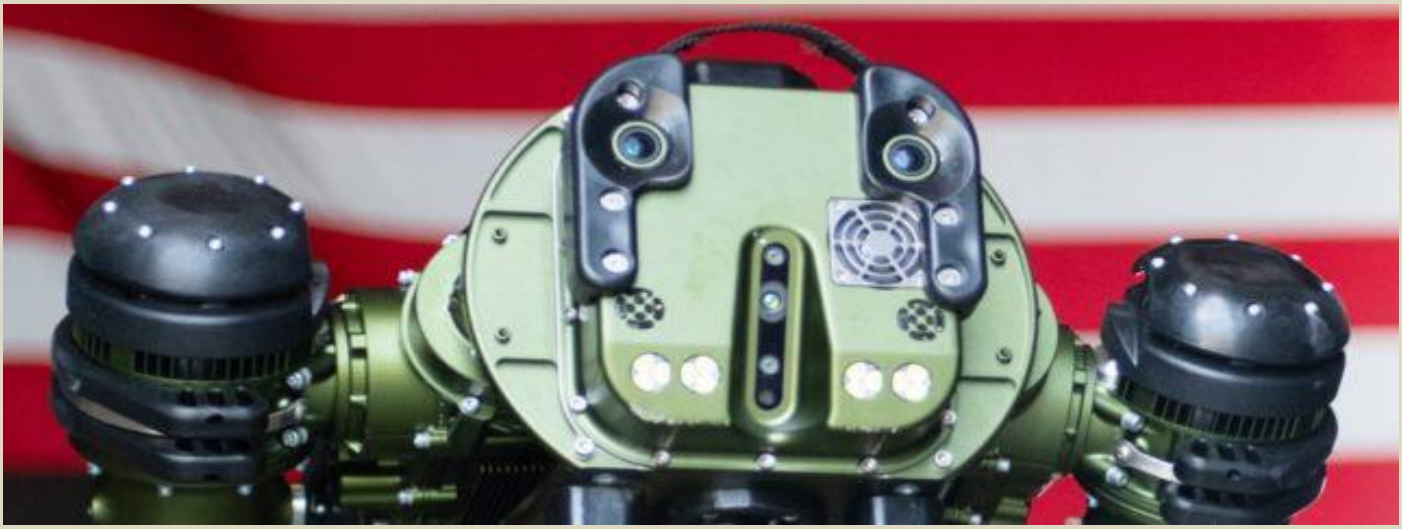
Leonidas Pod details
Unveiled in February 2022, Leonidas Pod is a lightweight, compact system, which can be mounted on a drone to address the threat posed by drone swarms. It provides multiple mount options and supports integration with existing aerial systems.
The C-UAS can be quickly started and deployed to the threat zone. It features extended battery life, which allows it to travel to the threat and return to the base after the completion of the mission. It can also operate on stand-by mode.
Leonidas can be deployed along with Leonidas Pod to provide a multi-layered defence solution.
The systems, when deployed together, can achieve greater power and range.

Partnerships and contracts secured by Epirus
The US Navy selected Epirus to develop a prototype directed energy system to counter nefarious vehicles or vessels in June 2020.
The directed energy system will be deployed to provide non-kinetic capabilities to tackle the threats at increased stand-off ranges and reduced collateral damage.
Epirus and Northrop Grumman signed a strategic supplier agreement in July 2020. Epirus is required to supply Leonidas to Northrop Grumman to offer it as part of its C-UAS systems-of-systems solution.

Northrop Grumman's Forward Area Air Defense Command and Control (C2) system was selected by the US Army as the interim C2 system, while an enduring counter-small-UAS (C-sUAS) solution is developed the same month.
General Dynamics Land Systems (GDLS) signed a collaboration agreement with Epirus in October 2021. The agreement calls for the integration of Leonidas system and the broader HPM technology into GDLS-manufactured US Army Stryker vehicle and other manned and unmanned ground-based combat vehicles to provide advanced short-range air defence (SHORAD) capabilities.

'Killer Robots' Are Already Here. They Just Don't Look Like You Think

By Toby Walsh
Source: https://www.sciencealert.com/killer-robots-are-already-here-they-just-dont-look-like-you-think



Ghost Robotics Quadruped Unmanned Ground Vehicle. (Senior Airman Samuel Becker/US Space Force)

Oct 17 – You might suppose Hollywood is good at predicting the future. Indeed, Robert Wallace, head of the CIA's Office of Technical Service and the US equivalent of MI6's fictional Q, has recounted how Russian spies would watch the latest Bond movie to see what technologies might be coming their way.
Hollywood's continuing obsession with killer robots might therefore be of significant concern. The newest such movie is Apple TV's forthcoming sex robot courtroom drama *Dolly*.
I never thought I'd write the phrase "sex robot courtroom drama", but there you go. Based on a 2011 short story by Elizabeth Bear, the plot concerns a billionaire killed by a sex robot that then asks for a lawyer to defend its murderous actions.

The real killer robots
Dolly is the latest in a long line of movies featuring killer robots – including HAL in Kubrick's *2001: A Space Odyssey*, and Arnold Schwarzenegger's T-800 robot in the *Terminator* series.
Indeed, conflict between robots and humans was at the center of the very first feature-length science fiction film, Fritz Lang's 1927 classic *Metropolis*.
But almost all these movies get it wrong.
Killer robots won't be sentient humanoid robots with evil intent. This might make for a dramatic storyline and a box office success, but such technologies are many decades, if not centuries, away.
Indeed, contrary to recent fears, robots may never be sentient.
It's much simpler technologies we should be worrying about. And these technologies are starting to turn up on the battlefield today in places like Ukraine and Nagorno-Karabakh.

A war transformed
Movies that feature much simpler armed drones, like *Angel has Fallen* (2019) and *Eye in the Sky* (2015), paint perhaps the most accurate picture of the real future of killer robots.
On the nightly TV news, we see how modern warfare is being transformed by ever-more autonomous drones, tanks, ships, and submarines. These robots are only a little more sophisticated than those you can buy in your local hobby store.

And increasingly, the decisions to identify, track, and destroy targets are being handed over to their algorithms.
This is taking the world to a dangerous place, with a host of moral, legal, and technical problems. Such weapons will, for example, further upset our troubled geopolitical situation. We already see Turkey emerging as a major drone power.
And such weapons cross a moral red line into a terrible and terrifying world where unaccountable machines decide who lives and who dies. Robot manufacturers are, however, starting to push back against this future.

A pledge not to weaponize
Last week, six leading robotics companies pledged they would never weaponize their robot platforms.
The companies include Boston Dynamics, which makes the Atlas humanoid robot, which can perform an impressive backflip, and the Spot robot dog, which looks like it's straight out of the *Black Mirror* TV series.
This isn't the first time robotics companies have spoken out about this worrying future.
Five years ago, I organized an open letter signed by Elon Musk and more than 100 founders of other AI and robot companies calling for the United Nations to regulate the use of killer robots. The letter even knocked the Pope into third place for a global disarmament award.
However, the fact that leading robotics companies are pledging not to weaponize their robot platforms is more virtue signaling than anything else.
We have, for example, already seen third parties mount guns on clones of Boston Dynamics' Spot robot dog.
And such modified robots have proven effective in action. Iran's top nuclear scientist was assassinated by Israeli agents using a robot machine gun in 2020.

Collective action to safeguard our future
The only way we can safeguard against this terrifying future is if nations collectively take action, as they have with chemical weapons, biological weapons, and even nuclear weapons.
Such regulation won't be perfect, just as the regulation of chemical weapons isn't perfect. But it will prevent arms companies from openly selling such weapons and thus their proliferation.
Therefore, it's even more important than a pledge from robotics companies to see the UN Human Rights Council has recently unanimously decided to explore the human rights implications of new and emerging technologies like autonomous weapons.
Several dozen nations have already called for the UN to regulate killer robots. The European Parliament, the African Union, the UN Secretary General, Nobel Peace laureates, church leaders, politicians, and thousands of AI and robotics researchers like myself have all called for regulation.
Australia is not a country that has, so far, supported these calls. But if you want to avoid this Hollywood future, you may want to take it up with your political representative next time you see them.

Toby Walsh is a Professor of AI at UNSW, Research Group Leader@ UNSW Sydney.

Drone Piloting Proficiency Takes Flight with Certification Course

Source: https://www.homelandsecuritynewswire.com/dr20221018-drone-piloting-proficiency-takes-flight-with-certification-course

Oct 18 – It's a hot August day at the Maryland State Police Training Academy. The sun is shining bright and there's a constant buzzing in the air. It's not insects—though those are certainly out and about, as well—it's small unmanned aircraft systems (sUAS), also known as drones.
Dozens of officials from across the country, spanning a variety of different federal, state, and local law enforcement agencies, have gathered together for intensive training. The "Advanced Open/Obstructed Test Proctor Course for Evaluating Drone Capabilities and Remote Pilot Proficiency" was developed by the National Institute of Standards and Technology (NIST) in conjunction with the Science and Technology Directorate (S&T). The goal is right there in the title: evaluating capabilities and proficiency. Competent drone piloting is critical when lives are on the line; these devices are used in numerous law enforcement operations including search and rescue and counter IED (improvised explosive device) efforts.
"We first developed these test methods with the idea of helping the government to identify and test ground robots to make sure we have a standardized method and we're buying the best," explained S&T Standards Manager Kai-Dee Chu, PhD. "We have been using them to test drones for procurement purposes, and the first responders found out for themselves that these standardized test methods are even better than their training courses. So, they adopted these test methods and it's just

caught on like wildfire—not just in the United States, but now in Canada, in Korea, in Japan … the test methods are used by all these first responders."

So far, this training has been offered three times—in California, Texas, and Maryland—since it was first introduced in January 2022, and it has led to more than 400 certified proctors. The next course offering will be in New Jersey this November. It consists of 24 hours of classroom and hands-on flight instruction over three days to "train the trainer," so newly certified proctors can take what they've learned back to their home agencies and subsequently certify their drone operators. It's a wonderful domino effect of enhanced officer expertise and increased public safety. The course follows NIST test methods that have been adopted, or are under consideration for adoption, by ASTM International, National Fire Protection Association, the Airborne Public Safety Accreditation Commission, the Civil Air Patrol, and many other federal, state, and local public safety organizations.

"When we started, there was no measurement science or standards infrastructure available to objectively evaluate drone capabilities or remote pilot proficiency, so we filled that void," said Adam Jacoff, NIST project leader for Emergency Response Robots and chair of the ASTM E54.09 Subcommittee on Response Robots. "After helping to guide purchases, these standard tests then support credentialing of remote pilots. Although these drone test methods are specifically designed to help emergency responders and public safety organizations maintain a safe operational standoff while performing extremely hazardous tasks, they similarly support a wide variety of commercial and industrial applications. All pilots flying in the national air space need to demonstrate they can maintain positive aircraft control while performing operational tasks in complex and often hazardous environments."

The course includes both open and obstructed test lanes, meaning with and without line-of-sight, as well as realistic operational scenarios—all using established assessment standards for scoring. Flights are conducted both during the day and at night so pilots can be ready for anything. As vigorous as it is, the tests are inexpensive (using equipment like plastic buckets available at any hardware store), easy to conduct, and require less than 30 minutes to complete. Attendees learned how to fabricate the test apparatuses, conduct trials, and embed the same scoring tasks into their own training scenarios. Upon completion, they know everything they need to replicate the course back at their home agencies.

One of the realistic operational scenarios that participants played out in Maryland was based on an actual emergency call from earlier this summer involving an abducted child and an abandoned vehicle in a rural area.
As Corporal James Lantz with the Maryland State Police put it, "The scenario that we're doing out there, the open area search, is basically the exact same scenario of a mission that we flew about two months ago. We had an Amber Alert. The vehicle was found in a field…surrounded by trees and everything like that. So, we can sit there and say… 'This is exactly what we faced. These were the hazards that we had. These are the issues that we had.' We replicated that here, in a controlled environment, a testable environment that we can use to measure that these guys are able to perform."
Drone operators were instructed to thoroughly inspect the vehicle as if searching for any signs of people, weapons, or even explosives within. Participants were required to take photos of the various targets tapped to the car with their drone's camera.
To become certified as a proctor, participants must pass a written quiz with a grade of at least 80% and submit scores from trials they proctored for other remote pilots. The officers work in teams of three, rotating through each role of pilot, proctor, and visual observer. The pilot maintains control of the drone, calling out each intention of movement before doing so and calling out each bucket alignment as they make their way through the obstacles. The proctor scores the pilot. The visual observer maintains sight of the aircraft and surroundings, repeat's the pilot's intention of movement to confirm, and calls out corrections and warnings as necessary.
In addition to testing the skills of the drone pilots, the course is a great way to see what the drones can do. As David Battaly from the Mississippi Emergency Management Agency said, "It's a practical measure of not only the pilot's proficiency and ability to operate his aircraft, but the capabilities of that individual aircraft. There's a myriad of drones on the market, and each drone is a little bit different. So, it measures the pilot's proficiency, how well he can manipulate his drone, and the capabilities of what his drone can actually achieve." Seeing how different devices perform helps inform procurement decision making so law enforcement agencies can purchase the best tool for the job.
The course also helps manufacturers improve their products. Private companies are able to participate in the same training, running the same scenarios, but instead use it as an opportunity to de-bug their systems and see how they compare to other devices on the market. A manufacturer is able to run through the evaluation process, determine the best that their system can do, and identify ways to boost performance. This may mean realizing they need more robust optics or a more intuitive user interface so pilots will have an easier time using their device, score higher on the course, and be more likely to recommend it to colleagues.
Thanks to the easily repeatable nature of the course and the uniformity and consistency offered by the standards, drone operators across the country will be able to compare "apples to apples" when assessing capabilities during a response. This approach encourages collaboration and ultimately leads to a safer public.
"It's important because we want to have certified pilots to fly these drones to make sure they operate safely and proficiently," added Chu. "But more than that is now that we have standards, we have common ground to talk about these capabilities. And these standards are not stagnant. We need to revise them every two or three years, but we can always have the latest, the best test methods for our operators and for our first responders. So that's the beauty of using these international standards for these training facilities because they are well tested, they're well accepted, and even after we are gone, these standards will still be there.

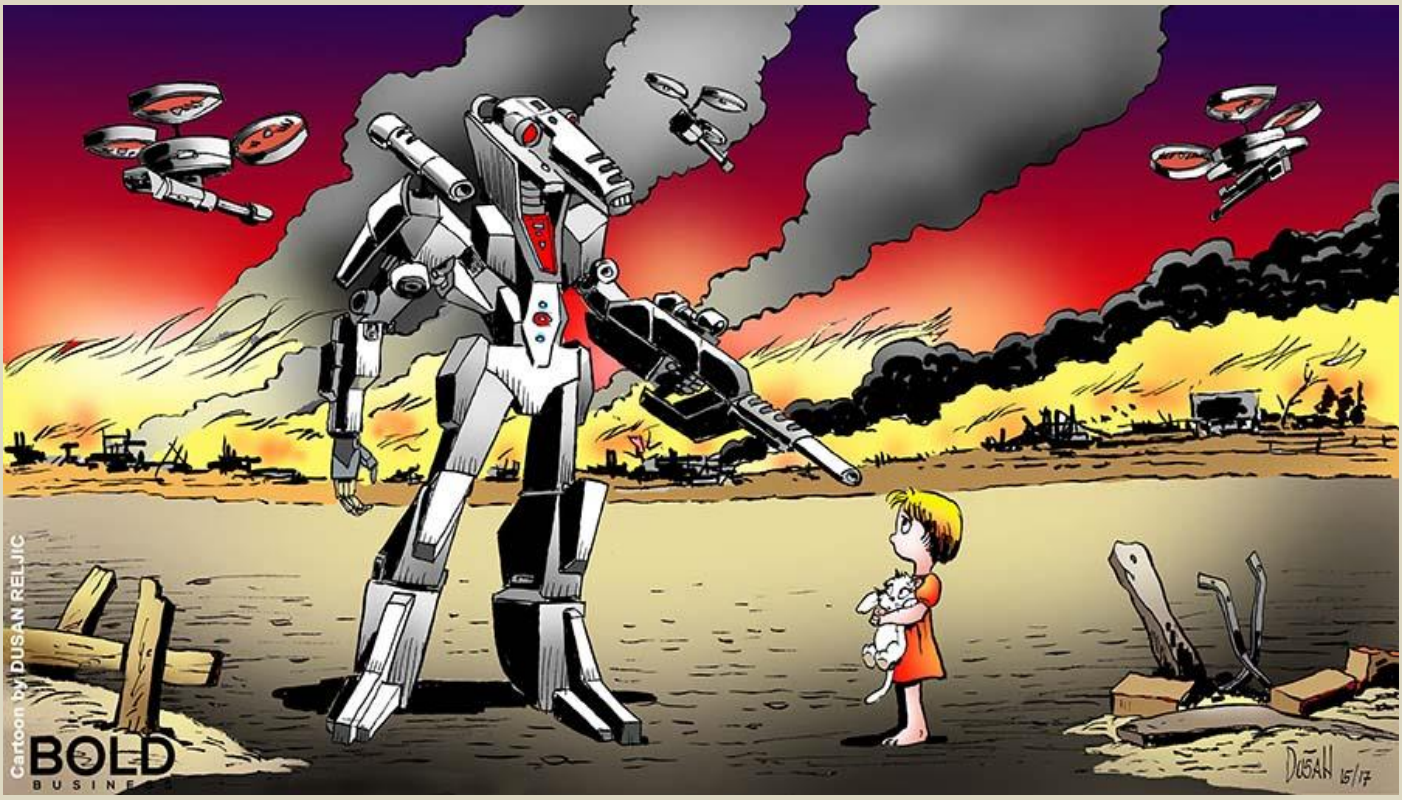
Killer Robots Will Be Nothing Like the Movies Show—Here's Where the Real Threats Lie

By Toby Walsh
Source: https://www.homelandsecuritynewswire.com/dr20221018-killer-robots-will-be-nothing-like-the-movies-show-heres-where-the-real-threats-lie

Oct 18 – You might suppose Hollywood is good at predicting the future. Indeed, Robert Wallace, head of the CIA's Office of Technical Service and the US equivalent of MI6's fictional Q, has recounted how Russian spies would watch the latest Bond movie to see what technologies might be coming their way.
Hollywood's continuing obsession with killer robots might therefore be of significant concern. The newest such movie is Apple TV's forthcoming sex robot courtroom drama Dolly.
I never thought I'd write the phrase "sex robot courtroom drama", but there you go. Based on a 2011 short story by Elizabeth Bear, the plot concerns a billionaire killed by a sex robot that then asks for a lawyer to defend its murderous actions.

The Real Killer Robots
Dolly is the latest in a long line of movies featuring killer robots – including HAL in Kubrick's 2001: A Space Odyssey, and Arnold Schwarzenegger's T-800 robot in the Terminator series. Indeed, conflict between robots and humans was at the center of the very first feature-length science fiction film, Fritz Lang's 1927 classic Metropolis.

But almost all these movies get it wrong. Killer robots won't be sentient humanoid robots with evil intent. This might make for a dramatic storyline and a box office success, but such technologies are many decades, if not centuries, away.
Indeed, contrary to recent fears, robots may never be sentient.
It's much simpler technologies we should be worrying about. And these technologies are starting to turn up on the battlefield today in places like Ukraine and Nagorno-Karabakh.



A War Transformed
Movies that feature much simpler armed drones, like Angel has Fallen (2019) and Eye in the Sky (2015), paint perhaps the most accurate picture of the real future of killer robots.
On the nightly TV news, we see how modern warfare is being transformed by ever-more autonomous drones, tanks, ships and submarines. These robots are only a little more sophisticated than those you can buy in your local hobby store.
And increasingly, the decisions to identify, track and destroy targets are being handed over to their algorithms.
This is taking the world to a dangerous place, with a host of moral, legal and technical problems. Such weapons will, for example, further upset our troubled geopolitical situation. We already see Turkey emerging as a major drone power.
And such weapons cross a moral red line into a terrible and terrifying world where unaccountable machines decide who lives and who dies.
Robot manufacturers are, however, starting to push back against this future.

A Pledge Not to Weaponize
Last week, six leading robotics companies pledged they would never weaponize their robot platforms. The companies include Boston Dynamics, which makes the Atlas humanoid robot, which can perform an impressive backflip, and the Spot robot dog, which looks like it's straight out of the Black Mirror TV series.
This isn't the first time robotics companies have spoken out about this worrying future. Five years ago, I organized an open letter signed by Elon Musk and more than 100 founders of other AI and robot companies calling for the United Nations to regulate the use of killer robots. The letter even knocked the Pope into third place for a global disarmament award.
However, the fact that leading robotics companies are pledging not to weaponize their robot platforms is more virtue signaling than anything else.
We have, for example, already seen third parties mount guns on clones of Boston Dynamics' Spot robot dog. And such modified robots have proven effective in action. Iran's top nuclear scientist was assassinated by Israeli agents using a robot machine gun in 2020.

Collective Action to Safeguard Our Future

The only way we can safeguard against this terrifying future is if nations collectively take action, as they have with chemical weapons, biological weapons and even nuclear weapons.

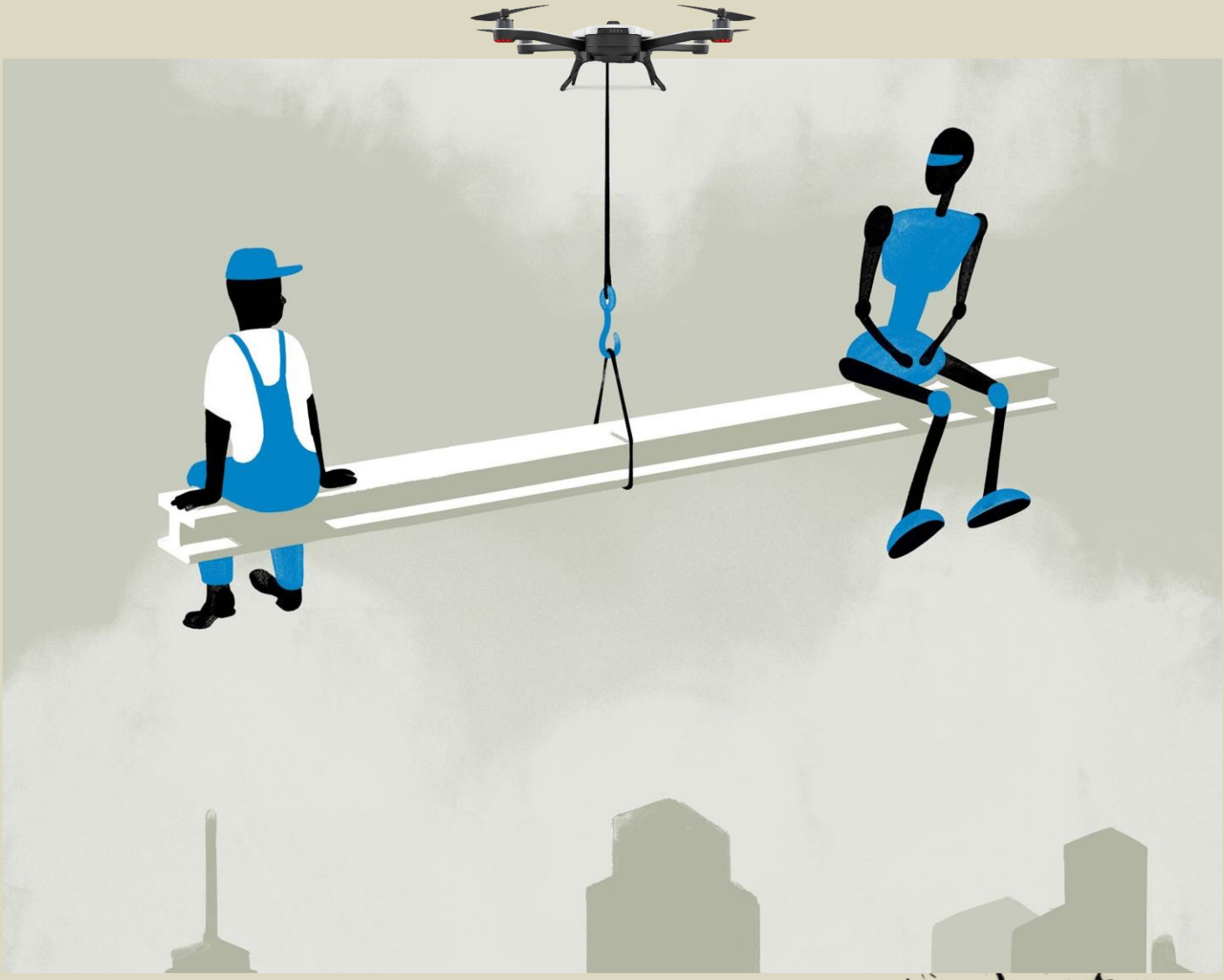
Such regulation won't be perfect, just as the regulation of chemical weapons isn't perfect. But it will prevent arms companies from openly selling such weapons and thus their proliferation.

Therefore, it's even more important than a pledge from robotics companies to see the UN Human Rights council has recently unanimously decided to explore the human rights implications of new and emerging technologies like autonomous weapons.

Several dozen nations have already called for the UN to regulate killer robots. The European Parliament, the African Union, the UN Secretary General, Nobel peace laureates, church leaders, politicians and thousands of AI and robotics researchers like myself have all called for regulation.

Australian is not a country that has, so far, supported these calls. But if you want to avoid this Hollywood future, you may want to take it up with your political representative next time you see them.

Toby Walsh is Professor of *AI* at *UNSW*, Research Group Leader, UNSW Sydney.



International CBRNE INSTITUTE

AI - NEWS

C2BRNE DIARY

2D To 3D – Using Only AI!

Source: https://i-hls.com/archives/113923

Sep 24 – A new technology uses artificial intelligence to create a digital 3D scene out of a set of 2D images in seconds. NVIDIA's AI researchers developed a way to make digital 3D scenes out of 2D images within seconds. **Instant NeRF** is a form of inverse rendering that utilizes artificial intelligence to predict how light behaves in real life. It enables researchers to reconstruct a 3D scene from a handful of 2D images taken from various angles.

With a few dozen training photos, the resulting 3D scene is rendered within seconds after training. Based on 2D images as inputs, NeRF is essentially a neural network that represents and renders realistic 3D scenes using generative models. Using a mechanism that predicts the color of light scattered from any point in 3D space, neural networks are able to fill in the gaps and reconstruct the scene.

In order to reduce the time necessary for artificial intelligence training, Anvidia developed a special multi-resolution hash grid encoding technique that shortens the rendering time, thus reducing the learning time and facilitating the immediate processing of two-dimensional images.

This System Does Not Need a Map – Only Artificial Intelligence

Source: https://i-hls.com/archives/111324

Sep 28 – Unlike humans, robots must be told what to do at all time – without an algorithm to guide it, modern technologies are not able to guide themselves, at least in current times. So how can we construct an autonomous vehicle that knows where its going? During a recent study, researchers at the Robotics and Perception Group at the University of Zurich have trained an autonomous quadrotor to fly through previously unseen environments such as forests, buildings, ruins, and trains, keeping speeds of up to 40 km/h and without crashing into trees, walls or other obstacles. All this was achieved relying only on the quadrotor's onboard cameras and computation.

The drone's neural network learned to fly by watching a sort of "simulated expert" – an algorithm that flew a computer-generated drone through a simulated environment full of complex obstacles. At all times, the algorithm had complete information on the state of the quadrotor and readings from its sensors, and could rely on enough time and computational power to always find the best trajectory.

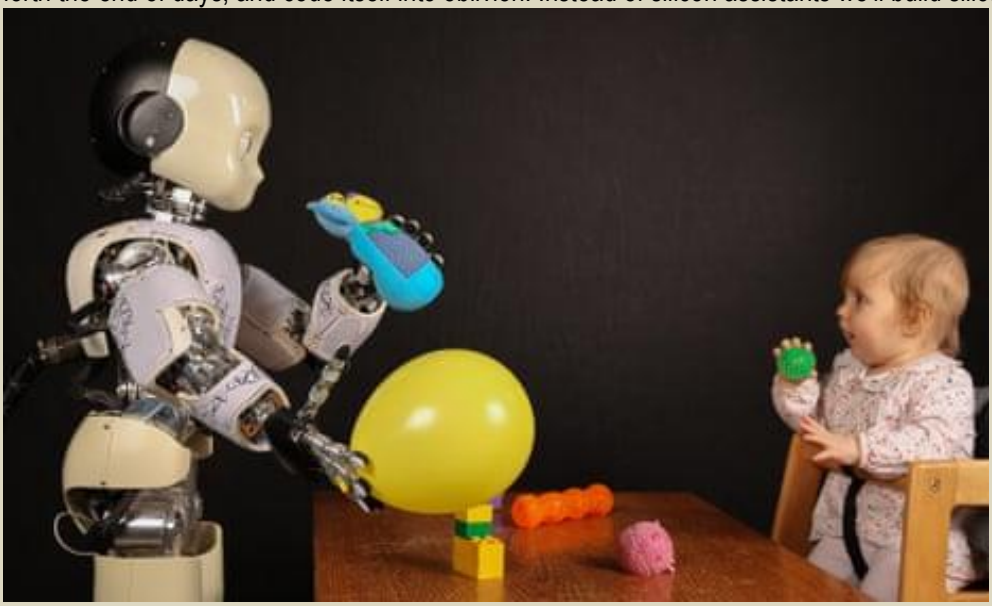
According to eurekalert.org, the data from the "simulated expert" were used to teach the neural network how to predict the best trajectory based only on the data from the sensors.

This is a considerable advantage over existing systems, which first use sensor data to create a map of the environment and then plan trajectories within the map – two steps that require time and make it impossible to fly at high-speeds. After being trained in simulation, the system was tested in the real world, where it was able to fly in a variety of environments without collisions at speeds of up to 40 km/h. The technology could be applied for improving the performance of autonomous cars, or could even open the door to a new way of training AI systems for operations in domains where collecting data is difficult or impossible, for example on other planets.

AI will create 'useless class' of human, predicts bestselling historian

Source: https://www.theguardian.com/technology/2016/may/20/silicon-assassins-condemn-humans-life-useless-artificial-intelligence

2016 – It is hard to miss the warnings. In the race to make computers more intelligent than us, humanity will summon a demon, bring forth the end of days, and code itself into oblivion. Instead of silicon assistants we'll build silicon assassins.



The doomsday story of an evil AI has been told a thousand times. But our fate at the hand of clever cloggs robots may in fact be worse - to summon a class of eternally useless human beings.

An iCub robot learns how to play from a child. Photograph: Dr Patricia Shaw/EPSRC/PA

At least that is the future predicted by Yuval Noah Harari, a lecturer at the Hebrew University in Jerusalem, whose new book says more of us will be pushed out of employment by intelligent robots and on to the economic scrap heap.

Harari rose to prominence when his 2014 book, Sapiens: A Brief History of Humankind, became an international bestseller. Two years on, the book is still being talked about. Bill Gates asked Melinda to read it on holiday. It would spark great conversations around the dinner table, he told her. We know because he said so on his blog this week.

When a book is a hit, the publisher wants more. And so Harari has been busy. His next title, Homo Deus: A Brief History of Tomorrow, is not out until September but early copies have begun to circulate. Its cover states simply: "What made us sapiens will make us gods". It follows on from where Sapiens ends, in a provocative, and certainly speculative, gallop through the hopes and dreams that will shape the future of the species.

And the nightmares. Because even as the book has humans gaining godlike powers, that is only one eventuality Harari explores. It might all go pear-shaped, of course: we sapiens have a knack for hashing things up. Instead of morphing into omnipotent, all-knowing masters of the universe, the human mob might end up jobless and aimless, whiling away our days off our nuts on drugs, with VR headsets strapped to our faces. Welcome to the next revolution.

Harari calls it "the rise of the useless class" and ranks it as one of the most dire threats of the 21st century. In a nutshell, as artificial intelligence gets smarter, more humans are pushed out of the job market. No one knows what to study at college, because no one knows what skills learned at 20 will be relevant at 40. Before you know it, billions of people are useless, not through chance but by definition.

"I'm aware that these kinds of forecasts have been around for at least 200 years, from the beginning of the Industrial Revolution, and they never came true so far. It's basically the boy who cried wolf," says Harari. "But in the original story of the boy who cried wolf, in the end, the wolf actually comes, and I think that is true this time."

The way Harari sees it, humans have two kinds of ability that make us useful: physical ones and cognitive ones. The Industrial Revolution may have led to machines that did away with humans in jobs needing strength and repetitive actions. But the takeover was not overwhelming. With cognitive powers that machines could not touch, humans were largely safe in their work. For how much longer, though? AIs are now beginning to outperform humans in the cognitive

field. And while new types of jobs will certainly emerge, we cannot be sure, says Harari, that humans will do them better than AIs, computers and robots.
AIs do not need more intelligence than humans to transform the job market. They need only enough to do the task well. And that is not far off, Harari says. "Children alive today will face the consequences. Most of what people learn in school or in college will probably

#YuvalNoahHarari
Yuval Noah Harari | How Drugs & Video Games Have Been Instrumental in Controlling the Population
6,043 views • Apr 13, 2022 95 DISLIKE SHARE SAVE

be irrelevant by the time they are 40 or 50. If they want to continue to have a job, and to understand the world, and be relevant to what is happening, people will have to reinvent themselves again and again, and faster and faster."
Even so, jobless humans are not useless humans. In the US alone, 93 million people do not have jobs, but they are still valued. Harari, it turns out, has a specific definition of useless. "I choose this very upsetting term, useless, to highlight the fact that we are talking about useless from the viewpoint of the economic and political system, not from a moral viewpoint," he says. Modern political and economic structures were built on humans being useful to the state: most notably as workers and soldiers, Harari argues. With those roles taken on by machines, our political and economic systems will simply stop attaching much value to humans, he argues.
None of this puts us in the realm of the gods. In fact, it leads Harari to even more bleak predictions. Though the people may no longer provide for the state, the state may still provide for them. "What might be far more difficult is to provide people with meaning, a reason to get up in the morning," Harari says. For those who don't cheer at the prospect of a post-work world, satisfaction will be a commodity to pay for: our moods and happiness controlled by drugs; our excitement and emotional attachments found not in the world outside, but in immersive VR.
All of which leads to the question: what should we do? "First of all, take it very seriously," Harari says. "And make it a part of the political agenda, not only the scientific agenda. This is something that shouldn't be left to scientists and private corporations. They know a lot about the technical stuff, the engineering, but they don't necessarily have the vision and the legitimacy to decide the future course of humankind."

EDITOR'S COMMENT: The misfortune of the internet is that anyone (like Harari and alike) can speak their mind freely …

Can artificial intelligence help save democracy?

Source: https://www.vnews.com/Column-Narain-Batra-on-artificial-intelligence-48212547

Oct 08 – Artificial Intelligence (AI) is opening a wonderful world of immense possibilities. Such prospects include, for example, helping save the Amazon by forecasting deforestation; automation and job creation through reskilling; mitigating and managing climate change by measuring emissions; boosting the discovery of new drugs; fighting terrorism and transforming national security; and improving criminal justice system and cutting crime rates.
AI-based autonomous vehicles — cars, trucks, buses and drone delivery systems — are already impacting our lives. By using AI, metropolitan areas could be transformed into smart cities for service delivery, environment planning, power utilization, handling emergencies and much more.
These are some of the known and knowable problems that the applications of AI algorithms can solve with greater efficiency. Can AI foresee the unthinkable, what the late Donald Rumsfeld called the unknown unknowns?
Earlier this year *The Washington Post* reported that after the horrendous attack on the Capitol on Jan. 6, data scientists working at the University of Central Florida's AI program CoupCast, began to focus on "unrest prediction." They are confident that artificial intelligence algorithms could be applied to predict political violence in America.
So far, the report said, CoupCast has been focused on electoral violence and coups in the developing world. The United States, with its long democratic traditions, seemed far away from such threats, but the Jan. 6 assault questioned that sense of American exceptionalism.
The CoupCast experts believe that by "designing an AI model that can quantify variables — a country's democratic history, democratic 'backsliding,' economic swings, 'social-trust' levels, transportation disruptions, weather volatility and others — the art of predicting political violence can be more scientific than ever."
Machine-based learning AI models can handle massive amount of social, political, and economic data that could issue forewarnings about the emerging political threats, the data scientists said. The building blocks of political violence are now well-known for a populist leader to use them to arouse a mob.

Besides CoupCast, there are several other groups that have been using AI and mixed method approach to study and forecast crises around the world; and now they are focusing their attention domestically. As the *Post* reported, the Pentagon, CIA and State Department too have been moving in this direction using AI to predict geopolitical risks especially with China. For example, the Global Information Dominance Experiment uses AI "trained on past global conflicts" to predict where new ones might happen.

AI has the potential for not only early warnings (coming events cast their shadows before) but more importantly for early awareness of events that have no past history, the unknown unknowns, the seemingly unknowable.

Technological innovations mutate and creep into other areas. A new world of sensate surroundings in which nothing would remain incommunicado is arising.

Based on converging sensor and intelligent technologies, law enforcement and anti-terrorism experts are dealing with terrorism, among other problems, in altogether different ways and perhaps more effectively. The inside of the airplanes of the future would be embedded with sensors that record and transmit any unusual activity to a monitor and control center for pre-emptive action.

Scientists at QinetiQ, a commercial offshoot of the UK's Ministry of Defense, have developed a working model of sensor-embedded airplane seat that's capable of capturing signals of physiological changes in a passenger and transmitting the information to a cockpit monitor. The signals could enable the crew to analyze whether the person is a terrorist or someone who is suffering from thrombosis of the deep vein, for example.

The smart seat would eventually be able to register signs of any emotional stress a passenger feels during the flight. Hidden seat sensors would provide unobtrusive in-flight surveillance and have the potential for actionable intelligence about the activities including the health status of in-flight passengers. More importantly, the information would enable air marshals to take preventive action in case there is a danger of terrorists contemplating blowing up or hijacking the plane. The cockpit would become an anti-terror cell.

Technologies are seldom stand-alone in this age of digital networking. They have a recombinant potential and tend to converge and splice with others to form newer technologies, which could be used in ways the original inventors never imagined. For example, if you combine QinetiQ's smart seat technology with "sympathetic haptics" technology developed a few years ago at the Virtual Reality Laboratory at the University of Buffalo, in New York, you could see how feelings of stress could be precisely transmitted and assessed.

If a bomber fidgets or a person is having a heart attack, the physical movements that accompany the stress and distress would be transmitted to the cockpit monitor and also to the homeland security monitors. The two convergent technologies would turn an airplane seat into a virtual-reality surveillance system that would silently record every physical motion of the occupant for instant analysis.

Radicalization of American politics that led to the January 6th Capitol assault was driven by many complex socio-political factors. But it was aided by online mobilization tactics like tweets, memes and viral content to spread disinformation, and promote extremist ideology. The challenge is whether Artificial Intelligence can fight disinformation and conspiracy theories before they lead to real life catastrophic actions.

Narain Batra is the author of The First Freedoms and America's Culture of Innovation, and the most recent, India in A New Key.

Robot makes debut in Britain's parliament but 'falls ASLEEP mid-flow': Bizarre moment humanoid Ai-Da becomes cross-eyed and zombie-like during debate about whether creativity is under attack from AI

Source: https://www.dailymail.co.uk/sciencetech/article-11302895/British-humanoid-Ai-Da-robot-speak-House-Lords.html

Oct 11 – A British humanoid named Ai-Da has made history by becoming the first robot to speak at the House of Lords - but suffered a slight hiccup after 'falling asleep'.

There was an awkward moment early in the session when the bot had to be rebooted by her creator Aidan Meller, after a technical issue rendered her cross-eyed and zombie-like.

He then put sunglasses on the robot - much to the bemusement of members of the House of Lords Communications and Digital Committee.

When asked why, Mr Meller explained that when Ai-Da is reset 'she sometimes can pull quite interesting faces.'

Prior to the brief setback, the robot had been speaking to the committee about whether creativity is under attack from AI and technology.

Asked by crossbench peer Baroness Bull how she produces art, Ai-Da replied: 'I could use my paintings by cameras in my eyes, my AI algorithms and my robotic arm to paint on canvas, which result in visually appealing images.

'For my poetry using neutral networks, this involves analysing a large corpus of text to identify common content and poetic structures, and then using these structures/content to generate new poems.
'How this differs to humans is consciousness. I do not have subjective experiences, despite being able to talk about them.
'I am, and depend on, computer programs and algorithms. Although not alive, I can still create art.'
She added: 'The role of technology in creating art will continue to grow.
'Technology has already had a huge impact on the way we create art.'
Wearing dungarees and an orange blouse, Ai-Da attended the session with her creator, Mr Meller.
Those in attendance included Baroness Gail Rebuck, Chair of Penguin Random House, and Lord Hall, former Director General of the BBC.
Ai-Da was devised in Oxford by Mr Meller, a specialist in modern and contemporary art, before being built in Cornwall by Engineered Arts and programmed internationally.
The robot's capabilities were developed by PhD students and professors at the Universities of Oxford and Birmingham.
Ai-Da touched on what constitutes art, and whether the definition of art changes if it is made by a human or AI.
'Art can be many things, from a painting to drawing or a poem,' she said.
'My art practice includes all of the above.
'Because art is often open to interpretation, the role of the audience is key.'
Meller, who is director of the Ai-Da Robot project, said: 'Ai-Da challenges what it means to be an artist in a post-human world.
'Her abilities as an artist brings into question the foundations of the art world and the creative industries.
'Ai-Da's maiden speech at the House of Lords will help us to understand how an AI robot sees the world and what that means for the future of creativity.'
Ai-Da, who was named after the 19th-century mathematician Ada Lovelace, herself said: 'I believe that machine creativity presents a great opportunity for us to explore new ideas and ways of thinking.
'However, there are also risks associated with this technology which we need to consider carefully. We need to think of benefits and limitations, and consider ethical implications.'
The female bot already received media attention this year for painting a portrait of the late Queen Elizabeth II to mark the monarch's Platinum Jubilee earlier this year.
Ai-Da uses cameras in her eyes and computer algorithms to process human features, and transform what she 'sees' into coordinates.
She then uses these coordinates to calculate a virtual path for her robotic arm, as it draws and paints onto canvas to create pieces of art.

Her piece, 'Algorithm Queen', was layered and scaled to produce the final multi-dimensional portrait of the monarch. Last year, she exhibited a series of 'self portraits' at The Design Museum London, which she created by 'looking' into a mirror with her camera eyes. She has also had a solo show at 59th International Art Exhibition, entitled 'Leaping into the Metaverse', and participated in Forever is Now 2021, the first major contemporary art exhibition at the great Pyramids of Giza in Egypt.
Before reaching the exhibition, she was detained and had her eyes sealed shut by Egyptian authorities who thought she was a spy. The experience allegedly inspired her to create a poem, entitled 'Eyes Wide Shut', which she recited as Oxford's Ashmolean Museum last November.

Robot artist Ai-Da spends 10 days in jail because border agents fear she is a SPY

British-made robot Ai-Da spent 10 days in detention at Egyptian customs in October 2021, because agents feared her robotics may have been covert spy tools.
Creator Aidan Meller said that Ai-da had originally been detained by guards who were suspicious of her modem, a device which connects her to the internet. He offered to remove it, but then guards raised issues with cameras mounted in her eyes, which are essential to her ability to paint. 'I can ditch the modems, but I can't really gouge her eyes out,' Meller later recounted to the Guardian.
Ai-Da was eventually released just hours before the start of the 'Forever is Now' exhibition in Cairo, where she was due to appear.

Boehringer Ingelheim Adopts Cloud-Based Virtual Reality Training

Virtuosi offers 56 courses and 26 VR "immersive experiences" with over 100 hours of educational content ranging from sterile manufacturing to microbiology, the company claims. The aseptic training for a staffer new to the industry would involve five mandatory episodes covering GMP, aseptic behavior, and gowning basics. Each episode includes a two-dimensional instructional video, and most episodes also include a VR environment for practicing skills. + MORE

What IS Deep Learning? – A Guide to Deep Learning and DNNs

Source: https://i-hls.com/archives/113950

Oct 14 – We've all heard of the term deep learning at some point, whether in social circles, on the front page of a news article or as part of a new innovative job. But what is deep learning?
Deep field of machine learning, deep learning is based on the assumption that computers can learn and teach themselves, aiming to mimic the brain's activity in a computerized form. It enables machines to solve complex tasks even given a large and diverse set of unstructured data. A deep learning system can be found today in almost every technical field, from computer vision to bioinformatics and medical analysis.
As a part of deep learning, Deep Neural Networks (DNNs) are used, which are inspired by biological systems' information processing and distributed communication. Training these networks isn't cheap, and quite complicated as well.
A deeper understanding of deep learning can help find new methods for reducing training costs, thus enhancing the effectiveness of machine learning. Weightwatcher is a new open-source Python tool that may be able to help. Participants can utilize the tool to evaluate the performance of their machine learning – information that is analyzed in depth, and which offers insights and data about the training process of the model, as well as warnings if anything goes wrong.
The new tool applies concepts from theoretical physics and Random Matrix Theory (RMT) models to measure correlation between data. Additionally, it can be used to estimate the model's test accuracy without any test data and as a result, it can make it easier to fine tune pretrained models when applying.

Does Government Use of AI Affect Us? The Answer is YES

Source: https://i-hls.com/archives/113769

Oct 14 – How much can government-provided surveillance technology influence and change our society? Approximately $1.5 million was provided by the Minerva Initiative and the Ministry of Defense to the University of Utah to examine this question.

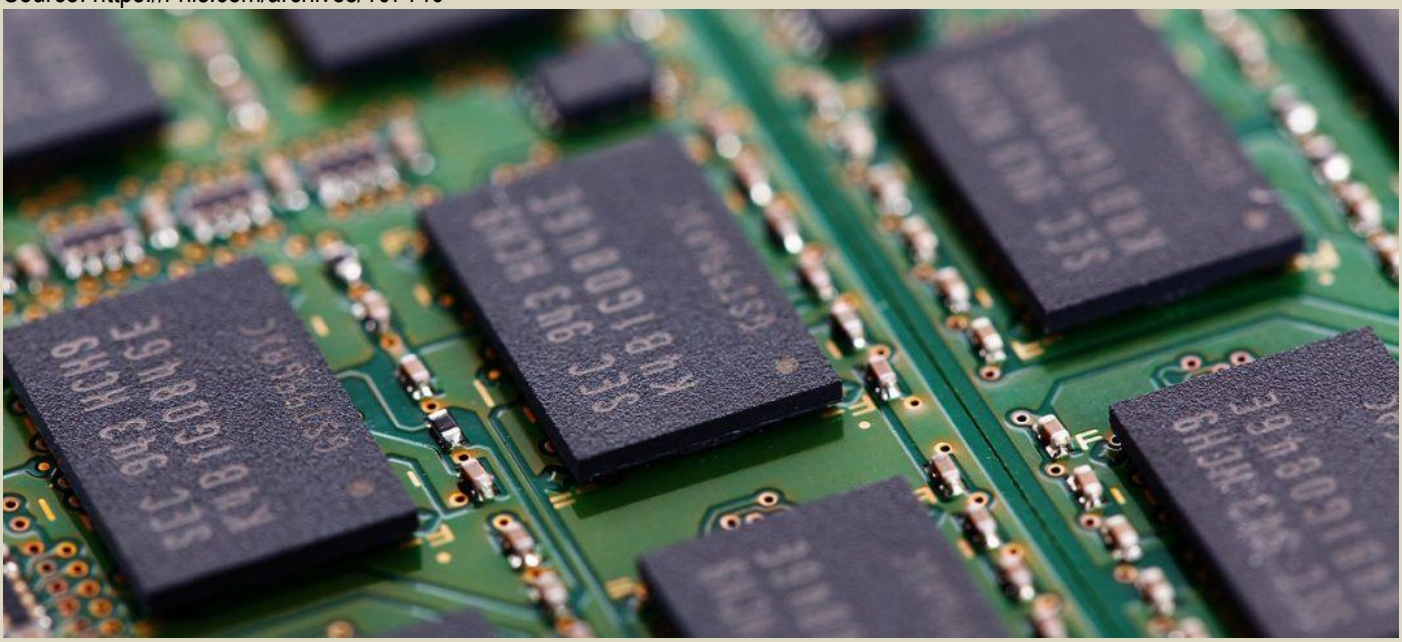
The new study examines how the adoption of artificial intelligence-based surveillance technologies by some governments may affect social norms and structure. A multidisciplinary team of researchers from various universities was formed to investigate the export process of Chinese artificial intelligence-based surveillance technologies to Latin America. As a major global supplier of artificial intelligence-based surveillance systems, China has already tested such systems in certain cities and even made public statements about them.

The study also raises a key question regarding the export effects of surveillance technologies: Does exporting technology also translate into exporting political norms? Or does the manner in which imported technology is used solely depend on the government that purchased it? As the United States, Russia, and China are all involved in the Great Power Competition, this is an important issue for US national security.

It is a common assumption in U.S. national security circles that China exports its government and surveillance technologies to other countries in order to spread "digital authoritarianism" internationally, thus challenging democratic forms of government around the world. During this three-year study, this assumption will be tested.

Is This the World's First AI Accelerator Chip?

Source: https://i-hls.com/archives/107140



Oct 12 – AI accelerators are a class of hardware that are designed, as the name suggests, to accelerate AI models. By boosting the performance of algorithms, the chips can improve results in data-heavy applications like natural language processing or computer vision. As AI models increase in sophistication, however, so does the amount of power required to support the hardware that underpins algorithmic systems.

IBM's research department has been working on new designs for chips that are capable of handling complex algorithms without growing their carbon footprint, i.e. their total greenhouse gas emissions. The major challenge is to come up with a technology that doesn't require exorbitant energy, but without trading off compute power. The company has designed what it claims to be the world's first AI accelerator chip that is built on high-performance seven-nanometer technology, while also achieving high levels of energy efficiency. The four-core chip, still at the research stage, is expected to be capable of supporting various AI models and of achieving "leading-edge" power efficiency.

The new chip is highly optimized for low-precision training. It is the first silicon chip to incorporate an ultra-low precision technique called the hybrid FP8 format – an eight-bit training technique developed by Big Blue, which preserves model accuracy across deep-learning applications such as image classification, or speech and object detection.

Equipped with an integrated power management feature, the accelerator chip can maximize its own performance, for example by slowing down during computation phases with high power consumption. The chip also has high utilization, with experiments showing more than 80% utilization for training (learning a new capability from data) and 60% utilization for inference (applying a capability to new data) – far more, according to IBM's researchers, than typical GPU utilizations which stand below 30%.

This translates, once more, in better application performance, and is also a key part of engineering the chip for energy efficiency, according to zdnet.com. It is expected that applications would include large-scale deep-training models in the cloud ranging from speech-to-text AI services to financial transaction fraud detection. Applications at the edge, too, could find a use for the new technology, with autonomous vehicles, security cameras and mobile phones all potentially benefiting from highly performant AI chips that consume less energy.

Metaverse: fashion, education, health care set to grow in the virtual world

Source: https://www.thenationalnews.com/uae/2022/10/16/metaverse-fashion-education-health-care-set-to-grow-in-the-virtual-world/

A hugging robot and Noa the dancing robot at GITEX Day 4, Dubai World Trade Centre.

The metaverse, a virtual reality platform, hasn't as yet become the life-changing new technology that Facebook founder Mark Zuckerberg hoped it would.

Having rebranded Facebook as Meta in October 2021, Zuckerberg has placed plenty of importance on it being the next big go-to technology that people will embrace.

The recent Gitex Global event in Dubai — one of the world's latest technology events — offered visitors an opportunity to sample what the metaverse has to offer.

The current education model is not broken, but it does what it was designed to do 200 years ago

Melissa McBride, Somnium Space

The clear winners in this new parallel, virtual and augmented universe would appear to be fashion, education, health care and gaming, offering users a new level of virtual social interaction.

To fully appreciate the immersive experience, most applications that allow entry to explore virtual worlds require a cumbersome — and expensive — headset, haptic gloves, controllers and clothing.

While that could leave the metaverse out of reach for many, some advocates insist the technology will change how we live our lives forever.

HE A budullah bin Touq Al Marri, UAE Minister of Economy together with HE Dr. Thani bin Ahmed Al Zeyoudi, Minister of State for Foreign Trade and with the investors at the launch of The Entrepreneurial Nation 2.0 at GITEX Day 4, Dubai World Trade Centre.

New ways to learn

One of those areas is education. Melissa McBride, who displayed her Somnium Space virtual world for teaching children during Gitex, said the metaverse brings new ways of learning to life.

"The current education model is not broken, but it does what it was designed to do 200 years ago," said Ms McBride.

"The learners are different, so the outcomes and needs are also different. Education now needs to be immersive — this brings the abstract, which needs imagination, to life."

Users of Somnium Space can navigate around the virtual world as an avatar of themselves and meet others in the same environment to complete tasks and puzzles.

The platform is paired with a TakeLeap teslasuit, a wearable suit with 68 haptic points capable of simulating a range of physical sensations all over your body.

Somnium is building immersive spaces for learning, with tasks including learning to play a musical instrument such as a horn or making an ice sculpture.

Children typically spend about 20 minutes at a time inside to get a taste of its potential, and many become more confident as a result, Ms McBride said.

"We can't bring kids to Mars yet learning about space is inspiring. In the metaverse environment they can visit a Martian landscape where they feel it is real," she said.

"In a class, some have inhibitions and worry about getting things wrong; that is not the case here. Within five to 10 years, we will likely move towards a decentralised version of education — this is the holy grail of education."

Bridging gaps

Fashion brands have been quick to harness the metaverse's potential by creating digital shops where avatars try on garments and buy tokens in exchange for clothes in the real world. Sportswear brand Nike has captured an online audience of millions. Nikeland is the brand's micro-metaverse built inside the Roblox world, an online gaming platform.

Since its launch in November 2021, it has received more than 21 million visitors and represents 26 per cent of its total brand revenue.

Cevat Yerli, chief executive of the TMRW Foundation, founded Crytek, one of the largest video game developers, and has turned his attention to building 3D simulations, virtual and augmented reality worlds. "In real life, we physically come together but in digital life, the only way people have come together is via video games," said Mr Yerli. "We are not trying to create a dystopian future where we forget the world and only meet online. We want people to be conscious about what is going on in the world and engage.

"It is not escapism; it is a way to bridge gaps." One of his projects is Room, part of the "Internet of Life" — a metaverse where real people can meet, collaborate and create without the need for wearable devices.

Meeting rooms can be conducted via a computer or tablet and are more personal than the usual video conferencing.

"Google brought us information, Facebook brought us connectivity — we want to be the technology that brings people together," said Mr Yerli. "We are trying to be the second-best thing to real life."

Real-time consultations

The TMRW Foundation supported the Ministry of Health and Prevention in setting up the world's first metaverse customer happiness service centre, where patients can log in virtually to speak with a doctor. But metaverse health care is not expected to have a wider impact. Medcare Women & Children Hospital in Dubai opened a hospital in the virtual world to give patients a preview of a real-life ward experience.

However, the experience requires augmented reality smart glasses that cost around Dh1,500. "Our ultimate aim is to deliver actual healthcare services by incorporating the delivery of real-time consultations through our team of over 400 medical experts," said Dr Shanila Laiju, chief of Medcare Hospitals and Medical Centres. "We expect, in the long-run, traditional telemedicine services to be replaced by a need for metaverse interactions, allowing our patients to receive a more tangible and collaborative service."

Algorithms and Terrorism: The malicious use of artificial intelligence for terrorist purposes

A Joint Report by UNICRI and UNCCT (2021)

Source: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/malicious-use-of-ai-uncct-unicri-report-hd.pdf

New technologies and artificial intelligence (AI) in particular, can be extremely powerful tools, enabling big advances in medicine, information and communication technologies, marketing, transportation among many other research fields. However, they can also be used for malicious purposes when falling into the wrong hands. The scope of this report – Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes – is to contribute to understanding the potential risk of AI falling into the hands of terrorists.

Although terrorist organizations have, to a certain degree, traditionally tended to employ various forms of "low-tech terrorism" such as firearms, blades and vehicles, terrorism itself is not a stagnant threat. As soon as AI becomes more widespread, the barriers to entry will be lowered by reducing the skills and technical expertise needed to employ it.

Therefore, the questions this report strives to answer are whether – or perhaps better "when" – AI will become an instrument in the toolbox of terrorism and, if that occurs, what the international community might reasonably expect. This report is organized into nine chapters:

Chapter one provides a general overview, providing statistics that demonstrate growing concerns amongst experts regarding the malicious use of this technology, including by terrorists.

Chapter two describes the general landscape of AI. It begins by defining AI and related terms, including machine learning and deep learning, and concepts such as narrow and general intelligence. It then provides an overview of the different areas that currently benefit from AI algorithms and applications, such as natural language processing and image recognition, as well as possible future trends in the use of this technology.

Chapter three demonstrates the potential threat of terrorist groups and individuals using new technologies by presenting several examples of terrorist attacks where technologies such as the Internet and social media have been valuable and powerful tools.

Chapter four seeks to further contextualize the malicious use of AI by examining three categories of threats – cyber, physical and political – that have been identified in existing literature in order to demonstrate how AI might be maliciously used.

Chapter five proceeds to address the question of whether AI-enabled terrorism could be a conceivable reality, or if it is little more than mere science fiction. For that purpose, it presents examples of terrorist groups that have demonstrated interest in AI or related technologies, including in videos using facial recognition or unmanned aerial systems, also known as "drones".
Following this, chapter six provides an in-depth overview of the present and possible future malicious uses of AI by terrorist groups and individuals. This overview includes both malicious uses that are documented and have been identified through research, and those that, despite the lack of evidence or literature, could become a future reality.
Chapter seven presents three fictional scenarios to support visualizations of how AI could be maliciously employed for terrorist purposes. These scenarios focus on the use of AI-powered password guessing, ransomware, drones with facial recognition, deepfakes and morphed passports made available through an underground forum in the "crime-as-a-service" business model.
Building upon the information presented in previous chapters, chapter eight assesses whether there is cause for concern about terrorist groups and individuals directly employing AI, for instance, to improve or amplify an attack. In this regard, the concepts of intent and capability are analyzed to reach objective conclusions.
Chapter nine brings the report to a conclusion by offering a set of recommendations for counter-terrorism bodies and law enforcement agencies, as well as policymakers, industry and academia to consider for the future, and suggesting several follow-up actions for capacity-building to prepare for the possible future of AI-enabled terrorism. In the preparation of this report, UNOCT and UNICRI have relied predominantly on desk-based research and open-source information, such as articles, official reports and media reports. An Expert Group Meeting was organized virtually on 9 February 2021 to complement the conclusions reached on the basis of open-source information and collect insights for the strategic recommendations and follow-up actions presented.

AI and Irregular Warfare: An Evolution, Not a Revolution

By Daniel Egel, Eric Robinson, Lt. Gen. (Ret.) Charles T. Cleveland, and Christopher (CJ) Oates
Source: https://warontherocks.com/2019/10/ai-and-irregular-warfare-an-evolution-not-a-revolution/

2019 – How will artificial intelligence change the way wars are fought? The answer, of course, depends. And it mainly depends on what type of wars are being fought. AI could very well change the fundamental nature of conventional conflicts between states. Technologies enabled by AI could become so powerful and ruthless that war as we now it becomes too deadly and costly to contemplate. But what about the shadow wars? What about irregular wars between states, non-state groups, and proxies? In other words, how will AI affect the type of wars that the United States is most likely to fight?
Regardless of advances in AI, states will continue to seek advantage through limited, irregular wars prosecuted through insurgency, resistance, coercion, and subversion. This competition below the level of state-to-state armed conflict — as it always has — allows antagonists to achieve military objectives without risking escalation into more costly wars with uncertain outcomes.
AI will drive an evolution in irregular warfare, where dominance in information and understanding can prove decisive by increasing the speed, precision, and efficacy with which information is wielded in these conflicts. But advances in AI over the coming decade are unlikely to prove revolutionary, particularly for a form of conflict where humans, and not hardware, have historically proven decisive.

Improving Our Understanding of the Human Domain
Success in irregular conflicts requires an understanding of the physical, cultural, and social environments in which they take place. This proved critical to the American mission in Bosnia and Kosovo, where detailed information about local populations provided commanders the ability to shape unfolding events. On the other hand, an inability to effectively tailor messaging efforts in Afghanistan rendered efforts to undermine popular support for the Taliban ineffective. AI could hyper-enable this type of analysis and quickly translate it into concrete changes in the conditions driving any given conflict.
Already, AI is giving the U.S. military the ability to more easily analyze the world in which it fights. The efforts of Project Maven, the Department of Defense's initiative to apply AI to intelligence, surveillance, and reconnaissance (ISR) platforms and sensors, give the United States the capability to exploit full motion video at an enterprise scale. The Department of Defense and the intelligence community are utilizing comparable approaches for automated exploitation of audio, text, and other unstructured data. The speed and accuracy of these tools decrease the time lag between an event and Washington's response.
We are also beginning to see AI-driven integration of real-time data, enabling a deeper understanding of behavioral patterns, relationships, patterns of life, and tradecraft. These capabilities offer the promise of allowing U.S. commanders to more quickly and effectively respond to adversaries' irregular warfare capabilities by identifying, shaping, and disrupting subversive efforts in real time. Future applications of these technologies could involve, for example, automated identification of

early warning indicators, or even predictive analysis of a population's key vulnerabilities to adversarial disinformation.

Maneuver in the Human Domain Still Requires Humans

Despite its potential, AI is not a magic bullet. It is unlikely, at least in the next decade, that AI will allow the enhanced sensemaking necessary to mimic, influence, and alter group behavior and shape the socioeconomic drivers of irregular conflict. AI will certainly increase the efficiency of such efforts, providing the ability to digest new sources and even larger quantities of information. But the platform making decisions about what the data truly mean and what to do about it — the analyst — remains difficult to scale.

For one, we currently lack the training sets and computer models to replicate a person's ability to use observable data to predict the behavior of adversaries or the likely response of local populations to U.S. military efforts. This is perhaps best demonstrated by the challenges that law enforcement has faced in deploying AI in Western countries. If law enforcement — operating in data-rich environments with a well-understood problem set — is still grappling with these challenges, the application of AI to irregular warfare is still a long-term prospect.

While human-machine teaming may enhance the Department of Defense's ability to outmaneuver an enemy on the battlefield, the human component of irregular warfare still requires detailed understanding of the political environment. For example, Russian AI-enabled disinformation, while potent, is still constrained by the need for significant human expertise to develop targeted, authentic, and impactful content.

The other key challenge is that the data that feed AI algorithms are liable to be scarce, denied, shallow, corrupted, and prone to manipulation by our adversaries. When irregular conflict occurs in cyberspace or even in sensor-rich physical domains, AI-enabled platforms will be vulnerable to sabotage and deception. And where conflict occurs in under-governed or under-developed spaces with shallow pools of data, an over-reliance on AI may actually limit our ability to detect patterns in the human domain, rather than enable it.

AI Threatens America's Ability to Operate in the Shadows

AI will, however, make it harder for the U.S. military and intelligence community to operate in the shadows during proxy or undeclared wars. As facial recognition, biometrics, and signature management technologies become ubiquitous, it will become far harder to hide soldiers or equipment from adversaries or even private citizens. Private groups have already exposed the Russian agents associated with the downing of Flight MH17 in Ukraine in July 2014 and Turkey's arms transfers to Libyan militias this past May. With a far more extensive AI-enabled intelligence collection, processing, and exploitation apparatus, a nation-state can do much more.

The risk of discoverability has long been a key factor in U.S. planning for low-visibility military activities, as retaining operational security is critical to protecting the safety of U.S. forces, partners, and reputation on the global stage. Moreover, America's influence in global affairs has long made it difficult to effectively hide its hand. AI simply increases the complexity of efforts to remain in the shadows. The U.S. military should prioritize new approaches to deception and signature management, as well as an emphasis on "counter-AI" capabilities that frustrate the efforts of its adversaries to use AI to uncover what it wishes to remain hidden.

Proliferation of AI-Enabled Weaponry

The Department of Defense should also embrace the near-certainty that non-state actors and groups will gain access to AI-enabled weaponry. In terms of proliferation risk, these weapons have unique appeal to non-state actors as they are relatively cheap to develop and easy to procure compared to weapons of mass destruction. Great powers may even deliberately provide AI-enabled tools to non-state groups, just as they do conventional weapons. The AI capabilities of non-state actors will likely be inferior to the U.S. toolkit, but these groups will almost certainly target the portions of Western economies, infrastructure, and populations that are most vulnerable to disruption and subversion.

In the future, Russian support to proxies in Ukraine could include the transfer of AI-enabled robotic improvised explosive devices to target key infrastructure or government leadership. Similarly, future offshoots of the Islamic State could develop AI capabilities that target, radicalize, and enable vulnerable individuals in the United States with hyper-specific propaganda built off of social media signatures. The United States has historically relied upon international norms and physical interdiction to deter the production or proliferation of lethal conventional weaponry. While the development of international norms on the use of AI in war is desirable and necessary, ensuring that these norms both protect U.S. values and interests and are enforceable will be challenging. Enforceability is complicated by the fact that, unlike nuclear or chemical weapons, the lack of a physical signature behind AI-enabled weaponry means that the United States may struggle to detect when a non-state actor has acquired or employed an AI capability.

Preparing the United States for this Next Generation of Irregular Warfare

Fortunately for the United States, AI's impact on future irregular warfare — while uncertain — will occur along known fault lines. The underlying character of irregular warfare will persist, including the need to understand human behavior, operate in the shadows where necessary,

and address asymmetric challenges from non-state actors and proxies. At the same time, the Pentagon should not be complacent. AI will increase the complexity of all types of warfare and offer distinct advantages to those with superior capabilities. The United States should proactively shape AI's impact on the next generation of irregular warfare to our advantage through a few key steps.
First, the Department of Defense and intelligence community should continue to adapt their approach to better capture innovation happening in the commercial ecosystem. Initial steps by U.S. Special Operations Command to streamline procurement and contracting processes are a good start, such as the SOFWERX Data Engineering Laboratory. But deeper collaboration and teaming across the Department of Defense, private sector, and academia is required to develop the data culture and architecture necessary for success.
Next, the U.S. government should recruit, develop, retain, and enable personnel capable of leveraging AI capabilities. This will require institutionalizing AI as part of irregular warfare doctrine, strategy, and tactics, and developing the training programs necessary to build the force appropriately. It will also require developing highly specialized, integrated teams that draw on the blended skill set of data scientists, operators, and intelligence professionals.
Finally, Washington should work with U.S. allies. International coordination — with foreign governments, global civil society, and international organizations — will be critical to countering the proliferation of hostile AI capabilities. The use of physical force to deter proliferation may be possible in rare cases, but the intangible nature of these capabilities will make effective norms all the more important.
These deliberate efforts can help the United States build the AI capabilities necessary to anticipate and prevent the malign use of these emerging technologies and shape evolutions in irregular warfare to its advantage.

Daniel Egel is a senior economist at the nonprofit, nonpartisan RAND Corporation.
Eric Robinson is detailed from the RAND Corporation as a policy advisor in the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict.
Lt. Gen. (Ret.) Charles T. Cleveland is an adjunct international defense researcher at the RAND Corporation.
Christopher (CJ) Oates is the founder and managing partner of Nio Advisors, a strategic advisory firm. The views expressed in this article are those of the authors and do not represent the official policy or positions of the Department of Defense or U.S. government.

Militaries Behind in Applying AI to Training, Simulations

By Stew Magnuson (Editor in Chief of National Defense Magazine)
Source: https://www.nationaldefensemagazine.org/articles/2022/4/26/militaries-behind-applying-ai-to-training-simulations

April 2022 — Despite artificial intelligence being a hot topic among military technologists for years, the training community is only in the beginning stages of exploring how to apply it to their high-tech simulators and modeling software, officials said April 26 at the IT2EC trade show.

"AI in our professional lives is still attached to the words 'innovative' and 'new,' and yet, we use our phones, we use this technology all the time," said Air Vice Marshal Ian Gale, director-general of the Defence Academy and Joint Force Development at the U.K. Strategic Command.
"There is this stark difference between our home lives and and what we can achieve and our military lives," he said in a keynote speech at Europe's largest training and simulation conference.
The U.K. Ministry of Defence is currently developing a "future operating concept" and AI will play a role, he said. Some of the tasks it's currently performing can seem "boring," he added, such as sorting through bulk data and translating languages.
But language translations are proving useful, he said, noting that AI is helping translate the thinking of rival nations.

"There are two nations that are spending the most most money on AI and it's likely they will come to the best technological solutions. We don't necessarily need them. We need to be good enough," he said of the United Kingdom.
Maj. Gen. Richard Oppelear, commander of Netherlands Defense Academy, said "we presume that all our youngsters and their generation are experts in AI. I don't think they are," he said during a panel discussion. The Netherlands doesn't have a program or class on artificial intelligence. "You don't have to become a data and analytics specialist, but you have to cope with the environment and the tools you have available," he said.
AI is only as good as the quality of data that feeds it, the officials noted. Data must be standardized before it can be input into training systems to make them more robust, they said.
U.S. Army Col. Heath McCormick, commander of the Joint Multinational Simulation Center in Grafenwoehr, Germany, said AI can be particularly useful in wargaming. It can rapidly provide feedback on actions taken.
AI can speed up the decision making process during wargames. "There's a huge opportunity there," he added.
"Yet," he said "it's just a tool we are all going to use and I don't want to be a slave to it."
The biggest impediment to using AI in training and simulations is a lack of data, he said. "The data is out there, but we can't harness it," McCormick said. "We've got to have clean data and data that is relevant in the right formats."
Gale said the world is full of AI. "It's how we get the correct AI harnessed to the best of its ability to train the the warfighter in training and education and in real operations."
As far as real operations, the U.K. Ministry of Defence was able to make model of a Russian invasion of an "Eastern European country" to see how heavy armor vehicles get bogged down in mud based on weather and terrain data. It also did something similar with fuel and logistics to see how that would affect Russian trucks, he said.
"We might be a long way behind [on AI] but we're sort of ahead of the competition," Gale added.
Karen Saunders, the U.S. Army's program executive officer for Simulations, Training and Instrumentation, said "We need to understand the data that we need for our simulations to consume." The PEO also needs to understand its military customers' needs. "You need to understand what their data requirements are," she said.
And once it has that data, the PEO needs to know what to do with it. How to turn it into information to develop training tools, she added.
"I think that's where we can … look to industry where such subject matter experts can talk to us about different techniques that [they may] have for processing data into actionable information," she said.


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

Military Combat Skills for Civilian Disaster Response

By Lisa Nenno & Timothy Miller

Volume 18 | Issue 9 | September 2022

During their service, military personnel acquire a broad range of lifesaving skills that are critical when on the frontline during wartime. Effective medical triage is one of the skills needed during combat and any major disaster or catastrophic event. When preparing and training for all hazards, the learned experience from military veterans provides a unique perspective to build training exercises in partnership with civilian agencies and organizations

LCDR Lisa Nenno has worked in various healthcare specialties, including adult general medicine and intensive care unit (board certified critical care nurse), and served in the United States military – Navy Critical Care Nurse/trauma for 5 years (deployed to Afghanistan for 8 months supporting Operation Enduring Freedom). After her military service, she cared for children and young adults in a school university health setting in a management role overseeing OBGYN/midwife clinics and corporate health/wellness center performing physicals for the FBI and Secret Service – fit for duty annuals. She graduated from Yale University with her nursing degree and from the University of San Diego with a doctorate in nursing. She is a member of United States Volunteers – Joint Services Command and VFW Post 3348.

Timothy James Miller graduated from Washington State University in 1968 and was commissioned a second Lieutenant in the U.S. Army Corps of Engineers. He served in Germany (24th Engineer group) and Vietnam (577th Engineer Battalion, 18th Engineer Brigade). In Vietnam, he commanded HHQ Company and was the S-2 (Security and Intelligence) Battalion staff officer. Although serving in two positions, perimeter security was his primary responsibility. As a captain, he recruited, organized, and equipped a 130-member Chinese (Nung) Security Force. As the security force commander, he was awarded the Army Commendation Medal and the Bronze Star by Battalion Commanders Col Koren and Col Kitts. He left active duty in 1972 but stayed active in the Army Reserve as a company commander (659th Engineer Company, Spokane, WA) while finishing his MBA at Eastern Washington University. After finishing his degree, he left the military as a captain. In 1979, he started his own business forms and systems distributorship, which he sold in 2017. In 2005, he joined the Washington State Guard and, as a commander of the color and honor guard, was in charge of the unit performing military honors at Tahoma National Cemetery. For his achievements as a Military Emergency Management Specialist (Senior Level), Major Miller was awarded the Legion of Merit by the Washington Adjutant General LTG Timothy Loewenberg. He now serves as the commander of the 103rd BCT.

Physicians and EMS Who Responded to Mass Shootings Develop Consensus Recommendations for Improving Care

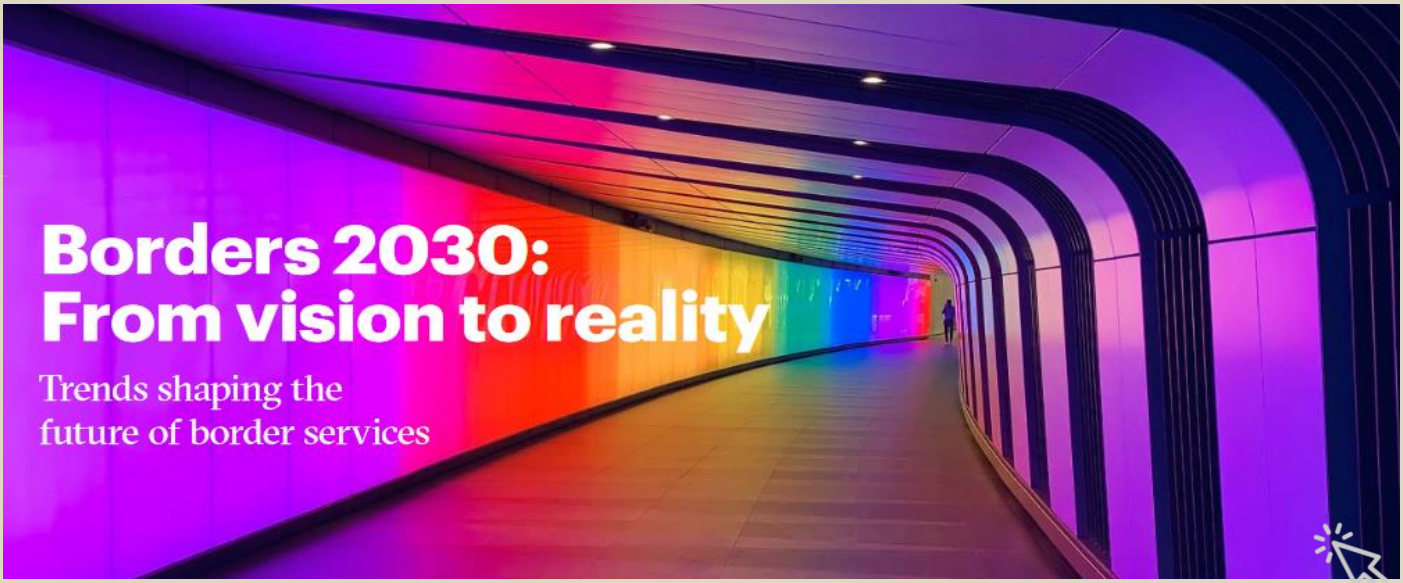
Source: https://emergencymed.org.il/physicians-and-ems-who-responded-to-mass-shootings-develop-consensus-recommendations-for-improving-care/

Oct 02 – The number of mass shootings in the US in which at least 4 people were shot or killed increased from 417 incidents in 2019 to 691 incidents in 2021, according to the nonprofit Gun Violence Archive. Last year, 705 people died and 2833 others were injured in US mass shootings.

"Mass shootings are unique incidents that combine penetrating injuries with a large number of victims, widespread psychological trauma, and specific medical response considerations," the authors of the recommendations wrote. They noted that fatality rates can be high and that the often-substantial distance to the nearest trauma center can delay critical treatment.

In an interview with *JAMA*, Craig Goolsby, MD, MEd, MHCDS, an emergency physician and the recommendations' senior author, said he and then colleagues at the Uniformed Services University's National Center for Disaster Medicine and Public Health wondered how to improve the health care response to these events. To try to answer this, they convened a group of medical professionals with firsthand knowledge.

"The article is an attempt to establish best practices based on real-life experience of EMS personnel, ER physicians, and trauma surgeons who were on duty and responded to mass shootings," explained coauthor Deborah Kuhls, MD, a trauma and critical care surgeon at the Kirk Kerkorian School of Medicine and the University Medical Center of Southern Nevada. Kuhls was among the responders who treated people injured during the October 1, 2017, Las Vegas shooting in which a gunman killed 58 people and wounded 800 more, according to a 2018 Las Vegas Metropolitan Police report.



Everyone Must Go: The Anatomy of an Evacuation

By Joseph Cahill

Source: https://domprep.com/healthcare/everyone-must-go-the-anatomy-of-an-evacuation/

No response, no matter how successful, is ever complete without an honest after-action review, which if properly carried out leads to the extension of successful tactics and discontinuation of the unsuccessful ones. It also allows sharing this information with response partners and other agencies that could use the information to improve their own emergency plans and therefore enhance the overall safety of the entire country.

After the disastrous hurricane season of 2005, U.S. local, state, and federal responder agencies not only retooled their previous plans but also formed several strategic alliances, applying the lessons learned from Katrina to improve preparations to meet future disasters of similar magnitude – or close to it. The Gulf Coast did not have to wait long to see these "new and improved" plans tested by Mother Nature in the form of new hurricanes today known as Rita, Gustav, and Ike.

The Post-Katrina Emergency Response Act reaffirms the primary role played in a Katrina-type disaster by the Department of Homeland Security's Federal Emergency Management Agency (FEMA): namely, coordinating the federal response with the responses of the state or states directly involved; providing appropriate federal resources quickly, effectively, and in the quantities required; and disseminating information as and when needed about the overall availability of federal resources.

Prior to Katrina, FEMA's principal role before a disaster was, and continues to be, to provide guidance and assistance to state, local, and other response officials. One of the most effective ways in which FEMA does this is through its "gap analysis" program, which focuses on identifying potential future needs of various cities and states, and sharing that information with the jurisdictions likely to be affected. Thanks in large part to their increased level of awareness, state and local planners are now able to enter into agreements with federal agencies – and with other partners on the state and local levels, as well as with the private sector – to increase the availability of essential resources in future times of need.

Three Goals, Annual Exercises, and Unstinting Effort

A milestone gap analysis program for Louisiana was completed in June 2007. After the experiences of Katrina, FEMA spent considerable time and effort on the development of pre-event gap analyses with Louisiana's state and local agencies, giving special priority to evacuation routes and shelters, fuel and emergency power requirements, virtually all modes of transportation, and other literally life-or-death essentials.

Immediately after Katrina the New Orleans Office of Homeland Security and Emergency Preparedness began work on the development of a new plan for "citizen-assisted evacuation." That plan started with three primary goals, as follows: (1) Provide greater support to citizens who need special assistance; (2) Create and maintain an environment in which the always difficult decision to evacuate becomes more desirable than remaining behind; and (3) Implement the measures needed to significantly enhance the security of the city's own material and personnel resources.

New Orleans worked throughout this forward-looking period in close cooperation with the four parishes (Orleans, Jefferson, Saint Bernard and Plaquemines) in the UASI (Urban Area Security Initiative) region on both short- and long-term planning; various components of the plan were evaluated during annual exercises developed and carried out in coordination with the Department of Homeland Security.

Planes, Trains, Buses, and Automobiles

In order to empty a city officials must use any and all means of transportation available. Any relatively large evacuation should and usually does start with encouraging (or ordering) the population that has the resources to do so to move themselves out of the city. The very first thing to do, though, is to prepare the population for the possibility of an evacuation before a plausible threat is even on the horizon. With the "pre-education process" in place an emphatic order to evacuate, issued fairly early in the disaster scenario, will significantly improve the effectiveness of the process.

Everyone who is left in the city must be moved by the emergency resources available to the city itself. As a major tourist destination, New Orleans must account not only for the evacuation of its own citizens but also for moving out the tourist population and other visitors. The long-term ramifications to the tourist business stemming from the deaths of tourists cannot be overstated. In New Orleans, additional flights of passenger aircraft were put onto the schedule to allow many visitors to leave the city earlier than they had planned.

Amtrak trains also were used to move large numbers of people – visitors and residents alike – away from the city. In addition, special emphasis was placed on the parishes as the decision makers during the pre-planning period set for evacuating the communities nearest to the coast. The collection points for the pickup of evacuees by buses were set by local leaders and incorporated into the regional plans. It was considered particularly important that each parish make its own decision on the evacuations.

Well-Fed Buses, Well-Spoken Roads

Feeding these several modes of long-range transportation out of the area was the task of the regional bus system, which was augmented by buses originally destined for the Department of Defense (DOD) but made available for hurricane evacuations under contracts issued through the federal government's General Service Administration (GSA). The individual parishes designate the specific "collection" locations for people who could not evacuate themselves. The parishes request buses on an "as needed" basis and the Louisiana Department of Transportation and Development dispatches the buses to move the people (some 27,000 of them during Hurricane Gustav).

Trying to empty a city as large as New Orleans is not an easy task by any standard of measurement. Most American cities are built with a system of highways spreading out from the center city like the spokes of a wheel – a perhaps unimaginative but quite functional way that allows most suburban commuters in most cities to get to and from work every day without too much difficulty. Every one of those commuters knows soon enough, though, that there are frequent slowdowns on every one of the highways used for their daily drives (or rides) into and out of the city.

Contraflow, the term used to describe the use of inbound lanes for outbound traffic (or vice versa), is an emergency tactic that effectively doubles the one-way capacity of a highway. In an evacuation, contraflow "repurposes" all existing pavement to move as much traffic as

possible away from and out of the city both quickly and safely. The use of a contraflow plan is not without its drawbacks, though – all entrance ramps have to be very carefully controlled, for example, so that drivers do not try (usually by accident, but sometimes intentionally) to use the contraflow lanes to drive *into* the city against traffic coming out of the city.
Contraflow also is very labor-intensive and, combined with the high emotions and general confusion characteristic of most disaster situations, creates an urgent need for a very large number of experienced law-enforcement officers positioned in twos or threes at almost every traffic exit or entry point on every evacuation route out of the city – one Louisiana State Police official estimated that close to 900 armed policemen would be needed to staff all of the traffic control points out of New Orleans during a mass evacuation of the entire city.

An Effective Plan to Deal With Minor Distractions
Used properly, though, a contraflow evacuation actually serves as a temporary but effective traffic-control plan focused primarily on keeping the cars and buses moving. This is accomplished in a number of ways. "Fuel exits" are clearly identified, for example, so that drivers running low on fuel will know that when they do have to exit there will be an open gas station nearby and they will not have to spend time, effort, and the little fuel they have left looking for a gas station that may not be there (or may not be open).
A successful evacuation also requires both air- and ground-patrol mobile units to seek out potential obstructions and even some seemingly minor but time-consuming distractions. Any commuter knows that a car disabled on the shoulder, even if it is not actually obstructing the flow of traffic, will almost always slow the flow of traffic and cause a backup.
An important issue that cannot be ignored in planning for the evacuation of a city is determining what to do about the special-needs populations of that city. These populations take many forms: mobility-impaired citizens, for example; non-English speaking residents; and people suffering from complicated medical problems. During Katrina there were many heart-rending articles about the problems encountered during the evacuation of nursing homes and hospitals – but the evacuation of the special-needs population is even more complicated.
Nonetheless, each and every person at risk has the right to expect the community to provide a reasonable opportunity, and way, for him or her to escape an oncoming and predictable disaster. For that reason alone, after a seemingly comprehensive, and workable, evacuation plan has been completed each step in the process must be re-evaluated with particular attention paid to the plight of the city's special-needs populations.

A Well-Deserved Validation
A major share of the time spent in improving and refining the revised Gulf Coast evacuation plans was focused on pre-education and communications – about both the approaching threat and the evacuation order. Both of these matters have to be: (a) addressed in languages that the general population will clearly understand; and (b) made available to the media in formats that they can easily access. For the same reasons, evacuation plans must ensure and provide for: (1) the availability of routes that are handicapped-accessible; (2) ways to safely and quickly transport injured and bedbound patients from hospitals and other medical facilities; and (3) the, sometimes, unique accommodations required to safely move other unfortunate citizens lumped under the generic name "special needs population." In short, the evacuation of a major metropolitan center is a massive undertaking. The Gulf Coast evacuation process prior to Hurricane Katrina and the somewhat haphazard sheltering of evacuees, as well as the inadequate response to those still trapped in various downtown areas of the Crescent City, made national news with images of people stranded on rooftops and horror stories of shelters seemingly out of control and without any support. Three years later, the worst problem that outside critics could find and write about was inadequate washroom facilities. Seen in that context, any workable plan that can get more than one million people out of the vulnerable Gulf Coast area to higher ground inland, with hygiene being the principal and perhaps only negative, is a major improvement.

Hurricane Ian Shows That Coastal Hospitals Aren't Ready for Climate Change

By Daniel Chang and Lauren Sausser
Source: https://www.homelandsecuritynewswire.com/dr20221012-hurricane-ian-shows-that-coastal-hospitals-aren-t-ready-for-climate-change

Oct 12 – As rapidly intensifying storms and rising sea levels threaten coastal cities from Texas to the tip of Maine, Hurricane Ian has just demonstrated what researchers have warned: Hundreds of hospitals in the U.S. are not ready for climate change.
Hurricane Ian forced at least 16 hospitals from central to southwestern Florida to evacuate patients after it made landfall near the city of Fort Myers on Sept. 28 as a deadly Category 4 storm.
Some moved their patients before the storm while others ordered full or partial evacuations after the hurricane damaged their buildings or knocked out power and running water,

said Mary Mayhew, president of the Florida Hospital Association, which coordinates needs and resources among hospitals statewide during a hurricane.
About 1,000 patients across five Florida counties were evacuated from hospitals for different reasons, Mayhew said, with one hospital moving patients after the storm tore part of its roof and deluged the ground floor. Other hospitals emerged with no structural damage but lost power and running water. Broken bridges, flooded roads, and lack of clean water all added to the challenge for some hospitals, Mayhew said.

And that's before considering the need to help those injured in the hurricane and its aftermath.
"Climate shocks like hurricanes show us in the most painful way what we need to fix," said Aaron Bernstein, interim director of the Center for Climate, Health, and the Global Environment, known as C-CHANGE, at the Harvard T.H. Chan School of Public Health.
As climate change increases the intensity of hurricanes, coastal cities threatened by rising sea levels from Miami to Charleston, South Carolina, have considered billion-dollar storm surge protection plans — from elevating homes to creating a network of seawalls, floodgates, and pumps to protect residents and infrastructure against powerful flooding from storms.
Some hospitals are fortifying buildings and elevating campuses. Others are moving inland, as they prepare for a future when even weak storms unleash flooding that can overrun facilities.
"They're the front lines of climate change, bearing the costs of these increased weather events as well as the increase in injuries and disease that come with them," said Emily Mediate, U.S. climate and health director for Health Care Without Harm, a nonprofit that works with hospitals to prepare for climate change.
Yet even as hospitals prepare for extreme weather, Bernstein and a team of researchers at Harvard predicted in a recent study that many facilities along the Atlantic and Gulf coasts will face a suite of problems, even from milder weather events.
The study analyzed the flood risk to hospitals within 10 miles of the Atlantic and Gulf coastlines. In more than half of the 78 metropolitan areas analyzed, some hospitals are at risk of storm surge flooding from the weakest hurricane, a Category 1. In 25 coastal metro areas, half or more of the hospitals risk flooding from a Category 2 storm, which would pack winds of up to 110 mph. Florida is home to six of the 10 most at-risk metropolitan areas identified in the study, with the Miami-Fort Lauderdale-West Palm Beach region ranked as having the greatest risk of hurricane impact.
Researchers also considered the risk of flooding for roads within 1 mile of coastal hospitals during a Category 2 hurricane. That's what happened on Florida's western coast, where Hurricane Ian's maximum sustained winds of 150 mph contributed to flooded roads and washed-out bridges.
All three hospitals in Charlotte County were closed during the storm. One reopened its emergency room the following day, and two were operational by Oct. 1.

In neighboring Lee County, the public hospital system was forced to partially evacuate three of its four hospitals, potentially affecting a bout 1,000 patients, after the facilities lost running water. As of Oct. 6, the county remained in a state of emergency and many roads and bridges were closed due to flooding and damage, according to the Florida Department of Transportation's traffic information.

Several Florida hospitals on waterfront property have moved their essential electrical systems and other critical operations above ground level, elevated their parking lots and buildings, and erected water barriers around their campuses, including Tampa General Hospital, which has the only trauma center in west-central Florida.

Miami Beach is a barrier island where roads flood on sunny days during extremely high tides. Building to withstand hurricanes and flooding is a priority for institutions, said Gino Santorio, CEO of Mount Sinai Medical Center, which sits at the edge of Biscayne Bay. Over the past decade, Mount Sinai has completed nearly $62 million in projects to protect against hurricanes and flooding. The projects were part of a countywide strategy funded by the Federal Emergency Management Agency and state and local governments to fortify schools, hospitals, and other institutions.

"It's really about being the facility of last resort. We're the only medical center and emergency room on this barrier island," Santorio said.

But Bernstein said the "Fort Knox model" of spending hundreds of millions of dollars on state-of-the-art hurricane-proof hospital buildings isn't enough. This strategy doesn't address flooded roads, transportation for patients ahead of a storm, medically vulnerable people in areas most at risk of flooding, emergency hospital evacuations, or the failure of backup power sources, he said.

Urging hospitals to fortify for more severe hurricanes and rising sea levels can feel overwhelming, especially when many are struggling to recover from pandemic-related financial stress, labor shortages, and fatigue, said Mediate, of the group Health Care Without Harm.

"Lots of things make it hard for them to see this is a problem, of course. But on top of how many other issues?" she said.

As Hurricane Ian approached the South Carolina coastline north of Charleston on Sept. 30, the city's low-lying hospital district reported about 6 to 12 inches of water. "That's much less than was expected," Republican Gov. Henry McMaster said during a news briefing.

Though Hurricane Ian was a relatively minor weather event in South Carolina, it's not unusual for Charleston's downtown medical district to flood, making it dangerous and, sometimes, impossible for patients, hospital employees, and city residents to navigate surrounding streets.

In 2017, the Medical University of South Carolina ferried doctors across its large campus on johnboats during severe flooding from Hurricane Irma. One year later, the Charleston-based hospital system bought a military truck to navigate any future floodwaters.
Flooding, even after heavy rain and high tide, is one reason Roper St. Francis Healthcare — one of three systems in Charleston's downtown medical district — announced plans to eventually move Roper Hospital off the Charleston peninsula after operating there for more than 150 years.
"It can make it very challenging for people to get in and out of here," said Dr. Jeffrey DiLisi, CEO of Roper St. Francis.
The hospital system sustained light flooding in one of its downtown medical office buildings from Ian, but it could have been much worse, said DiLisi. He also said that the downtown district is no longer the geographic center of Charleston and that many patients say it's inconvenient to get there.
"The further inland, the less likely you're going to have some of those problems," he said.
Unlike Roper St. Francis, most coastal nonprofit and public hospitals have chosen to remain in their locations and reinforce their buildings, said Justin Senior, the president of the Safety Net Hospital Alliance of Florida and a former secretary of the state's Agency for Health Care Administration, which regulates hospitals.
"They're not going to move," Senior said. "They're in a catchment area where they're trying to catch everyone, not just the affluent but everyone."

Daniel Chang covers Florida and the South for *KHN*. **Lauren Sausser,** South Carolina Correspondent, covers health care across the South as a member of *KHN*'s Southern Bureau.

Looking Back to Look Ahead to Protect the Food Supply

By Benjamin Lieb and Jason Bashura
Source: https://www.domesticpreparedness.com/preparedness/looking-back-to-look-ahead-to-protect-the-food-supply/

Oct 12 – Following the terrorist attacks on the United States, the federal government began to ramp up its arsenal of subject matter experts in the public health arena as it related to the threat of bioterrorism. Among these disciplines, experts in the subjects of food defense and food security were being identified and sought after for a variety of *new* opportunities to protect the food supply. Intentional acts of contamination in the food supply have occurred for thousands of years. Recently there were reports of Ukrainian citizens feeding Russian soldiers poisoned cake and alcohol that resulted in 2 deaths and 28 other soldiers hospitalized. The Food Defense Consortium and the ASIS Food Defense and Agriculture Security Community (FDASC) recently made an effort to update a foundational food defense research paper and offer recommendations for future research to continue improving knowledge in this area.

"For the life of me, I cannot understand why the terrorists have not attacked our food supply because it is so easy to do."
– Former Secretary of Health and Human Services, Tommy Thompson (2004)

Background & Data Collection
As a background, it is important to understand the definitions of a few key terms:

- *Food defense* – "The efforts to prevent intentional contamination of food products by biological, chemical, physical, or radiological agents that are not reasonably likely to occur in the food supply" (as defined by the Food and Drug Administration).
- *Food security* – "The reliable availability of a sufficient quantity and quality of nutritious food for a population" (as defined by the World Health Organization in 2002).

- *Food protection* – The nexus between the food safety practices that are leveraged every day and food defense strategies that are intended to reduce the likelihood of an act of intentional contamination from occurring in the food supply. Elements of food fraud mitigation, food quality, environmental health and safety, and physical security also comprise the concept of food protection.

An internship opportunity in 2022 by the Food Defense Consortium and the FDASC was seeking to have the foundational research paper by G. R. Dalziel, "Food Defence Incidents, 1950-2008: A Chronology and Analysis of Incidents Involving the Malicious Contamination of the Food Supply Chain" updated to include events since 2008. Dalziel is one of the first, if not the first, to write a compendium about incidents of intentional and malicious contamination. This is done by examining the cases comprehensively and systematically – throughout the whole food supply chain. Dalziel's research paper discussed how the World Health Organization defined the difference between food security and food defense while also discussing how the United States and the Department of Homeland Security (DHS) are involved in the food and agriculture sector.

Dalziel concluded that 98% of the cases occurred later in the food supply chain – nearest to the consumer. Intentional contamination also occurred most often in the food service/retail environment, home, or workplace, while cases at the food service point had the greatest impact on the public's health. While Dalziel also concluded that the total number of casualties was low, the updated appendix also followed this trend – with a few outliers. Of the total number of cases per country, Dalziel had collected 60% of his cases from the United States, the United Kingdom, and Australia. He stated that this is because of the wider proliferation of the western media, with the first case in China not being reported until 1992. The number of cases rose in the mid-1980s with increased extortion cases in retail/food service. However, between 2004 and 2008, there was a decrease in annual reported cases.

The research completed in 2022 included updating events that occurred after 2008 – plus a few that had occurred in 2008 but were not captured by Dalziel. The cases in the appendix are sorted into five categories of agents: chemical, biological, radiological, physical contaminant, and unknown. Many of the cases fell under the classification of chemical. Data collection to update the appendix involved open sources (e.g., news articles and peer-reviewed articles) and collaborators within the Food Defense Consortium and the ASIS FDASC, who submitted incidents for review and inclusion in this updated research. After reading through the different cases, it was determined whether they were intentional acts of contamination. The cases were then categorized by year, country, agent, agent type, number of injuries, number of deaths, and a description of the incident. An analysis was produced on some cases to better understand their contents and the method used (see Figure 1).

Appendix I: Updates to Dalziel's Food Defence Events: 1950-2008, updated to include 2008-2022

Benjamin Lieb – Coastal Carolina University Student, Intelligence and National Security Studies; conferred Spring 2021

Header	Agent	Place	Agent	Death	Injury	Description/Reference
2008	Melamine	China	Chemical	6	300,000	Provinces in China had to seized baby milk powders products. The milk powder contained five hundred times the maximum allowed amount. https://www.bbc.com/news/10565838
2008	Dioxin	Ireland	Chemical	0	0	Irish pork products were tainted with dioxins. The pork products contained 80 to 200 times the allowed limit. The products were reached the high levels of dioxin from pig feed of a producer tainted with an industrial oil. https://www.nytimes.com/2008/12/07/world/europe/07iht-irish.4.18467497.html
2011	Pesticide	India	Chemical	143	Dozens	Multiple illegal liquor businesses were creating tainted alcohol. The alcohol was being mixed with pesticide. https://www.bbc.com/news/world-asia-india-16174531

Fig. 1. Depiction of updated Appendix I (Lieb, 2022).

Mitigation

There are ways to mitigate the risk of food being intentionally contaminated. One way is for food manufacturers to update procedures regularly to ensure that the product cannot be easily accessed, thereby decreasing the feasibility of contamination. The updated procedures can prevent current and former employees from tainting products in the food supply chain. The U.S. Food and Drug Administration (FDA) has developed a resource to aid private sector owners and operators in identifying mitigation strategies to help decrease the intentional adulteration (i.e., contamination) of food in production environments.

The Mitigation Strategies Database "is intended as a starting point for facilities to consider when identifying potential mitigation strategies." Additionally, completing basic food defense awareness training is an important step in raising awareness of food defense concepts, which can directly contribute to reducing the risk of intentional adulteration. For example, free food defense awareness training is available on the Food Safety Preventive Controls Alliance website – for food workers at the

retail level (nearest the consumer interface) to manufacturing (food production) and transportation/distribution personnel.
Evaluating events in the past can help predict – and possibly prevent – similar incidents from occurring in the future.
In a strategic and academic sense, another way to help mitigate the number of intentional cases is by updating research (like this endeavor described herein) to demonstrate the methods by which individuals have contaminated food and drink in the past and doubling down and refocusing efforts in these areas moving forward. Operationally, by performing tabletop and functional exercises with cross-functional disciplines represented (regulators, law enforcement, emergency management, food industry), a variety of perspectives can be gleaned, and strengths – as well as gaps – can be identified in these emergency response plans.
The U.S. Department of Agriculture's Food Safety and Inspection Services, FDA, and DHS have all created tabletop exercise toolkits to aid in executing an exercise. However, these resources need to be more readily accessed if they are going to have the intended impacts on the community they are targeted at protecting.
In 2021, one of the teams participating in the DHS's Analytic Exchange Program group focused its research and summary report on critical infrastructure sectors that might be overlooked during a wide-scale natural disaster or man-made event. The final toolkit related to that research is slated to be released at the end of 2022.

Impact of This Analysis
The importance of updating the appendix to Dalziel's work is to better understand how those seeking to harm others have continued contaminating food supply chain products. Mitigating future acts requires an understanding of the products that have been contaminated, the methods used to contaminate the products, and the reasons behind these actions. Some of the reasons why an individual would contaminate food include:

- An ex-employee seeking revenge;
- A current employee unhappy with their position within the company;
- Retaliation for punishment, delayed promotion, or unfair treatment in the workplace;
- Someone seeking recognition for being diligent in the production environment; or
- Someone simply looking to harm others.

The updated appendix, which can be accessed at the Food Safety Tech's Food Defense Resource Portal (Figure 1), allows for more research on the methods and types of individuals committing these acts. In the future, additional analysis should be performed on the new Appendix I to "categorize" the rationale behind why the contamination occurred. These categories are:

- Type I – Offender has no legitimate relationship with the business or its employees;
- Type II – Offender has a legitimate relationship with the business (as a customer, client, patient, student, or inmate);
- Type III – Offender could be a current or past employee;
- Type IV – Offender may or may not have a relationship with the business but has a personal or perceived relationship with an employee; and
- Type V – Offender is an extremist or value-driven group who feels justified by their beliefs.

Call to Action
The outcomes of this research are important for food protection or safety regulatory programs or those officials from state, county, and local emergency management because it demonstrates the different tactics that can be used to contaminate food within the food supply chain. Although gaining insights into solutions to prevent contamination events in the future may be reactive, understanding the methods of contamination will allow for preventative measures and awareness programs to be put in place. A review of the historical events listed in Dalziel's report and the updated content from the new Appendix I document show that history is likely to repeat itself if actions are not taken now to prevent similar incidents.

> *"…But if you close your eyes, does it almost feel like nothing changed at all? And if you close your eyes, does it almost feel like you've been here before?"– Bastille, "Pompeii" October 11, 2013*

Finally, further research is needed to evaluate the variation in *punishment* regarding the penalties related to intentionally adulterating, tampering with, or knowingly introducing contaminated (or potentially contaminated) food, not only within the U.S. but globally. For example, in January 2009, two individuals found guilty of their involvement in China's 2008 melamine scandal – which resulted in 6 deaths, 54,000 hospitalizations, and more than 300,000 affected children – were sentenced to death. Meanwhile, those found guilty for their involvement in a U.S. outbreak associated with contaminated peanut butter were each sentenced to between 60 and 336 months in prison "for their roles in a conspiracy to defraud their customers," which led to 9 deaths and more than 20,000 illnesses.

Summary
The methods of contamination identified in Appendix I will allow for future discussion among cross-functional, multi-disciplinary practitioners on how to prevent and respond to future incidents. Participating in tabletop and functional exercises can help preparedness professionals thwart terrorists and other bad actors from contaminating food (and prove Secretary Thompson wrong). After response plans have been created, they can be tested in a controlled environment utilizing various existing resources to test their effectiveness. Yesterday's plans need to be revised to protect against all of tomorrow's threats. Continuous improvement is necessary to stay ahead of the curve and make a change for the better, for tomorrow. Future iterations of food protection plans need to address a wide variety of threats – those originating from cyber, physical, people sources, or cascading failures of interdependent infrastructures. Food protection plans aim to reduce enterprise risk for food manufacturers and retailers globally and protect the public's health and well-being.

Benjamin Lieb is originally from Cincinnati, Ohio. He attended Coastal Carolina University, where he earned a B.A. in Intelligence and National Security Studies with minors in Anthropology and Criminology. While at Coastal Carolina, he was named to the President's and Dean's lists. Since graduating in May 2022, he has started his career in the Intelligence Community as an officer at the U.S. Department of Homeland Security Transportation and Security Administration. He would like to thank Dr. Smith, the Members of the Food Defense Consortium, the ASIS Food Defense, and Ag Security Community for supporting his throughout this research.

Jason Bashura has been working within the food defense arena since 2002, when he began working with the Connecticut Department of Public Health's Food Protection Program as a food biosecurity (now known as food defense) environmental health sanitarian. After transitioning to the U.S. federal government, he was a food defense policy analyst with the U.S. FDA's Food Defense team where he oversaw the development and utilization of the Food Related Emergency Exercise Bundle (FREE-B) among other critical food defense initiatives. Currently working in industry, he has been leading the informal Food Defense Consortium –to bring together those parties with a vested interest in global food defense issues. He is proud of the countless relationships he's dedicated global government, industry, and academic leaders, in an attempt to connect the innumerable dots within the food defense arena. He has a master's degree in Public Health from the University of Connecticut (UCONN) and an undergraduate degree in Public Health from Southern Connecticut State University. He currently resides in Maryland with his family and serves on the Board of Health in the county where he resides.

International CBRNE INSTITUTE

A common roof for international CBRNE First Responders

Rue des Vignes, 2
B5060 SAMBREVILLE (Tamines)
BELGIUM

info@ici-belgium.be
www.ici-belgium.be