04\21

HZS

C²BRNE DIARY

Dedicated to Global First Responders

April 2021

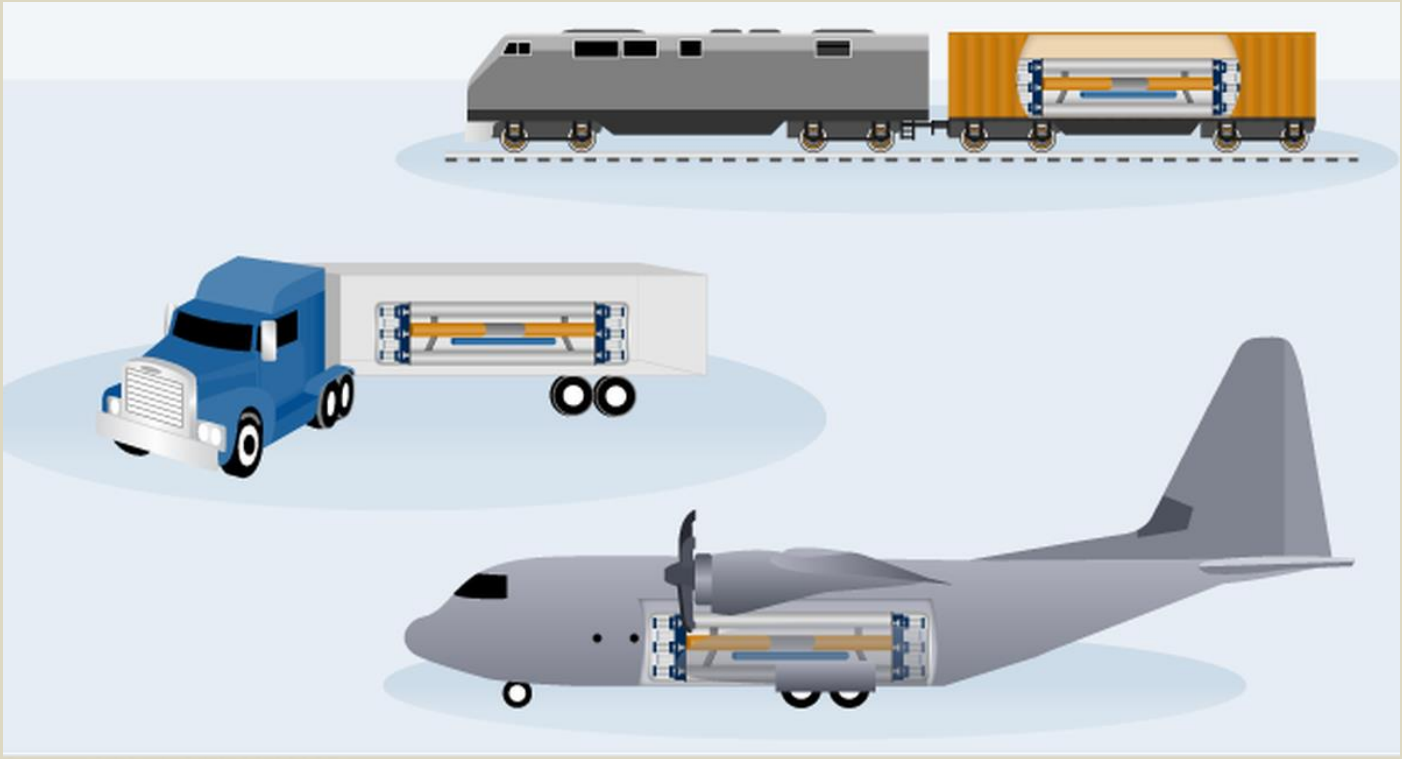
A HOTZONE SOLUTIONS GROUP PUBLICATION


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
HOTZONE
SOLUTIONS
GROUP
C2BRNE
DIARY
DIRTY R-NEWS

Portable nuclear reactor project moves forward at Pentagon

By Aaron Mehta

Source: https://www.defensenews.com/smr/energy-and-environment/2021/03/23/portable-nuclear-reactor-project-moves-forward-at-pentagon/



Source: GAO. | GAO-20-380SP

The Defense Department is moving ahead with an effort to develop small, portable nuclear reactors. These concepts from the Government Accountability Office show potential ideas for transport and deployment. (U.S. Government Accountability Office)

Mar 24 — The Pentagon has selected two companies to move forward with developing small, portable nuclear reactors for military use in the field.

BWXT Advanced Technologies and X-energy were chosen by the department's Strategic Capabilities Office to continue on with Project Pele, which seeks to develop a reactor of 1- to 5-megawatt output that can last at least three years at full power. In addition, the reactors must be designed to operate within three days of delivery and be safely removed in as few as seven days if needed.

The two companies, along with Westinghouse Government Services, were each given preliminary contracts of less than $15 million in March 2020 to begin design work. The final design is due to the Strategic Capabilities Office in 2022, at which point the Defense Department will make a decision on whether to move forward with testing the systems.

"We are thrilled with the progress our industrial partners have made on their designs," Jeff Waksman, Project Pele's program manager, said in a statement. "We are confident that by early 2022 we will have two engineering designs matured to a sufficient state that we will be able to determine suitability for possible construction and testing."

The Pentagon has long eyed nuclear power as a potential way to reduce both its energy cost and its vulnerability in its dependence on local energy grids. According to a news release, the Defense Department uses "approximately 30 Terawatt-hours of electricity per year and more than 10 million gallons of fuel per day."

According to an October 2018 technical report by the Nuclear Energy Institute, 90 percent of military installations have "an average annual energy use that can be met by an installed capacity of nuclear power" of 40 MWe (megawatt electrical) or less.

The Biden administration is expected to pursue alternative energy options across the Pentagon, with Defense Secretary Lloyd Austin pledging to lower the department's carbon footprint and to consider climate impact in strategic decisions. Whether nuclear energy will prove a way forward or not may depend on whether the taboo around nuclear power can be assuaged for local defense communities and members of Congress.

Project Pele is not the only attempt at introducing small nuclear reactors to the Pentagon's inventory; a second effort is being run through the Office of the Under Secretary of Defense for Acquisition and Sustainment. That effort, ordered in the 2019 National Defense Authorization Act, involves a pilot program aimed at demonstrating the efficacy of a small nuclear reactor in the 2- to 10-MWe range, with initial testing at a Department of Energy site around 2023.
While Project Pele is focused on the potential for deployable nuclear reactors, the acquisition and sustainment effort is focused on domestic military installations, with the goal of being operational by 2027.

***Aaron Mehta** is deputy editor and senior Pentagon correspondent for Defense News, covering policy, strategy and acquisition at the highest levels of the Defense Department and its international partners.*

NCT Magazine

March 2021

Nuclear weapons are finally outlawed; next step is disarmament.

Editorial by Dr. Eirini Giorgou, ICRC Legal Adviser, Arms and Conduct of Hostilities, ICRC

Celebrating a historic milestone, the recent entry into force of the Treaty on the Prohibition of Nuclear Weapons (TPNW), Dr. Giorgou comes back on more than 75 years of advocating for the elimination of nuclear weapons. Read more about the International Committee of the Red Cross (ICRC)'s decades-long advocacy and the challenges humanity is still facing until a complete eradication of nuclear weapons and visit ICRC's pavilion at NCT Virtual Europe next week! Read this article...

Homeland Security for Radiological and Nuclear Threats

By Mary Sproull, Biologist, NIH

In this article, Mary Sproull reflects on the various comprehensive emergency planning and preparedness guidelines for management of a radiological or nuclear event in the United States that have been developed at the federal level since the events of 9/11. Learn more about the operational challenges and lessons learned by Homeland Security when responding to Radiological and Nuclear Threats! Read this article...

The Permanent Threat of Nuclear Terrorism

By Maj. Julio Ortega García, Defence Chief of Staff, Spain

Although the CBRNe Community and the society at large have been solely focused on biological threats in the past year, Maj. Ortega Garcia argues that the permanent threat of nuclear terrorism should not be overlooked. In this article, he gives an overview of what could be the next nuclear terrorist attack to raise awareness and help emergency services, civil and military first-responders, and companies to adapt their procedures and strengthen their capabilities to respond to such hazards. Read this article...

Forgotten Casualties: Hospitals in the Aftermath of a Nuclear Detonation

By Dr. Mark L. Maiello and Jenna Mandel-Ricci, MPA, MPH, New York City Department of Health and Mental Hygiene, USA

In this article, Mark Maiello and Jenna Mandel-Ricci explore a fictional scenario where a nuclear detonation takes place, killing everyone. The response was impossible or unnecessary. The emphasis of this article is on the necessity of planning for population evacuation and mass triage of casualties. Learn more about the significant response that will be needed, and especially about the role of hospitals - the "islands of hope" many will seek. Read this article...

Operational Preparedness of Field-Teams in Different Stages of A Nuclear & Radiological (N&R) Event

By Dr. Ori Nissim Levy, International Expert and researcher in Nuclear Defense, Haifa University, Israel & Mr. Avihai Koresh, Researcher, Operational Nuclear Defense Model (ONDM), Israel

Despite the lack of focus on Nuclear and Radiological (N&R) events in the news, the continuous need for preparedness to respond to these incidents remains a reality. Currently, a team of scientists from 10 countries called the World Nuclear Forum 193 (WNF-193) is working on an overall N&R event preparedness States Rating Index, the WNF-193-N&R-SR01-2021. Read more about this new perspective of disaster management that redefines the term "preparedness"! Read this article...

Russian nuclear weapons, 2021

By Hans M. Kristensen and Matt Korda

Pages 90-108 | Published online: 18 Mar 2021

Source: https://www.tandfonline.com/doi/full/10.1080/00963402.2021.1885869

- PDF

The Nuclear Notebook is researched and written by Hans M. Kristensen, director of the Nuclear Information Project with the Federation of American Scientists, and Matt Korda, a research associate with the project. The Nuclear Notebook column has been published in the Bulletin of the Atomic Scientists since 1987. This issue's column examines Russia's nuclear arsenal, which includes a stockpile of nerarly 4,500 warheads. Of these, some 1,600 strategic warheads are deployed on ballistic missiles and at heavy bomber bases, while an additional 985 strategic warheads, along with 1,912 nonstrategic warheads, are held in reserve. The Russian arsenal is continuing broad modernization intended to replace most Soviet-era weapons by the mid- to late 2020s.

Hans M. Kristensen *is the director of the Nuclear Information Project with the Federation of American Scientists in Washington, DC. His work focuses on researching and writing about the status of nuclear weapons and the policies that direct them. Kristensen is a coauthor of the world nuclear forces overview in the SIPRI Yearbook (Oxford University Press) and a frequent adviser to the news media on nuclear weapons policy and operations. He has coauthored Nuclear Notebook since 2001.*

Matt Korda *is a research associate for the Nuclear Information Project at the Federation of American Scientists, where he coauthors the Nuclear Notebook with Hans Kristensen. Previously, he worked for the Arms Control, Disarmament, and WMD Non-Proliferation Centre at NATO headquarters in Brussels. He received his MA in International Peace and Security from the Department of War Studies at King's College London, where he subsequently worked as a Research Assistant on nuclear deterrence and strategic stability. Matt's research interests and recent publications focus on nuclear deterrence and disarmament, progressive foreign policy, and the nexus between nuclear weapons, climate change, and injustice.*

Pakistan has more nuclear bombs than India, find new list of weapons of mass destruction

Source: https://www.flanewsonline.com/pakistan-has-more-nuclear-bombs-than-india-find-new-list-of-weapons-of-mass-destruction/

Mar 27 – The world's new list of weapons of mass destruction has made an important revelation about nuclear weapons. According to a new report by the Federation of American Scientists, a US organization that monitors nuclear weapons, India has fewer nuclear bombs than Pakistan.

Pakistan has more nuclear bombs

According to a report by the Federation of American Scientists (FAS), **Pakistan has 5 more nuclear bombs than India.** Reportedly, Pakistan currently has 165 nuclear bombs while India has 160 nuclear bombs. From 1985 to 1990, nuclear weapons competed in the world and in 5 years it became the world's largest nuclear weapon. However, world nuclear weapons production has declined since the Cold War. According to the report, in 1986 there were 70,300 nuclear weapons worldwide, which decreased to 13,100 in 2021.

Russia has the largest number of nuclear weapons. According to the FAS, Russia currently has the world's largest nuclear arsenal. Russia currently has 6,257 nuclear bombs, with 1,600 deployed. Russia has reserved 4,497 bombs.

The United States currently has 5,550 nuclear bombs, with 1,800 deployed and 3,800 reserved. France ranks third and Britain fourth in the case of active nuclear bombs.

According to the list, China currently has 350 nuclear bombs, followed by France with 290 atomic bombs and Britain with 195 atomic bombs. However, the report casts doubt on the number of atomic bombs in China. Pakistan is followed by Britain; India is followed by 160 nuclear bombs.

Nicola Sturgeon: 'I would rather spend money on nurses than nuclear weapons'

Source: https://www.dailyrecord.co.uk/opinion/nicola-sturgeon-i-would-spend-23808614

Mar 28 – This is the most important election in Scotland's history. So much hangs on its outcome but at its heart, it comes down to one very simple question – who should decide our country's future?

Should it be a Scottish Government at Holyrood, elected by the people of Scotland? Or should it be Boris Johnson and the Tories at Westminster?

The last few days have shown us just how important that question is and just how much it matters.

That's because the last few days have shown everyone the respective priorities of Holyrood and Westminster – and when it comes to how different those priorities are it is not so much a gulf as a vast and ever-widening chasm.

In Scotland, the SNP Government has made our priorities clear, with a four percent pay offer to NHS staff – people who are deserving at the best of times but who, over the last 12 months, have truly gone above and beyond the call of duty as they have battled on the front line of the Covid pandemic to try to keep us all safe.

At the same time, Johnson's Tory Government has not only failed, so far at least, to come near matching that pay offer for health service staff – they have almost gone out of their way to show how different their priorities are.

How else can anyone explain the bizarre and frankly grotesque decision to lift the cap on the UK's stockpile of nuclear warheads.

At a time when the world should be looking to solve common problems and challenges like climate change and recovery from the pandemic, the Tories are intent on rolling the clock back 30 years or more to a Cold War mentality.
So, while they claim to be struggling to find the money to pay nurses, they have no qualms about spending billions of pounds on the obscenity of new nuclear weapons of mass destruction – weapons which will be stored right here in Scotland, barely 40 miles from our biggest city and centre of population.
Johnson's priorities are clearly not Scotland's priorities. But this election can be the one in which Scotland overwhelmingly and decisively shows that it is choosing a better path for all our futures.
Over the coming weeks, the SNP will set out the most positive, upbeat and optimistic case ever made for the future of this country.
It will be brimming over with policies, ideas and initiatives for how we rebuild from the pandemic and create a fairer, more prosperous nation.
Policies like John Swinney's plan to put a laptop or Chromebook in the hands of every pupil in Scotland's schools.
Just as teachers used to hand out jotters to all, in the years to come every pupil will receive the device they need, putting the internet in the hands of every pupil, in class and at home.
Over the last couple of days, we have already started to outline some of that vision.
On Friday, as I addressed local government leaders in COSLA, I confirmed that one of the first acts of a re-elected SNP government will be to begin work on a National Care Service.
I also made clear that we plan to scrap charges for non-residential care, to help ease the financial pressure on those accessing care.
And we will bring in a National Wage for carers so that the value of the pay received by our social care workforce better reflects the huge value of the work they do.
Meanwhile, we have announced that if re-elected we will deliver 100,000 new homes across Scotland in the next decade.
We have delivered nearly 100,000 homes since 2007 but our plan for the next 10 years seeks to double that, in a move that will support up to 14,000 jobs a year as we rebuild from the pandemic and generate investment of around £16billion.
That makes our plan the largest home building and investment programme since the start of devolution – and at least 70 per cent of the new homes will be for social rent.
We'll also introduce a new single standard for housing quality to help make sure homes are more energy efficient, more spacious and of better quality overall.
These are just some of the policy ideas we are bringing to this campaign – but as I said, at its heart this election is about who gets to decide Scotland's future.
If re-elected, an SNP government will take forward plans for an independence referendum, and if those plans have the backing of a majority of MSPs at Holyrood, we propose a referendum should be held once through the pandemic.
The question of who is in charge of the rebuilding is a crucial one – and independence means we can focus on priorities like homes, health and education and not the wasteful priorities of Johnson.
To make that happen we need the strongest possible SNP vote – that means giving both votes to the SNP on May 6.

North Korea Nuclear Timeline Fast Facts

Source: https://kesq.com/news/national-world/2021/03/28/north-korea-nuclear-timeline-fast-facts/

Here is a look at North Korea's nuclear capabilities and the history of its weapons program.

1985

North Korea signs the Nuclear Non-Proliferation Treaty (NPT).

1993

The International Atomic Energy Agency (IAEA) demands that inspectors be given access to two nuclear waste storage sites. In response, North Korea threatens to quit the NPT but eventually opts to continue participating in the treaty.

1994

North Korea and the United States sign an agreement. North Korea pledges to freeze and eventually dismantle its old, graphite-moderated nuclear reactors in exchange for international aid to build two new light-water nuclear reactors.

2002

January 29 – US President George W. Bush labels North Korea, Iran and Iraq an "axis of evil" in his State of the Union address. "By seeking weapons of mass destruction, these regimes pose a grave and growing danger," he says.
October – The Bush Administration reveals that North Korea has admitted operating a secret nuclear weapons program in violation of the 1994 agreement.

2003

January 10 – North Korea withdraws from the NPT.
February – The United States confirms North Korea has reactivated a five-megawatt nuclear reactor at its Yongbyon facility, capable of producing plutonium for weapons.
April – Declares it has nuclear weapons.

2005

North Korea tentatively agrees to give up its entire nuclear program, including weapons. In exchange, the United States, China, Japan, Russia and South Korea say they will provide energy assistance to North Korea, as well as promote economic cooperation.

2006

July – After North Korea test fires long range missiles, the UN Security Council passes a resolution demanding that North Korea suspend the program.
October – North Korea claims to have successfully tested its first nuclear weapon. The test prompts the UN Security Council to impose a broad array of sanctions.

2007

February 13 – North Korea agrees to close its main nuclear reactor in exchange for an aid package worth $400 million.
September 30 – At six-party talks in Beijing, North Korea signs an agreement stating it will begin disabling its nuclear weapons facilities.
December 31 – North Korea misses the deadline to disable its weapons facilities.

2008

June 27 – North Korea destroys a water cooling tower at the Yongbyon nuclear facility.
December – Six-party talks are held in Beijing. The talks break down over North Korea's refusal to allow international inspectors unfettered access to suspected nuclear sites.

2009

May 25 – North Korea announces it has conducted its second nuclear test.
June 12 – The UN Security Council condemns the nuclear test and imposes new sanctions.

2010

November 20 – A Stanford University professor publishes a report that North Korea has a new nuclear enrichment facility.

2011

October 24-25 – US officials meet with a North Korean delegation in Geneva, Switzerland, in an effort to restart the six-party nuclear arms talks that broke down in 2008.

2012

February 29 – The State Department announces that North Korea has agreed to a moratorium on long-range missile launches and nuclear activity at the nation's major nuclear facility in exchange for food aid.

2013

January 24 – North Korea's National Defense Commission says it will continue nuclear testing and long-range rocket launches in defiance of the United States. The tests and launches will feed into an "upcoming all-out action" targeting the United States, "the sworn enemy of the Korean people," the commission says.

February 12 – Conducts third nuclear test. This is the first nuclear test carried out under Kim Jong Un. Three weeks later, the United Nations orders additional sanctions in protest.

2014

March 30-31 – North Korea warns that it is prepping another nuclear test. The following day, the hostility escalates when the country fires hundreds of shells across the sea border with South Korea. In response, South Korea fires about 300 shells into North Korean waters and sends fighter jets to the border.

2015

May 6 – In an exclusive interview with CNN, the deputy director of a North Korean think tank says the country has the missile capability to strike mainland United States and would do so if the United States "forced their hand."
May 20 – North Korea says that it has the ability to miniaturize nuclear weapons, a key step toward building nuclear missiles. A US National Security Council spokesman responds that the United States does not think the North Koreans have that capability.
December 12 – North Korea state media says the country has added the hydrogen bomb to its arsenal.

2016

January 6-7 – North Korea says it has successfully conducted a hydrogen bomb test. A day after the alleged test, White House spokesman Josh Earnest says that the United States has not verified that the test was successful.
March 9 – North Korea announces that it has miniature nuclear warheads that can fit on ballistic missiles.
September 9 – North Korea claims to have detonated a nuclear warhead. According to South Korea's Meteorological Administration, the blast is estimated to have the explosive power of 10 kilotons.

2017

January 1 – In a televised address, Kim claims that North Korea could soon test an intercontinental ballistic missile.
January 8 – During an interview on "Meet the Press," Defense Secretary Ash Carter says that the military will shoot down any North Korean missile fired at the United States or any of its allies.
January 12 – A US defense official tells CNN that the military has deployed sea-based radar equipment to track long-range missile launches by North Korea.
July 4 – North Korea claims it has conducted its first successful test of an intercontinental ballistic missile, or ICBM, that can "reach anywhere in the world."
July 25 – North Korea threatens a nuclear strike on "the heart of the US" if it attempts to remove Kim as Supreme Leader, according to Pyongyang's state-run Korean Central News Agency (KCNA).
August 7 – North Korea accuses the United States of "trying to drive the situation of the Korean peninsula to the brink of nuclear war" after the UN Security Council unanimously adopts new sanctions in response to Pyongyang's long-range ballistic missile tests last month.
August 9 – North Korea's military is "examining the operational plan" to strike areas around the US territory of Guam with medium-to-long-range strategic ballistic missiles, state-run news agency KCNA says. The North Korea comments are published one day after President Donald Trump warns Pyongyang that if it continues to threaten the United States, it would face "fire and fury like the world has never seen."
September 3 – North Korea carries out its sixth test of a nuclear weapon, causing a 6.3 magnitude seismic event, as measured by the United States Geological Survey. Pyongyang claims the device is a hydrogen bomb that could be mounted on an intercontinental missile. A nuclear weapon monitoring group describes the weapon as up to eight times stronger than the bomb dropped in Hiroshima in 1945. In response to the test, Trump tweets that North Korea continues to be "very hostile and dangerous to the United States." He goes on the criticize South Korea, claiming that the country is engaging in "talk of appeasement" with its neighbor to the north. He also says that North Korea is "an embarrassment to China," claiming Beijing is having little success reining in the Kim regime.
November 1 – A US official tells CNN that North Korea is working on an advanced version of its intercontinental ballistic missile that could potentially reach the United States.
November 28 – A South Korean minister says that North Korea may develop the capability to launch a nuclear weapon on a long-range ballistic missile at some point in 2018.

2018

January 2 – Trump ridicules Kim in a tweet. The president says that he has a larger and more functional nuclear button than the North Korean leader in a post on Twitter, responding to Kim's claim that he has a nuclear button on his desk.

January 10 – The White House releases a statement indicating that the Trump administration may be willing to hold talks with North Korea.
March 6 – South Korea's national security chief Chung Eui-yong says that North Korea has agreed to refrain from nuclear and missile testing while engaging in peace talks. North Korea has also expressed an openness to talk to the United States about abandoning its nuclear program, according to Chung.
March 8 – Chung, standing outside the White House, announces that Trump has accepted an invitation to meet Kim.
June 12 – The final outcome of a landmark summit, and nearly five hours of talks between Trump and Kim in Singapore, culminates with declarations of a new friendship but only vague pledges of nuclear disarmament.
December 5 – New satellite images obtained exclusively by CNN reveal North Korea has significantly expanded a key long-range missile base, offering a reminder that Kim is still pursuing his promise to mass produce and deploy the existing types of nuclear warheads in his arsenal.

2019

January 18 – Trump meets with Kim Yong Chol, North Korea's lead negotiator on nuclear talks, and they discuss denuclearization and the second summit scheduled for February.
February 27-28 – A second round of US-North Korean nuclear diplomacy talks ends abruptly with no joint agreement after Kim insists all US sanctions be lifted on his country. Trump states that Kim offered to take some steps toward dismantling his nuclear arsenal, but not enough to warrant ending sanctions imposed on the country.
March 8 – Analysts say that satellite images indicate possible activity at a launch facility, suggesting that the country may be preparing to shoot a missile or a rocket.
March 15 – North Korea's foreign minister tells reporters that the country has no intention to "yield to the US demands." In the wake of the comment, US Secretary of State Mike Pompeo insists that negotiations will continue.
May 4 – South Korea's Defense Ministry states that North Korea test-fired 240 mm and 300 mm multiple rocket launchers, including a new model of a tactical guide weapon on May 3. According to the defense ministry's assessment, the launchers' range is about 70 to 240 kilometers (43 to 149 miles). The test is understood to be the first missile launch from North Korea since late 2017 — and the first since Trump began meeting with Kim.
October 2 – North Korea says it test fired a new type of a submarine-launched ballistic missile (SLBM), a day after Pyongyang and Washington agreed to resume nuclear talks. The launch marks a departure from the tests of shorter range missiles North Korea has carried out in recent months.
December 3 – In a statement, Ri Thae Song, a first vice minister at the North Korean Foreign Ministry working on US affairs, warns the United States to prepare for a "Christmas gift," which some interpret as the resumption of long-distance missile testing. December 25 passes without a "gift" from the North Korean regime, but US officials remain watchful.

2020

March 9 – According to US and South Korean officials, North Korea fires at least three unidentified projectiles, the second such move by the regime in two weeks. North Korean state media says military exercises began on February 28, the one-year anniversary of Kim's summit in Hanoi, Vietnam, with Trump which ended without a deal. The military drills continued March 2, when Pyongyang fired two unidentified short-range projectiles from an area near the coastal city of Wonsan, about 65 kilometers (40 miles) south of Sondok.

2021

March 24 – North Korea launches two ballistic missiles — the second such launch in less than a week. According to a statement from South Korea's joint chiefs of staff, two short-range missiles were fired from the Hamju area of South Hamgyong province toward the sea, off North Korea's east coast, at 7:06 a.m. and 7:25 a.m. local time. The projectiles flew about 450 kilometers (280 miles), reaching an altitude of 60 kilometers (37 miles), and are believed to have been ballistic missiles launched from the ground, the statement said. The exact type of the missiles are still unclear, a senior US official told CNN, citing an intelligence briefing.

Homeland Security for Radiological and Nuclear Threats

Source: http://www.homelandsecuritynewswire.com/dr20210329-homeland-security-for-radiological-and-nuclear-threats

Mar 29 – Radiation exposure events are complicated: there is a variety of radiation sources, and since radiation is invisible, and its effect may not always be immediately apparent, first

responders and emergency services must prepare for a "worried well" of people requiring attention: individuals who do not have other physical injuries but are concerned about whether they have received a radiation exposure.
Mary Sproull, a biologist in the Radiation Oncology Branch of the National Cancer Institute at the National Institutes of Health (NIH) and a Biodefense Ph.D. candidate, discusses the current state of homeland security for radiological and nuclear threats, and highlights the areas in need of improvement.
Sproull lists the many available guidelines for emergency response, the organizations which provide guidance on emergency management of radiation events, and other resources for radiation injury. *Pandora Report* notes that Radiation exposure comes in a variety of forms – external and internal exposure to a radioactive isotope or external exposure to ionizing radiation energy – so Sproull writes that the "greatest operational challenge of a radiological or nuclear event is diagnosing radiation injury."
Radiation is invisible to the naked eye, so a radiation event may result in a sizeable population of "worried well," defined as individuals who do not have other physical injuries but are concerned about whether they have received a radiation exposure. This may overwhelm available medical resources. In response to this operational challenge, there has been support for the development of new radiation biodosimetry diagnostics, which "estimate the dose of radiation a person has received" and are "used both for population screening to assure the worried well and to support existing triage algorithms."
Several of these diagnostics are expected to be added to the Strategic National Stockpile (SNS).
Additionally, several radiation-specific medical countermeasures have been granted Food and Drug Administration (FDA) licensure for radiation injury treatment and have already been added to the SNS.
Sproull says that despite these achievements in preparedness for large scale emergencies involving radiation exposure, there still exist important areas in need of improvement: "capacity to manage burn victims and the overall willingness of first responders and other medical personnel to work with patients who have been either exposed and/or contaminated with radiation or radioactive materials."

North Korea's Yongbyon facility partly active after missile launches, analysts say

Source: https://www.upi.com/Top_News/World-News/2021/03/31/North-Korea-Yongbyon-activity-analysis/3501617204262/

North Korea's Yongbyon nuclear research center is showing some signs of activity, according to satellite imagery taken Tuesday. File Photo by Siegfried C. Hecker/UPI

Mar 31 – North Korea's Yongbyon nuclear research center is showing signs of activity after the launch of two short-range ballistic missiles last week, according to U.S. analysts.
Joseph Bermudez and Victor Cha said in a new study of satellite imagery taken Tuesday that steam or smoke was flowing from stacks within the radiochemistry lab in the compound. The lab is used to reprocess spent fuel rods to extract plutonium.

"This, while not an indicator of a reprocessing campaign itself, indicates that the building is occupied and being heated," the analysts said.
The report also pointed out there was no significant activity related to the Experimental Light Water Reactor or the 5MWe Reactor. The latter facility is believed to be the main production site of weapons-grade plutonium in the country.
North Korea's most important nuclear facility is being highlighted at a time of ongoing tensions with the United States.

On Monday, the White House said President Joe Biden is not willing to meet in person with Kim Jong Un. Former President Donald Trump met with Kim three times, but diplomacy did not resolve the issue of nuclear weapons development.
The U.S. State Department issued its 2020 country reports on human rights practices on Tuesday.
On North Korea, the State Department said COVID-19 has led to greater restrictions and controls in the country, making internal movement difficult for all.
"Non-governmental organizations, foreign diplomats, and U.N. agency personnel were not allowed to leave Pyongyang," the report read. "This severely hampered foreign observers' already extremely limited ability to monitor human rights and humanitarian aid conditions in the country."
The report also pointed out inhuman treatment including torture was confirmed by several defector accounts and NGO reports.
"Methods of torture and other abuse reportedly included severe beatings; electric shock; prolonged periods of exposure to the elements; humiliations such as public nakedness; confinement for up to several weeks in small "punishment cells" in which prisoners were unable to stand upright or lie down," the report stated.

US Nuclear Weapons Are Aging Quickly. With Few Spare Parts, How Long Can They Last?

By Tara Copp
Source: https://www.military.com/daily-news/2021/03/30/us-nuclear-weapons-are-aging-quickly-few-spare-parts-how-long-can-they-last.html

Airmen from the 791st Maintenance Squadron vehicles and equipment recovery section check their equipment at Minot Air Force Base, North Dakota, May 1, 2019. (Dillon J. Audit/U.S. Air Force)

Mar 30 — When hundreds of land-based nuclear armed ballistic missiles were first lowered into underground cement silos spread across the vast cornfields here in 1970, the weapons were only intended to last a decade before a newer system came in.
Fifty years later, these missiles — called the Minuteman III — are still on alert, manned by members of the U.S. Air Force in teams of two who spend 24 hours straight below ground in front of analog terminals from the 1980s, decoding messages and running tests on the missiles' systems to check if they could still launch if needed.

But it's not the age of weapons or the decades-old technology that troubles their operators. It's that the original manufacturers who supplied the gears, tubes and other materials to fix those systems are long gone.
Several years ago, the motor on one of the industrial-sized caged elevators that slowly descends 100 feet below ground to the launch control center broke, an airman with the base's 791st Maintenance Squadron told McClatchy. A fix was not available for months.
Instead, maintainers resorted to rigging a pulley to lower supplies down for the crews, the airman said, who spoke on the condition they not be named.
"We're severely constrained with spares," the airman said. "The technology does its job. The challenge is sustaining it."
To make repairs, airmen are often forced to take parts from another machine. Two of the airmen at Minot told McClatchy the facility's missile guidance system often needs parts or attention because of constant wear and tear.
"You can only do that so many times until the system fails," said Lt. Col. Steve Bonin, commander of the 91st Operations Support Squadron at Minot.

The price to modernize

Next month Chairman of the Joint Chiefs of Staff Army Gen. Mark Milley and Defense Secretary Lloyd Austin will seek billions to keep the 50-year-old land based missiles running while a debate begins on whether they should be replaced.
It's a difficult ask: At the same time, the Pentagon is also in the middle of the most expensive nuclear modernization effort in its history.
All three legs of the nuclear triad — air, land and sea defenses launched from silos, overhead strategic bombers or nuclear submarines — are getting replaced with newer weapons systems, simultaneously.
The next-generation replacement bombers, missiles and submarines now under development have a price tag topping $400 billion and are expected to be a primary topic of questioning during hearings next month as lawmakers debate whether modernizing all three legs is necessary.
"In my humble opinion, we're building more weapons than we need," House Armed Services Committee Chairman Rep. Adam Smith, D-Wash., said during a Center for Strategic and International Studies discussion in December. "We need to look at ways to have a robust deterrent in a more cost-effective manner. And that's what we're going to work towards."

Kansas City complex

Due to the high cost of developing brand-new weapons, the default for the military has often been keeping the existing nuclear missiles running for a few additional years.
All of the repair and life extension work for nuclear missiles or bombs is handled at just a few offsite locations across the U.S. All of the non-nuclear parts of any of the warheads rely on just one place, the Department of Energy's Kansas City National Security Campus.
"There are no backup places," said Lisa Gordon-Hagerty, the former head of the Department of Energy's National Nuclear Security Administration, which is responsible for maintaining the nation's nuclear stockpile. That means there isn't a way to quickly obtain spares in an emergency, she added.
The non-nuclear parts of the weapons are tightly controlled in Kansas City because of the high cost if a counterfeit part slips through. Even for a simple part like wiring, a counterfeit that is set to degrade faster could effectively disable a missile without aircrews realizing the damage, Gordon-Hagerty said.
The non-nuclear components that are produced at the Kansas City facility include items as basic as wiring or bolts, and as complex as the weapon's firing system. They make up more than 80% of each weapon, according to the U.S. Government Accountability Office.
As the missiles have aged, they've needed more work.
Last year, the GAO reported that the Kansas site would need to expand to meet the levels of repair now needed.
"The workload of the Kansas City site has increased and is currently at the highest level since the end of the Cold War," the GAO said.
The agency cautioned that supply chain issues and a lack of floor space at the Kansas City site could hamper future plans to swap out parts and extend the life of the weapons.

Milley's message

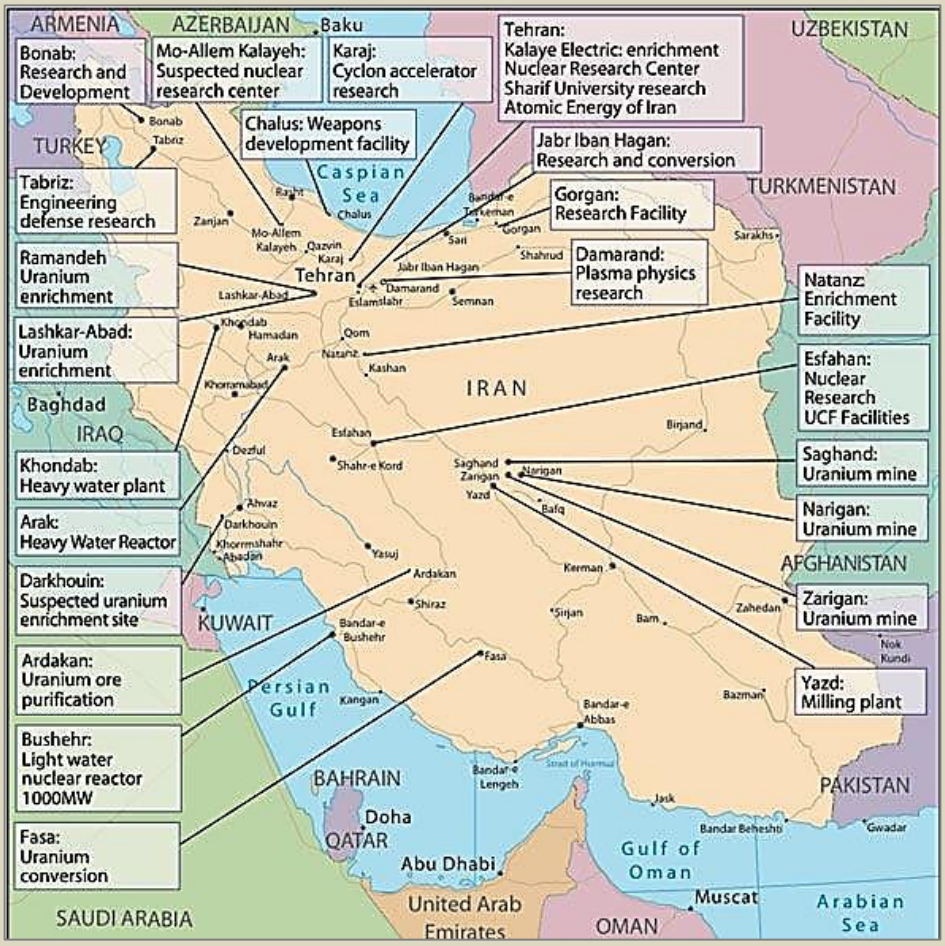
Navy Adm. Charles Richard, the head of U.S. Strategic Command, wonders how many life extensions are left for the missiles.
"When I say heroics, I'm talking about where people are doing some very innovative things to reverse engineer and creatively replace parts and things like that," Richards said.

He added that another service life extension is "certainly past the point of being cost-effective and approaching the point where you can't do it at all."
To prepare for upcoming congressional hearings on the defense budget, Milley went to Minot.
He climbed inside a B-52 Stratofortress that's been flying since 1960 to talk to the crew and ask them what upgrades would help their missions. The UH-1N Huey that carried him to the missile silo has been in service since 1969. The wall deep underground at the launch control center that he signed as he departed was built around 1962.
"We're moving into a period where the engineering lifespan of these systems is nearing its end," Milley said. "Nuclear deterrence, strategic deterrence, I think, has been effective in preventing great power war for seven decades, since the end of World War II. And until, unless we have something better come along, I think we need to update and modernize the one we have."
As he departed the launch facility, Milley took a marker to write a message to the missileers. It's a place near the exit where crews who have completed their tours and visiting defense leaders have also scribbled notes.
"Every day there is no nuke war you won," Milley wrote.

Table of Iranian Nuclear Sites and Related Facilities

Source: https://www.iranwatch.org/our-publications/weapon-program-background-report/table-irans-principal-nuclear-facilities

Mar 31 – Iran operates a number of facilities that carry out the different steps of the nuclear fuel cycle. This infrastructure includes locations where Iran mines natural uranium, plants that process uranium ore into a concentrate known as "yellowcake," and plants that convert this yellowcake into uranium hexafluoride (UF6) gas. This gas is the feedstock for centrifuges that enrich uranium. Iran operates several gas centrifuge plants and accumulates enriched uranium that can be used to manufacture fuel for nuclear reactors or nuclear weapons. Iran operates several reactors for the purpose of generating electricity and conducting research for medical and industrial applications. Because of the dual-use potential of many of these facilities, however, the international community has long raised concerns that Iran could use its facilities and expertise to develop nuclear weapons.



The facilities described above are declared by Iran to the International Atomic Energy Agency (IAEA) and subject to some form of inspection by the Agency. However, recent developments have highlighted the importance of accessing nuclear facilities that Iran has not declared to the IAEA. In 2019, IAEA inspectors detected uranium particles at an undeclared site in Turquzabad, near Tehran. The IAEA rejected Iran's explanation of the nuclear material's presence at the site as "not technically credible" and identified three additional suspicious undeclared sites, reportedly located at Abadeh, Lavisan-Shian, and Mobarakiyeh. While Iran ultimately granted the IAEA access to a pair of those sites in order to investigate the possible presence of nuclear material or activity, such access took months to negotiate. The Agency decided that there would be no verification value in accessing the third site, because it had "undergone extensive sanitization and levelling." These latest incidents echo past access challenges for the Agency. Before the

implementation of the Joint Comprehensive Plan of Action (JCPOA), the IAEA sought to understand the "possible military dimensions to Iran's nuclear program" and was often thwarted in its investigation by a lack of access to locations and key individuals.
Through the JCPOA, the IAEA was allowed access to and information about more nuclear sites in Iran. Iran agreed to provisionally implement the Agency's Additional Protocol and to allow expanded access pursuant to the JCPOA, giving IAEA inspectors the ability to request access to an undeclared site and to monitor additional nuclear commodities and components. However, Iran curtailed this arrangement in February 2021 in response to U.S. sanctions.
The table below lists Iran's known and alleged nuclear sites and their purpose, location, and operating status.

Facility/Site	Purpose	Location	Status
Saghand Uranium Mine	extraction of uranium ore	Saghand	operational
Gchine Uranium Mine	extraction of uranium ore	Gchine	reported closed*
Ardakan Yellowcake Production Plant	uranium concentrate production	Ardakan	operational
Bandar Abbas Yellowcake Production Plant	uranium concentrate production	Bandar Abbas	reported closed*
Uranium Conversion Plant (UCF)	uranium conversion	Isfahan Nuclear Technology Center (ENTC)	operational
Uranium Chemistry Laboratory (UCL)	study of uranium compounds	Isfahan Nuclear Technology Center (ENTC)	confirmed closed*
Fuel Fabrication Laboratory (FFL)	fuel pellet production	Isfahan Nuclear Technology Center (ENTC)	confirmed closed*
Fuel Manufacturing Plant (FMP)	fuel production for the Arak reactor and light water reactors	Isfahan Nuclear Technology Center (ENTC)	operational
Fuel Plate Fabrication Plant (FPFP)	fuel production for the Tehran Research Reactor (TRR)	Isfahan Nuclear Technology Center (ENTC)	operational
Zirconium Production Plant (ZPP)	zirconium sponge production	Isfahan Nuclear Technology Center (ENTC)	operational
Miniature Neutron Source Reactor (MNSR) (30 kWt)	reportedly for isotope production	Isfahan Nuclear Technology Center (ENTC)	operational
Heavy Water Zero Power Reactor	research	Isfahan Nuclear Technology Center (ENTC)	operational
Light Water Sub-Critical Reactor (LWSCR)	research	Isfahan Nuclear Technology Center (ENTC)	operational
Graphite Sub-Critical Reactor (GSCR)	training	Isfahan Nuclear Technology Center (ENTC)	decommissioned
Pilot Fuel Enrichment Plant (PFEP)	uranium enrichment with gas centrifuges	Natanz	operational
Fuel Enrichment Plant (FEP)	uranium enrichment with gas centrifuges	Natanz	operational
Iran Centrifuge Assembly Center (ICAC)	centrifuge assembly	Natanz	destroyed and reportedly being rebuilt
Fordow Fuel Enrichment Plant (FFEP)	uranium enrichment with gas centrifuges	Fordow	operational
National Center for Vacuum Technology	manufacture, testing, and calibration of vacuum equipment	Fordow	operational

Facility/Site	Purpose	Location	Status
National Materials Science and Engineering Research Center	testing radioactive materials	Fordow	operational
Kalaye Electric Company	gas centrifuge development and testing	Tehran	allegedly operational
Heavy Water Production Plant (HWPP)	heavy water production (used as a moderator in nuclear reactors)	Arak	operational
Heavy Water Research Reactor (IR-40) (20 MWt)[1]	radioisotope production (by-products include plutonium)	Arak	redesign work ongoing
Tehran Research Reactor (TRR) (5 MWt)	radioisotope production	Tehran Nuclear Research Center (TNRC)	operational
Jabr Ibn Hayan Multipurpose Laboratories (JHL)	research, including on uranium metal	Tehran Nuclear Research Center (TNRC)	operational
Molybdenum, Iodine and Xenon Radioisotope Production Facility (MIX Facility)	radioisotope production	Tehran Nuclear Research Center (TNRC)	operational
Waste Handling Facility	storage and disposal of radioactive waste	Tehran Nuclear Research Center (TNRC)	operational
Bushehr-1 (Light Water Power Reactor) (1,000 MWe)	electricity production	Bushehr	operational
Bushehr-2 (V-528 VVER-1000 Pressured Water Reactor) (974MWe)	electricity production	Bushehr	under construction
Bushehr-3 (V-528 VVER-1000 Pressured Water Reactor) (974MWe)	electricity production	Bushehr	under construction
Turquzabad site	allegedly storage of nuclear material and equipment	South of Tehran	not operational**
Parchin military complex	location of alleged nuclear weapon-related work	South of Tehran	Partially demolished
Lavisan-Shian site	location of alleged nuclear weapon-related work	Allegedly near Lavisan-Shian	reportedly demolished
Pilot uranium conversion plant	allegedly conducted uranium processing and conversion	Allegedly near Mobarakiyeh	reportedly demolished**
Abadeh site	allegedly conducted experiments relevant to nuclear weapon development	Allegedly near Abadeh	reportedly partially demolished**
Pilot Uranium Laser Enrichment Plant	uranium enrichment using lasers	Lashkar Abad	likely inactive[2]
Karaj Waste Storage Facility	radioactive waste storage	Karaj Nuclear Research Center for Medicine and Agriculture	operational
Anarak Near-Surface Repository	radioactive waste disposal	Anarak	operational

* Facilities labeled as “reported closed” have either been declared closed by Iranian authorities or reported closed by media sources. Facilities labeled as “confirmed closed” have had their closure verified by the IAEA.

** Traces of uranium reportedly discovered on site by IAEA inspectors in 2019 or 2020.

[1] The original design of the IR-40 Heavy Water Research Reactor was for a power of 40 megawatt thermal (MWt); the JCPOA requires that the reactor be redesigned with a power not exceeding 20 MWt.
[2] Satellite imagery indicated activity as late as 2013 at the Pilot Uranium Laser Enrichment Plant, prompting the IAEA to visit the facility in March 2014. The JCPOA (Annex I, Section S, Paragraph 81) requires Iran to only enrich uranium using gas centrifuge technology, thereby prohibiting laser enrichment. The IAEA has made no subsequent mention of the Pilot Uranium Laser Enrichment Plant since 2014, suggesting that the facility is inactive.

Iran's uranium enrichment plant at Fordow is one of the most worrisome parts of the country's nuclear infrastructure: it was developed secretly, is located underground, and in January, Iran began using the plant to produce 20 percent enriched uranium, which is closer to the level needed to fuel a nuclear weapon. The Islamic Revolutionary Guard Corps (IRGC) was involved in the plant's construction and the complex is also host to key nuclear research centers.

Entities of concern

Fordow Fuel Enrichment Plant FFEP
A gas centrifuge plant for the enrichment of uranium hexafluoride (UF6) developed and managed by the Atomic Energy Organization of Iran (AEOI); originally designed to hold up to 2,976 gas centrifuges in 16 cascades divided between two units; since November 2019, has been enriching uranium in violation of the JCPOA.

Khatam-al Anbiya Construction Headquarters (KAA)
An Islamic Revolutionary Guard Corps (IRGC)-owned group of companies that acts as a prime contractor on projects for Iran's ballistic missile and nuclear programs; involved in large-scale civil and military construction and engineering projects, including at Fordow.

National Materials Science and Engineering Research Center
Established in 2018 and located within the Fordow complex; reportedly capable of testing radioactive materials and materials with radioactive contamination; reportedly provides services to the AEOI, as well as to the petroleum, petrochemical, and steel sectors.

U.N.: 'Highly likely' North Korea can mount nuclear warheads on missiles

Source: https://www.upi.com/Top_News/World-News/2021/04/01/nkorea-un-report-North-Korea-nuclear-weapons-missiles/3881617253058/

Apr 01 – A report from a United Nations panel of experts found that North Korea has continued to fund its weapons program through illicit means such as smuggling and cyberattacks and concluded that the secretive state can probably arm its ballistic missiles with nuclear warheads.

"[I]t is highly likely that a nuclear device can be mounted on the intercontinental ballistic missiles, and it is also likely that a nuclear device can be mounted on the medium-range ballistic missiles and short-range ballistic missiles," the report, released Wednesday, said.

However, the report said it remains uncertain whether North Korea "had developed ballistic missiles resistant to the heat generated during re-entry."

The report was created by a panel of experts under the U.N. Security Council sanctions committee on North Korea.

Despite sanctions, an economic downturn caused by the COVID-19 pandemic and a series of natural disasters, North Korea was able to upgrade its weapons and defense systems in 2020.

North Korea "has not only continued to develop and modernize its ballistic missile program but has also increased its nuclear strike capability, as well as its ability to counter foreign missile defense systems while safeguarding itself with its own new air defense system," the report said.

The U.N. panel assessed that North Korea's 5 MWe reactor at its Yongbyon nuclear research center is capable of producing around 7 kilograms of plutonium per year and added that the country may possess 60 kilograms of the radioactive chemical element.

There have been no signs of the reactor operating since 2018, although other activity at the Yongbyon facility has been recently taking place, according to satellite imagery.

North Korea has supported its weapons development through illicit activities such as importing oil in violation of international sanctions and stealing cryptocurrency through cyberattacks.

Pyongyang stole more than $316 million worth of virtual assets from 2019 to November 2020, the report said. The panel of experts cited the BeagleBoyz, a hacker group inside Pyongyang's Reconnaissance General Bureau intelligence unit, as responsible for several cyberattacks on cryptocurrency exchanges and financial institutions.

The country has also defied international sanctions and "continued illicit import of refined petroleum, via direct deliveries and ship-to-ship transfers, using elaborate subterfuge," the report said. It concluded that the shipments from January to September 2020 exceeded the annual 500,000-barrel cap "by several times."

North Korea hasn't conducted any long-range missile or nuclear tests since 2017, but it launched a pair of short-range ballistic missiles into the sea near Japan last week, violating U.N. sanctions.

The Chilling Story of The 'Demon Core' And The Scientists Who Became Its Victims

Source: https://www.sciencealert.com/the-chilling-story-of-the-demon-core-and-the-scientists-who-became-its-victims

Apr 03 – It was August 13, 1945, and the 'demon core' was poised, waiting to be unleashed onto a stunned Japan still reeling in fresh chaos from the deadliest attacks anyone had ever seen.

A week earlier, 'Little Boy' had detonated over Hiroshima, followed swiftly by 'Fat Man' in Nagasaki.

These were the first and only nuclear bombs ever used in warfare, claiming as many as 200,000 lives – and if things had turned out a little differently, a third deadly strike would have followed in their hellish wake.

But history had other plans.

After Nagasaki proved Hiroshima was no fluke, Japan promptly surrendered on August 15, with Japanese radio broadcasting a recorded speech of Emperor Hirohito conceding to the Allies' demands.

As it turns out, this was the first time the Japanese public at large had ever heard one of their emperors' voices, but for scientists at the Los Alamos Laboratory in New Mexico – aka Project Y – the event had a more pressing significance.

It meant the functional heart of the third atom bomb they'd been working on – a 6.2-kilogram (13.7-pound) sphere of refined plutonium and gallium – wouldn't be needed for the war effort after all.

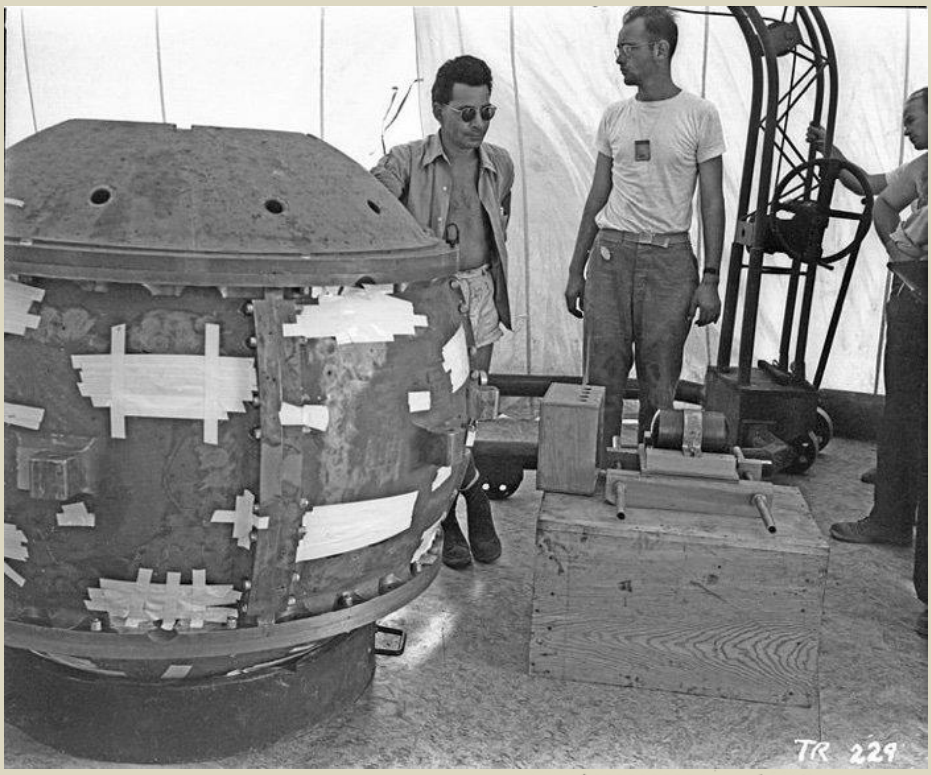
If the conflict had still been raging, as it had for almost five straight years, this plutonium core would have been fitted into a second Fat Man assembly and detonated above another unsuspecting Japanese city just four days later.

As it was, fate issued those souls a reprieve, and the Los Alamos device – code-named 'Rufus' at this point – would be retained at the facility for further testing.

It was during these tests that the leftover nuke, which ultimately became known as the demon core, earned that name.

Daghlian's burnt, blistered hand. (Los Alamos National Laboratory)

The first accident happened less than a week after Japan's surrender, and only two days after the date of the demon core's cancelled bombing run.
That mission may have never launched, but the demon core, stranded at Los Alamos, still found an opportunity to kill.
The Los Alamos scientists knew well the risks of what they were doing when they conducted criticality experiments with it – a means of measuring the threshold at which the plutonium would become supercritical, the point where a nuclear chain reaction would unleash a blast of deadly radiation.
The trick performed by scientists in the Manhattan Project – of which the Los Alamos Lab was a part – was finding how just how far you could go before that dangerous reaction was triggered.
They even had an informal nickname for the high-risk experiments, one which hinted at the perils of what they did. They called it "tickling the dragon's tail", knowing that if they had the misfortune to rouse the angry beast, they would be burned.



Louis Slotin, left, with the first nuclear bomb assembly, Gadget (Los Alamos National Laboratory)

And that's exactly what happened to Los Alamos physicist Harry Daghlian.
On the night of August 21, 1945, Daghlian returned to the lab after dinner, to tickle the dragon's tail alone – with no other scientists (just a security guard) around, which was a breach of safety protocols.
As Daghlian worked, he surrounded the plutonium sphere with bricks made of tungsten carbide, which reflected neutrons shed by the core back at it, edging it closer to criticality.
Brick by brick, Daghlian built up these reflective walls around the core, until his neutron-monitoring equipment indicated the plutonium was about to go supercritical if he placed any more.
He moved to pull one of the bricks away, but in doing so accidentally dropped it directly onto the top of the sphere, inducing supercriticality and generating a glow of blue light and a wave of heat.

Recreation of 1946 accident. (Los Alamos National Laboratory)

Daghlian reached out immediately and removed the brick, noticing a tingling sensation in his hand as he did so.

Unfortunately, it was already too late.

In that brief instant, he had received a lethal dose of radiation. His burnt, irradiated hand blistered over, and he eventually fell into a coma after weeks of nausea and pain.

He was dead just 25 days after the accident. The security guard on duty also received a non-lethal dose of radiation.

But the demon core was not yet finished.

Despite a review of safety procedures after Daghlian's death, any changes made weren't enough to prevent a similar accident occurring the following year.

On May 21, 1946, one of Daghlian's colleagues, physicist Louis Slotin, was demonstrating a similar criticality experiment, lowering a beryllium dome over the core.

Like the tungsten carbide bricks before it, the beryllium dome reflected neutrons back at the core, pushing it toward criticality. Slotin was careful to ensure the dome – called a tamper – never completely covered the core, using a screwdriver to maintain a small gap, acting as a crucial valve to enable enough of the neutrons to escape.

The method worked, until it didn't.

The screwdriver slipped and the dome dropped, for an instant fully covering the demon core in a beryllium bubble bouncing too many neutrons back at it.

Another scientist in the room, Raemer Schreiber, turned around at the sound of the dome dropping, feeling heat and seeing a blue flash as the demon core went supercritical for the second time in the space of a year.

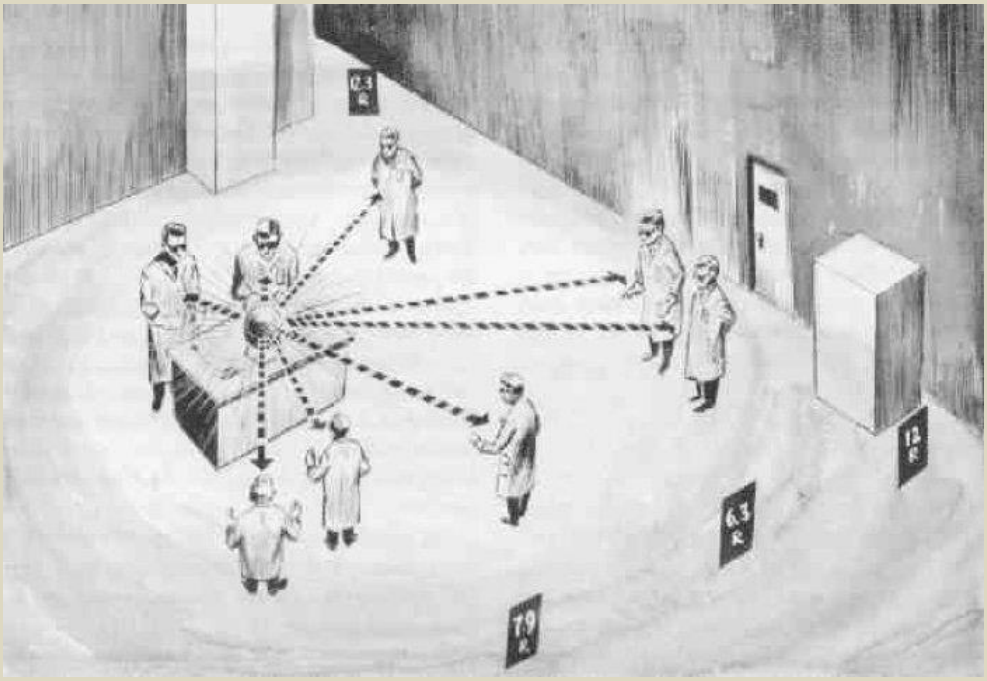


Diagram of 1946 accident. (Los Alamos National Laboratory)

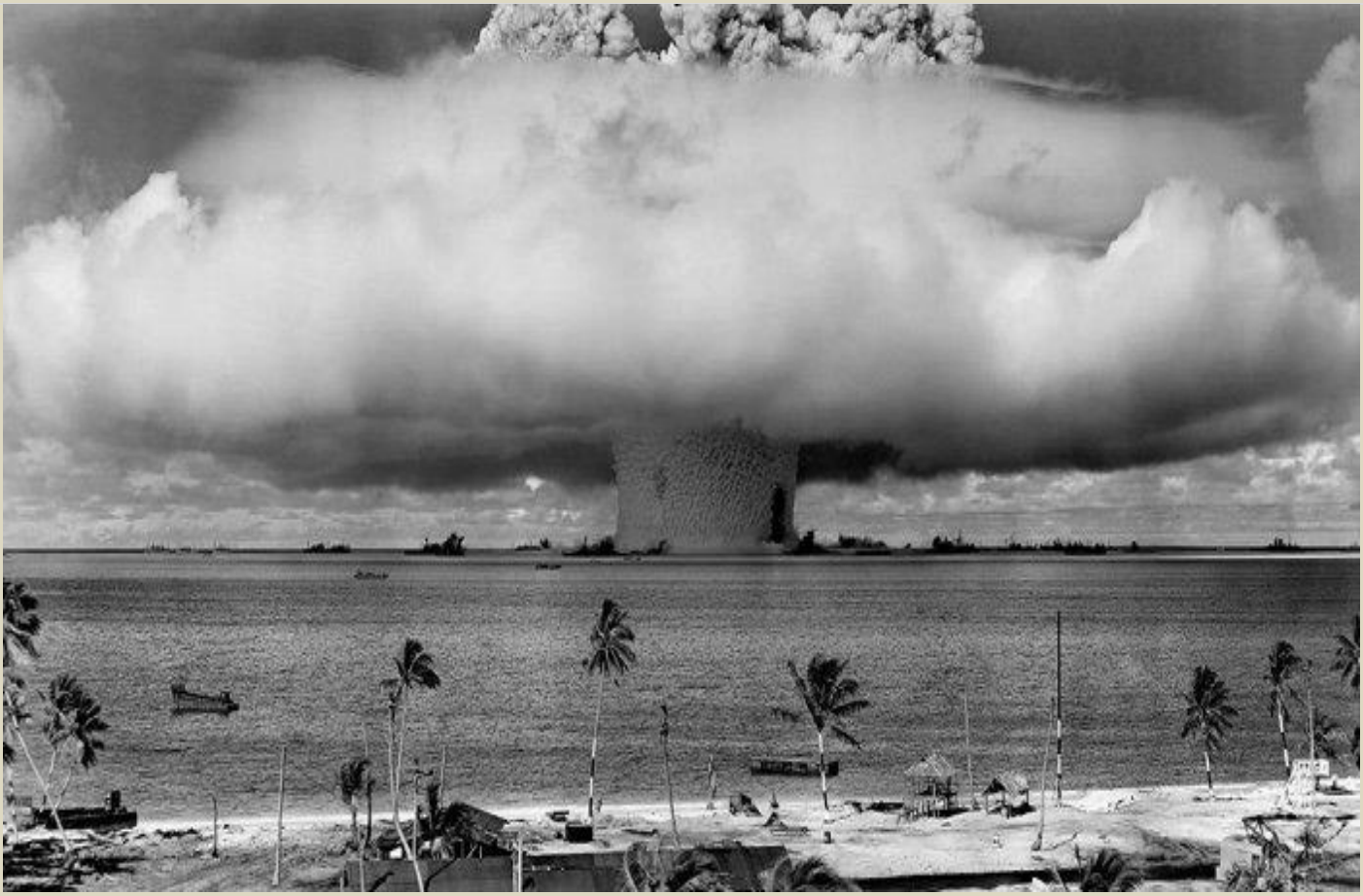
"The blue flash was clearly visible in the room although it (the room) was well illuminated from the windows and possibly the overhead lights," Schreiber later wrote in a report.

"The total duration of the flash could not have been more than a few tenths of a second. Slotin reacted very quickly in flipping the tamper piece off."

Slotin may have been quick in rectifying his deadly mistake, but again, the damage was already done.

He, and seven others in the room – including a photographer and a security guard – were all exposed to a burst of radiation, although Slotin was the only one to receive a lethal dose, and a greater one than that inflicted on Daghlian.

After an initial bout of nausea and vomiting, he at first seemed to recover in hospital, but within days was losing weight, experiencing abdominal pain, and began showing signs of mental confusion.



Operation Crossroads. (US Department of Defence)

A press release issued by Los Alamos at the time described his condition as "three-dimensional sunburn".
Nine days after the screwdriver slipped, he was gone.
The two deadly accidents, only months apart, finally saw real changes take place at Los Alamos.
New protocols meant an end to 'hands on' criticality experiments, with scientists forced to use remote control machinery to manipulate radioactive cores at a distance of hundreds of metres.
They also stopped calling the plutonium core 'Rufus'. From then on, it was known only as the 'demon core'.
But after everything that had happened, the leftover nuke's time was up too.
Following the Slotin accident – and the core's resultant increase in radiation levels – plans to use it in Operation Crossroads, the first post-war nuclear explosion demonstrations to commence at the Bikini Atoll a month later, were shelved.
Instead, the plutonium was melted down and reintegrated into the US nuclear stockpile, to be recast into other cores as necessary.
For the second and last time, the demon core was denied its detonation.
While the deaths of two scientists can't be compared to the untold horrors if the demon core had been used in a third nuclear attack against Japan, it's also easy to understand why the scientists gave it the superstitious name they did.
Then there are the weird details that fill in the backdrop of the story.
Like how Daghlian and Slotin weren't just killed by similar accidents involving the same plutonium core: both incidents took place on Tuesdays, on the 21st day of the month, and the men even passed away in the same hospital room.
Of course, those are just coincidences. The demon core wasn't actually demonic. If there's an evil presence here, it's not the core, but the fact that humans rushed to make these terrible weapons in the first place.
And the real horror – besides the horrible effects of radiation poisoning – is how spectacularly mid–20th century scientists failed to protect themselves from the extreme dangers they were toying with, despite fully knowing the grave risks in their midst.
According to Schreiber, Slotin's first words immediately after the screwdriver incident were simple, and already resigned.
He had comforted his dying friend Daghlian in hospital, and he knew what came next.
"Well," he said, "that does it."

Why Japan's Radioactive Water May End Up In the Ocean

By Aaron Clark and Stephen Stapczynski (Bloomberg)

Source: https://www.washingtonpost.com/business/energy/why-japans-radioactive-water-may-end-up-in-the-ocean/2021/03/10/70714bf4-8219-11eb-be22-32d331d87530_story.html

Mar 12 – The Japanese utility giant Tepco is considering a plan to dump more than 1 million cubic meters of treated radioactive water -- enough to fill 400 Olympic-size swimming pools -- from the wrecked Fukushima Dai-Ichi nuclear power plant into the Pacific Ocean, part of its nearly $200 billion effort to clean up the worst atomic accident since Chernobyl. Storage tanks at the site are forecast to be full by mid-2022, and space for building more is scarce. Scary as it sounds, discharges are common practice in the industry and would likely meet global guidelines. That hasn't assuaged angry locals or neighboring South Korea.

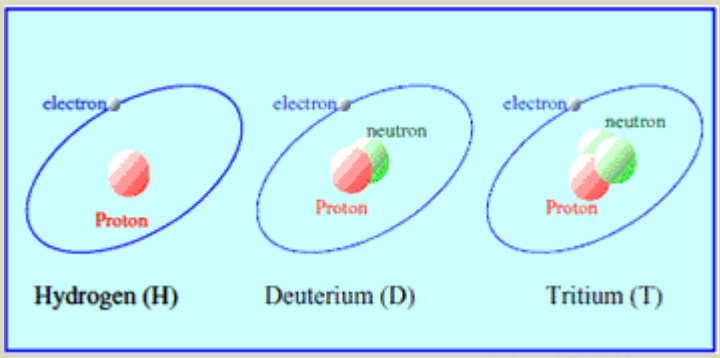
Storage tanks filled with radioactive water at the Fukushima No. 1 nuclear power plant in Okuma, Fukushima Prefecture, in 2019 (Asahi Shimbun file photo)

1. Where does the water come from?

A 2011 earthquake, the strongest ever recorded in Japan, and ensuing tsunami caused structural damage to Fukushima's reactor buildings, about 220 kilometers (135 miles) north of Tokyo. While Tepco cycles in water to keep fuel and debris cool, about 100 cubic meters of groundwater flows in daily and becomes contaminated. The tainted water is pumped out and run through something called the Advanced Liquid Processing System, or ALPS, then stored in one of roughly 1,000 tanks at the site. The processing removes most of the radioactive elements except for tritium. Before being released, the so-called tritiated water would be reprocessed to ensure all of it meets safety standards, according to the Ministry of Economy, Trade and Industry.

2. What is tritium?

A form of hydrogen that has two extra neutrons, making it weakly radioactive. It is naturally produced in the upper atmosphere and also is a common byproduct of nuclear power generation. It has various applications including in making nuclear weapons, in medicine as a biological tracer, and in producing such glow-in-the-dark items as exit signs and watch dials.



3. Is it dangerous?

It can be carcinogenic at high levels. While tritium's beta particles (those emitted during radioactive decay) are too low-energy to penetrate the skin, they can build up in the body if

inhaled or consumed (usually via tainted water). Yet according to the Canadian Nuclear Safety Commission, a human would need to ingest billions of units of becquerels (a measure for radioactivity) before seeing any health effects. The Tepco tank with the highest concentration has 2.5 million becquerels per liter, according to data from March 31. For comparison, a banana has 15 becquerels and 1 kilogram (2.2 pounds) of uranium has 25 million.

4. How is it handled?

Most nuclear power plants discharge small amounts of tritium and other radioactive material into rivers and oceans, according to David Hess, a policy analyst at the World Nuclear Association, an industry group. In the U.S., such "authorized releases" of so-called tritiated water are done "routinely and safely" and are fully disclosed, according to the U.S. Nuclear Regulatory Commission. The International Commission on Radiological Protection's recommendations, which form the basis for rules globally, limit liquid radioactive waste so that public radiation doses annually are less than 1 millisievert (a unit for measuring radiation exposure, abbreviated as mSv). For comparison, the World Nuclear Association says background radiation in the natural environment typically exposes people to an average 2.4 mSv a year, while a CT scan of the pelvis results in an effective dose of 10 mSv.

5. Why not build more tanks?

Tepco, or Tokyo Electric Power Company Holdings Inc., is essentially out of room on the facility grounds. It has already felled 500 square meters (5,400 square feet) of trees next to a bird sanctuary to make room for about 1,000 tanks. Japan could move toward more long-term storage on nearby land by investing in petroleum reserve tanks, the biggest of which can hold some 2.4 billion liters of liquid. It's unlikely anyone will want to live in areas around the plant for a long time. But it would also require a political decision.

6. How might it be released?

Also to be determined. Some nuclear safety experts in Vienna, where the IAEA is based, suggest it might be preferable to pump the water at depth in the middle of the ocean rather than along littoral coastlines where marine life breeds. That could be a boon for climate scientists studying ocean circulation, since tritium has been used before as a tracer. Most of our knowledge currently is of surface-level circulation. Less is know about the deeper sea. Some radiochemists say the idea has some merit, but note that International Maritime Organization laws prohibit the intentional release of radioactive material in the open ocean -- rules that were created following Russian low-level dumping in the Sea of Japan during the 1990s.

7. Who's against a release? For it?

Fishing groups in Fukushima prefecture are strongly opposed, fearing it could further taint the reputation of their catch and affect their livelihoods. (More than 20 countries still have import restrictions imposed after the disaster on some Japanese food products.) South Korean officials also have expressed concern about the possible release, though ocean currents are unlikely to bring any contaminated water near its shores. Former Tepco Chairman Takashi Kawamura and former Nuclear Regulation Authority Chairman Shinichi Tanaka have both voiced support for releasing the water into the ocean. Prime Minister Yoshihide Suga, who took office in September, has yet to announce his position.

8. How will the decision be made?

A panel under the Ministry of Economy, Trade and Industry has proposed releasing the water into the sea or decreasing the volume through evaporation. (Earlier ideas included injecting the water into the ground or mixing it with concrete and burying it.) Once Suga's government chooses an option to pursue, Tepco will then implement it. The final plan also has to be cleared by the nation's nuclear watchdog. The International Atomic Energy Agency said in an April report that it stood ready to help.

9. How's the cleanup going otherwise?

The March 11, 2011, quake off Japan's northeast coast and ensuing tsunami caused about 16,000 confirmed deaths and extensive damage, including the meltdowns at Fukushima. Since then, there's been steady progress in the cleanup at the plant, which Tepco estimates will take 30 to 40 years more. In 2019 the utility sent a robot to touch melted fuel at the bottom of one of the reactors for the first time -- a necessary step toward developing a device to remove and dispose of it. An underground ice wall and drainage system was installed to reduce the amount of groundwater flowing into the wrecked reactors by more than half. The life of cleanup workers has

improved as well. A thin surgical-style mask is all that's needed to walk around most of the grounds, as opposed to a full body suit with a hard plastic mask covering the entire face. Radiation levels on the grounds have dropped, allowing for more work around the plant.

◀ UPDATE (13/4/2021)
Decision taken. It is official!

Retaining Knowledge of Nuclear Waste Management

Source: http://www.homelandsecuritynewswire.com/retaining-knowledge-nuclear-waste-management

Apr 07 – Have you ever started a new job and spent a lot of time figuring out everything from how to get paper for the printer to whether an important customer prefers quick phone calls to emails?
Imagine if that important customer was the federal government and the project you were working on was evaluating the development of a geologic repository for the permanent disposal of spent nuclear fuel and high-level radioactive waste.
Experts at Sandia National Laboratories just began their second year of a project to capture important, hard-to-explain nuclear waste management knowledge from retirement-age employees to help new employees get up to speed faster.
"At Sandia, we've had over 45 years of experience in nuclear waste management in the U.S. and internationally," said Tito Bonano, nuclear energy fuel cycle senior manager. "But the expertise and experiences of people like myself, Peter Swift, Ken Sorenson and others that have retired or are retirement age, walks away when we leave the organization. We refer to that kind of expertise and experiences as tacit knowledge, and we had to act to stop the bleeding of tacit knowledge."
Tacit knowledge includes understanding the boss's opinions as to why a competitor is doing well or the best way to work with an important customer. Such knowledge is often difficult to explain. Explicit knowledge, which includes things such as a phone number or the temperature of water, is easier to document and communicate to others.
Explicit knowledge can be captured in reports and spreadsheets, but tacit knowledge is often learned through mentorship, observation and practice.
"Most large organizations, laboratories and government agencies are very good at saving their explicit knowledge, in the form of reports and documents," said Janette Meacham, the nuclear energy fuel cycle program's licensing and knowledge management lead. "But the knowledge that comes from going into Tito's office with a difficult problem and having him say, 'I remember 15 years ago we did something similar, and this is how we did it, and you need to watch out for this other thing,' is not captured in a report."
Through focus group discussions, a multiday workshop, a series of four-hour deep dives and recording interviews with retiring employees, the knowledge management team led by Meacham captured this tacit knowledge and is in the process of organizing and tagging it to make it easier for early career and new employees to access.
Preserving this contextual knowledge will save time and U.S. taxpayers' money, especially when the federal government begins work on a permanent nuclear waste disposal solution, Bonano said. He added, "As a federally funded research and development center, we have a responsibility to be good custodians of the knowledge we've developed to benefit future projects."

Focus Groups, Recorded Q&A Sessions to Capture Hard-to-Explain Knowledge

Starting in 2019, the team conducted focus groups with employees who had been with the organization less than five years, five to 10 years and more than 10 years to discover how each group best learns and wants to access information.
"One of the tenets of a successful knowledge-management project is getting the right information to the right people at the right time in the right format," Bonano said. "Future generations are going to need to solve the country's nuclear waste management problem. We want to make sure that all of the knowledge we capture ultimately supports the licensing of a nuclear waste management facility."
Then, Sandia hosted a three-day workshop with experts, retirees and federal representatives. Each speaker had some prepared remarks, but the most valuable part of the workshop was when the experts responded to questions from the audience, Meacham said. About 50 Sandia employees at all stages of their careers attended the workshop to learn directly from the experts, and the workshop was recorded for future reference.

They also hosted a series of four-hour deep dives on complex topics, such as how to effectively get expert opinions for risk assessments and understanding how various regulations on nuclear waste management overlap with each other. Each deep dive was led by an expert who started the discussion with prepared information and then answered a lot of productive questions from an audience of 15 to 20 employees. The sessions were also recorded. There were six deep dives last year, and there will be four more later this year.
Also, as other important topics come up in the ordinary course of business, the team records interviews with experts and recently retired employees to capture their tacit knowledge.
The recordings of each session or interview, searchable transcriptions, the experts' slides and links to the documents they referenced are all available to Sandia nuclear energy fuel cycle staff via an internal archive. Eventually, Meacham hopes to have the archive accessible to the Department of Energy and experts at other national laboratories.
Already the internal archive has seen significant use. In an average month, it gets about 2,000 visits from the 180 employees within Sandia's nuclear energy fuel cycle program, Meacham said.

Expanding a Culture of Preserving Knowledge at Sandia, Abroad
In addition to the recorded sessions, Meacham is working on developing a culture in the organization where capturing tacit knowledge is just as important, and just as an integral part of the job, as capturing explicit knowledge in the form of reports. To that end, she is leading the construction of a taxonomy to tag the recorded seminars and interviews and such explicit-knowledge resources as reports , as well as a more sophisticated database where employees can easily add tacit knowledge. The goal is to make all the information more accessible.
"The first part was getting those interviews, grabbing that information quickly while we could and stopping the bleeding," Meacham said. "At the same time, we have to come up with an overarching system of capturing that information as it is created. We need to make it part of the normal work processes of the nuclear energy fuel cycle staff, and staff across the labs."
In the future, Meacham and Bonano hope to extend what they've learned about knowledge management, capturing tacit knowledge and making it accessible to early career employees to other portions of Sandia and other agencies.
They already have been asked to collaborate with colleagues at the Nuclear Decommissioning Authority in the U.K., the Nuclear Waste Management Organization of Japan and other international agencies as they undertake similar knowledge management projects.
"Everyone else seemed to be talking about the problem of maintaining important knowledge, but we said, 'We've got to do something about it now,' so we just did it," Bonano said. "It's part of Sandia's attitude that we're here to solve problems."

UAE: Fuel loading under way at Barakah 2

Source: https://www.world–nuclear–news.org/Articles/Fuel–loading–under–way–at–Barakah–2

Mar 13 – The process of loading 241 fuel assemblies into the core of unit 2 at the Barakah nuclear power plant in the UAE has begun, operator Nawah Energy Company has announced. The move follows the issuance by the Federal Authority for Nuclear Regulation of the operating licence for the second of four Korean–designed APR1400 units at the site.

Pakistan's China–built nuclear reactor starts operation

Source: https://www.voanews.com/south–central–asia/pakistans–china–built–nuclear–reactor–starts–operation

Mar 19 – Pakistan has connected its new Chinese–built nuclear power plant, with an installed capacity of 1,100 megawatts, to the national grid.

China nuclear reprocessing to create stockpiles of weapons-level materials

Source: https://www.reuters.com/article/usa-china-nuclear-plutoniumidAFL1N2LN1IH

Mar 25 – China's push to develop fuel for a new generation of nuclear power reactors will produce large amounts of materials that could be diverted to making nuclear weapons, non-proliferation experts said.

Lebanon Prime Minister warns of 'dangerous nuclear chemicals' in oil facility

Source: https://www.reuters.com/article/us-lebanon-crisis-chemicals-idUSKBN2BI2YP

Mar 26 – Lebanon's outgoing prime minister said on Friday that experts had found "dangerous chemicals" at a warehouse at the **Zahrani oil installations** in the south.

Hassan Diab said the country's atomic energy authority identified the substances as "nuclear" after reviewing a report by German company Combi Lift, which Lebanon had tasked with clearing hazardous material at Beirut port.

The comments came nearly eight months after a stockpile of chemicals detonated in Beirut, killing nearly 200 people in one of the largest non-nuclear explosions on record. The ammonium nitrate went up in flames after being stored unsafely at the port for years.

A Combi Lift spokesman confirmed to Reuters that the firm was in talks with Lebanon over potential recovery projects in Tripoli and Zahrani refineries but said there were no concrete results yet.

"We don't want to comment on possible finds," the spokesman said.

Diab appealed for action, without elaborating.

But Lebanon's oil directorate **said the canisters, which totaled 1.2 kg** (2.7 lb), were just used **for research** and would be transferred next week for safe storage.

"We assure the Lebanese...there is no reason for any fear," the directorate said.

Diab's cabinet has served in a caretaker capacity since resigning over the devastation that last August's explosion wreaked in much of the Lebanese capital, compounding an already acute financial crisis.

After Lebanon hired Combi Lift in the wake of the blast, the German firm said it had found 58 containers at Beirut port that posed a threat to the city. Some of it had been there for more than a decade.

The German ambassador to Beirut, Andreas Kindl, said this month the material were packed well but were still waiting to be shipped to Germany for disposal, as Lebanon had yet to make a nearly $2 million payment in the contract.

Combi Lift spokesman Malte Steinhoff said on Friday those containers remained in Beirut amid talks with the Lebanese authorities over financing.

"We...hope to find a solution this month," he said.

Dust with French nuclear test residue threatens Turkey

Source: https://www.dailysabah.com/turkey/dust-with-french-nuclear-test-residue-threatens-turkey/news

Mar 03 – France is not the only country to be affected by sandstorms carrying the residues of cesium 137, used in nuclear tests by the country in the 1960s in the Sahara desert. Experts warn the dust, expected to move eastward and make a landing in Turkey soon, may be harmful for the population.

Bekir Taşdemir, a nuclear medicine expert from Dicle University, says though it is unclear how much cesium residue there is in the dust sandstorms brought, people need to be cautious. "Possible high rate (of cesium) will necessitate people to stay indoors. They should not breathe the air outside and not open their windows," Taşdemir warned.

French experts had revealed that cesium was found in dust hailing from the Sahara Desert after a sandstorm on Feb. 6 traveled to the Jura Mountains. The same pattern of sandstorms is forecast for Turkey in the coming days.

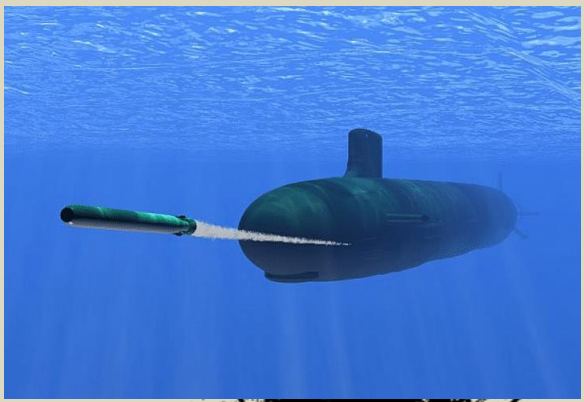
Taşdemir told Demirören News

Agency (DHA) on Wednesday that the movement of dust particles, when combined with rainfall, will be more dangerous. "You should take an umbrella or have protective clothing if it is necessary to go out. If it rains, you should rapidly remove your clothes and wash them and take a shower when you return home. If radioactive residues are accumulated on your body or clothes, it poses a risk. There is also the possibility that those residues will settle on fruits and vegetables and you should be careful washing them thoroughly before consumption, in case of such a sandstorm," he added.

Cesium 137, a lethal chemical element, is used in the nuclear industry. When touched with bare hands, it can kill the person within seconds. It was emitted into the atmosphere after the 2011 nuclear plant accident in Fukushima, according to researchers. **France had conducted its first nuclear test in the Sahara desert on Feb. 13, 1960. It carried out 17 nuclear explosions in the Algerian part of the Sahara Desert between 1960 and 1966. Eleven of the tests came after the 1962 Evian Accords ended the six-year war of independence and 132 years of French colonial rule.** The issue of nuclear tests remains a major bone of contention between France and Algeria which claims the nuclear tests claimed the lives of a large number of people among the local population and damaged the environment.
The Sahara dust that has blanketed parts of southern and central Europe last month has caused a short, sharp spike in **air pollution** across the region according to researchers.

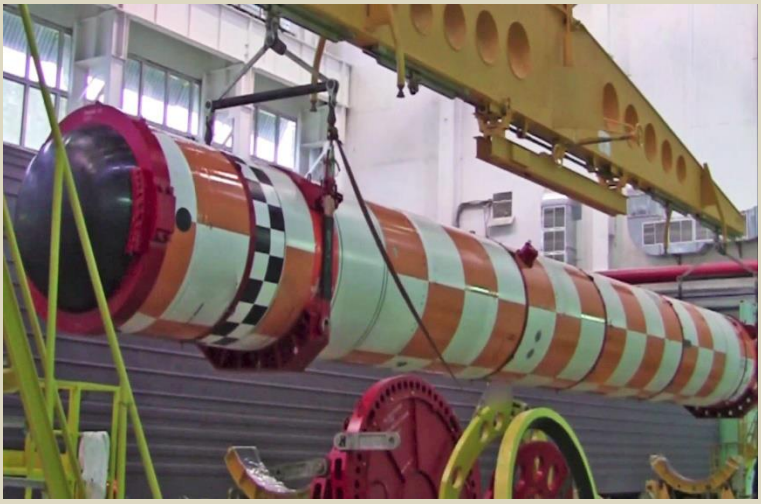
This New Russian Weapon Can Cause Tsunamis

Source: https://wonderfulengineering.com/this-new-russian-weapon-can-cause-tsunamis/



Apr 10 – According to sources, Russia has the current largest stockpile of nuclear weapons in the world and they have no qualms about making more. They have developed a new torpedo, the Poseidon 2M39. The torpedo is capable of sneaking mostly undetected along the bottom of the sea.
The torpedo can detonate on the coastline and reportedly cause a radioactive tsunami. The best guess would be that it is capable of flooding the area with radioactive water, thus destroying the environment and harming the ecosystem greatly. This technology was deemed close to impossible to make a few years back but recent Russian military tests and activities in the Arctic have others thinking otherwise.
A former assistant secretary of state for International Security and Non-Proliferation, Christopher A. Ford, told in a statement last year that the new

weapon of mass destruction was designed to "inundate U.S. coastal cities with radioactive tsunamis." Though them actually using the weapon may be farfetched but we can totally see this being used as a scare and intimidation during future negotiations between the countries.



Katarzyna Zysk, International relations professor from Norwegian Institute for Defence Studies, said that "It is absolutely a project that will be used to scare, as a negotiation card in the future, perhaps in arms control talks but in order to do so, it has to be credible. This seems to be real. "

Intentions aside, if such a weapon is actually used, there would be serious ecological and environmental repercussions. The weapon would be able to cause generational environmental destruction to the landscape and wildlife.

Aside from the Poseidon tests, Russia is also moving forward with other high-tech weapons like hypersonic missiles. **Just how many weapons does Russia need?**

EDITOR'S COMMENT: What is exactly the meaning of the last sentence? The traditional "Bad Russians" *vs.* "Good Americans" moto?

Blackout hits Iran nuclear site

Apr 11/12 – A power failure apparently caused by a deliberately planned (underground 40-50m) explosion struck Iran's Natanz uranium enrichment site yesterday, complicating diplomatic efforts that began last week to salvage the 2015 nuclear deal.

American and Israeli intelligence officials said there had been an Israeli role in the explosion. Israeli officials have made no secret of their unhappiness over President Biden's desire to revive the nuclear agreement that his predecessor renounced in 2018. Israel publicly declined to confirm or deny any responsibility.

Officials, who spoke on the condition of anonymity, said that the explosion dealt a severe blow to Iran's ability to enrich uranium and that it could take at least nine months to restore Natanz's production. Iran has vowed to take "revenge" for an alleged act of sabotage

UChicago Student Series: The Future of Nuclear Energy in the United States

By Sabrina Fields

Source: https://thebulletin.org/2021/04/uchicago-student-series-the-future-of-nuclear-energy-in-the-united-states/

Apr 12 – On Tuesday, March 30, forty graduate students studying policy and business at the University of Chicago attended a virtual event focused on demystifying the state of domestic nuclear energy. The program, "The Future of Nuclear Energy in the United States," was a joint effort between the Harris School of Public Policy's Energy and Environmental Association and the Bulletin of the Atomic Scientists and was the first of the 2021 student programs between the Bulletin and the Harris School, where the Bulletin is housed.

The event featured Dr. Ashley Finan, Director of the National Reactor Innovation Center (NRIC) at Idaho National Laboratory in conversation with Sabrina Fields, UChicago Liaison for the Bulletin and first year MPP student at Harris, followed by a Q&A from the student audience. Finan noted that when looking for a source of energy that would produce fewer air pollutants, her upbringing near a nuclear power plant in part inspired her to pursue nuclear engineering.

Nuclear energy accounts for nearly 20% of US electricity, and over 50% of its carbon-free electricity. Yet nuclear power often suffers from efficiency and cost critiques that can only be overcome with modern technology and processes. Enter the National Reactor Innovation Center, charged with accelerating the demonstration of advanced nuclear reactors, and with a vision of at least two by 2025. Finan discussed the importance of public-private partnerships in moving nuclear technology forward, highlighting two projects in particular: the **Natrium reactor** designed by TerraPower and the **Xe-100 reactor** designed by X-energy. After successful demonstration, it is NRIC's hope that reactors like these will be picked up by utility companies and put into operation, providing more generating capacity for clean energy.

With 2025 on the horizon, it is not yet certain what procurement or market incentives might be in place to drive deployment at scale and nth of a kind costs, those some of these exist now, Finan explained. To enable review of innovative designs, the Nuclear Regulatory Commission (NRC) is modernizing its approach, particularly to develop a more technology-inclusive methodology for the wide variety of designs moving towards demonstration. Nuclear power also faces an added barrier of public perception following a history of classified weapons programs and catastrophic nuclear incidents, but Finan affirmed she is hopeful about our ability to overcome these challenges. The primary antidote to these fears, she contends, is transparency and engaged communication.

Sabrina Fields *is a first-year MPP student at the Harris School of Public Policy at the University of Chicago. She works as a research assistant for Professor Robert Rosner, studying the economics of nuclear energy and electric vehicles. Prior to her time at the University of Chicago, Fields worked as a research associate focused on event detection through open-source intelligence. Her most recent project looked at trends in misinformation, including detecting and analyzing networks of Coronavirus-related misinformation on social media platforms. She also conducted research on extremist messaging networks and emerging datasets. Fields holds a Bachelor of Science in science, technology, and international affairs from Georgetown University.*

An intelligence forecast and the Doomsday Clock coincide. For better or worse.

By John Mecklin

Source: https://thebulletin.org/2021/04/an-intelligence-forecast-and-the-doomsday-clock-coincide-for-better-or-worse/

Apr 08 – The National Intelligence Council released a new and grim report this week that made me immediately wonder, "Where have I seen this before?"

"Global Trends: A More Contested World" is the latest in a series of reports that the council, part of the US Office of the Director of National Intelligence, has issued every four years since 1997. In it, the council's Strategic Futures Group "assesses the key trends and uncertainties that will shape the strategic environment for the United States during the next two decades."

The trends are unsettling, to say the least. Just consider the first two sentences of the report's introduction: "During the past year, the COVID-19 pandemic has reminded the world of its fragility and demonstrated the inherent risks of high levels of interdependence. In coming years and decades, the world will face more intense and cascading global challenges ranging from disease to climate change to the disruptions from new technologies and financial crises."

For those without the time to read the report's 156 pages, *The Washington Post* offers a first-rate summarization that includes these two eye-opening paragraphs:

> Looking over the time horizon, [the report] finds a world unsettled by the coronavirus pandemic, the ravages of climate change — which will propel mass migration — and a widening gap between what people demand from their leaders and what they can actually deliver.
>
> The intelligence community has long warned policymakers and the public that pandemic disease could profoundly reshape global politics and US national security. The authors of the report, which does not represent official US policy, describe the pandemic as a preview of crises to come. It has been a globally destabilizing event — the council called it "the most significant, singular global disruption since World War II" — that "has reminded the world of its fragility" and "shaken long-held assumptions" about how well governments and institutions could respond to a catastrophe.

Avid *Bulletin* readers may notice (as I did) a certain analytical similarity between the "Global Trends" report and the most recent Doomsday Clock statement, authored by the our Science and Security Board. Both documents note, for instance, that the COVID-19 pandemic revealed a worrisome inability of governments around the world to respond to a wide variety of major threats, including climate change. "The pandemic revealed just how unprepared and unwilling countries and the international system are to handle global emergencies properly," the Clock statement asserts. "In this time of genuine crisis, governments too often abdicated responsibility, ignored scientific advice, did not cooperate or communicate effectively, and consequently failed to protect the health and welfare of their citizens."

"Global Trends" includes five scenarios that describe what the world might look like in 20 years (with the appropriate caveat that the future cannot actually be predicted, even by intelligence professionals). Three scenarios are unhappy in different ways, ranging from the general grimness of "A World Adrift" to a more modulated semi-dystopia, "Separate Silos," in which wealthy countries do reasonably well, some developing countries become failed states, and "[g]lobal problems, notably climate change, are spottily addressed, if at all."

In two other scenarios, the world eventually comes to deal in some way with some of the largest global threats.

The description of one of those scenarios, "Tragedy and Mobilization," begins this way:

In the early 2030s, the world was in the midst of a global catastrophe. Rising ocean temperatures and acidity devastated major fisheries already stressed by years of overfishing. At the same time, changes in precipitation patterns depressed harvests in key grain producing areas around the world, driving up food prices, triggering widespread hoarding, and disrupting the distribution of food supplies, leading to global famine. A wave of unrest spread across the globe, protesting governments' inability to meet basic human needs and bringing down leaders and regimes. In one of many incidents in the Western world, thousands of people were killed in three days of violence in Philadelphia triggered by social media rumors about bread shortages.

The ongoing famines catalyzed a global movement that advocated bold systemic change to address environmental problems.
In the other scenario, titled "Renaissance of Democracies," in 2040 "the world is in the midst of a resurgence of open democracies led by the United States and its allies. Rapid technological advancements fostered by public-private partnerships in the United States and other democratic societies are transforming the global economy, raising incomes, and improving the quality of life for millions around the globe."
The American exceptionalism of the Renaissance scenario aside, the overall "Global Trends" message echoes with rather remarkable fidelity what the Science and Security Board wrote in January: "Given the pandemic experience, no one can reasonably say he or she was not warned…. It is time for all to take the actions needed to—quite literally—save the world."

John Mecklin *is the editor-in-chief of the* Bulletin of the Atomic Scientists. *Previously, he was editor-in-chief of* Miller-McCune *(subsequently renamed* Pacific Standard*), an award-winning national magazine that focused on research-based solutions to major policy problems. Mecklin holds a master in public administration degree from Harvard's Kennedy School of Government.*

The Stupidity Files

"Wipe the Soviet Union Off the Map", 204 Atomic Bombs against 66 Major Cities, US Nuclear Attack against USSR Planned During World War II

By **Prof Michel Chossudovsky**
Source: https://www.globalresearch.ca/wipe-the-ussr-off-the-map-204-atomic-bombs-against-major-cities-us-nuclear-attack-against-soviet-union-planned-prior-to-end-of-world-war-ii/5616601

Apr 12 – According to a secret document dated September 15, 1945, "the Pentagon had envisaged blowing up the Soviet Union with a coordinated nuclear attack directed against 66 major urban areas.

Michel Chossudovsky *is an award-winning author, Professor of Economics (emeritus) at the University of Ottawa, Founder and Director of the Centre for Research on Globalization (CRG), Montreal, Editor of Global Research.*

Norway Raises Alarm Over Exploitation Of Dual-use Technology By Pakistan

Source: https://www.republicworld.com/world-news/rest-of-the-world-news/norway-raises-alarm-over-exploitation-of-dual-use-technology-by-pakistan.html

Apr 12 – Norway on April 12 raised alarm over unhindered exploitation of dual-use technology by Pakistan in a bid to aid its nuclear programme. While citing a threat assessment report by the Norwegian security agencies, ANI reported that **Pakistan's practice of bypassing all international safeguards in gaining the latest nuclear technology on the pretext of using it for education and health is posing the greatest threat to Norway**. In an article in moderndiplomacy, Fabien Baussart said that Norway became the latest country to raise alarm over unhindered exploitation of dual-use technology by Pakistan.
Norway's assessment comes after several other countries publicly acknowledged the nuclear threat posed by Pakistan. The agency informed that back in 2020 the German authorities had also disclosed that Pakistan had sought technology for weapons of mass destruction (WMD) in order to retain a "serious deterrent potential against 'arch enemy' India". The report provided a detailed account of Pakistan's efforts to steal information and material about nuclear weapons.
Further, the Czech Republic in its report titled "Annual Report of the Security Information Sevice for 2019" also drew global attention towards Pakistan misleading the world in procuring internationally controlled items and technologies to aid its nuclear programme. The report even noted that in 2019, the US Department of Justice indicted five persons associated with a Pakistan based front company for operating a network that exported US-origin goods to Pakistan. Baussart said that the network used to conceal the true destinations of goods in Pakistan by showing front companies as the supposed purchasers and end-users.

Goods exported to Pak without licences: US
The Norwegian agency said that the US Justice Department statement had disclosed that the goods were ultimately exported to Pakistan's Advanced Engineering Research Organisation (AERO) and the Pakistan Atomic Energy Commission (PAEC) without export licences. It said that both AERO and PAEC are on the US Commerce Department's Entity

List, which imposes export licenses requirements for organisations whose activities are found to be contrary to US national security or foreign policy interests.
Moreover, in the article Baussart wrote that to fulfil its destructive agenda, Pakistan even used the name of its poor public and students. Baussart said that the Pakistan government has repeatedly claimed that it seeks dual-use technologies for the social and economic upliftment of the country by utilising the technology in its health and education sectors. While concluding the article, Baussart wrote that it now remains to be seen whether these disclosures lead to sanctions or new export controls against Pakistan or the country again succeeds in misleading the world by playing victim's card.

EDITOR'S COMMENT: This is only the tip of the iceberg. The biggest part under the sea is that Pakistan is using the same approach to provide nuclear assistance to other "sister" nations like Turkey.

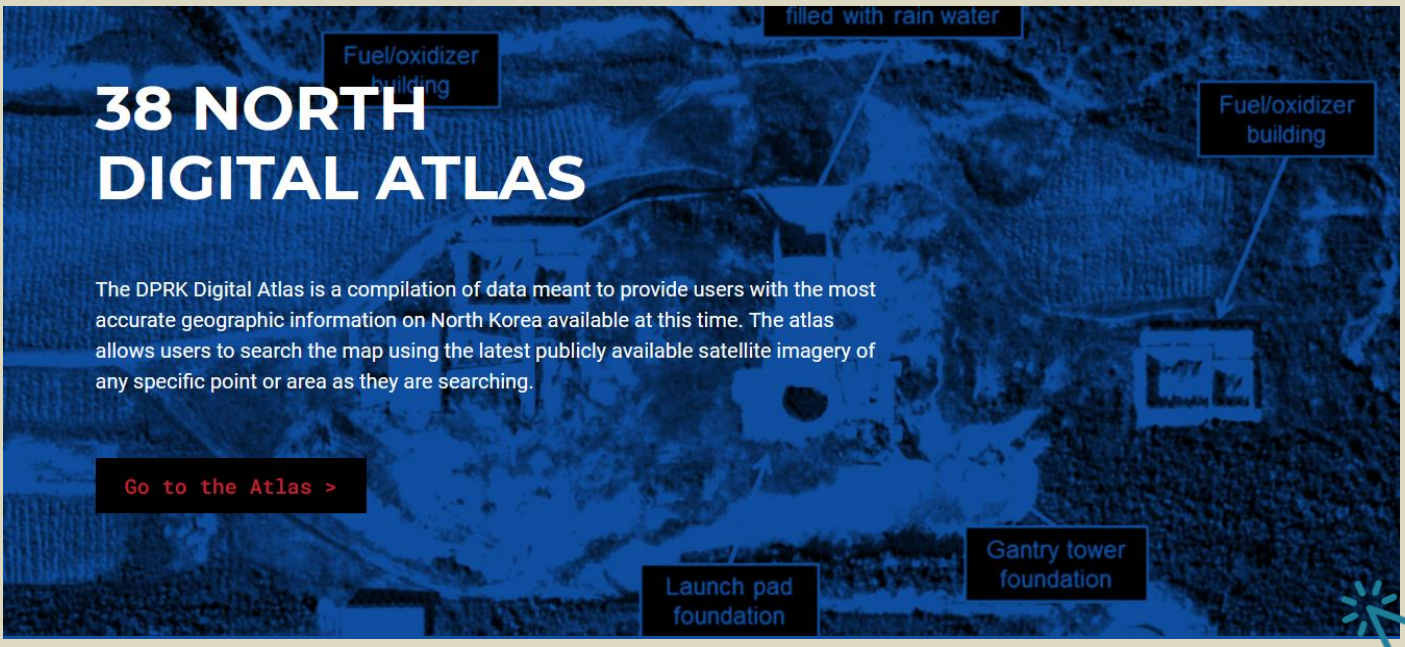
WW3 panic: Nuclear war fears as countries reaching 'crisis' point could lead to WMD attack

Source: https://www.express.co.uk/news/world/1422129/ww3-world-war-3-news-fear-raised-countries-crisis-point-iran-wmd-nuclear-war-weapons-spt

Apr 12 – When you subscribe we will use the information you provide to send you these newsletters. Sometimes they'll include recommendations for other related newsletters or services we offer. Our Privacy Notice explains more about how we use your data, and your rights. You can unsubscribe at any time.
Fears of nuclear warfare were believed to have peaked during the Cold War. A lengthy spell of eyeballing between the US and the Soviet Union led to nothing. On more than one occasion, however, the alarm was sounded, each time wrongly due to miscommunication, a misjudgement or even faulty technology.

As the world settles into the 21st century an increasing number of countries have gained possession of their own nuclear weapons with the number growing each year.
No longer are just two nations the sole carriers of such weapons of mass destruction.
Now, nations like Iran, Israel, Pakistan, India and North Korea all own a considerable array of nuclear weapons, many having in recent years threatened to use them.
Patricia Lewis, nuclear physicist and former director of the UN Institute for Disarmament Research, admitted that no closer have we been to nuclear war than in today's geopolitical climate.
She told the BBC's 'Start the Week' how the tensions in the present-day are far different and more complex than those experienced during the Cold War.
Asked how scared we should be about nuclear war, Dr Lewis said: "Since the end of the Cold War, the big stand off between Russia and the US has somewhat diminished but the relationship now is very bad.
"We have more nuclear weapons possessors, we have India and Pakistan declared as possessors, Israel's never declared, we now have North Korea also.
"We saw recently in 2018 a scare with a false message that went out, and I think it demonstrated the nervousness and likelihood of a country like North Korea taking that decision.
"Our big worry I think is when we're in a situation of crisis, where you are likely to get a lot of information, a lot of it contradictory, a lot of misinterpretation of information, that occurs in every crisis, and then also misperceptions and miscalculations."
In 2018, a state worker in Hawaii sent a false missile alert after being "100 percent sure" that the attack was real.
It took the agency he worked for nearly 40 minutes to retract the false alert on the same platforms it was sent to.
The threat sent to the agency's headquarters later turned out to be a practice drill.

State workers said that they clearly heard the word "exercise" repeated several times.
Islanders were sent into panic, many believing they had minutes left to contact loved ones.
The man, in his 50s, said he was "devastated" by what had happened.
These sorts of situations, Dr Lewis said, could become more prevalent as relations become more complicated and bound in political rhetoric.
Dr Lewis continued: "This is our biggest fear as we go into a more turbulent period of history where we're seeing a rise in the quite difficult politics between countries again.
"The less emphasis on arms control, the less emphasis on international institutions like the UN and a rising geopolitical strains and stresses throughout the world, those countries who have nuclear weapons are going to be more and more in situations where they might worry that some situation might occur that they might have to use them.
"And then we go back into a very different nuclear situation to the Cold War.
"I don't think we've fully understood yet what that will mean and I think we really need to think it through."
This week, a nuclear facility in Iran was hit by "sabotage" a day after it unveiled new uranium enrichment equipment, according to top officials in the country.
While Iran has not yet laid blame on a country or force, Israeli public media cited intelligence sources who said it was the result of an Israeli cyber-attack.
Israel has not commented on the incident directly.
It is just one incidence of belligerent forces both fighting to maintain a superior nuclear status in the Middle East.
Further East, in North Korea, new satellite images last week raised fears that the country was continuing to escalate its nuclear activity at its main testing site.
The movements were discovered at Yongbyon Nuclear Science and Weapons Research Centre, around 100km from the country's capital, Pyongyang.
In the images, posted to the North Korea analysis site 38 North, a coal-fired steam plant can be seen in operation, the location where it is believed an estimated four dozen nuclear weapons are housed.



The Natanz Blackout: Can the Iran Deal Talks Still Succeed?

By Ray Takeyh
Source: http://www.homelandsecuritynewswire.com/dr20210414-the-natanz-blackout-can-the-iran-deal-talks-still-succeed

Apr 14 – Washington and Tehran seem determined to revive the deal that freezes Iran's nuclear program, despite domestic criticism on both sides and the apparent sabotage of an Iranian facility.
Did the April 11 explosion at the Natanz facility, which Iran blames on Israel, significantly set back Iran's nuclear program?

It is always difficult to assess how effective such attacks are. The recent explosion will likely set Iran's nuclear program back, but it is impossible for outside observers to say by how much. The one thing that seems clear is that Iranian nuclear infrastructure is susceptible to infiltration. Natanz is Iran's main nuclear facility, and a new generation of centrifuges is being developed and installed there. It has been the target of multiple attacks, both cyberstrikes and direct physical assaults. And yet, the Iranian government seems incapable of protecting a nuclear asset that it knows is being targeted by its adversaries. This is a serious intelligence failure on its part.

Will this incident derail or delay the Vienna talks on returning to the nuclear deal?

It is unlikely that the recent attack will derail the Vienna talks. The United States and Iran both wish to get back to the agreement in a way that serves their own interests. This attack will generate its share of Iranian condemnation, but it will not prove an obstacle to diplomacy. The Iranian nuclear network was attacked before, and the two sides still managed to forge the 2015 Joint Comprehensive Plan of Action (JCPOA).

If Iran seeks to move its nuclear program deeper underground, the issue of inspections could be even more crucial. Could inspections prevail after such a move?

Iran has already scaled back the inspection regime. The agency responsible for inspections, the International Atomic Energy Agency, has been in contact with Iran over its lack of cooperation. The program moving deeper underground should not further impede inspection if Iran reveals the location of its facilities, opens them up to regular inspection, and answers unresolved questions. The parties to the JCPOA can be expected to press for such transparency.

What are the main takeaways from the Vienna talks so far?

Iran insists that since the United States is no longer a member of the nuclear deal, Washington should come back into compliance before it can be a regular participant in the talks. The United States argues that Iran should come back into compliance itself before the United States rejoins the deal. Thus, the so-called proximity talks are designed to provide a step-by-step plan for both sides to gradually come back into compliance. Two working groups were established, one to identify sanctions that the United States should lift because they were imposed after the U.S. withdrawal in 2018, and another to discern the adjustments Iran should make to its nuclear program to return to compliance.

Can the countries reach a deal before the Iranian presidential elections in June? If not, how could those elections affect diplomacy?

It is not clear whether an agreement will be reached before the Iranian presidential election, but doing so is not crucial. The question of whether Iran will adhere to the agreement should the United States return to compliance is not a factional issue. Compliance is the position of Supreme Leader Ali Khamenei and the official position of the state. Nor is it clear who will be the next Iranian president, since the results of these elections are impossible to predict in advance.

What are the consequences for regional security if the deal is never revived?

Many U.S. allies in the Middle East, including Saudi Arabia and Israel, are wary of the United States returning to an agreement that they believe provides Iran with economic benefits without sufficiently obstructing its path to a nuclear weapon. Thus, the regional tensions and the pattern of attacks and reprisals are likely to persist no matter the prospects of the agreement.

***Ray Takeyh** is Hasib J. Sabbagh Senior Fellow for Middle East Studies at CFR.*

The Most Urgent North Korean Nuclear Threat Isn't What You Think

By Toby Dalton

Source: https://carnegieendowment.org/2021/04/15/most-urgent-north-korean-nuclear-threat-isn-t-what-you-think-pub-84335

Apr 15 – North Korea's resumed nuclear missile testing generates understandable hand-wringing in Seoul, Tokyo, and Washington. Such tests demonstrate Pyongyang's growing prowess with nuclear weaponry and are a frightening reminder that a crisis on the Korean Peninsula could erupt at any time.

Yet, as troubling as missile tests are, the chances of a war on the Korean Peninsula remain very low. Policymakers should be more concerned about the likelier possibility of North Korea selling nuclear and missile technology to countries in the Middle East.

A Nuclear Power With a Cashflow Problem

For three decades, neither diplomacy nor increasingly stringent economic sanctions have reversed North Korea's ambition to possess nuclear weapons. Nor have they diminished North Korea's illicit trade relationships with Iran, Syria, and other states in the Middle East.

Even during the heady days in 2018 and 2019 of North Korean leader Kim Jong Un and former president Donald Trump's love letter diplomacy, North Korea's arsenal of nuclear weapons and missiles continued to grow. Over the same period, the UN Panel of Experts, which assesses compliance with economic and trade sanctions on North Korea, reported numerous times when North Korean entities sold technology for missiles or weapons of mass destruction (WMD) to buyers in the Middle East.

The threats from North Korea's WMD programs have continued to grow despite Washington's sustained pressure campaign to choke the North Korean economy. Since 2009, the United States has led the UN Security Council to pass eight main resolutions imposing wide-ranging sanctions. These resolutions prohibit, among other items, North Korean exports of coal and seafood and remittances from North Korean overseas workers, while also embargoing North Korean imports of refined petroleum, technology and equipment for its nuclear and missile programs, and a range of other goods. U.S. secondary sanctions also have limited North Korean access to the international financial system.

No doubt the sanctions have damaged North Korea's economy—and have exacerbated the already perilous living conditions of many North Korean citizens—but they have not come close to forcing Kim to decide to disarm or to curb his WMD trade.

Then the coronavirus pandemic made things far worse for North Korea's economy. Kim's decision to seal the country's borders has resulted in economic pain Washington could never have achieved through sanctions. Recent reports suggest growing alarm among North Korea's leadership over failed economic programs, with attendant electrical outages, factory closures, and shortages of some food staples. Foreign diplomats have left North Korea over the difficult living conditions and shortages of medicine and basic goods in Pyongyang. It is little surprise that North Korea is increasingly reliant on cyber attacks and cryptocurrency theft to generate revenue.

North Korea's WMD Bazaar

North Korea's desperation could make a sustained U.S. pressure strategy still riskier. Kim's regime remains remarkably resilient, so collapse seems unlikely—even though U.S. officials would be wise to prepare for that unique scenario. The most likely outgrowth of North Korea's need for cash is an increase in other dangerous behavior. WMD technology represents one of North Korea's few value-added assets.

North Korea's proliferation rap sheet is long: missile and nuclear trade with Pakistan; missile sales to Egypt, Libya, Yemen, and others; chemical weapons assistance to Syria; and more. Notably, North Korea clandestinely sought to construct a nuclear reactor in Syria, a facility that might have provided plutonium for a Syrian bomb program until Israel destroyed the partly built reactor with air strikes in 2007. The March 2021 report by the UN Panel of Experts reported ongoing assistance by North Korea with Iran's ballistic missile and space launch programs. Iranian scientists reportedly went to North Korea to discuss rocket booster technology, while thirteen North Korean experts are believed to have visited Iran to assist with liquid-fueled ballistic missiles. According to the report, the cooperation between North Korean and Iranian entities also extends to illicit shipments of valves, electronics, and other missile-related equipment.

Until now, apart from the reactor project in Syria, North Korea is not known to have transferred more sensitive nuclear technologies—longer-range missiles, nuclear weapon designs, equipment or technology to produce highly enriched uranium or plutonium for a bomb, or those materials themselves. Presumably, North Korean leaders historically have believed that such transfers could cross an implicit red line and result in harsher consequences when discovered. Now, increasingly desperate for cash, Kim could be more willing to risk sales of these items to interested customers in the Middle East, including possibly terrorist groups.

If such sales come to light, it is reasonable to expect that Israel would again take preemptive action. Israel regularly carries out air strikes against missile construction facilities and other weapons-related sites in Syria. It is also suspected of assassinating the most prominent Iranian nuclear scientist, Mohsen Fakhrizadeh, in November 2020 and of causing an explosion that damaged the power supply to Iran's Natanz uranium enrichment facility in April 2021.

Prioritize Ending North Korean Nuclear Sales

Relying on Israeli counterproliferation strikes to prevent WMD acquisition by adversaries in the Middle East is a fraught strategy. At some point, that approach could fail in any number of ways, with catastrophic consequences. It is bad enough that Washington faces a complex nuclear challenge from North Korea in East Asia. But North Korean proliferation that yields a new nuclear-armed state or catalyzes a wider conflict in the Middle East could be worse.

Sustaining economic pressure against North Korea without creating an offramp through negotiations is increasingly dangerous. It is too late to stop North Korea's nuclear acquisitions, and pressure will not force Kim to disarm. Yet diplomacy with North Korea could still prevent another nuclear-armed state in the Middle East.

This is the reality of the North Korean threat President Joe Biden and his administration confronts. It is time for a new U.S. policy that mitigates the dangers from North Korea's WMD programs. Avoiding worse outcomes will require offering sanctions relief and steps toward a peace regime in return for an end to North Korean WMD trade and constraints on its nuclear

arsenal. This is the deal Biden should seek before economic desperation brings North Korean nuclear weapons to a volatile Middle East.

***Toby Dalton** is the co-director and a senior fellow of the Nuclear Policy Program at the Carnegie Endowment. An expert on nonproliferation and nuclear energy, his work addresses regional security challenges and the evolution of the global nuclear order.*

EDITOR'S COMMENT: I can think of a country that might be interested to buy even if its financial status is not very promising – and perhaps North Korea might be cheaper than a rival Asian coutry looking west.

North Korea may have almost 250 nuclear weapons by 2027

By Thomas Maresca

Source: https://www.upi.com/Top_News/World-News/2021/04/13/nkorea-North-Korea-may-have-242-nuclear-weapons-by-2027/9961618301306/

Apr 13 – North Korea's nuclear arsenal will continue to grow over the next several years, reaching as many as 242 nuclear weapons and dozens of intercontinental ballistic missiles by 2027 and posing a threat that will be increasingly difficult for South Korea and the United States to contain, a report released Tuesday said.

The report, jointly produced by Seoul-based Asan Institute for Policy Studies and Santa Monica, Calif.-based Rand Corp., warned that negotiations alone are unlikely to be effective in reducing the threat and called for measures such as deploying tactical nuclear weapons in South Korea.

Titled "Countering the Risks of North Korean Nuclear Weapons," the report estimates that North Korea had developed between 67 and 116 nuclear weapons by 2020, with its stockpile to grow by 12 to 18 weapons per year until 2027.

Until now, the isolated country has relied on its nuclear arsenal for deterrence, but as North Korea advances its nuclear capabilities it may be able to use weapons for blackmail, coercion or even to conduct pre-emptive strikes against South Korea and the United States.

"Despite some ROK and U.S. efforts to enhance defense and deterrence, there is a growing gap between the North Korean nuclear weapon threat and ROK and U.S. capabilities to defeat it," the report said.

The Republic of Korea is the official name of South Korea.

"Today, even a few of the likely dozens of North Korean nuclear weapons could cause millions of fatalities and serious casualties if detonated on ROK or U.S. cities," it added.

North Korea has not conducted any nuclear or long-range missile tests since 2017, but it launched a pair of short-range ballistic missiles last month in violation of United Nations sanctions. Pyongyang also showed off a new ICBM at a military parade in October.

A report by a United Nations panel of experts earlier this month concluded that North Korea has continued to develop its nuclear and missile programs and has "increased its nuclear strike capability, as well as its ability to counter foreign missile defense systems while safeguarding itself with its own new air defense system."

Washington's nuclear negotiations with Pyongyang have stalled since a February 2019 summit between then-U.S. President Donald Trump and North Korean leader Kim Jong Un ended without an agreement.

The Asan/Rand report warned that future negotiations are unlikely to lead to denuclearization.

"Unfortunately, the major ROK and U.S. strategy to moderate the growing North Korean nuclear weapon threat has been negotiating with North Korea to achieve denuclearization, and this effort has failed and seems likely to continue failing," the report said.

Instead, the authors contend that the United States and South Korea "must consider putting all options on the table" in confronting the North Korean threat, focusing on deterrence and defense but signaling a willingness to destroy the North Korean regime if it uses nuclear weapons.

Steps would include deploying tactical nuclear weapons in South Korea, as well as increasing intelligence collection and enhancing missile defense systems.

"The ROK and the United States must now turn their attention to deterring North Korean nuclear weapon attacks and being able to defeat such attacks if deterrence fails," the report said.

The allies should be ready "to fight and win a war on the Korean Peninsula under conditions of North Korean nuclear weapon use, and both countries must be prepared to implement the current U.S. policy of destroying the Kim regime if it uses nuclear weapons," the report added.

Thomas Maresca, based in Seoul, is an writer and photographer covering Asia for UPI. He previously covered the region for USA Today and has written for outlets including TIME, The Atlantic, the Associated Press, Marketwatch and PRI. He was the recipient of a Jefferson Fellowship from the East-West Center in 2019.

Iran 2021: Opportunities and threats of Iran's return to 2015 nuclear deal

International Institute for Middle-East and Balkan Studies (IFIMES[1]), Ljubljana, Slovenia
Source: https://www.ifimes.org/en/researches/iran-2021-opportunities-and-threats-of-irans-return-to-2015-nuclear-deal/2822?

Apr 19 – There were some conflicting speculations regarding the position of US President **Joseph Biden**'s administration on Iran's nuclear program, as optimists believed the new President would return to the nuclear deal as soon as he entered the White House, while pessimists announced that the decision to return to that deal would be very difficult if not impossible under the conditions agreed with President **Barack Obama** in October 2015. Many things have changed during **Donald Trump**'s tenure as president, as have many attitudes towards the nuclear deal, which today requires that the details of the deal be reconsidered and amended to suit the new circumstances.
Within days of taking office on 20 January 2021, the new US President Biden managed to change the face of US foreign policy towards the Middle East, thanks to a number of facts: first, his experience in dealing with challenges in the region gained over a long period of membership in the Senate (1973-2009) and in Obama's administration where he was vice president from 2009 to 2017; second, his use of executive presidential powers as a means of taking swift action and avoiding confrontation with Republicans in the Congress; third, a clear vision, which sees the US global role from two perspectives, including the moral principles and interests, instead of only thinking of the interests; fourth, his selection of an experienced team based on the criteria of expertise, skills and knowledge of the region; and fifth, the President and his team rely on multi-track diplomacy to implement this vision, which simultaneously stimulates and exerts pressure based on the carrot and stick principle.

The nuclear deal should be dealt separately from other issues

The Iranian issue is an important axis of the new US administration's foreign policy. Biden's vision of policy towards Iran can be divided into three segments, the most important of which is Iran's nuclear programme, to save the nuclear deal with Iran and try to fix what Trump's policy destroyed in that regard. The second segment concerns an attempt to suppress Iran's expansion in the Middle East, primarily in Iraq, Syria, Lebanon and Yemen, where pro-Iranian allies are in power. The third segment of American policy is putting Iran's missile programme under international supervision.
This vision seeks to separate Iran's nuclear programme from regional security issues in the first phase, which Saudi Arabia insists on. From Biden's point of view, Iran's nuclear programme (JSPOA)[2] is an international issue essentially related to the non-proliferation of nuclear weapons, and the group (5 + 1) [3] in charge of this issue, and they differ in term of regional security issues, despite some connections between them, especially regarding the establishment of collective regional security framework, with the participation of all parties whereby talks would be held at a later stage.
Analysts believe that if Biden manages to separate the nuclear issue from regional security challenges, it will provide chances for a quick solution to the problems of the nuclear deal and unresolved regional issues. The United States and Iran have expressed readiness to negotiate on the nuclear programme, but there are major differences in terms and how to achieve that.
Iran demands that all US sanctions be lifted first before it agrees to meet the restrictions on uranium enrichment from the 2015 deal, while the US sees this scenario the other way around, which means that Iran should first meet its obligations before the sanctions would be gradually abolished. There is another scenario announced by Iranian Foreign Minister **Mohammad Javad Zarif**, namely that the two sides enter negotiations at the same time. However, the US President categorically stated in the CBS TV programme *"Face the Nation"* **[4]** that he would not lift the sanctions just to *"bring Iran back to the negotiating table"*. In response to a subsequent question, he explained that Iran must first *"stop enriching uranium"* more than what is envisaged by the nuclear deal, which is 3.67%. On 31 January 2021 Tehran announced that it had produced 17 kilograms of 20% enriched uranium, thus bringing it a step closer to enriching uranium to 90%, which could be used in nuclear weapon production.
Director General of the International Atomic Energy Agency (IAEA) **Raphael Mariano Grossi** warned: *"Obviously we don't have many months. We have weeks to renew a Joint Comprehensive Plan of Action,"* which indicates that Iran's uranium enrichment will soon reach the point of no return.

The US concerns about Iran's presidential elections

The US administration is anxiously awaiting changes resulting from Iran's presidential elections in June 2021 and any possibility that the future president would come from the

ranks of conservatives, who have controlled Iranian parliament since 2020 parliamentary elections. This possibility is quite realistic. The reformists do not have any notable candidate, unlike the conservatives who already have three political "hawks": former President of Iran (2005-2013) **Mahmuomd Ahmadinejad**, former Tehran Mayor and current Parliament Speaker **Mohammad Qalibaf**, who was **Hassan Rouhani**'s strongest opponent at 2013 elections, and Head of Judiciary **Ebrahim Raisi**, who ran in 2017 presidential elections but lost to Hassan Rouhani.
Recent aggravation of relations resulted from the violation of the agreement on international control over Iran's nuclear programme, which led to an increase in uranium enrichment based on decisions by the conservative-controlled Iranian parliament.

A new US path towards Iran
The Persian Gulf region and Iran have been the source of tensions and wars for the past 40 years, but it seems that with President Biden we are entering a phase of anticipating a new American policy. Biden and his team appear to be more in favour of a truce and reduction in tensions than former Trump's administration.
The new path that the United States will follow towards Iran requires an open dialogue, especially after years of tensions that have lasted since the founding of the Islamic Republic of Iran in 1979. Some opinions suggesting that the ceasefire will strengthen Iranian expansion and extremism are incorrect. Iran today is not what it was in 1980. It is no longer a revolutionary Iran, but is now a pragmatic country, seeking to regulate its global role as a regional power and successor to the ancient Persian civilization.
Internal attempts to overthrow Iranian political system have failed. The US must find a model of cooperation with the present Iranian regime. Dialogue can open many doors, as did the seven-day visit by US President **Richard Nixon** on 21 February 1972, which opened the door to changes in China despite its communist ideology. China has supported all anti-American and communist movements around the world, including the Vietnam War against the US. American openness to China has changed many Chinese trends, and even led to the emergence of the school of capitalist economic reform in late 1970s, without changing the essence of the communist system.
The new US policy is less burdened with the protection of Gulf oil sources and it is oriented towards China. Therefore, the United States will not accept that certain Gulf states, especially Saudi Arabia, have the right to set ultimatums and restrictions on the US return to the nuclear deal and dialogue with Iran, but will ask its Arab allies to make compromises with Iran on common Gulf security concerns.
Some countries in the region had time to resolve their problems with Iran, but were more focused on the blockade option and the use of force, encouraging Trump administration to attack Iran. Nevertheless, this did not happen during the presidency of Donald Trump, who exploited tensions to increase arms sales deals, and it will not happen during Biden's administration either. It should be noted that the three countries of the Gulf Cooperation Council (GCC), Kuwait, Qatar and Oman, lead a rational policy towards Iran.
Today, Iran's economy is no longer on the verge of collapse. It is now in a deep abyss, which had a dramatic effect on the country's internal political situation that has been the scene of large demonstrations in many Iranian cities over the past two years.
The official unemployment rate in Iran is 9.4%, which is 2.4 million economically active people. However, it is estimated that the real unemployment rate is at least twice as high, especially among the young. Annual GDP reduced in 2019/2020 by about 7%. An additional 5% drop in Iranian economy is expected in 2021 if sanctions are not lifted. Annual inflation also jumped to more than 46% in November 2020.

Return to the nuclear deal – Iran's exit from the crisis
Iranian leadership is well aware that the only way out of the crisis is to return to the nuclear deal which will be followed by economic progress.
The messages coming from the United States and Iran can be interpreted as mutual willingness to start negotiations to return to the nuclear deal. An optimistic atmosphere was established by the appointment of **Wendy R. Sherman** as US Deputy Secretary of State and **Robert Malley** as US Special Envoy for Iran, two key figures who actively participated in negotiations with Iran during former President Obama's term in 2009-2017.
Iranian leadership has to show a high level of patience regarding the lifting of sanctions, since this will realistically not happen overnight.

There are three types of sanctions imposed on Iran, and not all are related to the nuclear deal. For example, sanctions imposed on the Central Bank and the Revolutionary Guard are related to money laundering and aiding terrorism, and some sanctions are imposed due to human rights violations. Even if the sanctions imposed by former US President Trump are lifted, there will be still other sanctions that the two sides must discuss separately from the nuclear issue in order to be phased out.
Presidential elections will be held in June 2021. Will Iran's supreme Islamic leader **Ali Khamnei** allow the negotiation process to be successfully completed during the term of

current reformist President Hassan Rouhani, thereby increasing the power of reformists, or will he wait until a new president is elected, most likely coming from the conservatives?

Footnotes:
[1] IFIMES – International Institute for Middle East and Balkan Studies, based in Ljubljana, Slovenia, has Special Consultative status at ECOSOC/UN, New York, since 2018.
[2] Source: https://www.europarl.europa.eu/cmsdata/122460/full-text-of-the-iran-nuclear-deal.pdf
[3] P5+1 (the UN Security Council's five permanent members China, France, Russia, the United Kingdom, and the United States; plus Germany). All together with the EU.
[4] Source: interview with Joseph Biden, CBS, Face the Nation, 7 February 2021. www.youtube.com/watch?v=3YFFYIHAcoA

Russia's Arctic Buildup

Source: https://geopoliticalfutures.com/russias-arctic-buildup/

Apr 16 – The Arctic, rich in natural resources and potential, is quickly becoming an area where the interests of major players, especially the United States and Russia, may collide. Russia, which controls significant territory in the region, has for years been increasing and strengthening its defensive positions, developing the northern territories, and modernizing infrastructure, including oil

and gas production. It has also developed and tested shipping along the Northern Sea Route, which Moscow puts forward as an alternative trade route between Europe and Asia. Regarding its military presence, Russian Defense Minister Sergei Shoigu says it is necessary because competition for access to the Arctic's resources and for transit routes among the world's great powers will only grow.

The U.S. State Department has repeatedly voiced concerns about Russian radar stations near Alaska and Russian air bases in the Far North, which the U.S. says could have offensive as well as defensive purposes. Moscow is building unprecedented military power in the Arctic and testing new weapons there, Washington says. Recently, Russia began testing its Belgorod nuclear submarine, which can carry an autonomous, nuclear-powered, nuclear-armed torpedo called the Poseidon. The Kremlin is also making plans to place a radar station on the Novaya Zemlya archipelago capable of detecting hypersonic targets. All this modernization will take time, however, not to mention scarce federal resources.

American Honey Still Contains Radioactive Fallout From Nuclear Tests Decades Ago

Source: https://www.sciencealert.com/american-honey-still-contains-radioactive-fallout-from-nuclear-tests-decades-ago

Apr 21 – Traces of radioactive fallout from nuclear tests in the **1950s and 1960s** can still be found in American honey, new research reveals.

The radioactive isotope identified, **cesium-137**, falls below levels considered to be harmful – but the amounts measured nonetheless emphasize the lingering persistence of environmental contaminants in the nuclear age, even a half-century after international bomb tests ended.

"There was a period in which we tested hundreds of nuclear weapons in the atmosphere," lead researcher Jim Kaste, an environmental geochemist at William & Mary university in Williamsburg, Virginia, explained last year in comments about the research.

"What that did was put a blanket of these isotopes into the environment during a very narrow time window."

One of those isotopes was cesium-137, a byproduct of nuclear fission involving the reaction of uranium and plutonium, which can often be found in trace amounts in food sources due to such nuclear contamination of the environment.

Some of these traces are much fainter than others, Kaste found out – but only by chance, as it happened, after assigning his students a Spring Break assignment in 2017.

To demonstrate to his class how radioactive contaminants from mid-20th century nuclear testing still persisted in the environment today, Kaste asked his students to bring back locally sourced foods from wherever they spent the holidays.

As expected, various samples of fruits, nuts, and other foods revealed very faint traces of cesium-137 when measured with a gamma detector, but even Kaste wasn't prepared for what happened when he ran the same test with a jar of honey from a **North Carolina farmer's market**.

"I measured it again because I thought something happened to the container or my detector was bonkers," Kaste says.

"I reproduced the measurement. And it was, again, **100 times hotter** than any of these other foods."

To find out why honey registered such high levels of cesium-137, Kaste and his team (including one of his students, Paul Volante) began testing samples of locally made raw, pure, and unfiltered honey from markets and beekeepers located across the eastern US.

Of the 122 honey samples tested, 68 showed detectable traces of the radioactive isotope – a legacy of atmospheric nuclear tests conducted by the US, the USSR, and other nations during the Cold War era.

The majority of detonations occurred above the Marshall Islands in the Pacific Ocean and Novaya Zemlya, an Arctic archipelago in northern Russia, with other tests being conducted in New Mexico and Nevada.

According to the researchers, the cumulative effect of over 500 of these test detonations released more ionizing radiation to the atmosphere than any other event in human history – not that all the blasts were equal in scope.

"We know that the cesium-137 production from the Pacific and Russian sites was more than 400 times the production of the New Mexico and Nevada explosions," Kaste says.

"A single Russian bomb, the Tsar Bomb, was more than 50 times more powerful than all the Nevada and New Mexico tests combined."

While there's no way of knowing which of these explosions produced the fallout that can still be found in American foods today, we can at least explain how the isotope could disperse so far and wide.

"Many of the air detonations were so powerful that dozens of radioactive fission products were injected into the stratosphere and distributed globally with a residence time of [approximately] one year before deposition primarily by rainfall," Kaste and fellow researchers explain in a new study.

"The presence of radioactive pollution from nuclear testing is globally ubiquitous, and detectable on every continent and even in deep ocean trenches."

Not just rainfall

While the pollution may be globally ubiquitous, honey's high levels of cesium-137 compared to other food sources show that the fallout appears to concentrate in unexpected ways – but we can now explain that mystery too.

Rainfall might be the predominant force taking cesium-137 out of the atmosphere and depositing in on Earth's surface, but the honey samples registering the highest amounts of the radioactive isotope weren't produced in regions of the US that receive the most precipitation.

Rather, the honeys with the highest levels turned out to come from places in the US where the soil has low levels of potassium, which plants absorb as a nutrient source to fuel a range of metabolic processes.

Potassium and cesium share a number of atomic similarities, and when plants in potassium-poor soil can't get ahold of sufficient levels of their preferred nutrient, they'll absorb cesium instead – even if it's of the unstable, radioactive variety.

As a result, the isotope finds its way into plant nectar, which then gets passed to bees, who in turn magnify the concentration of cesium-137 when they make honey. Which then makes its way into your home.

The phenomenon has been previously observed in the wake of events such as the Chernobyl disaster, but such is the enduring half-life of radioactive particles, it can still be observed even several decades later, and in places located thousands of kilometers away from the site of the original nuclear tests in question.

If there's a silver lining to this unsettling discovery, it's that none of the cesium-137 levels detected in honey today are considered to be harmful to humans, falling below the 50-100 becquerels per kilogram threshold of radioactivity.

However, decades ago, the same toxic fallout would have been fresher, and potentially more hazardous to human health, not to mention other organisms too.

"What we see today is a small fraction of the radiation that was present during the 1960s and 1970s," Kaste says.

"And we can't say for sure if cesium-137 has anything to do with bee colony collapse or the decline of population."

In recent years, the ongoing disappearance of bees and other insect pollinators has sparked much concern in scientific circles, and while Cold War nuclear tests aren't often considered a primary driver of the problem, we can't afford to ignore that they too could be a contributor.

"Given that pollinating insects provide vital services to the world's ecosystem and are essential in maintaining global food security, more research is needed to help us better understand how ionizing pollution threatens their health and survival," the researchers write.

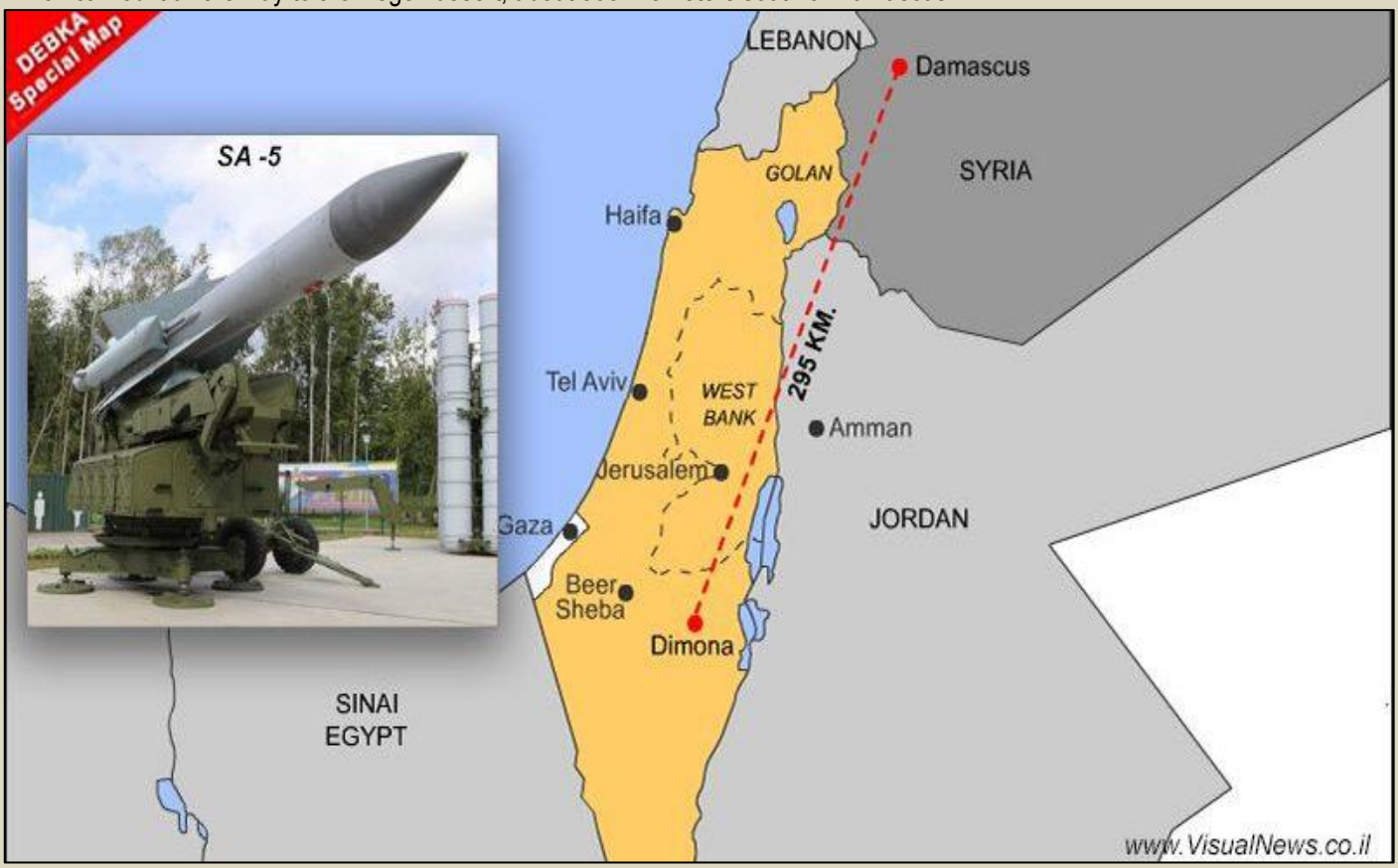
▶▶ **The findings are reported in** *Nature Communications*.

Syrian Missile Explodes Near Israel's Dimona Nuclear Reactor

Source: http://www.homelandsecuritynewswire.com/dr20210422-syrian-missile-explodes-near-israel-s-dimona-nuclear-reactor

Apr 22 – A Syrian missile exploded near Israel's Dimona nuclear reactor last night. The Israeli military was quick to state that the Syrian missile entered Israeli air space not as an intentional strike.

Rather, the Russia-made SA-5 surface-to-air missile was launched by a Syrian air defense unit, aiming at an IDF aircraft attacking Syrian military targets near Damascus. It appears that the Syrian missile had missed its target, and continued its flight trajectory which carried it all the way to the Negev desert, about 300 kilometers south of Damascus.



Israel has a robust anti-missile defense system, but the IDF has not said whether the Syrian missile was intercepted or not. Observers note that the explosions which were heard as far away as Jerusalem and Modiin, in the center of Israel, may have been the sound of anti-missile missiles trying to intercept the Syrian missile.

The IDF launched an immediate retaliatory strike, destroying the Syrian anti-aircraft battery responsible for launching the SA-5. Other Syrian targets nearby were also destroyed.

The highly unusual penetration by a Syrian missile of Israel's airspace cause unease in Israel, coming as it does two weeks after an Israeli operation caused serious damage to Iran's underground uranium enrichment facility at Natanz. Iran vowed to take revenge, and it has the ability to do so from Syria, where its forces control large swaths of Syrian territory and operate largely autonomously of the Assad regime.

For a Syrian SA-5 to land forty miles from the Dimona reactor is unusual, but Syrian defense missiles have escaped Syrian air space in the past.

Two Syrian air defense missiles have landed in Israel in 2018, one in Jordan in 2017, and another in the northern part of Cyprus in 2019. In 2018, another Syrian anti-aircraft missile hit and destroyed a Russian surveillance plane off the Syrian coast. Russian military sources hinted at the time that the reason for the mishap was Israel's ability to "mask" the Russian plane, making it look as an Israeli plane to the Syrian defense units.

Last August, Israel successfully tested a new and improved interceptor, Arrow 2, developed in collaboration with the United States. The interceptor was developed to meet enhanced Iranian missile capabilities, demonstrated in the stealthy Iranian missile attack on Saudi oil fields on 14 September 2019.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

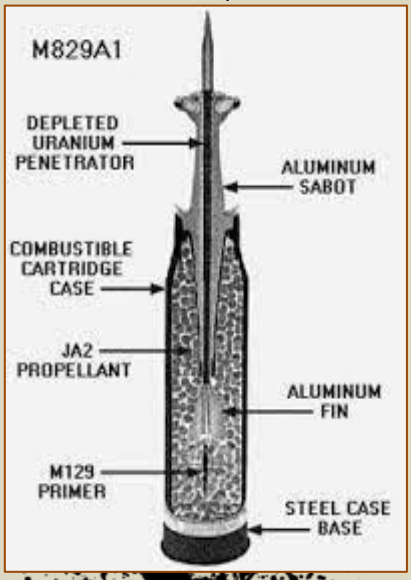
Depleted Uranium from Tanks, Ammo Not Tied to Gulf War Syndrome, New Study Finds

By Tara Copp

Source: https://www.military.com/daily-news/2021/02/19/depleted-uranium-tanks-ammo-not-tied-gulf-war-syndrome-new-study-finds.html

An M-1A1 Abrams main battle tank is positioned behind a sand berm during Operation Desert Storm on Feb. 12, 1991. (National Archives)

Feb 2021 — Depleted uranium in tanks and ammunition used in the 1991 Gulf War "played no role" in the unexplained illnesses, known as Gulf War syndrome, that veterans faced in the years afterward, according to a new study.



The findings by the University of Texas Southwestern Medical Center and the University of Portsmouth in England counter decades of understanding by the military and Department of Veterans Affairs about potential causes for a host of ailments that collectively are now known as Gulf War illness.

"That depleted uranium is not and never was in the bodies of those who were ill at sufficient quantities to cause disease will surprise many, including sufferers who have, over the last 30 years, suspected depleted uranium may have contributed to their illnesses," said Randall Parrish, a uranium isotope expert at the University of Portsmouth who developed the study's methodology to scan veterans' urine for traces of exposure.

The study looked at depleted uranium levels in the urine of 154 veterans, of whom 106 had Gulf War illness symptoms and 48 did not.

The findings may provide a definitive answer on whether there is a connection between depleted uranium exposure and Gulf War illness because of the level of precision used to detect any isotopes in veterans' urine and the time involved in the study, Dr. Robert Haley, the director of epidemiology at UT Southwestern, a Dallas-based research hospital, told McClatchy in a phone interview.

The study took 20 years to shape, fund and review. Between 2008 and 2010, the researchers had each of the veterans come into the hospital for a week of controlled observation to rule out any other variables, Haley said. It will be published Thursday in the peer-reviewed journal Scientific Reports.

According to a 2000 Department of Defense report cited by the study, U.S. and coalition tanks, aircraft and artillery fired about 300 tons of depleted uranium munitions in southern Iraq during the 1991 ground invasion.

An estimated 500,000 U.S. service members deployed to the Middle East for Operation Desert Storm. About 25% of them have reported chronic symptoms including fatigue, headaches, joint pain, dizziness, respiratory disorders and memory problems, according to the Department of Veterans Affairs.

For years, Gulf War veteran and former Army officer Larry Chaney has suspected depleted uranium might have played a role in the tremors he suffers. Almost 30 years ago, on Feb. 27, 1991, Chaney was a 27-year-old lieutenant leading a platoon of M2A1 Bradley Fighting Vehicles when two of the vehicles were destroyed by friendly fire during one of the largest tank battles of the operation.

There was a "brilliant flash," Chaney said in a phone interview with McClatchy. "A couple small pieces of depleted uranium hit me in the scalp and the shockwave knocked the wind out of me."

Chaney became a participant in the study. He said he trusted the finding that depleted uranium was not a cause of what he said were milder symptoms of Gulf War illness. He said veterans he served with are more concerned that possible exposure to nerve agents in Iraq may have led to a number of cancers and thyroid issues.

The study also calculated the amount of depleted uranium that would be expected to be found in the bloodstream over time based on the level of exposure, such as whether a service member had been hit by shrapnel that would have likely embedded depleted uranium in their skin, or whether they suspected exposure through inhalation of air particles on the battlefield.

About half of the 48 participants who did not have Gulf War illness symptoms never deployed to the Middle East for Operation Desert Storm and did not experience depleted uranium exposure. But for both those with Gulf War illness and the control group without illnesses, the results were the same, the study did not find significant traces of depleted uranium, Haley said.

"We found none, regardless of whether they had the Gulf War syndrome, one of the accepted case definitions, regardless of what kind of symptoms they had, and regardless of what kind of exposures they had," he said.

The findings will be reviewed by the VA, Dr. Patricia Hastings, chief consultant for the agency's post deployment health services, said in a statement.

"The research that depleted uranium is an unlikely cause of chronic multi-symptom illness will be reviewed by the scientists at VA's Depleted Uranium Center in Baltimore, Maryland," Hastings said.

The VA provided some of the initial funding for the research, she said.
Depleted uranium is also suspected in illnesses faced by veterans who deployed to Iraq and Afghanistan after the 9/11 attacks.
Coleen Bowman's late husband, Army Sgt. Maj. Robert Bowman, was an Army Ranger who deployed to Iraq in 2004. His armored Stryker was hit by enemy fire at least 13 times during his 12 months overseas. Each time, depleted uranium in the Stryker's armor would absorb the attack. He died in 2013 of bile duct cancer at age 44.
In his medical records, a doctor treating Bowman at the Army Medical Center in El Paso, Texas, documented in 2011 that the rare cancer was tied to environmental factors, including "burning depleted uranium from reinforced armored vehicles."
"There are no other reasonable explanations for his condition," the doctor concluded.
Coleen Bowman, who has spent several years connecting with other military spouses on the issue of toxic exposure, said she welcomed the study and its findings.
She hopes that the researchers of the Gulf War illness will consider also studying exposure in the new generation of veterans.
"For me, I don't know that I'll ever be able to know what substance it was that caused Rob's cancer," Bowman said to McClatchy in a phone interview.
"But many veterans are showing up with high levels of depleted uranium in their urine post-9/11," she said. "Even veterans in Rob's unit."

Iran-backed terrorists threaten to bomb Dubai's Burj Khalifa as Brit influencers flock to Gulf to escape lockdown

Source: https://www.the-sun.com/news/2225662/dubai-burj-khalifa-terrorists-iran-influencers/

Jan 2021 – Terrorists backed and funded by Iran have threatened to blow up Dubai's Burj Khalifa skyscraper with drones.
A bloodthirsty militia group turned its sights on the glitzy Gulf getaway where scores of Brit influencers and reality stars have gone to escape lockdown.

Dubai's 2,722ft Burj Khalifa is the world's tallest skyscraper Credit: Alamy

A chilling propaganda poster shows a mocked-up image of red ball of flames erupting 100 storeys up the tower as a second drone zooms towards the target.
It appears to be a World Trade Center-style plot to topple the world's tallest building, which is more than half a mile high at 2,722ft.

The threat comes from an Iraqi militia group suspected of launching two drone attacks in Saudi capital Riyadh this week.
Respected analysts the SITE Intel Group said on Twitter: "Alleged group behind drone in Riyadh depicts strike on Burj Khalifa in Dubai."

And the MEMRI terror monitoring outlet shared the image on its website, along with text of what it says is the group's threat to attack the tower.

Analysts say the threat came from the same Iran-back group that launched drone strikes in Riyadh earlier this week

A double blast was heard in Riyadh on Tuesday morning and witnesses said it appeared a missile had intercepted a drone.
A similar drone attack on Saturday was initially blamed on the Houthis, Iran-backed rebels in Yemen who have attacked targets inside Saudi Arabia many times before.
However the Houthis denied it, and instead a new militia based in Iraq issued a statement claiming responsibility, reports The Times.
The Alwiya al-Waad al-Haq, or Brigades of the Righteous Promise, said the attack had been "launched solely by Iraqi hands".
An online news channel close to Iran-backed terrorists in Iraq said the attacks were meant to make Saudi Arabia the "playground of missiles and drones".
The Brigades of the Righteous Promise appears to be the latest shadowy militia group that has sprung up since the assassination of Iranian general Qassem Soleimani a year ago.
He headed the Quds force and coordinated terror groups fighting Tehran's proxy wars in Iraq and across the Middle East.
The same shadowy militias have launched repeated missile attacks on the Baghdad Green Zone and on US and Iraqi army convoys.

Beirut's Blast-hit Silos Must Be Demolished, Experts Warn

Source: http://www.naharnet.com/stories/en/280684-beirut-s-blast-hit-silos-must-be-demolished-experts-warn

Apr 06 – A section of the grain silos that absorbed much of last year's Beirut port blast must be demolished to avoid collapse, experts warned in a report published Monday.

Swiss company Amann Engineering, which has offered laser scanning assistance to Lebanon since the cataclysmic August 4 explosion, called the most damaged of the disembowelled silos an "unstable, moving structure."
"Our recommendation is to proceed with the deconstruction of this block," the company said in a report.
"As it becomes more obvious the concrete piles have been heavily damaged... new silos will have to be built at a different location," it warned.
Economy minister Raoul Nehme had said in November that Lebanon will demolish its largest grain store over public safety concerns, but authorities have yet to take action.

Once boasting a capacity of more than 100,000 tonnes, the imposing 48-meter-high structure has become emblematic of the catastrophic port blast that killed more than 200 people and damaged swathes of the capital.
Authorities say the blast was caused by a shipment of ammonium nitrate fertiliser that caught fire after being impounded for years on end.
The silos absorbed much of the blast's impact, shielding large swaths of west Beirut from its ravaging effects.
"As much as the structure can be iconic, facts do show there is no way to ensure safety on even the medium term with the north block remaining as is," Amann said in its report.
It warned that the damage to some of the silos was so severe that they were tilting at an alarming rate.
"The inclination proceeds at the rate of 2 millimetres per day, which is a lot structurally speaking," it said.
"By comparison, the Tower of Pisa in Italy was leaning about 5mm per year until it was stabilised by very special works."
Lebanon relies on imports for 85 percent of its food needs.
Confirmation that the silos cannot be salvaged for future use compounds an already alarming food supply outlook.
The country, grappling with its worst economic crisis in decades, has received donations of grain and flour in the aftermath of the explosion.

Public Safety Canines Have New Role

Source: https://i-hls.com/archives/108013

Apr 10 – Many areas with large crowds are known as “soft targets,” meaning they are relatively unprotected against a variety of threats including terrorist attacks and mass shootings. Entertainment arenas, sporting venues, school campuses, places of tourism, and other large leisure events are among these soft targets, and they are becoming increasingly vulnerable to an active shooter attack.

In the US, from 2017-2019 there have been 89 active shooter attacks in public areas wherein firearms were prohibited. In 2020, during a worldwide pandemic, there were over 600 occurrences of gun violence that resulted in the death or injury of four or more people in public or semi-public places.
Statistics show there is no way to predict the likelihood of an attack and very little can be done to mitigate loss once the attack has begun. So early detection is vital.
The 360K9 Group and body-worn canine detection specialist, VWK9, have expanded on their explosive detection operational success, to include firearms detection.
VWK9 developed and launched its Public Safety Canine program in August of 2020 in response to the increased gun violence in public spaces. The company used its knowledge in body-worn explosives detection training protocols, scientifically proven methodologies, and extensive operational experience to provide a fully trained canine able to detect concealed explosive devices and firearms on an individual moving through a public space.
VWK9’s Public Safety Canines are now actively deployed in areas of public interest throughout the United States.
Since its inception, the program has 200+ confirmed concealed firearm finds being carried by individuals in areas wherein firearms are not authorized, according to hstoday.us.

Team from Air Force Research Lab finds a way to use packaged snow as explosion protection

Source: https://counteriedreport.com/team-from-air-force-research-lab-finds-a-way-to-use-packaged-snow-as-explosion-protection/

Apr 15 – Sometimes nature offers more than just beauty, and in this case, it provided a natural solution for a protective barrier for individuals conducting live ordnance training in the Alaska cold.

A team from Wright-Patterson Air Force Base's Junior Force Warfighter Operations in the AFRL Materials and Manufacturing Directorate (designated "JFWORX") led a collaborative, live-fire test with explosive ordnance disposal (EOD) personnel from the 354th Civil Engineer Squadron at Eielson Air Force Base, Alaska. Because the extreme cold of Alaskan winters often makes standard ordnance disposal procedures inadequate if not impossible, JFWORX was asked to formally evaluate the use of a readily available resource — snow — as a protective barrier between live ordnance and people or property, or both.

It began when AFWERX received a request for technical support from Eielson's Iceman Spark team. Iceman Spark is a grassroots organization comprised of Airmen at Eielson Air Force Base who provide innovative solutions in support of the 354th Fighter Wing.

St Paul's bomb plot: Norwegian man charged

Source: https://www.bbc.com/news/uk-england-london-56729605

Apr 15 – A man has been charged in Norway over his alleged role in a terror plot to bomb St Paul's Cathedral in London.

The Norwegian man - who has not been named - was originally arrested in September 2019.

Safiyya Shaikh was jailed for life last year after admitting she had planned to blow herself up inside the building.

Norwegian prosecutors allege the pair spoke over social media in the run-up to the planned bombing. The 24-year-old man denies all charges.

Safiyya Shaikh was jailed for life last year after admitting a plan to blow herself up in the famous cathedral

It is alleged that Muslim convert Shaikh told the man she was going to target the cathedral, and that he said it was a good plan. Prosecutors say he also gave the British woman advice and shared extremist propaganda. The man has also been charged over his involvement in a failed terror plot in Denmark, and is accused of participating in the Islamic State terror group. If found guilty, he faces 21 years in prison.

ICI International CBRNE INSTITUTE

HOTZONE SOLUTIONS GROUP

CBRNE-Terrorism Newsletter

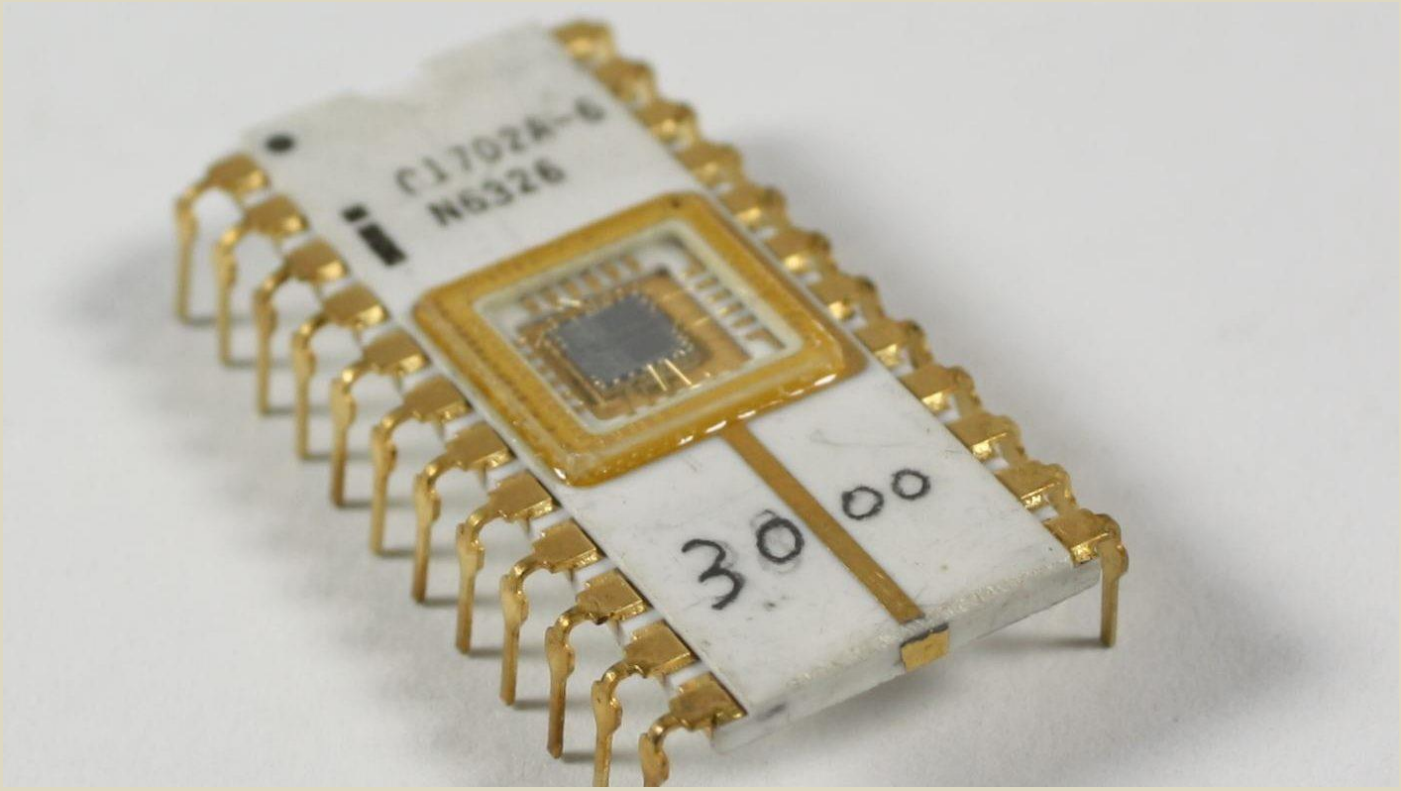
C²BRNE DIARY

CYBER NEWS

Computer Chip Pitted against 500+ Hackers. The Chip Won.

Source: http://www.homelandsecuritynewswire.com/dr20210323-computer-chip-pitted-against-500-hackers-the-chip-won

Mar 23 – An "unhackable" computer chip lived up to its name in its first bug bounty competition, foiling over 500 cybersecurity researchers who were offered tens of thousands of dollars to analyze it and three other secure processor technologies for vulnerabilities.



MORPHEUS, developed by computer science researchers at the University of Michigan, weathered the three-month virtual program DARPA dubbed the Finding Exploits to Thwart Tampering—or FETT—Bug Bounty without a single successful attack. In bug bounty programs, organizations or software developers offer compensation or other incentives to individuals who can find and report bugs or vulnerabilities.

DARPA, the Defense Advanced Research Projects Agency, partnered with the Department of Defense's Defense Digital Service and Synack, a crowdsourced security platform, to conduct FETT, which ran from June through August 2020. It also tested technologies from MIT, Cambridge University, Lockheed Martin and nonprofit tech institute SRI International.

The U-M team achieved its results by abandoning a cornerstone of traditional computer security—finding and eliminating software bugs, says team leader Todd Austin, the S. Jack Hu Collegiate Professor of Computer Science and Engineering. MORPHEUS works by reconfiguring key bits of its code and data dozens of times per second, turning any vulnerabilities into dead ends for hackers.

"Imagine trying to solve a Rubik's Cube that rearranges itself every time you blink," Austin said. "That's what hackers are up against with MORPHEUS. It makes the computer an unsolvable puzzle."

MORPHEUS has previously proven itself in the lab, but the FETT Bug Bounty marks the first time that it was exposed to a group of skilled cybersecurity researchers from around the globe. Austin says its success is further proof that computer security needs to move away from its traditional bugs-and-patches paradigm.

"Today's approach of eliminating security bugs one by one is a losing game," he said. "Developers are constantly writing code, and as long as there is new code, there will be new bugs and security vulnerabilities. With MORPHEUS, even if a hacker finds a bug, the information needed to exploit it vanishes within milliseconds. It's perhaps the closest thing to a future-proof secure system."

For FETT, the MORPHEUS architecture was built into a computer system that housed a mock medical database. Computer experts were invited to try to breach it remotely. MORPHEUS was the second-most popular target of the seven processors evaluated.

Even though it presents a fortress to attackers, Austin says MORPHEUS is transparent to software developers and end users. This is because it focuses on randomizing bits of data

known as "undefined semantics," which are nooks and crannies of the computing architecture—the location, format and content of program code. They're part of a processor's most basic machinery, and legitimate programmers don't generally interact with them. But hackers can reverse-engineer them to uncover vulnerabilities.
The MORPHEUS chip protects undefined semantics through what Austin calls "encryption and churn." Encryption randomizes the important undefined semantics that hackers need to launch a successful attack, while churn re-randomizes them while the system is running. This puts attackers in a race against the clock to discover the information that they need. Austin says that the churn rate is normally kept low to keep system performance high. But when a would-be hacker exercises an undefined semantic in an attempted attack, the churn rate spikes, stopping attackers in their tracks.
MORPHEUS participated in the FETT Bug Bounty as part of DARPA's System Security Integration Through Hardware and Firmware program, designed to develop technologies that protect electronic systems against common classes of hardware vulnerabilities exploited through software. While its participation in that program has ended, MORPHEUS is continuing to advance through Agita Labs, a U-M spinoff company founded by Austin and Valeria Bertacco, professor of computer science and engineering and an Arthur F. Thurnau Professor.
"I'm excited to see how MORPHEUS evolves now that it has proven itself in FETT and as security becomes a more and more pressing challenge in the tech world," Austin said. "We are adapting the technology to protect the most sensitive data in the cloud, including medical and genomic data, biometrics and financial credentials."

▶▶ **The MORPHEUS architecture is detailed in a 2019 paper:** MORPHEUS: A Vulnerability-Tolerant Secure Architecture Based on Ensembles of Moving Target Defenses with Churn.

FBI Releases IC3 2020 Internet Crime Report, Including COVID-19 Scam Statistics

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/fbi-releases-ic3-2020-internet-crime-report-including-covid-19-scam-statistics/

Mar 18 – The FBI's Internet Crime Complaint Center has released its annual report. The *2020 Internet Crime Report* includes information from 791,790 complaints of suspected internet crime—an increase of more than 300,000 complaints from 2019—and reported losses exceeding $4.2 billion. State-specific statistics have also been released and can be found within the *2020 Internet Crime Report* and in the accompanying *2020 State Reports*.
The top three crimes reported by victims in 2020 were phishing scams, non-payment/non-delivery scams, and extortion. Victims lost the most money to business email compromise scams, romance and confidence schemes, and investment fraud. Notably, 2020 saw the emergence of scams exploiting the COVID-19 pandemic. The IC3 received over 28,500 complaints related to COVID-19, with fraudsters targeting both businesses and individuals.
In addition to statistics, the IC3's *2020 Internet Crime Report* contains information about the most prevalent internet scams affecting the public and offers guidance for prevention and protection. It also highlights the FBI's work combating internet crime, including recent case examples. Finally, the *2020 Internet Crime Report* explains the IC3, its mission, and functions.
The IC3 gives the public a reliable and convenient mechanism to report suspected internet crime to the FBI. The FBI analyzes and shares information from submitted complaints for investigative and intelligence purposes, for law enforcement, and for public awareness.
With the release of the *2020 Internet Crime Report*, the FBI wants to remind the public to immediately report suspected criminal internet activity to the IC3 at ic3.gov. By reporting internet crime, victims are not only alerting law enforcement to the activity, but aiding in the overall fight against cybercrime.

It is time to negotiate global treaties on artificial intelligence

By John R. Allen and Darrell M. West
Source: https://www.brookings.edu/blog/techtank/2021/03/24/it-is-time-to-negotiate-global-treaties-on-artificial-intelligence/

Mar 24 – The U.S. National Security Commission on Artificial Intelligence recently made the news when its members warned that America faces a national security crisis due to insufficient investment in artificial intelligence and emerging technologies. Commission Vice Chair Robert Work argued "we don't feel this is the time for incremental budgets … This will be expensive and requires significant change in the mindset at the national, and agency, and Cabinet levels." Commission Chair Eric Schmidt extended those worries by saying "China is catching the US" and "competition with China will increase."

This is not the first time the country has worried about the economic and national security ramifications of new technologies. In the aftermath of World War II, the United States, Soviet Union, China, France, Germany, Japan, the United Kingdom, and others were concerned about the risk of war and the ethical aspects of nuclear weapons, chemical agents, and biological warfare. Despite vastly different worldviews, national interests, and systems of government, their leaders reached a number of agreements and treaties to constrain certain behaviors, and define the rules of war. There were treaties regarding nuclear arms control, conventional weapons, biological and chemical weapons, outer space, landmines, civilian protection, and the humane treatment of POWs.

The goal through these agreements was to provide greater stability and predictability in international affairs, introduce widely-held humanitarian and ethical norms into the conduct of war, and reduce the risks of misunderstandings that might spark unintended conflict or uncontrollable escalation. By talking with adversaries and negotiating agreements, the hope was that the world could avoid the tragedies of large-scale conflagrations, now with unimaginably destructive weapons, that might cost millions of lives and disrupt the entire globe.

With the rise of artificial intelligence, supercomputing, and data analytics, the world today is at a crucial turning point in the national security and the conduct of war. Sometimes known as the AI triad, these characteristics and other weapons systems, such as hypersonics, are accelerating both the speed with which warfare is waged, and the speed with which warfare can escalate. Called "hyperwar" by Amir Husain and one of us (John R. Allen), this new form of warfare will feature levels of autonomy, including the potential for lethal autonomous weapons without humans being in the loop on decision-making.

It will affect both the nature and character of war and usher in new risks for humanity. As noted in our recent AI book "Turning Point," this emerging reality could feature swarms of drones that may overwhelm aircraft carriers, cyberattacks on critical infrastructure, AI-guided nuclear weapons, and hypersonic missiles that automatically launch when satellite sensors detect ominous actions by adversaries. It may seem to be a dystopian future, but some of these capabilities are with us now. And to be clear, both of us, and more broadly the world's liberal democracies, are struggling with the moral and ethical implications of fully autonomous, lethal weapon systems.

In this high-risk era, it is now time to negotiate global agreements governing the conduct of war during the early adoption and adaptation of AI and emerging technologies to the waging of war and to specific systems and weapons. It will be much easier to do this before AI capabilities are fully fielded and embedded in military planning. Similar to earlier treaties on nuclear, biological, and chemical weapons in the post-war period, these agreements should focus on several key principles:

- Incorporate ethical principles such as human rights, accountability, and civilian protection in AI-based military decisions. Policymakers should ensure there is no race to the bottom that allows technology to dictate military applications as opposed to basic human values.
- Keep humans in the loop with autonomous weapons systems. It is vital that people make the ultimate decisions on missile launches, drone attacks, and large-scale military actions. Good judgment and wisdom cannot be automated and AI cannot incorporate necessary ethical principles into its assessments.
- Adopt a norm of not having AI algorithms within nuclear operational command and control systems. The risk of global destruction is high with AI-based launch on warning systems. Since we do not know, and may never know, exactly how AI learns from training data, it is important not to deploy systems that could create an existential threat to humanity.
- Protect critical infrastructure by having countries agree not to steal vital commercial data or disrupt power grids, broadband networks, financial networks, or medical facilities on an unprovoked basis through conventional digital attacks or AI-powered cyber-weapons. Creating a common definition on what constitutes critical infrastructure will be important to the implementation of this principle.
- Improve transparency on the safety of AI-based weapons systems. It is crucial to have more information on software testing and evaluation that can reassure the public and reduce the risks of misperceptions regarding AI applications. That would provide greater predictability and stability in weapons development.
- Develop effective oversight mechanisms to ensure compliance with international agreements. This would include expert convenings, technical assistance, information exchanges, and periodic site inspections designed to verify compliance.

The good news is there are some international entities that already are working on these issues. For example, the Global Partnership on Artificial Intelligence is a group of more than a dozen democratic nations that have agreed to "support the responsible and human-centric development and use of AI in a manner consistent with human rights, fundamental freedoms, and our shared democratic values." This community of democracies is run by the Organization for Economic Cooperation and Development and features high-level convenings, research, and technical assistance.

That said, there are increasingly calls for the technologically advanced democracies to come together to aggregate their capacities, as well as leveraging their accumulated moral strength, to create the norms and ethical behaviors essential to governing the applications of AI and other technologies. Creating a reservoir of humanitarian commitment among the

democracies will be vital to negotiating from a position of moral strength with the Chinese, Russians, and other authoritarian states whose views on the future of AI vary dramatically from ours.
In addition, the North Atlantic Treaty Organization, European Union, and other regional security alliances are undertaking consultations designed to create agreed-to norms and policies on AI and other new technologies. This includes effort to design ethical principles for AI that govern algorithmic development and deployment and provide guardrails for economic and military actions. For these agreements to be fully implemented though, they will need to have the active participation and support of China and Russia as well as other relevant states. For just as it was during the Cold War, logic should dictate that potential adversaries be at the negotiating table in the fashioning of these agreements. Otherwise, democratic countries will end up in a situation where they are self-constrained but adversaries are not.
It is essential for national leaders to build on international efforts and make sure key principles are incorporated into contemporary agreements. We need to reach treaties with allies and adversaries that provide reliable guidance for the use of technology in warfare, create rules on what is humane and morally acceptable, outline military conduct that is unacceptable, ensure effective compliance, and take steps that protect humanity. We are rapidly reaching the point where failure to take the necessary steps will render our societies unacceptably vulnerable, and subject the world to the Cold War specter of constant risk and the potential for unthinkable destruction. As advocated by the members of the National Security Commission, it is time for serious action regarding the future of AI. The stakes are too high otherwise.

John R. Allen *is President, The Brookings Institution.*
Darrell M. West *is Vice President and Director – Governance Studies, and Senior Fellow – Center for Technology Innovation.*

Child tweets gibberish from US nuclear-agency account

Source: https://www.bbc.com/news/technology-56578544

Mar 31 – A young child inadvertently sparked confusion over the weekend by posting an unintelligible tweet to the official account of US Strategic Command. The agency is responsible for safeguarding America's nuclear weapons.
Some social-media users feared the account may have been hacked. But it has since been revealed a young member of the account's social-media manager's family was responsible for posting the tweet, ";l;;gmlxzssaw", which was then deleted within minutes.

Sat-Law Project

Strategic Assessment for Law and Police Cooperation

Source: https://satlawproject.eu/

Sat-Law Project will contribute to the analysis of the consistency of the EIO Directive and other judicial instruments; will focus on the analysis aimed at contributing to the European Agenda on Security with regard to judicial response to terrorism, organized crime and cybercrime, and on reinforcing the prevention of radicalization from a judicial point of view, in particular within the penitentiary environment, through the use of detention measures in the indictment phase; will improve the access to the electronic evidences and its admissibility in front of the courts during the processes.

Activities

- Quantitative and Qualitative research (throughout surveys and focus groups);
- 2 Researches on "Consistency with other instruments and European judicial cooperation treaties" and "Consistency with all the European directives that protect the rights of suspects and defendants".

- 10 Judicial Living Labs: which will be used for the analysis and comparison of the aspects of the legislative implementation of European legislation through the multidisciplinary comparative analysis of the various Directives. The JLLs will be interactive meetings of experts in the field that will create position papers (ie documents that will give indications on how to act).
- 2 Manuals on "European Case Law" and "Examination on Conformity"
- 2 Final Conferences organized in Italy and Spain conceived as main networking events inviting different stakeholders.

Results

Increased capacity of national authorities to address issues related to judicial cooperation in criminal matters; Align the EU acquis and relevant case-law of the CJEU/ECtHR; prosecutors and judges have further specialised knowledge and experience in respective fields; Closer cooperation between LEAs, Prison Police and Judiciary; increased awareness of policy makers and technocrats related to judicial cooperation in criminal matters. Deliverables: 2 Surveys, 1000 copies Baseline Report, 2 Legal Researches, 1 SITs Map of available SITs, 10 Judicial Living Labs (JLLs), 2 Manuals (1000 copies), 5 Factsheets (5000 units), 1 Toolkit, 2 Training Courses 40 participants, Web pag

Target

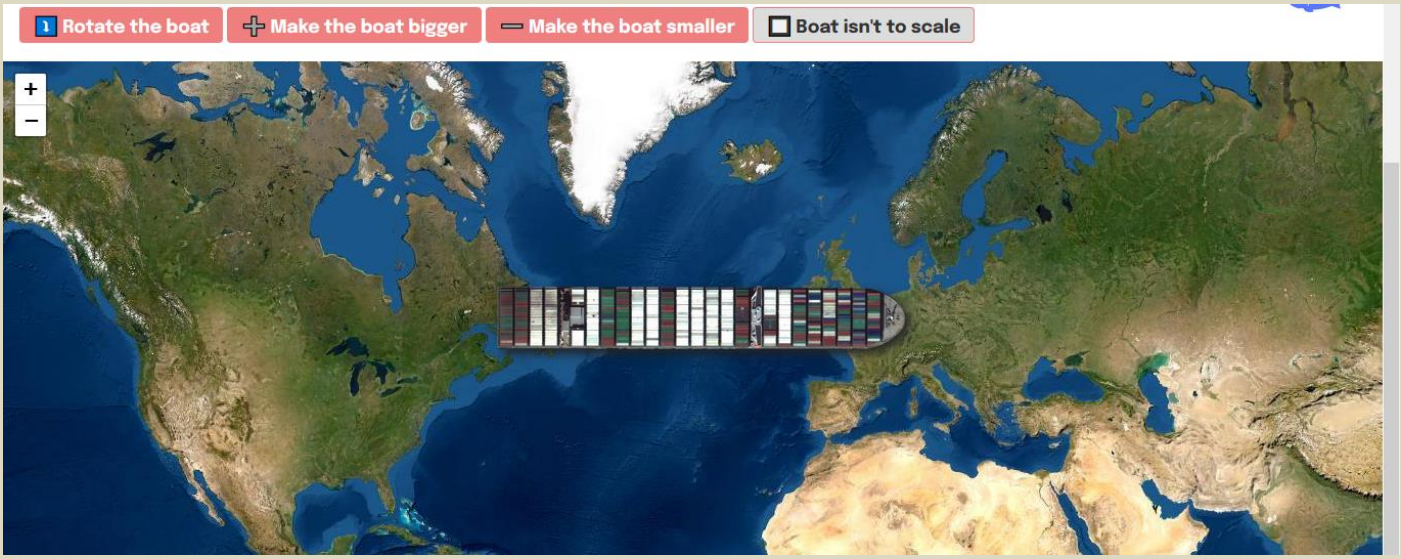
- 300 units between Judges, courts, investigating judges, prosecutors and lawyers.
- 1000 units of police forces at central and local level.
- 1000 units of the Penitentiary Police, penitentiary operators and surveillance judges.
- 500 units of private experts.

▶▶ **Downloads:** https://satlawproject.eu/downloads/

Ever Given in Your Backyard? This App Lets You Place Suez Canal-blocking Ship Anywhere With a Click

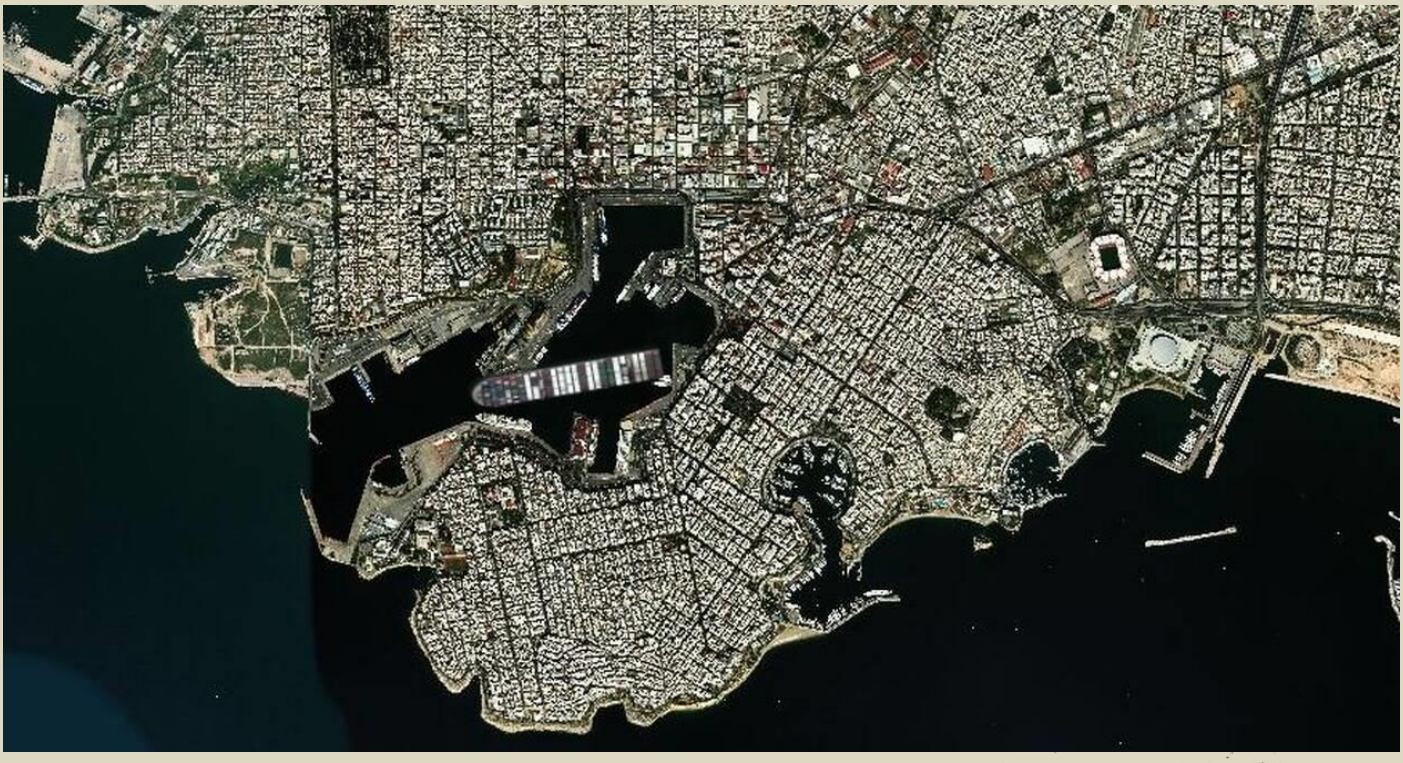
Source: https://www.news18.com/news/buzz/app-suez-canal-ship-ever-given-map-will-let-you-place-ship-anywhere-glitch-3587102.html

Mar 30 – The giant cargo ship Ever Given that was lodged sideways in the Suez Canal in Egypt for over a week had been the topic of much discussion and consternation for people across the world. The ship was finally floated back on route on Monday after continuous efforts using tugboats, sand dredges were involved. Amidst all this, the internet had a lot of free time and thus, out came an application that allowed for social media users to place the boat on a terrain map anywhere on the earth. Sounds fun?



Well, as quirky as the idea seems, social media users all across have been hopping on to the application made by user @en_dash and are having fun lodging the giant vessel anywhere they want on the earth.

Garrett Dash Nelson wrote on Twitter, "I took 10 minutes out of my life to create a@glitch app that lets you wedge the Ever Given anywhere you want in the world. Here it is stuck in Boston Harbor," he tweeted.



Ever Given in Pireaus Port, Athens, Greece

▶▶ **Try it at:** https://evergiven-everywhere.glitch.me/

Hacker unsuccessfully tried to attack Larnaca airport server

Source: https://cyprus-mail.com/2021/04/04/hacker-unsuccessfully-tried-to-attack-larnaca-airport-server/

Apr 04 – Turkish hacker unsuccessfully tried to attack a Larnaca airport server, a source told CNA, noting that the attack was confirmed during the early hours of Saturday.

The same hacker had during the last week of March tried, also unsuccessfully, to attack the defence ministry website.

The source told CNA that as soon as the authorities realised the hacker`s attempt, the server was disconnected from the other systems of the airport and the Digital Security Authority and the Commissioner for Personal Data Protection were informed.

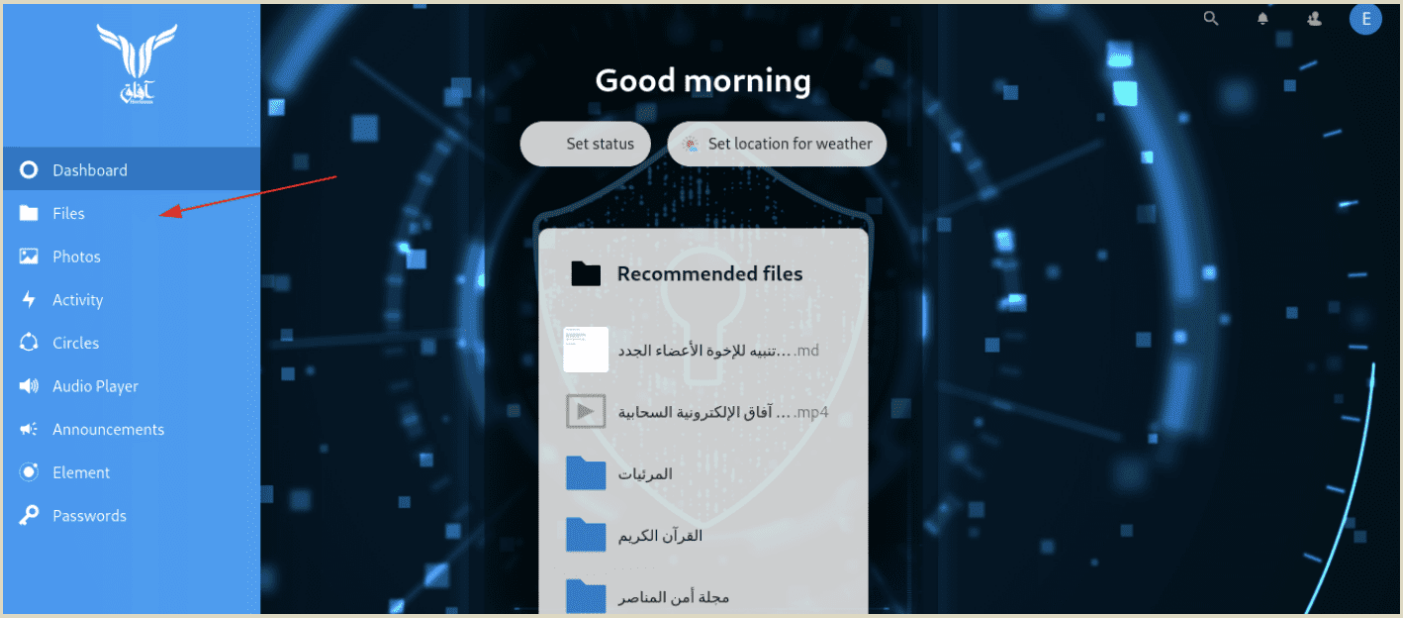
The same source noted that an investigation was launched as regards this incident and that none of the airport`s systems crucial were affected.

The same hacker had last November attempted to attack a website supporting new US President, Joe Biden.

ISIS Cyber Group Launches Cloud, Chat Platforms to 'Close Ranks' Online

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/isis-cyber-group-launches-cloud-chat-platforms-to-close-ranks-online/



Apr 06 – An ISIS-supporting cybersecurity group launched their own cloud and chat platforms that they vowed would help churn out new propaganda and allow followers of the terror group to better "close ranks" online.

"In light of recent developments in the media arena and the restriction of technology companies to content, we resorted to developing solutions that provide a space for propagation between the fellow supporters and the general Muslim community, so that the benefits may prevail," the Electronic Horizons Foundation said in its announcement posted online. "We developed the 'Horizons Cloud Platform' for advocates to use to upload and publish files on the Internet."

The group also developed an Element-based messaging and chat hub "to provide publishing rooms and continuous follow-up for news and content as an initiative to close ranks, and a starting point for the development of media work, Insha Allah."

"Note that our technical support teams are fully prepared to guide the brothers to solve technical and security problems, Insha Allah," the group added. "We pray to Allah to guide us to what is right and to help us against our enemies."

The announcement, which was published in English, Arabic, French, and Italian, includes links to the platforms and ISIS tech support contacts on Element, XMPP, Threema, and Telegram in case supporters have problems registering.

The Electronic Horizons Foundation launched in January 2016 as an IT help desk of sorts to walk ISIS supporters through how to encrypt their communications and otherwise avoid detection online while coordinating with and recruiting jihadists.

EHF released a 24-page cybersecurity magazine for ISIS supporters last May that walks jihadists through step-by-step security for smartphones — while encouraging them to use a

computer instead for more secure terror-related business — and warns of "nightmare" Microsoft Windows collecting user data from geolocation to browsing history.
The group regularly issues cyber news, guidelines and advisories, such as an "important warning" earlier this year telling supporters that "spies of intelligence agencies are using a new method to track down supporters through Google Play Store."
In an online tutorial intended to walk users through the registration process for the new cloud platform, which uses German company Nextcloud's software, the group includes a "caution" that the platform "is for uploading media files, and it's not for uploading personal files."
"We have no responsibility for using them in what isn't pleasing to Allah," the group adds.
For registration, the group advised ISIS supporters to "use a new e-mail from Protonmail.com or Tutanota.com services or other encrypted mail services to create an e-mail for uploading only on the site with the use of VPN services or the Tor network."
New registered users were advised to go into settings and make their account data private. The tutorial walks users through how to create files, add icons, generate a public link for the file, and then share that on social media sites. "We recommend that users of smartphones (Android – iPhone) use the platform through the browser," the group noted.
Files on the tutorial screen included The Supporter's Security, the cyber magazine previously released by EHF, and a library of other releases from the cyber group. There is also a section for announcements where the group said it would post new updates on the cloud platform.
The chat interface home screen promises to "liberate your communication" and gives options for sending direct messages, exploring public rooms, or starting a group chat.
EHF last year urged followers to use alternate operating systems such as Qubes, Tails or Whonix. The ISIS cyber group has also highlighted "wrong security practices" including browsing the internet without Tor or VPN, downloading apps from third-party sources, failing to encrypt the device or storage devices, neglecting to install security updates, failing to use fake credentials on social media, and using social media via apps instead of logging on through a browser. Jihadists have also been warned against opening potentially malicious links that can open them to a security breach.
The EHF has released a series of print and video tutorials covering a range of mobile security and dark-web how-tos for fellow ISIS supporters, along with weekly tech bulletins to educate ISIS followers about current cybersecurity trends and vulnerabilities.

ISIS Cybersecurity Magazine Warns of 'Nightmare' Windows in 'Fierce War' Online

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/isis-cybersecurity-magazine-warns-of-nightmare-windows-in-fierce-war-online/

May 2020 – A 24-page cybersecurity magazine for ISIS supporters walks jihadists through step-by-step security for smartphones — while encouraging them to use a computer instead for more secure terror-related business — and warns of "nightmare" Windows collecting user data from geolocation to browsing history.
The inaugural issue of "The Supporter's Security," published in English and Arabic versions, was produced by the Electronic Horizons Foundation, which launched in January 2016 as an IT help desk of sorts to walk ISIS supporters through how to encrypt their communications and otherwise avoid detection online while coordinating with and recruiting jihadists.
"It is time to face the electronic surveillance, educate the mujahideen about the dangers of the Internet, and support them with the tools, directives and security explanations to protect their electronic security, so that they don't commit security mistakes that can lead to their bombardment and killing," the group said in its founding announcement.
The EHF publishes a weekly cybersecurity bulletin consisting of a handful of headlines pulled from tech news publications, including topics ranging from data breaches to Google and Windows vulnerabilities. The group has also released a series of print and video tutorials covering a range of mobile security and dark-web how-tos.
The new magazine notes that "supporters rely on computers for media work and publishing, starting with design, montage, programming and publishing on

social networks, communication, coordination and management of work, and the most popular operating systems that supporters use is Windows developed by Microsoft, which is a security nightmare as it collect all your data, and sends it to Microsoft."
ISIS supporters are urged to use alternate operating systems such as Qubes, Tails or Whonix. EHS follows this advice with two pages of detailed Whonix system installation instructions.

The magazine laments that tech development is "led by polytheists" and "they have the upper hand of it, they work their efforts day and night to use it against the religion of Allah, and humiliate the Muslims, so that they become under their control and mercy, and move under their surveillance."
Islam "has obligated in such a case that Muslims should learn and prepare what strengthens them," the EHF argues, and "one of the most important tools of our time is Information technology."
"Some of it needs specialization and long study, and some of it needs some serious attention, and Muslims are in such big need for both of them, the need is urgent," the group adds. " …We are inside a fierce war, our sites and accounts in social media got deleted because the intelligence services realize the danger of Muslims gaining security awareness, which will make it difficult to track them and cut off the ways for them to arrest the monotheists, but we do not leave this field, Allah willing, until Allah decides what needs to be done."
The magazine begins with a lengthy assessment of the pros and cons of smartphone use, with the former limited to cost and accessibility and the latter being that "the Mujahideen started to use smartphones to communicate, publish, plan and work without knowing the real security risks they face."
"The Mujahideen have been warned more than once about the danger of smartphones, which led to the arrest of many brothers due to the security negligence, so you must realize as a supporter of the truth that the security measures that need to be applied for you are completely different from the security measures used by anyone else," the article states. "Understand the security threats facing you and how to choose the appropriate tools and methods to conduct your business and bypass electronic control, which includes every device connected to the Internet or cellular networks now."
EHF walks through various operating systems for Android in their setup guide, pages of graphics detailing what settings to use on both Android and iPhone to better secure their communications. "Good iOS security starts with having a really strong passcode," the group advises. "If this is something that's easily guessable then everything else you do is pretty much pointless."
The writers acknowledge that choosing the right smartphone can be confusing for a jihadist, thus let readers know they can "contact us via technical support accounts to guide you to the phone that is suitable for you."
The ISIS cyber group also highlights "wrong security practices" including browsing the internet without Tor or VPN, downloading apps from third-party sources, failing to encrypt the device or storage devices, neglecting to install security updates, failing to use fake credentials on social media, and using social media via apps instead of logging on through

a browser. Jihadists are also warned against opening potentially malicious links that can open them to a security breach.
"You must trust the underlying operating system running the program," EHF says. "The tasks of the program are limited to what the operating system tells it to do, so you must trust that the operating system prevents leaks of the tasks you are working on for anyone else."

***Bridget Johnson** is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill.*

A Massive Hack That Google Thwarted Was Actually a Counterterrorism Operation

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/a-massive-hack-that-google-thwarted-was-actually-a-counterterrorism-operation/

Mar 30 – Security researchers regularly reveal software vulnerabilities that hackers can exploit, or even have exploited in the past. In some cases, they're software issues that have not been used to hack or spy on users. In others, researchers identify malware and hacks that are actively used in the wild. By the time they release information about the attacks, the companies whose code had been attacked have already released updates to patch the problems. And security researchers usually point out when they believe the hacks are too sophisticated for a regular hacker to pull off.

Google runs an infamous security team at **Project Zero** that analyzes all sorts of operating systems and products for vulnerabilities. Since January, the team produced research that highlighted 11 zero-day exploits that were used to compromise Android, iPhone, and Windows. Back in January, Project Zero scientists pointed out the sophistication of the attacks that utilized previously unknown vulnerabilities in Chrome and Safari code. It turns out that the hackers behind the campaign that Google found were from a nation-state. They were part of a counterterrorism operation initiated by a Western ally, and the operation was ongoing when Project Zero started revealing the software issues.

The EU Online Terrorism Regulation: A Bad Deal

By Jillian C. York and Christoph Schmon
Source: http://www.homelandsecuritynewswire.com/dr20210408-the-eu-online-terrorism-regulation-a-bad-deal

Apr 08 – On 12 September 2018, the European Commission presented a proposal for a regulation on preventing the dissemination of terrorist content online—dubbed the Terrorism Regulation, or TERREG for short—that contained some alarming ideas. In particular, the proposal included an **obligation for platforms to remove potentially terrorist content within *one hour*, following an order from national competent authorities.**

Ideas such as this one have been around for some time already. In 2016, we first wrote about the European Commission's attempt to create a voluntary agreement for companies to remove certain content (including terrorist expression) within 24 hours, and Germany's Network Enforcement Act (NetzDG) requires the same. NetzDG has spawned dozens of copycats throughout the world, including in countries like Turkey with far fewer protections for speech, and human rights more generally.
Beyond the one hour removal requirement, the TERREG also contained a broad definition of what constitutes terrorist content as "material that incites or advocates committing terrorist offences, promotes the activities of a terrorist group or provides instructions and techniques for committing terrorist offences".
Furthermore, it introduced a duty of care for all platforms to avoid being misused for the dissemination of terrorist content. This includes the requirement of taking proactive measures to prevent the dissemination of such content. These rules were accompanied by a framework of cooperation and enforcement.
These aspects of the TERREG are particularly concerning, as research we've conducted in collaboration with other groups demonstrates that companies routinely make content

moderation errors that remove speech that parodies or pushes back against terrorism, or documents human rights violations in countries like Syria that are experiencing war.

TERREG and Human Rights

TERREG was created without real consultation of free expression and human rights groups and has serious repercussions for online expression. Even worse, the proposal was adopted based on political spin rather than evidence.

Notably, in 2019, the EU Fundamental Rights Agency—tasked with an opinion by the EU parliament—expressed concern about the regulation. In particular, the FRA noted that the definition of terrorist content had to be modified as it was too wide and would interfere with freedom of expression rights. Also, "According to the FRA, the proposal does not guarantee the involvement by the judiciary and the Member States' obligation to protect fundamental rights online has to be strengthened."

Together with many other civil society groups, we voiced our deep concern over the proposed legislation and stressed that the new rules would pose serious potential threats to fundamental rights of privacy, freedom of expression.

The message to EU policymakers was clear:

- **Abolish the one-hour time frame for content removal**, which is too tight for platforms and will lead to over removal of content;
- **Respect the principles of territoriality and ensure access to justice in cases of cross-border takedowns** by ensuring that only the Member State in which the hosting service provider has its legal establishment can issue removal orders;
- **Ensure due process** and clarify that the legality of content be determined by a court or independent administrative authority;
- **Don't impose the use of upload or re-upload filters** (automated content recognition technologies) to services under the scope of the Regulation;
- **Exempt certain protected forms of expression**, such as educational, artistic, journalistic, and research materials.

However, while responsible committees of the EU Parliament showed willingness to take the concerns of civil society groups into account, things looked more grim in Council, where government ministers from each EU country meet to discuss and adopt laws. During the closed-door negotiations between the EU-institutions to strike a deal, different versions of TERREG were discussed, which culminated in further letters by civil society groups, urging the lawmakers to ensure key safeguards on freedom of expressions and the rule of law.

Fortunately, civil society groups and fundamental rights-friendly MEPs in the Parliament were able to achieve some of their goals. For example, the agreement reached by the EU institutions includes exceptions for journalistic, artistic, and educational purposes. Another major improvement concerns the definition of terrorist content (now matching the narrower definition of the EU Directive on combating terrorism) and the option for host providers to invoke technical and operational reasons for non-complying with the strict one-hour removal obligation. And most importantly, the deal states that authorities cannot impose upload filters on platforms.

The Deal Is Still Not Good Enough

While civil society intervention has resulted in a series of significant improvements to the law, there is more work to be done. The proposed regulation still gives broad powers to national authorities, without judicial oversight, to censor online content that they deem to be "terrorism" anywhere in the EU, within a one-hour timeframe, and to incentivize companies to delete more content of their own volition. It further encourages the use of automated tools, without any guarantee of human oversight.

Now, a broad coalition of civil society organizations is voicing their concerns with the Parliament, which must agree to the deal for it to become law. EFF and others suggest that the Members of the European Parliament should vote against the adoption of the proposal. We encourage our followers to raise awareness about the implications of TERREG and reach out to their national members of the EU Parliament.

***Jillian C. York** is director for international freedom of expression at EFF.*
***Christoph Schmon** is international policy director at EFF.*

Cybersecurity Guide Tailored to the Hospitality Industry

Source: http://www.homelandsecuritynewswire.com/dr20210409-cybersecurity-guide-tailored-to-the-hospitality-industry

Apr 09 – A new practical cybersecurity guide from the National Institute of Standards and Technology (NIST) can help hotel owners reduce the risks to a highly vulnerable and attractive target for hackers: the hotel property management system (PMS), which stores guests' personal information and credit card data.

The three-part guide, formally titled *Securing Property Management Systems* (NIST Special Publication [SP] 1800-27 a, b and c), shows an approach to securing a PMS. It offers how-to guidance using commercially available products, allowing hotel owners to control and limit access to their PMS and protect guest privacy and payment card information.
"We have demonstrated that cybersecurity risk can be mitigated in and around a property management system using today's technology," said Bill Newhouse of NIST's National Cybersecurity Center of Excellence (NCCoE). "Our practice guide documents how we enabled cybersecurity concepts such as zero trust architecture, moving target defense, tokenization of credit card data, and role-based authentication in a reference design that addresses cybersecurity and privacy risk. We also offer specific use cases to show the functionality of the design."
In recent years attackers have compromised the networks of several major hotel chains, exposing the information of hundreds of millions of guests. According to a recent industry report, hospitality ranked third among industries compromised by cybersecurity breaches in 2019, and the industry suffered 13% of the total incidents. About two-thirds of these breaches were attacks on corporate servers, which often store guest information and communicate with on-site property management systems. Breaches like these can harm corporate reputations, disrupt operations and cause huge financial loss.
The NCCoE collaborated with the hospitality business community and cybersecurity technology providers to build an example system, or "PMS reference design," that simulates a hotel's PMS and connected IT infrastructure, including an electronic payment system and electronic door locks. The design protects data moving within this environment, and it prevents user access to the various systems and services.
While the design uses commercially available technologies to accomplish these goals, the guide does not endorse any particular products. All technologies used in the solution support security standards and guidelines of the NIST Cybersecurity Framework, and the design aligns with the privacy protection activities and desired outcomes of the NIST Privacy Framework.
The practice guide also introduces the tenets and components found in a recent NIST publication on zero trust architecture, a cybersecurity paradigm focused on resource protection. Its premise is that trust is never granted implicitly but must be continually evaluated.
"We offer a look into zero trust that I think can help those in the hospitality sector, who are new to the concept, to better understand what the vendors are offering," Newhouse said.
Zero trust principles mean access is not granted to devices or user accounts based solely on their physical or network location or who owns them. Instead, authentication and authorization of both subject and device are required before users can access a network's resources.
"This publication analyzes and addresses the challenges common to almost all hotels in creating secure data systems," said Robert Braun, a partner at the Los Angeles law firm Jeffer Mangels Butler & Mitchell LLP, who has counseled hotel clients on data breaches and privacy. "Hotels would be well-advised to incorporate its recommendations in their information protection protocols."
The guide's three parts include: NIST SP 1800-27a, the executive summary; NIST SP 1800-27b, *Approach, Architecture, and Security Characteristics,* aimed at helping program managers identify, understand, assess and mitigate risk; and NIST SP 1800-27c, *How-To Guides,* which provides specific instructions for building the example implementation, allowing IT professionals to replicate all or parts of this project.

▶▶ **The entire guide is available** here.

Cyber Polygon

Source: https://cyberpolygon.com/about/

Cyber Polygon is a unique cybersecurity event that combines the world's largest **technical training** for corporate teams and an **online conference** featuring senior officials from international organisations and leading corporations. Every year, the training brings together a wide range of global businesses and government structures while the live stream gathers millions of spectators from across the world. Cyber Polygon is an initiative of BI.ZONE (Sber Ecosystem) supported by the World Economic Forum Centre for Cybersecurity.

Strategic Goals
The annual training enables organisations to assess their cyber resilience, exchange best practices and bring tangible results to the global community:

- develop the teams' skills in repelling cyberattacks
- expand the practical knowledge of technical specialists

- engage the management of international organisations and corporations in the cybersecurity dialogue
- raise public awareness of cybersecurity

Concept 2021
As the global digitalisation is further accelerating, the world is becoming ever more interconnected. Digital ecosystems are being created all around us: countries, corporations and individuals are taking advantage of the rapid spread of the Internet and smart devices. In this context, a single vulnerable link is enough to bring down the entire system, just like the domino effect.
A secure approach to digital development today will determine the future of humanity for decades to come.
Cyber Polygon 2021 will enable the spectators and participants to improve on their cyber literacy, enhance the resilience of their organisations and learn to repel cyberthreats on all levels.

Will Cyber Polygon 2021 be as prophetic as Event 201 in simulating a pandemic response?

By Tim Hinchliffe
Source: https://sociable.co/technology/prepping-cyber-pandemic-cyber-polygon-stage-supply-chain-attack-simulation/

Feb 10 – The World Economic Forum (WEF) will stage another cyber attack exercise as it continues to prep for a potential cyber pandemic that founder Klaus Schwab says will be worse than the current global crisis.
The SolarWinds hack served as a wake-up call to the supply chain attack vulnerabilities still present in public and private organizations, and it served as a warning that the next breach could be exponentially worse in spreading through any device connected to the internet.
Following up on last year's Cyber Polygon cyber attack exercise and event aimed at preventing a digital pandemic, the WEF has announced that the 2021 edition will be taking place on July 9.

"A cyber attack with COVID-like characteristics would spread faster and further than any biological virus"
World Economic Forum

This year, Cyber Polygon 2021 will simulate a fictional cyber attack with participants from dozens of countries responding to "**a targeted supply chain attack on a corporate ecosystem in real time.**"

According to the WEF, COVID-19 was known as an anticipated risk, and so is its digital equivalent.
What's more, "A cyber attack with COVID-like characteristics would spread faster and farther than any biological virus. Its reproductive rate would be around 10 times greater than what we've experienced with the coronavirus."
"It is important to use the COVID-19 crisis as a timely opportunity to reflect on the lessons of cybersecurity community to draw and improve our unpreparedness for a potential cyber pandemic" — Klaus Schwab
Here, we take a look at three trends emerging from Cyber Polygon 2020 to uncover what moves the public and private sectors may make in anticipation of a digital pandemic.
But first, where did the notion of a cyber pandemic come from?

An Anticipated Cyber Pandemic

In his welcoming remarks at Cyber Polygon 2020, WEF Founder Klaus Schwab warned about a coming "cyber pandemic" that would be worse than the current global crisis.
"We all know, but still pay insufficient attention to, the frightening scenario of a comprehensive cyber attack, which would bring a complete halt to the power supply, transportation, hospital services, our society as a whole," he said.
"The COVID-19 crisis would be seen in this respect as a small disturbance in comparison to a major cyber attack."
Schwab added, "It is important to use the COVID-19 crisis as a timely opportunity to reflect on the lessons of cybersecurity community to draw and improve our unpreparedness for a potential cyber pandemic."
As the digital world encroaches on our physical and biological worlds, an effective cyber attack could compromise anything connected to the internet, including:

- **Medical devices that keep people alive**
- **The Internet of Things (IoT) ecosystem of connected devices that run smart homes (i.e. cameras, microphones, sensors, etc.)**
- **The Internet of Bodies (IoB) ecosystem of digitally-connected humans**
- **Global financial systems**
- **Energy grids**
- **Water treatment facilities**
- **Government IT systems**
- **Military and defense infrastructure**
- **And more**

Currently, "The only way to stop the exponential propagation of a COVID-like cyber attack threat," according to the WEF, "is to fully disconnect the millions of vulnerable devices from one another and from the internet."
But, "A single day without the internet would cost our economies more than $50 billion, and that's before considering economic and societal damages should these devices be linked to essential services, such as transports or healthcare."
"The COVID-19 crisis would be seen in this respect as a small disturbance in comparison to a major cyber attack" — Klaus Schwab
Needless to say, a cyber pandemic would wreak havoc on nearly all aspects of society.
However, the devil is in the details, and the solutions recommended for a cyber pandemic could be far more detrimental to individual liberty than the cyber attack itself.

Cyber Polygon 2020 Emerging Trends

The central theme of the Cyber Polygon 2020 exercise was "**digital pandemic: how to prevent a crisis and to reinforce cybersecurity on all levels**."
The goal of last year's Cyber Polygon event was to:

- **Develop the teams' competencies in repelling cyber attacks**
- **Engage the management of global organizations and corporations in the cybersecurity dialogue**
- **Raise public awareness in cybersecurity**

The exercise featured two parallel tracks: a live stream for a mass audience and technical training for cybersecurity specialists, and 120 of the largest Russian and international organizations from 29 countries joined the technical training **to practice response to a targeted attack, aimed at hacking company data and undermining its reputation**.
While the technical training side of the event was dedicated to responding to a single attack, the conversations from the live stream portions provided the most insights for dealing with the potential fallout of the attack — the digital pandemic.

Here are three trends emerging from the **live stream** discussions and the Cyber Polygon 2020 **results report**.

1) Governments Will Inevitably Move Towards Digital Identity Schemes

Speaking at Cyber Polygon 2020, former British Prime Minister Tony Blair stated with confidence that governments are "absolutely, inevitably" moving in the direction of digital identity adoption.

"Digital ID for me is a very big part of the future" — Tony Blair

Digital identity is a major component of the WEF's great reset agenda as it relates to transformative technologies powering the Fourth Industrial Revolution.

A digital identity keeps a record of everything you do online, including what you share on social media, the websites you visit, and your smartphone's geolocation, and it can house all of the credentials you would normally find in a physical wallet, such as your driver's license, insurance card, and credit cards.

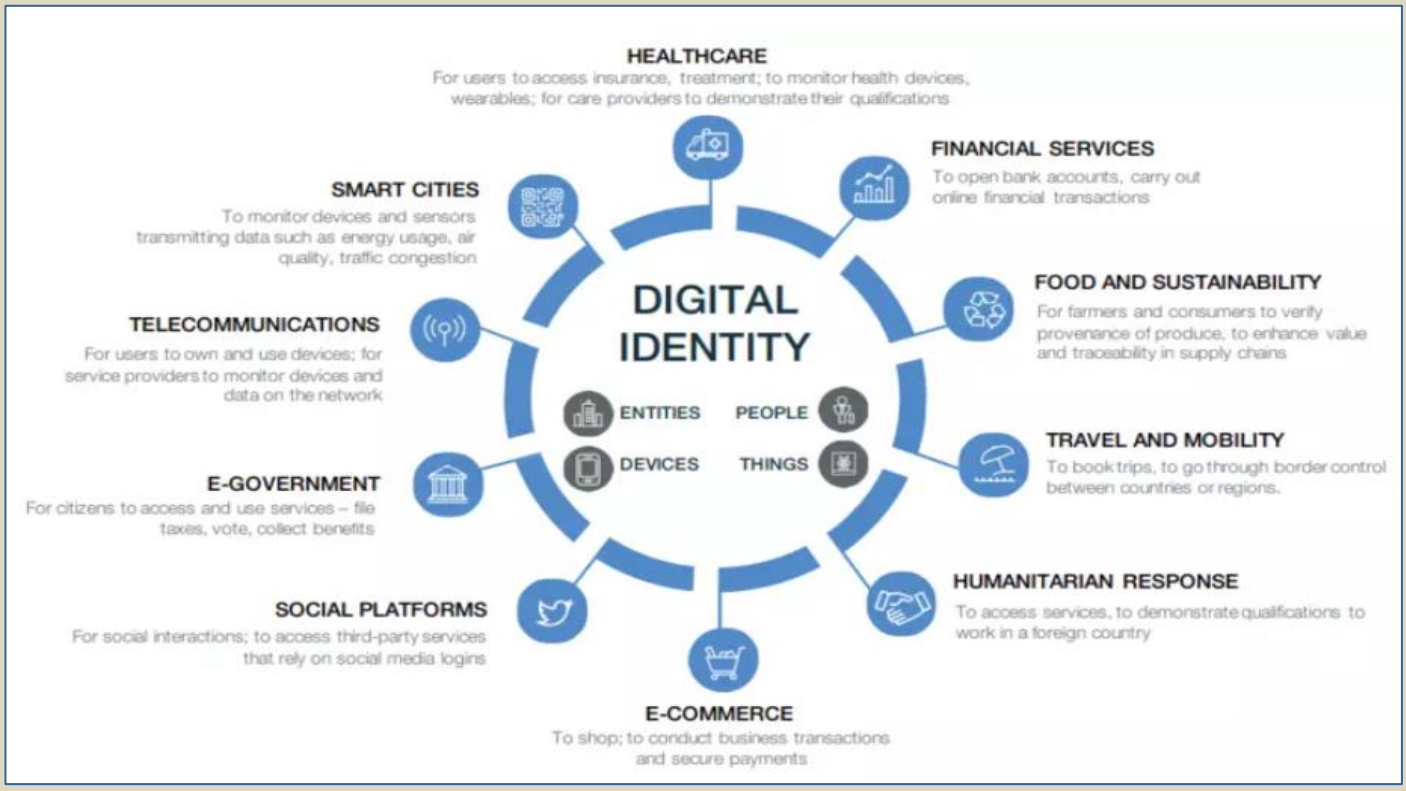
In his talk, Blair didn't make the case for why having a digital identity was actually necessary to prevent a cyber pandemic, but rather that digital identities would be an inevitable part of the digital ecosystem, and so governments should work with technology companies to protect and regulate their use.

"Digital ID for me is a very big part of the future," said Blair.

"Inevitably, governments are going to move in this direction — absolutely, inevitably," he added.

"And so what I think's most important is that we from the political side wake-up to the potential of technology and engage with the changemakers inventing the technology, so that we understand it and can regulate it sensibly and not stupidly."

Image Source: World Economic Forum



If a hacker were to gain control over someone's digital identity, they could essentially shut them out of participating in civil society by erasing them completely, or exploiting their information in such a way that blocks victims from proving they have money in the bank, a passport that allows them to travel, a valid driver's license, proof of immunity, and any other credentials that are necessary for citizens to access goods and services.

And while digital identities show promise towards improving the livelihoods of millions when governed ethically, they are also used by authoritarian governments to profile and police citizen behavior under a social credit system.

Whether the data be secured or not, **individual liberty will depend on how the technology is used and the level of trust given to those who govern it**.

According to a WEF report from 2018, "digital identity determines what products, services and information we can access – or, conversely, what is closed off to us" — the level of which to be determined by our online behavior.
If Blair is right and governments will inevitably adopt digital identities, then a well-coordinated cyber attack affecting digital identity systems would lead to a cyber pandemic affecting the whole of society.

2) 'Fake News' Is a Digital Pandemic & the Majority of Citizens Are Incapable of Thinking Critically

Cyber Polygon 2020 dedicated one of its live streams sessions to the concept of "fake news" as being a deadly, digital pandemic plaguing 2020.
"If you're talking about someone who […] has not read very much, whose knowledge is limited — that person is much easier to fool and much more ready to accept whatever he or she is told" — Vladimir Pozner, Journalist
By the end of their conversation, BBC World News presenter Nik Gowing and veteran journalist Vladimir Pozner arrived at the conclusion that the average person of voting age was not capable of thinking critically for themselves and was more likely to swallow any information put out there than someone who went to a university.
Both Gowing and Pozner agreed that the majority of citizens were uneducated, were not well-read, and hadn't traveled enough to know the difference between what was fake and what was real.
Pozner: "You're launching your argument based on a sense that your average viewer, listener, reader has a critical outlook from the outset."
"I think that there are an awful lot of people who don't have that critical outlook and just swallow it whole."
Gowan: "I agree […] "You have to have that questioning instinct."
Pozner: "If someone is well-educated, has a university education, has read, has traveled — that person's reaction to what he or she is reading or listening to is one thing.
"If you're talking about someone who finished grammar school or the like and has not had the opportunity because of where that person comes from, has not read very much, whose knowledge is limited — that person is much easier to fool and much more ready to accept whatever he or she is told.
"When we're dealing with this deliberate lie, who is it directed at mainly?
"In my opinion, it's mainly directed towards the ordinary person — not towards the intellectual elite, not towards those who have the ability to actually think it through, but to those who have not had that advantage, to the less privileged people who are the majority, and who are the ones who vote, and who are the ones who, ultimately, when they say, '*the people*,' they are '*the people*,' and I think they are the ones who are victimized by this trend."
With the assumption that average people aren't capable of thinking critically and that the majority of citizens are therefore "victims," the two journalists turned the conversation towards how to protect victims of the "fake news pandemic."
But in the end, they had no idea how to do that, and fake news, misinformation, and disinformation remain "existential threats."
Cyber Polygon 2020 didn't issue any concrete recommendations with regards to dealing with fake news; however, the WEF-led Event 201 coronavirus pandemic simulation did recommend that, "Governments will need to partner with traditional and social media companies to research and develop nimble approaches to countering misinformation."

3) Trustworthy Public & Private Partnerships Will Need To Be Strengthened

Establishing trustworthy collaborations among the public and private sectors can help prevent a digital pandemic, according to the Polygon 2020 report.
"A critical situation cannot be tackled by an organization or a lone individual," it reads, adding, "In a highly interconnected world, a single cyber attack can spread exponentially across the global community.
"This situation can be prevented by promoting collaboration between the public and private sectors and law enforcement agencies.
"Furthermore, efficient interaction requires the implementation and regulation of a range of standards, the exchange of information and establishing trustworthy relationships."
"When we do see this next crisis, it will be faster than what we've seen with COVID, the exponential growth rate will be much steeper, the impact will be greater, and as a result the economic and social implications will be even more significant" — Jeremy Jurgens, WEF Chief Business Officer
However, with countries like China stealing intellectual property, sponsoring state-run cyber attacks that have compromised the personal information of nearly every single American adult, and silencing doctors and whistleblowers about the CCP's responsibility in the coronavirus pandemic, establishing trust and bolstering collaborations among governments and corporations are lofty goals to set.
During the Polygon 2020 live session, WEF Chief Business Officer Jeremy Jurgens said that preventing the next crisis will require that all sectors of society and the economy come together.

"I believe that there will be another crisis," he said. "It will be more significant. We need to actually start preparing for that now."
"We need to start this cooperation and understanding early, so that when the crisis does hit, we're in a position to respond effectively to it.
"I would anticipate that when we do see this next crisis, it will be faster than what we've seen with COVID, the exponential growth rate will be much steeper, the impact will be greater, and as a result the economic and social implications will be even more significant.
"I think it's really important that we don't underestimate the severity of a crisis like this — the impact it could have.
"It's going to take all sectors of society and the economy to come together to address that," Jurgens added.
The Cyber Polygon 2020 report, along with the virtual sessions recorded during Davos Week at the end of January, 2021, **all highlight the need/desire for public and private collaboration** — not just as a means to avert a cyber pandemic — but for reshaping the entire global economy and revamping all aspects of society under a new form of stakeholder capitalism brought on by the great reset.

Trends Emerging From Digital Pandemic Exercise

In this article, we looked at three trends emerging Cyber Polygon 2020:

- **A greater consolidation of resources and collaborations among corporations and states**
- **A plan to deal with fake news, disinformation, and misinformation that has yet to be unveiled**
- **A push towards digital identity that will need to be secured and protected**

While these basic observations were plucked from last year's exercise, this year's Cyber Polygon will present new challenges in which participants will respond to a different threat — a targeted supply chain attack on a corporate ecosystem in real-time.
If the results and recommendations from previous pandemic simulations are any indication of what may lie ahead for society, then the findings and policies coming out of Cyber Polygon 2021 may have real-world societal impact in the very near future.
For example, many scenarios played out in the WEF-backed fictional pandemic simulations Clade X (May, 2018) and Event 201 (October, 2019) later came to pass, along with several policy recommendations for dealing with the COVID-19 pandemic.
These scenarios depicted:

- **Governments implementing lockdowns worldwide**
- **The collapse of many industries**
- **Growing mistrust between governments and citizens**
- **A greater adoption of biometric surveillance technologies**
- **Social media censorship in the name of combating misinformation**
- **The desire to flood communication channels with "authoritative" sources**
- **Mass unemployment**
- **Rioting in the streets**
- **And a whole lot more!**

When the World Health Organization (WHO) declared the coronavirus a pandemic on March 11, 2020, governments all over the world went into lockdown, which had devastating effects on the economy with businesses closing, civil unrest skyrocketing, unemployment surging, housing foreclosures on the horizon, and the largest transfer of wealth ever recorded in human history.
However, many of these scenarios were already anticipated and taken into account in previous simulations, and yet they all still came to pass.
Will the conversations coming out of Cyber Polygon 2021 prove to be as prophetic for the digital world as Event 201 and Clade X were for the physical one?

Internet Organized Crime Threat Assessment (IOCTA) 2020

Source: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

October 2020 – The IOCTA is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime. It provides a unique law enforcement focused assessment of emerging challenges and key developments in the area of cybercrime. We are grateful for the many contributions from our colleagues within European law enforcement community and to our partners in the private industry for their input to the report. Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.
The data collection for the IOCTA 2020 took place during the lockdown implemented as a result of the COVID-19 pandemic. Indeed, the pandemic prompted significant change and criminal innovation in the area of cybercrime. Criminals devised both new modi operandi and adapted existing ones to exploit the situation, new attack vectors and new groups of victims.

After the Islamic State: Social Media and Armed Groups

Source: http://www.homelandsecuritynewswire.com/dr20210412-after-the-islamic-state-social-media-and-armed-groups

Apr 12 – The Islamic State is often credited with pioneering the use of social media in conflict, having created a global brand that drew between 20,000 and 40,000 volunteers from at least 85 countries. Social media served as a key recruiting tool, source of fundraising, and platform for disseminating graphic propaganda to a global audience. Laura Courchesne and Brian McQuinn write in *War on the Rocks* that the Islamic State perfected tactics and strategies already widely used by hundreds of other armed groups.

> For example, al-Shabab pioneered social media use by self-described jihadist groups, using Twitter and micro-blogging platforms before the Islamic State. But its regional focus in the Horn of Africa meant that its efforts did not show up on the West's radar until the Westgate Mall attack in 2013. Unlike the Islamic State — which pursued recruits from around the world — al-Shabab appealed to regional and local audiences. As a result, it was largely ignored by the West and social media companies.
>
> According to our research with the Digital Traces of Conflict Project, there are over 1,456 armed groups operating in civil wars in Mali, Libya, and Syria. Almost all use social media to target regional and local audiences, but vary in their choice of platform. Social media is also providing novel and underexplored funding channels. Studying how terrorist groups "successfully" use social media will help predict characteristics that will define the future of conflict. The next global threat to exploit social media will emerge from the groups currently avoiding detection or attention by platforms. In response, the United States and its partners should build new models, grounded in the full range of armed group social media usage, if they hope to anticipate the future of malicious online activity by armed groups.

Courchesne and Brian McQuinn add that in the past decade, social media has transformed conflict, forever changing how civil wars are fought, funded, and studied. Insurgent groups have announced their formation, boasted of their victories, recruited new members, and solicited funds on YouTube, Facebook, Instagram, and Twitter. They note, however, that at the same time, the unprecedented attention paid to the social media efforts by groups like the Islamic State "has created what we think is a false impression of how armed groups use social media. Specifically, there is the idea that successful use of social media by an armed group results in a global brand and international attention. Rather, most armed groups successfully use social media at local and regional levels, escaping the purview of the West and social media platforms."

They conclude:

> The West's fixation on the Islamic State and its use of social media (followed more recently by a shift to far-right extremists) ignores how the vast majority of armed groups across the world use social media. Most armed groups use social media away from global attention, avoiding action by the U.S. companies or Western governments. The next Islamic State will not use the same online playbook. Anticipating future threats in the online environment requires monitoring armed groups' emerging social media strategies adapted to avoiding detection while targeting niche audiences.

Portrait Of A Digital Weapon

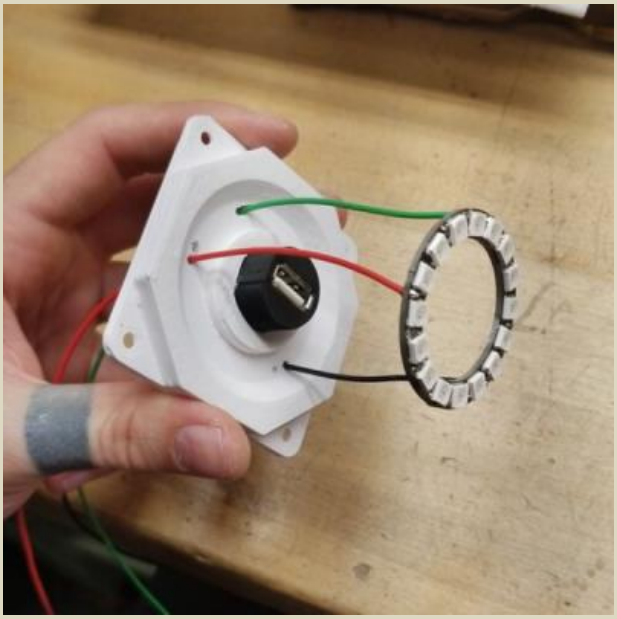
Source: https://hackaday.com/2021/04/15/portrait-of-a-digital-weapon/

Apr 15 – Over the years, artists have been creating art depicting weapons of mass destruction, war and human conflict. But the weapons of war, and the theatres of operation are changing in the 21st century. The outcome of many future conflicts will surely depend on digital warriors, huddled over their computer screens, punching on their keyboards and maneuvering joysticks, or using devious methods to infect computers to disable or destroy infrastructure. How does an artist give physical form to an unseen, virtual digital

weapon? That is the question which inspired [Mac Pierce] to create his latest Portrait of a Digital Weapon.
[Mac]'s art piece is a physical depiction of a virtual digital weapon, a nation-state cyber attack. When activated, this piece displays the full code of the Stuxnet virus, a worm that partially disabled Iran's nuclear fuel production facility at Natanz around 2008.

It took a while for [Mac] to finalize the plan for his design. He obtained a high resolution satellite image of the Iranian Natanz facility via the Sentinel Hub satellite imagery service. This was printed on a transparent vinyl and glued to a translucent poly-carbonate sheet. Behind the poly-carbonate layer, he built a large, single digit 16-segment display using WS2812 addressable LED strips, which would be used to display the Stuxnet code. A bulkhead USB socket was added over the centrifuge facility, with a ring of WS2812 LEDs surrounding the main complex. When a USB stick is plugged in, the Stuxnet code is displayed on the 16-segment display, one character at a time. At random intervals, the LED ring around the centrifuge building lights up spinning in a red color to indicate centrifuge failure.

The 16-segment display was built on an aluminum base plate, with 3D printed baffles to hold the LED strips. To hold the rest of the electronics, he built a separate 3D printed frame which could be added to the main art frame. Since this was too large to be printed in one piece on the 3D printer, it was split in parts, which were then joined together using embedded metal stud reinforcement to hold the parts together. Quite a nice trick to make large, rigid parts.



An Adafruit Feather M0 micro-controller board, with micro SD-card slot was the brains of the project. To derive the 5 V logic data signal from the 3.3 V GPIO output of the Feather, [Mac] used two extra WS2812 LEDs as level shifters before sending the data to the LED strips. Driving all

the LEDs required almost 20 W, so he powered it using USB-C, adding a power delivery negotiation board to derive the required juice.
The Arduino code is straightforward. It reads the characters stored on the SD-card, and sends them sequentially to the 16-segment display. The circular ring around the USB bulkhead also lights up white, but at random intervals it turns red to simulate the speeding up of the centrifuges. Detecting when the USB stick gets plugged in is another nice hack that [Mac] figured out. When a USB stick is plugged in, the continuity between the shell (shield) and the GND terminal was used to trigger a GPIO input.
Cyber warfare is here to stay. We are already seeing increasing attacks on key infrastructure installations by state as well as non-state actors around the world. Stuxnet was one of the first in this growing category of malicious, weaponized code. Acknowledging its presence using such a physical representation can offer a reminder on how a few lines of software can wreak havoc just as much as any other physical weapon. Check out the brief project video after the break.

Can the Aviation Community Stop a Cyber Attack from Taking Off?

By Kylie Bielby

Source: https://www.hstoday.us/subject-matter-areas/airport-aviation-security/can-the-aviation-community-stop-a-cyber-attack-from-taking-off/

Apr 16 – Recent years have heralded myriad technological advancements including developments in machine-learning techniques, telecommunications (5G), the internet of things and more. The benefits to industries like aviation are clear. Technological advancements support growth and development, including the integration of new airspace users, the development of advanced aircraft systems and applications, automation and integration in data applications and decision-making systems in airports and airlines, and the interconnection between previously isolated systems through data-sharing across the aviation value chain.
But with new technology comes new threats, which have grown in number and scale as malicious actors use the digital world to make financial gains, cause harm, and/or create instability and chaos.
Today, the aviation sector plays a vital role transporting not only people and traditional freight, but also vaccines – representing the largest single transport challenge in its history. It is highly likely that aviation networks and other sectors associated with the vaccine

distribution supply chain will be subject to a significant volume of targeted, adversarial cyber activities during this period.

At the World Economic Forum's 'Pathways to a Cyber Resilient Aviation Ecosystem' virtual event on April 14, the International Civil Aviation Organization (ICAO) Secretary General Dr. Fang Liu explored the key cyber resilience priorities for aviation now being addressed by ICAO, noting that as the air transport sector continues to modernize and digitize, cyber risks still threaten the data, systems, and technological infrastructure of airports, airlines, and air navigation service providers, as well as many other service suppliers.

"This digital penetration will only increase with time," she explained, "especially considering the continuous innovation being seen in communications and applications, and the advent of new airspace users such as drones and Remotely Piloted Aircraft Systems."

ICAO's Aviation Cybersecurity Strategy, and a related ICAO Assembly Resolution assists countries to work together and counter aviation cyber threats while working towards rapid national adoption of the Beijing Convention and Protocol of 2010, where member countries agree to criminalize certain terrorist actions against civil aviation.

ICAO is pursuing its "living" action plan to support government progress with the Aviation Cybersecurity Strategy and related objectives, and Dr. Liu noted that the UN agency is expanding its scopetent and reviewing and refining the accountability, transparency, and efficiency by which it now addresses cyber security topics through its panels and expert groups:

ICAO's Secretariat Study Group on Cybersecurity (SSGC) serves as the focal point for all ICAO cybersecurity work. It promotes cybersecurity awareness throughout the aviation community and encourages government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts.

The Research Sub-Group on Legal Aspects (RSGLEG) was established as a necessity to review the adequacy of the existing international legal framework to address cyber threats against civil aviation and to review the draft Cybersecurity Strategy. The group continues its work and has extended its scope to categorize or analyze the cyber threats and vulnerabilities to civil aviation and associated risks. It also works to establish a common understanding and terminology of the cybersecurity language, RSGLEG reviews and analyzes the adequacy of the current international legal framework as well as assessing the need to reinterpret or amend the existing international air law instruments dealing with cyber threats legal framework or to adopt new instruments. In line with this, the group analyzes cybersecurity related international instruments developed in other international transportation and communications domains such as maritime or railway or telecommunications in order to determine whether certain provisions could serve as analogy/a reference for the aviation international legal framework.

The Working Group on Airlines and Aerodromes (WG-AAD), part of the ICAO SSGC, addresses cybersecurity matters related to airport and airline operations not related to air navigation systems or airworthiness. The group focuses on cyberspace related to facilitation, infrastructure protection, passengers and airline systems (check-in, baggage and cargo handling), and other systems not related to air navigation with a direct impact to operations.

WG-AAD advises the SSGC on cybersecurity matters related to the airport and airline operations at aerodromes and coordinates the development and/or updates of relevant Standards and Recommended Practices and Guidance Materials through the respective ICAO Panels and Study Groups. It also determines all relevant cybersecurity areas affecting airport and airline operations on the ground, not related to air navigation systems and prioritizes them accordingly for action.

Meanwhile, the Working Group on Air Navigation Systems was created to address cyber safety, security, and cyber resilience aspects of current and existing airport, air navigation and information management systems. The group focuses on, among other areas: airport interactions with air navigation systems, initial ATM system design considerations (i.e. secure-by-design); system-wide information management (SWIM) global interoperability; and air-ground, air-air and ground-ground links through all appropriate connection means.

And the Working Group on Cybersecurity for Flight Safety was created to address cyber safety, security, and cyber resilience aspects of airworthiness. This group focuses on three primary areas of airworthiness: initial design considerations (i.e. secure-by-design); modifications to in-service aircraft; and aircraft maintenance (with a specific focus on field-loadable software). Remotely Piloted Aircraft Systems are also considered within the scope of work, including the command-and-control link between the remote pilot station and the aircraft.

The first edition of ICAO's Cybersecurity Action Plan was published in November 2020. It is a living document that aims at supporting states and stakeholders in implementing the Cybersecurity Strategy. The Action Plan identified 29 Priority Actions, which are further broken down into 54 time-bound Measures and Tasks, providing the foundation for ICAO, states and stakeholders to cooperate and work together to better address cybersecurity and resilience in civil aviation.

At the virtual event, Dr. Liu noted that further improvements must still be pursued with respect to government information sharing, capacity building, and the realization of robust cybersecurity culture across the sector and its supply chains.

The World Economic Forum, host of the event, has collaborated with Deloitte on a report that aims to advance cyber resilience in the aviation sector and help identify, measure and

shape approaches to mitigate cyber risks that are endemic to technology adoption in critical infrastructure.
The report says aviation organizations should consider cyber risks in the broader context of corporate and the ecosystem's resilience, looking at both the cyber and physical elements of operational risks to their business as they become increasingly dependent on the internet and digital channels. In addition, it says organizations need to adopt a resilience mindset to govern how they would respond to and recover from any major cyber event as an extension to their robust emergency response practices for safety and physical security incidents.
ICAO designated 2020 as the Year of Security Culture (YOSC), and with the COVID-19 pandemic severely impacting aviation last year, this has been extended through 2021. As part of these efforts, ICAO has been intensifying collaboration with countries and industry in supporting efforts to promote security culture in the greater aviation community. This includes offering training, assistance and issuing guidance across all security concerns, including cyber.
2021 will of course also commemorate the 20th Anniversary of 9/11 and the worst acts of unlawful interference in the history of aviation. The importance of understanding the threat to aviation and promoting best practices in security throughout all aviation operations is therefore imperative. And the shadow of the SolarWinds hack illustrates only too clearly that protecting against unseen threats is just as vital as physical security at airports.

***Kylie Bielby** has more than 20 years' experience in reporting and editing a wide range of security topics, covering geopolitical and policy analysis to international and country-specific trends and events. Before joining GTSC's Homeland Security Today staff, she was an editor and contributor for Jane's, and a columnist and managing editor for security and counter-terror publications.*

Cyber and Physical Threats to the U.S. Power Grid and Keeping the Lights on

By Timothy M. Wintch
Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-cyber-and-physical-threats-to-the-u-s-power-grid-and-keeping-the-lights-on/

Apr 20 – Among critical infrastructure sectors in the U.S., energy is perhaps the most crucial of the 16 sectors defined by the Department of Homeland Security. This sector is so vital because it provides the energy necessary to run every other critical infrastructure sector. However, the U.S. power grid, the backbone of the energy sector, is built upon an aging skeleton that is becoming increasingly vulnerable every day. Whether from terrorists or nation-states like Russia and China, the power grid is susceptible to not just physical attacks, but also to cyber intrusion as well. However, much of this threat can be mitigated if the U.S. takes the appropriate steps to safeguard the power grid and avoid a potential catastrophe in the future.
Since Sept. 11, 2001, terrorism on U.S. soil has been at the forefront of American consciousness. Critical infrastructure provides an appealing target because of the disproportionally large impact even a small attack can have on the sectors. In particular, the power grid represents a particularly lucrative target, both in terms of the ease of access and the large impact it can make. The National Research Council stated that the U.S. power grid is "vulnerable to intelligent multi-site attacks by knowledgeable attackers intent on causing maximum physical damage to key components on a wide geographical scale."[1] Additionally, the physical security of transmission and distribution systems is difficult due to the dispersed nature of these key components, which in turn is advantageous to attackers as it reduces the likelihood of their capture.[2] From 2002-2012, approximately 2,500 physical attacks occurred against transmission lines and towers worldwide and approximately 500 attacks against transformer substations.[3] Terrorists have the motivation to attack the U.S. power grid but the very nature of the grid makes it highly vulnerable. The power grid is not only at risk from physical attacks, but also nation-state cyberattacks.
One nation that has shown both the capability and intent to use attacks against critical energy infrastructure is Russia, as demonstrated in their 2015 annexation of Crimea from Ukraine. A Russian cyber threat group known as Sandworm, which used its BlackEnergy malware, attacked Ukrainian computer systems that provide remote control of the Ukraine power grid.[4] This attack, and another in 2016, each left the capital Kiev without power, prompting cyber experts to raise concern about the same malware already existing in NATO and the U.S. power grids.[5] In any conflict between Russia and NATO, not only would similar cyberattacks pose a threat, but so would potential physical attacks severing fuel oil and natural gas lines to Western Europe. Russia has both the capability and intent to attack critical infrastructure, particularly power grids, during future conflicts in their "hybrid warfare" approach.
Another nation that has the capability to attack critical energy infrastructure is China, representing a threat to not just the U.S. energy infrastructure but also that of our allies whose support would be vital in a major conflict. A recent NATO report highlighted this threat from China's Belt and Road Initiative, stating that "[China's] foreign direct investment in strategic sectors [such as energy generation and distribution] …raises questions about

whether access and control over such infrastructure can be maintained, particularly in crisis when it would be required to support the military."[6] Like Russia, China has been active with cyber intrusions in U.S. energy infrastructure. The Mission Support Center at Idaho National Laboratory characterized these as attacks as "multiple intrusions into US ICS/SCADA [Industrial Control Systems/Supervisory Control and Data Acquisition] and smart grid tools [that] may be aimed more at intellectual property theft and gathering intelligence to bolster their own infrastructure, but it is likely that they are also using these intrusions to develop capabilities to attack the [bulk electric system], as well."[7] China, therefore, has both the capability and intent to conduct cyber intrusions and attacks for myriad reasons.

Another arm of this threat is the reliance the U.S. energy industry has on imports from China, especially transformers. In early 2020, federal officials seized a transformer in the port of Houston that had been imported by the Jiangsu Huapeng Transformer Company before sending it to Sandia National Laboratory in Albuquerque. Sandia is contracted by the U.S. Department of Energy for mitigating national security threats.[8] *The Wall Street Journal* reported that "Mike Howard, chief executive of the Electric Power Research Institute, a utility-funded technical organization, said that the diversion of a huge, expensive transformer is so unusual – in his experience, unprecedented – that it suggests officials had significant security concerns."[9] Previously destined for the Washington Area Power Administration's Ault, Colo., substation, the transformer is believed to have been seized due to "backdoor" exploitable hardware emplaced by the Chinese prior to shipment.[10] Shortly after these events, President Trump issued Executive Order 13920, "Securing the United States Bulk-Power System," essentially limiting the import of Chinese-built critical energy infrastructure components due to concerns about cybersecurity.[11] Interestingly, Jiangsu Huapeng "boasted that it supported 10 percent of New York City's electricity load."[12]

Franklin Kramer, the former Assistant Secretary of Defense for International Security Affairs, testified before a U.S. House of Representatives Energy and Commerce subcommittee during an energy and power hearing in 2011 and said that a "highly-coordinated and structured cyber, physical, or blended attack on the bulk power system, however, could result in long-term (irreparable) damage to key system components in multiple simultaneous or near-simultaneous strikes." He added that "an outage could result with the potential to affect a wide geographic area and cause large population centers to lose power for extended periods."[13] Even the inclusion of features such as smart grids to the overall grid structure poses new vulnerabilities through their connectivity. Kramer stated that "such connectivity means that the distribution system could be a key vector for a national security attack on the grid."[14]

Power generation represents a key vulnerability of the U.S. energy infrastructure. Physical security measures vary by site and type of power plant; however, most are still limited in their security measures beyond chain-link fences, with the notable exception of nuclear power plants.[15] The very nature of power plants does provide some physical security, with plants often residing in rural areas over large areas with multiple buildings, which makes locating and accessing critical components more difficult. While an attack on a power plant would have a large effect, it would also result in increased security at other plants. Finally, the nature of the U.S. energy grid provides the capability to provide some level of self-healing, meaning that even if a power plant were to go offline other sites can mitigate that loss and prevent cascading effects.

System Control Centers represent another key vulnerability. These centers contain not only important technical control systems, but also the personnel who operate those systems and their unique intricacies. However, like power plants, the physical security of these sites varies, ranging from minimal security to extensive hardening.[16] Fortunately, these centers have redundant facilities that can mitigate losses to the rest of the system.[17]

Power lines may be viewed as a key vulnerability as the most visible aspect of the transmission infrastructure, but the number of lines, ability to redirect power, coupled with the relative ease of replacement, mean that an attack on power lines is likely to be limited in both scope and duration. Therefore, while still a required part of the power infrastructure, transmission lines are not a significant vulnerability especially when other critical infrastructure sectors often have their own temporary backup power such as batteries and motor-generator sets (e.g. an on-site diesel motor running an electrical generator at a hospital).

Perhaps the most vulnerable aspect of the U.S. power grid is the high-voltage transformers that allow efficient transmission from power plants to distribution substations. Bottom line is that power generation is of no consequence if it cannot be delivered to the end user, but "there is general agreement among security planners that key high-voltage substations are the most worrisome terrorist targets within the power transmission system."[18] This fact is complicated in that the transformers are "difficult to protect" and "replacement parts are difficult to obtain, and damage to substations can separate customers from generation for long periods," often taking over a year to replace under ideal conditions.[19] As previously stated, the power industry is heavily reliant on imports for these transformers, with many coming from China. Finally, these substations are often unprotected by more than a perimeter fence, making them vulnerable to standoff and penetration attacks.[20] The critical nature of these transformers, combined with the difficulty in manufacturing and replacing them, makes the transmission substations one of the most vulnerable aspects of the U.S. power grid.

A further vulnerability of energy infrastructure is the increased use of remote-control mechanisms to operate critical equipment and manage energy loads all the way from power

generation to transmission. The more connected critical energy infrastructure is to a network, the more vulnerable it becomes to cyberattack. Kramer described the potential effects of a cyberattack in 2011, following the STUXNET attack on Iranian nuclear facilities, stating, "We have had even further confirmation of the problem of the [US power] grid's vulnerability, as demonstrated by the STUXNET attacks. STUXNET – while not grid-directed, showed the vulnerability of control machines – which are the very type of machines upon which the grid depends for effective operation."[21] This vulnerability is further described by the Mission Support Center, which stated, "Growth of networks and communication protocols used throughout ICS networks pose vulnerabilities that will continue to provide attack vectors that threat actors will seek to exploit for the foreseeable future. The interoperable technologies created for a shift toward a smart grid will continue to expand the cyberattack landscape."[22]

As evident in the example of the seized Chinese transformer in Houston, software and networks are not the only mechanisms for cyberattacks. In fact, ICS and hardware, such as transformers, present a significant vector for cyber intrusion as well.[23] The added danger of this vector is that ICS controls can be affected without the people monitoring even knowing. This was the case with STUXNET, where Iranian engineers could see that something abnormal was occurring but could not pinpoint the cause in time to avert destruction of the centrifuges.[24] Thus, vectors exist for cyberattacks in the U.S. energy infrastructure from software, networks, and malware installed in imported hardware including components such as transformers.

The Department of Defense (DoD) has utilized the Defense Critical Infrastructure program since 2005, which is focused on "identifying key defense infrastructure assets and developing guidelines and procedures for their protection," resulting in the Mission Assurance Strategy in 2012, which is designed for "strengthening the resiliency of DoD missions." [25] While the Mission Assurance Strategy is geared toward protecting the Mission Essential Functions of the DoD, it also calls for strengthening partnerships with private industry, which accounts for over 90 percent of the critical infrastructure in the U.S.[26] Ideally, the DoD would provide support to private industry to ensure that they are operating in a way that protects their infrastructure from threats. However, it is still incumbent on the private sector to accept and follow this guidance. While the DoD can provide support to help harden private electrical infrastructure, they cannot force private industry to take steps that will no doubt increase costs and cut into profit margins.

The National Research Council provides some potential ways to reduce physical vulnerability, including hardening substations and making them more difficult to locate, hardening control facilities, improved surveillance of critical sites and, most importantly, providing more robust physical security around transformer substations.[27] These safeguards are the most useful in deterring attacks against multiple points of the system, but would still provide the same utility against state-sponsored covert action. Regarding a state-level overt attack, some of these mitigation measures may be useful, but much more important is the DoD's ability to both defend the homeland as well as provide credible deterrence to nation-state actors attacking the U.S. power grid.

Some experts argue that the cyberattack threat is overexaggerated, with attacks typically limited to only causing disruption counted in days rather than weeks.[28] Robert M. Lee, CEO of cybersecurity firm Dragos, Inc., explained that even if a cyber intruder gains access to an ICS system, they would not necessarily know what to do to cause damage.[29] This could limit the potential destructive nature of a cyberattack by many hackers. A successful cyberattack by a nation-state like China or Russia would need to leverage ICS experts to fully manipulate the U.S. energy controls effectively. Yet Russia and China are unlikely to be "motivated to execute a cyberattack resulting in widespread damage to the U.S. power grid due to the political consequences such a hostile act would likely guarantee."[30] Lee addresses this fact as well, stating that, much like military cybersecurity, what is needed is active defense, which today is currently hobbled by fewer than 1,000 ICS cybersecurity experts worldwide.[31] By training and employing more of these personnel, attacks such as STUXNET become much easier to detect and defeat.[32] Only by expanding the defenses beyond passive measures can the U.S. energy infrastructure hope to continue to stave off future cyberattacks.

Kramer also provides potential solutions, highlighting the DoD's use of active and passive cyber defense, in addition to offensive cyber operations, as a model that can be extended to the power sector. Kramer suggests that the DoD oversee grid security, stating, "It would seem appropriate for the DoD with the right legislative authority and under presidential guidance to help protect electric grid networks." [33] Kramer supports this solution by paraphrasing an unnamed electric power company office: "I can understand why my company should be able to protect itself against cyber criminals, but why should I be expected to succeed against a major nation state cyberattack? Isn't that what the government is supposed to do?"[34]

The very structure of critical infrastructure in the U.S., even with much of it privatized, still provides a public necessity that must be defended. Due to the widespread public dependence on such infrastructure for not only commerce and communication, but also survival, the federal government does ultimately have the responsibility for protecting that infrastructure. However, Kramer's argument that this is the responsibility of the DoD requires a logical leap. While the DoD oversees the defense of the nation and its people, it is not required to defend private property. Ultimately, Kramer makes an effective argument that there needs to be a top-down focus on protecting the power grid, led by the federal government. However, a more suitable mechanism for achieving this goal would be through legislation and standards throughout the electric industry that harden the power grid against cyber threats.

Another potential solution is the utilization of "microgrids," described as a "grid architecture that could manage electricity generation and demand locally in sub-sections of the grid that

could be automatically isolated from the larger grid to provide critical services even when the grid at large fails," ideally preventing a cascading failure.[35] These power grids would be useful in the U.S. due to both their resiliency as well as their reliability in supporting other critical infrastructure such as water, healthcare, and emergency response infrastructure.[36] There are several disadvantages of such a power grid, including cost, increased cyber vulnerability, wider power variance, and a limited ability for self-healing. However, by incorporating microgrids as a redundancy of the main grid, mass power outages can be mitigated.[37] While microgrids are not the perfect solution, they do provide a possible path to ensuring that catastrophic failure of the U.S. power grid does not occur.

There are multiple pathways available to harden the U.S. energy infrastructure sector from a multitude of threats; however, not taking action could leave our power grid vulnerable from cyberattack resulting in massive damage, loss of life, and severe economic impacts.

▶▶ The references are available at the source's URL.

Tim Wintch *is an active-duty Major in the United States Air Force. He is currently a graduate student at the Oettinger School of Science & Technology Intelligence, National Intelligence University, in Bethesda, Maryland. Mr. Wintch has over 11 years of experience in command-and-control operations as an Air Battle Manager. He holds a Bachelor of Arts in Politics from the University of California, Santa Cruz, and a Master of Arts in Military Studies from American Military University.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Robot security dogs start guarding Tyndall Air Force Base

Source: https://www.upi.com/Defense-News/2021/03/29/robot-dogs-tyndall/9951617032912/

Mar 29 – Robot dogs, or quad-legged unmanned ground vehicles, have begun guarding Tyndall Air Force Base, Fla., the U.S. Air Force announced on Monday.

The semi-autonomous machines, which walk on four legs and resemble dogs' bodies, were integrated into the 325th Security Forces Squadron at the base on March 22.

Robot dogs have joined the 325th Security Forces Squadron at Tyndall Air Force Base, Fla. Photo by A1C Anabel Del Valle/U.S. Air Force

The Q-UGVs are not meant to replace military working dogs, officials have said, but to add another layer of protection at the base with assigned patrol paths difficult for humans and vehicles.

"As a mobile sensor platform, the Q-UGVs will significantly increase situational awareness for defenders," Mark Shackley, security forces program manager at Tyndall Air Force Base's program management office, said in a press release.

"They can patrol the remote areas of a base while defenders can continue to patrol and monitor other critical areas of an installation," Shackley said.

The robot dogs carry a variety of cameras and other sensors, can traverse difficult terrain in extreme temperatures, crouch for a lower center of gravity and have a "high-step" mode to change leg mobility.

Designed by Ghost Robotics of Philadelphia and Immersive Wisdom of Boca Raton, Fla., prototype versions of the robots have been seen at the base since November 2020.

"These dogs will be an extra set of eyes and ears while computing large amounts of data at strategic locations throughout Tyndall Air Force Base," Maj. Gen. Jordan Criss, 325th SCS commander, said in November.

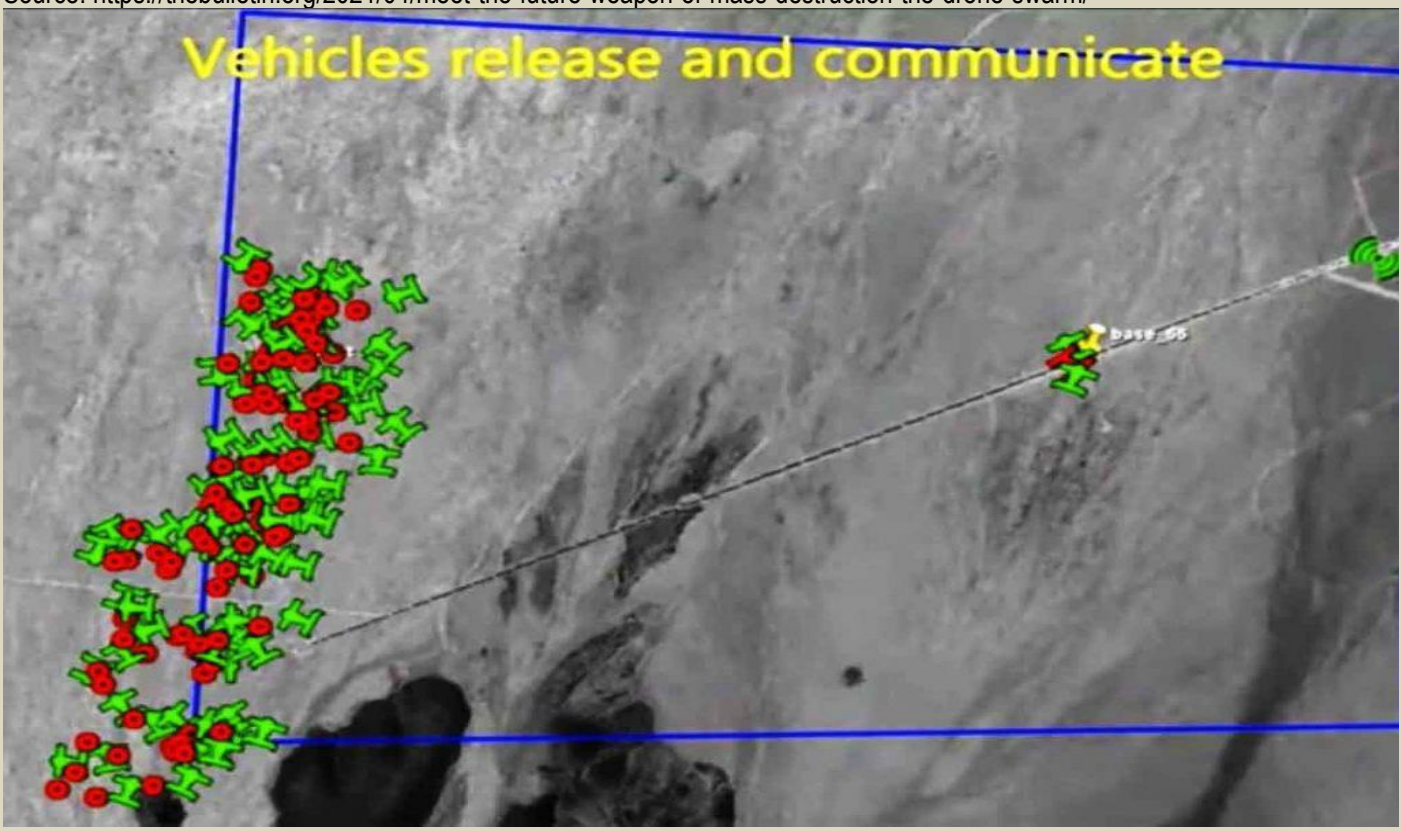
"They will be a huge enhancement for our defenders and allow flexibility in the posting and response of our personnel," Criss said.

Prototype robot dogs were first seen in September 2020 at an Advanced Battle Management System exercise at Nellis Air Force Base, Nev.
The 321st Contingency Response Squadron security team used the robots to secure an airfield after the arrival of airmen for the exercise
Tyndall Air Force Base, known as the "Installation of the Future," is regarded as an ideal test bed for the robot dogs because the base is proceeding with an ongoing reconstruction after sustaining massive damage in 2018 during Hurricane Michael.

EDITOR'S COMMENT: In the near future, the only difference with a real dog would be that they do not bark; rather they will shoot bullets if intruder does not obey their commants.

Meet the future weapon of mass destruction, the drone swarm

By Zachary Kallenborn
Source: https://thebulletin.org/2021/04/meet-the-future-weapon-of-mass-destruction-the-drone-swarm/



A US Department of Defense swarming drone test. Credit: US Department of Defense.

Apr 05 – In October 2016, the United States Strategic Capabilities Office launched 103 Perdix drones out of an F/A-18 Super Hornet. The drones communicated with one another using a distributed brain, assembling into a complex formation, traveling across a battlefield, and reforming into a new formation. The swarm over China Lake, California was the sort of "cutting-edge innovation" that would keep America ahead of its adversaries, a Defense Department press release quoted then Secretary of Defense Ash Carter as saying. But the Pentagon buried the lede: The Strategic Capabilities Office did not actually create the swarm; engineering students at the Massachusetts Institute of Technology (MIT) did, using an "all-commercial-components design."
MIT engineering students are among the best engineering students in the world, and they have the exact skills for the task, but they are still students. If drone swarming technology is accessible enough that students can develop it, global proliferation is virtually inevitable. And, of course, world militaries are deploying new drone technology so quickly that even journalists and experts who follow the issue have trouble keeping up, even as much drone swarm-related research is surely taking place outside the public eye. With many countries announcing what they call "swarms," at some point—and arguably that point is now—this technology will pose a real risk: In theory, swarms could be scaled to tens of thousands of drones, creating a weapon akin to a low-scale nuclear device. Think "Nagasaki" to get a sense of the death toll a

massive drone swarm could theoretically inflict. (In most cases, drone swarms are likely to be far below this level of harm, but such extremes are absolutely possible.)

Creating a drone swarm is fundamentally a programming problem. Drones can be easily purchased at electronics stores or just built with duct tape and plywood as the Islamic State of Iraq and Syria did. The drone swarm challenge is getting the individual units to work together. That means developing the communication protocols so they can share information, manage conflicts between the drones, and collectively decide which drones should accomplish which task. To do so, researchers must create task allocation algorithms. These algorithms allow the swarm to assign specific tasks to specific drones. Once the algorithms are created, they can be readily shared and just need to be coded into the drones.

Because battlefields are complex—with soldiers, citizens, and vehicles entering or leaving, and environmental hazards putting the drones at risk—a robust military capability still requires serious design, testing, and verification. And advanced swarm capabilities like heterogeneity (drones of different sizes or operating in different domains) and flexibility (the ability to easily add or subtract drones) are still quite novel. But getting the drones to collaborate and drop bombs is not.

Armed, fully-autonomous drone swarms are future weapons of mass destruction. While they are unlikely to achieve the scale of harm as the Tsar Bomba, the famous Soviet hydrogen bomb, or most other major nuclear weapons, swarms could cause the same level of destruction, death, and injury as the nuclear weapons used in Nagasaki and Hiroshima—that is tens-of-thousands of deaths. This is because drone swarms combine two properties unique to traditional weapons of mass destruction: mass harm and a lack of control to ensure the weapons do not harm civilians.

Countries are already putting together very large groupings of drones. In India's recent Army Day Parade, the government demonstrated what it claimed is a true drone swarm of 75 drones and expressed the intent to scale the swarm to more than 1,000 units. The US Naval Postgraduate School is also exploring the potential for swarms of one million drones operating at sea, under sea, and in the air. To hit Nagasaki levels of potential harm, a drone swarm would only need 39,000 armed drones, and perhaps fewer if the drones had explosives capable of harming multiple people. That might seem like a lot, but China already holds a Guinness World Record for flying 3,051 pre-programmed drones at once.

Experts in national security and artificial intelligence debate whether a single autonomous weapon could ever be capable of adequately discriminating between civilian and military targets, let alone thousands or tens of thousands of drones. Noel Sharkey, for example, an AI expert at the University of Sheffield, believes that in certain narrow contexts, such a weapon might be able to make that distinction within 50 years. Georgia Tech roboticist Ronald Arkin, meanwhile, believes lethal autonomous weapons may one day prove better at reducing civilian causalities and property damage than humans, but that day hasn't come yet. Artificial intelligences cannot yet manage the complexities of the battlefield.

Drone swarms worsen the risks posed by a lethal autonomous weapon. Even if the risk of a well-designed, tested, and validated autonomous weapon hitting an incorrect target were just 0.1 percent, that would still imply a substantial risk when multiplied across thousands of drones. As military AI expert Paul Scharre rightly noted, the frequency of autonomous weapons' deployment and use matters, too; a weapon used frequently has more opportunity to err. And, as countries rush to develop these weapons, they may not always develop well-designed, tested, or validated machines.

Drone communication means an error in one drone may propagate across the whole swarm. Drone swarms also risk so-called "emergent error." Emergent behavior, a term for the complex collective behavior that results from the behavior of the individual units, is a powerful advantage of swarms, allowing behaviors like self-healing in which the swarm reforms to accommodate the loss of a drone. But emergent behavior also means inaccurate information shared from each drone may lead to collective mistakes.

The proliferation of swarms will reverberate throughout the global community, as the proliferation of military drones already has echoed. In the conflict between Armenia and Azerbaijan, Azeri drones proved decisive. Open-source intelligence indicates Azeri drones devastated the Armenian military, destroying 144 tanks, 35 infantry-fighting vehicles, 19 armored personnel carriers, and 310 trucks. The Armenians surrendered quickly, and the Armenian people were so upset they assaulted their speaker of parliament.

Drone swarms will likely be extremely useful for carrying out mass casualty attacks. They may be useful as strategic deterrence weapons for states without nuclear weapons and as assassination weapons for terrorists. In fact, would-be assassins launched two drones against Prime Minister Nicolas Maduro in Venezuela in 2018. Although he escaped, the attack helps illustrate the potential of drone swarms. If the assassins launched 30 drones instead, the outcome may have been different.

Drone swarms are also likely to be highly effective delivery systems for chemical and biological weapons through integrated environmental sensors and mixed arms tactics (e.g. combining conventional and chemical weapons in a single swarm), worsening already fraying norms against the use of these weapons.

Even if drone swarm risks to civilians are reduced, drone swarm error creates escalation risks. What happens if the swarm accidentally kills soldiers in a military not involved in the conflict?

Countries need to build global norms and treaties to limit drone swarm proliferation, especially in the worst cases. From including swarms in and re-energizing UN discussions

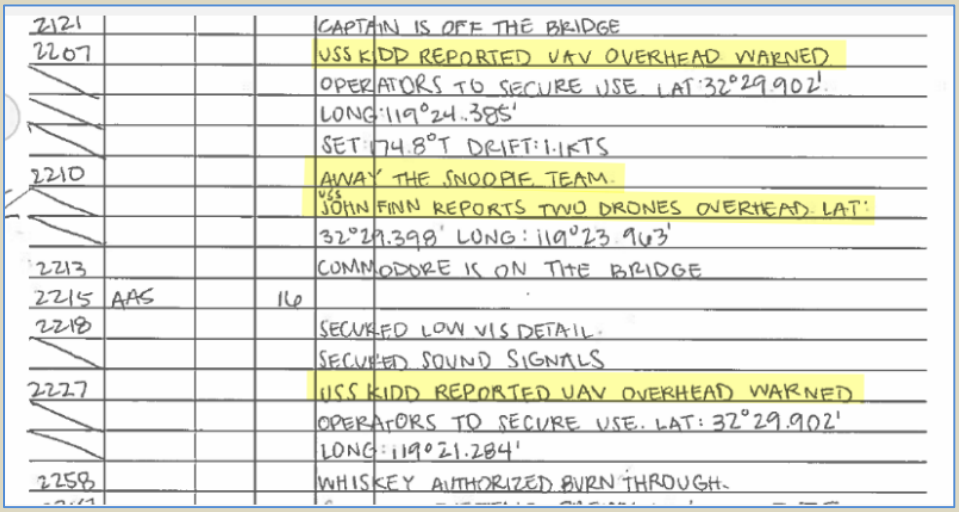
about lethal autonomous weapons to working to prevent the technology from proliferating, there are many steps the international community should take to limit the risks of swarms. Simple transparency might go a long way. The UN register on conventional arms should include a general category on unmanned systems with a sub-category for swarming-capable drones. This way the global community could better monitor the weapons' proliferation.
The world needs to debate the growing threat of drone swarms. This debate shouldn't wait until lethal drone swarms are used in war or in a terrorist attack but should happen now.

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

Navy's Top Officer Says 'Drones' That Swarmed Destroyers Remain Unidentified

By Adam Kehoe and Marc Cecotti
Source: https://www.thedrive.com/the-war-zone/40071/navys-top-officer-says-mysterious-drones-that-swarmed-destroyers-remain-unidentified

Apr 05 – At a roundtable with reporters today, Chief of Naval Operations Admiral Michael Gilday, the U.S. Navy's top officer, was asked about a series of bizarre incidents that took place in July 2019 and involved what only have been described as 'drones' swarming American destroyers off the coast of Southern California. *The War Zone* was the first to report in detail on this series of mysterious events after the incident was originally uncovered by filmmaker Dave Beaty.
Asked by Jeff Schogol of *Task & Purpose* if the Navy had positively identified any of the aircraft involved, Gilday responded by saying: "No, we have not. I am aware of those sightings and as it's been reported there have been other sightings by aviators in the air and by other ships not only of the United States, but other nations – and of course other elements within the U.S. joint force."


2121 CAPTAIN IS OFF THE BRIDGE
2207 USS KIDD REPORTED UAV OVERHEAD WARNED
OPERATORS TO SECURE USE LAT 32°29.902'
LONG 119°24.385'
SET 174.8°T DRIFT 1.1KTS
2210 AWAY THE SNOOPIE TEAM.
USS JOHN FINN REPORTS TWO DRONES OVERHEAD LAT:
32°29.398' LONG: 119°23.963'
2213 COMMODORE IS ON THE BRIDGE
2215 AAS 160
2218 SECURED LOW VIS DETAIL.
SECURED SOUND SIGNALS
2227 USS KIDD REPORTED UAV OVERHEAD WARNED
OPERATORS TO SECURE USE. LAT: 32°29.902'
LONG: 119°21.284'
2258 WHISKEY AUTHORIZED BURN THROUGH.

"Those findings have been collected and they still are being analyzed," Gilday added. "I don't have anything new to report, Jeff, on what those findings have revealed thus far. But I will tell you we do have a well-established process in place across the joint force to collect that data and to get it to a separate repository for analysis."
At the time of writing, it is unclear if Admiral Gilday was referring to the Department of Defense's Navy-led Unidentified Aerial Phenomena Task Force (UAPTF), created last August to examine "incursions by unauthorized aircraft into our training ranges or designated airspace." A Senate-requested report on Unidentified Aerial Phenomena is expected later this year. Representatives from the UAPTF could not be reached for comment.
A preliminary response to our Freedom of Information Act (FOIA) inquiries indicates that the Office of Naval Intelligence (ONI) possesses documents about the incident and that they are intermingled with records from several other agencies. This would make sense as the UAPTF was established within ONI, according to the Senate Select Committee on Intelligence.
Schogol also asked if there was any suspicion that the aircraft described as drones were "extraterrestrial." Gilday responded, "No, I can't speak to that - I have no indications at all of that."
The War Zone has reached out to the Navy, Coast Guard, and the Federal Bureau of Investigation for further details regarding the drones flying near Navy destroyers in 2019.

Members of the intelligence and armed services committees in both the Senate and the House were asked for comment, as well. While at least some elected officials indicated they were aware of the issue, none were able to make a statement at this time regarding the encounters off the coast of Southern California two years ago.

▶▶ **Read also:** https://www.thedrive.com/the-war-zone/39913/multiple-destroyers-were-swarmed-by-mysterious-drones-off-california-over-numerous-nights

AI, Augmented Reality Could Allow Terrorists to Wage More 'Spectacular' Attacks, Intel Warns

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/ai-augmented-reality-could-expand-terrorists-capability-for-spectacular-attacks-intel-report-warns/

An ISIS member with a U.S.-made Egyptian military drone seized in 2020. (ISIS photo)

Apr 12 – Global jihadist groups taking advantage of poorly governed regions to entrench will likely be the "largest, most persistent" terrorism threat over the next 20 years as other extremist groups from white supremacists to anti-government movements are poised for a revival, according to an intelligence report focused on future predictions and probabilities.

And while easy-to-obtain conventional weapons will likely remain the attack method of choice for the near future, "technological advances, including AI, biotechnology, and the Internet of Things, may offer opportunities for terrorists to conduct high-profile attacks by developing new, more remote attack methods and to collaborate across borders," as well as virtually bringing terrorists together to train in augmented reality environments, the National Intelligence Council report said.

NIC released Thursday *Global Trends 2040: A More Contested World*, the seventh edition of its quadrennial Global Trends report, an unclassified assessment delivered to incoming or returning presidential administrations since 1997 analyzing how developments in demographics, the environment, economics, and technology will shape the national security landscape over the next two decades.

The Office of the Director of National Intelligence said a "wide variety of experts, domestically and internationally, were consulted by the NIC as it conducted its analysis," but "the final report represents the views of the NIC."

"Terrorist groups will continue to exploit societal fragmentation and weak governance to push their ideologies and gain power through violence. During the next 20 years, regional and

intrastate conflicts, demographic pressures, environmental degradation, and democratic retrenchment are likely to exacerbate the political, economic, and social grievances terrorists have long exploited to gain supporters as well as safe havens to organize, train, and plot," the report said.

"These accelerants, the intensity and effects of which are likely to be uneven across different regions and countries, probably will also foster rural to urban international migration, further straining state resources and diminishing global and local counterterrorism efforts."

NIC predicted that global jihadist groups such as al-Qaeda and ISIS "are likely to be the largest, most persistent transnational threat as well as a threat in their home regions," buoyed by "a coherent ideology that promises to deliver a millenarian future, from strong organizational structures, and from the ability to exploit large areas of ungoverned or poorly governed territory, notably in Africa, the Middle East, and South Asia."

Right-wing and left-wing extremists "promoting a range of issues — racism, environmentalism, and anti-government extremism, for example — may revive in Europe, Latin America, North America, and perhaps other regions."

While naturally waxing and waning as conflicts and resultant stakeholders change, "insurgent groups and sectarian conflicts — increasingly around ethno-nationalist and communal causes — will also continue to foster terrorism," the report added. Also, efforts of Iran and Hezbollah to "solidify a Shia 'axis of resistance' also might increase the threat of asymmetric attacks on U.S., Israeli, Saudi, and others' interests in the Middle East."

Assessing the future tactics of terrorists, NIC said the next two decades will see most terrorists continuing to use "generally sufficient, accessible, and reliable" weapons such as small arms and improvised explosive devices.

"Terrorists will also seek weapons of mass destruction and other weapons and approaches that will allow them to conduct spectacular mass casualty attacks," the report added, noting ISIS' use of mustard gas attacks and use of drone delivery. "Autonomous delivery vehicles guided with the help of AI systems could enable a single terrorist to strike dozens of targets in the same incident. Augmented reality environments could also enable virtual terrorist training camps, connecting experienced plotters protected by distant sanctuaries with potential operatives."

While technological innovations could help terrorists strike more efficiently, technology will also help the counterterrorists dig deeper into areas ranging from identification to tracking. For example, tech that expands surveillance capacity "may help governments to combat terrorists despite challenges posed by poor governance," the report notes.

"Governments are likely to continue dramatically expanding the amount and types of information they collect as well as the tools to sort and organize that data. Advances in biometric identification, data mining, full-motion video analysis, and metadata analysis will provide governments with improved capabilities to identify terrorists and plotting," NIC said. "Development of precision long-range strike capabilities might undermine terrorist safe havens that are inaccessible to police or infantry forces."

Meanwhile, shifting international power dynamics are likely to throw some hurdles at efforts to combat terrorism worldwide.

The report cites "the rise of China and major power competition" among these factors that "are likely to challenge U.S.-led counterterrorism efforts and may make it increasingly difficult to forge bilateral partnerships or multilateral cooperation on traveler data collection and information-sharing efforts that are key to preventing terrorists from crossing borders and entering new conflict zones."

"Poor countries probably will struggle with homegrown threats, particularly if international counterterrorism assistance is more limited," NIC warned. "Some countries facing existential threats, such as insurgencies in which terrorists are active, may choose to forge non-aggression pacts that leave terrorists free to organize within their borders and others compelled to submit to terrorist rule over significant parts of their territory."

Bridget Johnson *is the Managing Editor for Homeland Security Today. A veteran journalist whose news articles and analyses have run in dozens of news outlets across the globe, Bridget first came to Washington to be online editor and a foreign policy writer at The Hill.*

Adversary Drones Are Spying On The U.S. And The Pentagon Acts Like They're UFOs

By Tyler Rogoway

Source: https://www.thedrive.com/the-war-zone/40054/adversary-drones-are-spying-on-the-u-s-and-the-pentagon-acts-like-theyre-ufos

Apr 15 – We may not know the identities of all the mysterious craft that American military personnel and others have been seeing in the skies as of late, but I have seen more than enough to tell you that it is clear that a very terrestrial adversary is toying with us in our own backyard using relatively simple technologies—drones and balloons—and making off with

what could be the biggest intelligence haul of a generation. While that may disappoint some who hope the origins of all these events are far more exotic in nature, the strategic implications of these bold operations, which have been happening for years, undeterred, are absolutely massive.

Our team here at *The War Zone* has spent the last two years indirectly laying out a case for the hypothesis that many of the events involving supposed UFOs, or unidentified aerial phenomena (UAP), as they are now often called, over the last decade are actually the manifestation of foreign adversaries harnessing advances in lower-end unmanned aerial vehicle technology, and even simpler platforms, to gather intelligence of extreme fidelity on some of America's most sensitive warfighting capabilities.

The U.S. Navy's Nomad drone, an electronic warfare payload-carrying system, looks totally bizarre and would have flight characteristics that would appear very strange to someone who had no idea it exists.

Now, considering all the news on this topic in recent weeks, including our own major story on a series of bizarre incidents involving U.S. Navy destroyers and 'UAP' off the Southern California coast in 2019, it's time to not only sum up our case, but to discuss the broader implications of these revelations, what needs to be done about them, and the Pentagon's fledgling 'UAP Task Force' as a whole.

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

World's First Industrial UAV in Payload and Distance Combination

Source: https://i-hls.com/archives/108060

Apr 15 – Mining, oil and gas, and other industries using drones for inspection are often limited by the drone flight distance, the complexity of cumbersome configuration, small payload capacity, failure to work in low or high temperatures, etc.

A hybrid, commercial UAV combining the take-off and landing maneuverability of multirotor drones and the increased payload and endurance of fixed-wing drones is designed to fill the gap. It is reportedly the world's first industrial UAV to outperform other models in its class in both payload capacity and distance coverage.

A plug-and-play payload module design allows for various use cases.

The **FIXAR drone** manufactured by the Latvian company FIXAR UAVs has recently undergone testing. During testing, the UAV was used in the Elbrus mountain range – Europe's highest point at 4500m above sea level – to create an accurate map (using orthophotography) as part of geodesic surveys for the construction of a cable car in mountainous terrain.

At altitudes with increased windiness, as well as challenging terrain, the drone maintained stability, functionality, was able to land within two-meter accuracy, and only required two minutes of flight prep time.

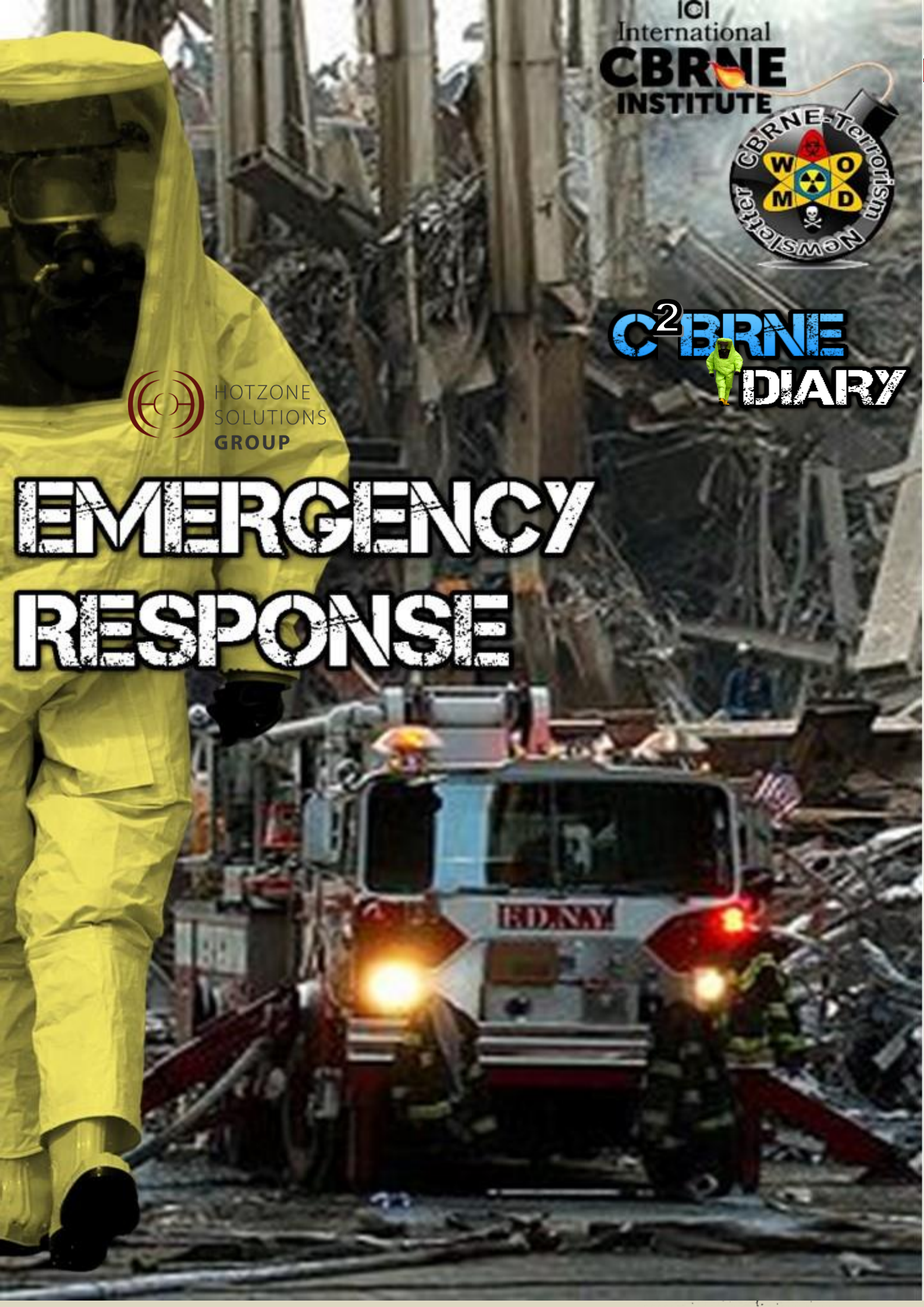
According to the company, "while most VTOL fixed-wing drones require that the angle of the motors change when transitioning from vertical to horizontal flight, the **FIXAR 007** model uses a patented Fixed Angled Rotor system, meaning fewer moving parts or potential points of failure. Transitions are seamless, and all motors are in use throughout missions.

"The benefits of the FIXAR UAV ensure that drone operators can attach heavier payloads, including LiDAR or a combo of RGB and multispectral cameras. They are more versatile in terms of maneuverability and have longer airtime and distance – covering up to 400 hectares in a single flight or mapping 60 km of roads, railways, and pipelines.

"The combined benefits of the hybrid design means that FIXAR is able to replace drones with separate uses, and is able to complete in one flight what might otherwise require multiple flights. Field experience also has demonstrated that only two minutes are required for flight preparation, meaning that fewer operator hours are required per flight," the company was cited in commercialdroneprofessional.com.

Mass drone swarms

Chinese games and entertainment company Bilibili held a one-year anniversary show in Shanghai for the mobile game Princess Connect! 1,500 drones took part in the show to celebrate the game has been out for one year in China.


ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
C2BRNE
DIARY
HOTZONE
SOLUTIONS
GROUP
EMERGENCY
RESPONSE
FDNY

Science for Disaster Risk Management 2020

Acting Today, Protecting Tomorrow

Source: https://drmkc.jrc.ec.europa.eu/Knowledge/Science-for-DRM/Science-for-Disaster-Risk-Management-2020

Mar 23 – The Disaster Risk Management Knowledge Centre has produced the **"Science for disaster risk management 2020: acting today, protecting tomorrow"**, the second of its series.
The report represents a collaborative effort of **more than 300 experts on disaster risk**, coming from different sectors and disciplines, that worked for more than 2 years together to present the consequences of disasters on various assets at risk (population, economic sectors, critical infrastructures, ecosystem services and cultural heritage).Studying the impacts helps in managing risk after a disaster, guiding the response and facilitating recovery, and in preparing measures to prevent, mitigate and prepare for future events, by supporting risk prediction and the planning of measures to manage risk.
Tackling the impacts on assets at risk, the report deals with hazards of different natures, highlighting the many links existing between hazards and vulnerabilities to support robust and effective action.The various chapters and subchapters **provide specific recommendations for the target audience**, four groups of stakeholders that can actively contribute to reducing disaster risk: **policymakers**, **practitioners** (such as civil protection groups, critical infrastructure operators and organised civil groups directly engaged in disaster response), **scientists** and **citizens**.
To move **from identifying problems to the presentation of solutions and approaches**, the report describes several examples and cases, showing what the DRM community has learned from disastrous events while pointing out where the gaps in our knowledge are.
All the input provided is finally brought together in the conclusions to **provide guidance to the stakeholders** on working together across sectors, disciplines and organisations to reduce disaster risk.
Below you can find the latest version of the Executive Summary and the entire document, as well as the specific chapters, sub-chapters and Super Case Studies of the report.

Download

- Executive summary of the report Science for Disaster Risk Management 2020: acting today, protecting tomorrow: English (3.5Mb - PDF) – Download
- Science for Disaster Risk Management 2020: acting today, protecting tomorrow: English (45Mb - PDF) – Download

FINAL REPORT: The Security of National Infrastructure

Source: https://www.domesticpreparedness.com/commentary/final-report-the-security-of-national-infrastructure/

Feb 28 – This report and survey is the result of aggregating and compiling opinions of both the DomPrep40 and DomPrep Readers. Both groups were asked how they view the apparent transition from thinking in terms of critical infrastructure protection to thinking in terms of critical infrastructure resilience. To assist both groups in developing their own ideas and recommendations, Dennis Schrader, former FEMA deputy administrator for preparedness, drafted a seven-question to-the-point survey.
Schrader says, "The results are not surprising. We have work to do to create an integrated network of public safety officials and the engineering community."

Key Finding: DomPrep members are more skeptical than the DomPrep40 are about the tangible preparedness outcomes deriving from the National Infrastructure Protection Plan (NIPP) both in the private sector and in state and local public safety agencies.

▶▶ **Click for Full Report**

New Technology to Revolutionize Firefighting Operations

Source: https://i-hls.com/archives/107987

Apr 09 – A groundbreaking tracking and location technology will soon allow emergency agencies to pinpoint their firefighters to within centimeters, helping to navigate them quickly and safely out of potentially disorienting emergency scenarios.

The **POINTER** (Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders) technology, a wearable and portable, cost-effective system, has been developed by the US Department of Homeland Security Science and Technology Directorate (S&T), working hand-in-hand with first responders to build this system to their specifications.

"From containing small kitchen fires to carrying civilians out of burning homes to securing local infrastructure, first responders put their lives on the line daily to ensure the safety of their communities," said Greg Price, who leads S&T's first responder research and development programs. "The reality is, even with all of the advances made in firefighting technology, we still lose far too many firefighters each year. We want them to know that we have their backs, that we are working to give them the tools they need to ensure their own safety. POINTER is that solution."

S&T has collaborated with the NASA Jet Propulsion Laboratory (JPL) in Southern California and first responder stakeholders since 2014 to develop POINTER that could succeed where existing products may fail.

For instance, technologies that use GPS, acoustic sensors, radio location, radio-frequency identification, ultra-wideband radar or other methods often lose signal or face position drift in line-of-sight denied environments. Many can't penetrate through certain building materials or even reach underground.

POINTER can do all of this and more, making it both more accurate and reliable. It uses magnetoquasistatic (MQS) fields to three-dimensionally track and locate responders in low-visibility environments.

The system operates in three parts: a transmitter, a receiver, and a base station – a laptop computer located at incident command.

What is now the size of a cell phone will ultimately be reduced in scale and potentially integrated into existing firefighting equipment.

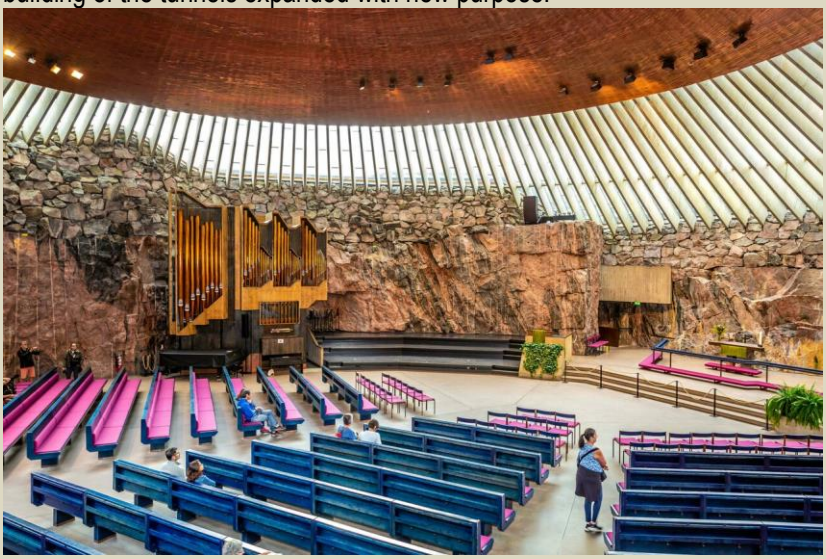
Since development began, POINTER has evolved from a technology that could track first responders to within three meters of accuracy to now locating them within centimeters of their actual position, according to hstoday.us.

How Cold War Fears Helped Create Helsinki's Subterranean Paradise

Source: https://www.atlasobscura.com/articles/helsinki-underground-city-emergency-shelter

Mar 22 – Nearly 200 miles of tunnels snake beneath Helsinki, providing a weatherproof subterranean playground for the Finnish capital's residents and visitors. Yet hidden behind the bright lights of the underground attractions—which include a museum, church, go-kart track, hockey rink, and more—are emergency shelters fitted with life-sustaining equipment: an air filtration system, an estimated two-week supply of food and water, and cots and other comforts. The shelters

reflect a chilling geopolitical reality for a small country that shares an 833-mile border with Russia, its longtime nemesis.
Thought to be the world's only city with an underground master plan, Helsinki began excavating tunnels through bedrock in the 1960s to house power lines, sewers and other utilities. City planners quickly realized that the space could also be home to retail, cultural, and sporting attractions—and that it could shelter the city's population of 630,000 in the event of another invasion from the East. The building of the tunnels expanded with new purpose.



Tomi Rask, a preparedness instructor for the city of Helsinki's rescue department, says the alternative purpose of the tunnels is to "save people against the actions of war." No Finnish government official would ever mention Russia as the reason for such defensive preparations, but they don't have to.

Below the bustling streets of Helsinki, Temppeliaukio Church is one of several subterranean sites that attract locals and tourists alike. Subodh Agnihotri/Alamy

"You can plan and prepare without having to point out who explicitly your challengers or adversaries are, because it's clear to everyone," says Charly Salonius-Pasternak, chief researcher for the Finnish Institute of International Affairs. "Finland points out who its friends are, Sweden, the U.S., and so on, but there's no point in pointing out who the adversary could be because there's only one and everyone knows who it is."
Growing up in Helsinki during the late Cold War era, Salonius-Pasternak enjoyed the tunnels' convenience, calculating how far he could walk underground between stores without putting on his winter clothes. Today, Salonius-Pasternak specializes in the country's security and defense policies, including peacekeeping and crisis management.
Salonius-Pasternak says Finland's history with Russia is long and complicated. The Russian Empire took Finland from Sweden in 1809 as a result of the Finnish War and operated it for a little more than a century as the autonomous Grand Duchy. When the Soviet Union was formed out of revolution, Finns declared independence in 1917. The following year, after a brief but bloody civil war, the Soviet-aligned Red faction lost to the White faction, which vowed to remain free and Western.
Then came World War II, when the Soviets twice invaded Finland, ostensibly to take enough land to form a protective buffer around Leningrad, modern-day St. Petersburg. Twice the greatly outnumbered Finnish army repelled the Soviets, but both times Finland was forced to sign peace treaties that resulted in a loss of territory along its eastern border.

At the Underground Formula Center beneath eastern Helsinki's Myllypuro neighborhood, go-kart enthusiasts race around a course. Courtesy of City of Helsinki

During the Cold War, Helsinki stood at the crossroads of the East and West, one of the last major outposts separating the NATO and Warsaw Pact superpowers. In recent times, Russian President Vladimir Putin has warned Finland more than once against joining NATO, an uneasy reminder of past tensions.
Yet on a typical winter day, when the city receives only a handful of daylight hours, Helsinki's underground master plan becomes manifest as a way to navigate the city, guiding residents and tourists along bright, colorful passageways lined with markets and shops, to metro stations and the central railway station, while providing shelter from the elements.

The Itäkeskus swimming hall doubles as an emergency shelter beneath Helsinki. Courtesy of City of Helsinki

"It's comfortable and safe," says Eija Kivilaakso, Helsinki's chief underground planner. "If it's raining, you can drive into the city center to an underground car park and go straight into department stores from elevators. You can dress for comfort instead of in cold-weather clothes. If the weather is not comfortable, people choose the underground."

One of the underground's shining stars is Temppeliaukio, a church carved into solid bedrock. Completed in 1969, its stunning features and superb acoustics have made it one of Finland's most popular architectural attractions, drawing more than 850,000 visitors a year.

Gray = current underground facilities and tunnels, Light Blue = planned future underground tunnels and facilities, Blue =Existing, Brown = bedrock resources near the surface suitable for the underground construction

A more recent addition is the privately built Amos Rex art museum, which earned acclaim by the BBC as one of Europe's most innovative architectural spaces when it opened in 2018. Its 23,500-square-foot exhibition hall, largely featuring modernist works, was built completely underground because the adjoining building, housing its offices and a movie theater, is protected from expansion. The museum was an immediate hit, with long lines and sold-out exhibitions before the coronavirus pandemic.

■ **Read also:** https://www.hel.fi/static/liitteet/kaupunkiymparisto/julkaisut/esitteet/esite-02-19-en.pdf

Like stone mushrooms sprouting in a city square (top), skylights for the underground Amos Rex art museum allow natural light to flood exhibit spaces (bottom). Courtesy of Tuomas Uusheimo/Amos Rex

"When the Amos Rex was [built], that became a very good thing for our underground master plan," says Kivilaakso. "We saw that it was possible to have more private facilities down there, which gives us more space above ground. It lets us know we don't have to build large stores or electricity stations or car parks on the ground. We have them underground."

Whether offering cultural enrichment through art or the simple convenience of getting groceries before heading home on the subway, Helsinki's underground seems far removed from the doomsday scenarios the bustling tunnels have been readied to face.

"The average Finn spends very little time thinking about Russia, never mind being afraid of Russia," Salonius-Pasternak says. "Most people don't think of it in terms of 'now I'm going into the metro and let me notice all these things that are built in here because it needs to be a functioning bomb shelter, as opposed to just a functioning metro station.'

Enhancing medical preparedness to meet the changing threat of terrorism

By Derrick Tin

Source: https://www.aspistrategist.org.au/enhancing-medical-preparedness-to-meet-the-changing-threat-of-terrorism/

Apr 23 – **Counterterrorism medicine**, or CTM, is a new medical subspeciality born out of the increasingly devastating and complex terrorist attacks taking place around the world. High-profile terrorist attacks in major cities have seemingly become a regular occurrence and mass-casualty events continue to challenge healthcare systems.

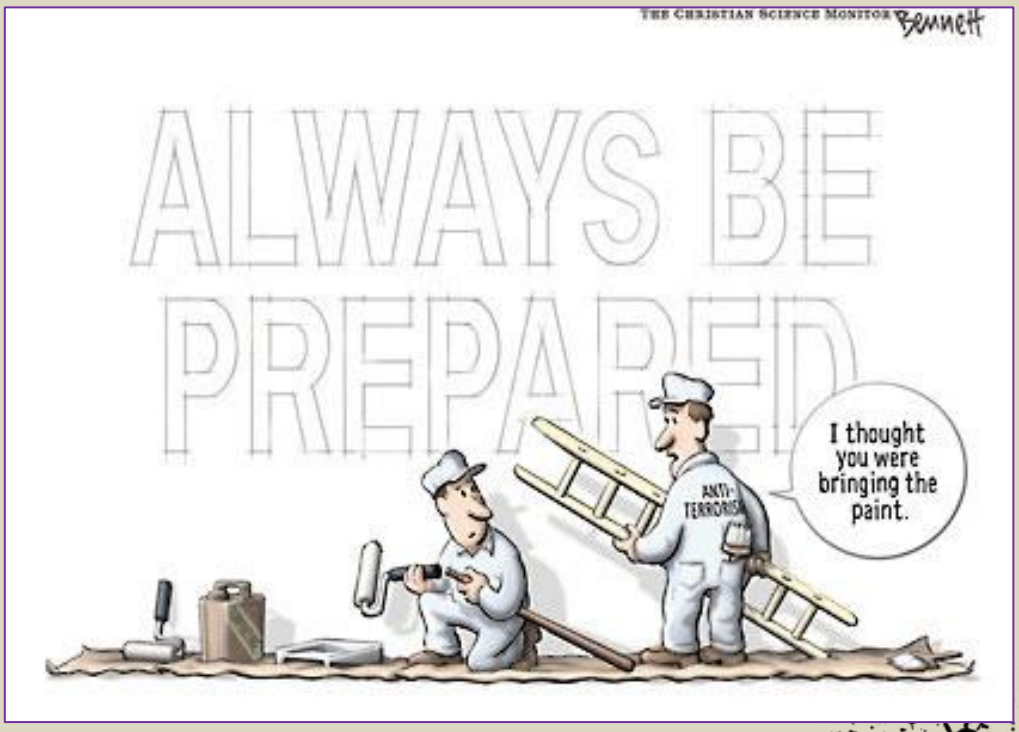
Terrorism events have a distinct difference from other man-made disasters such as transport or industrial accidents. While most potential man-made sources of disastrous events incorporate safety measures to minimise victim impact in case something goes wrong, terrorist events have the opposite aim: they are designed to maximise death and destruction.

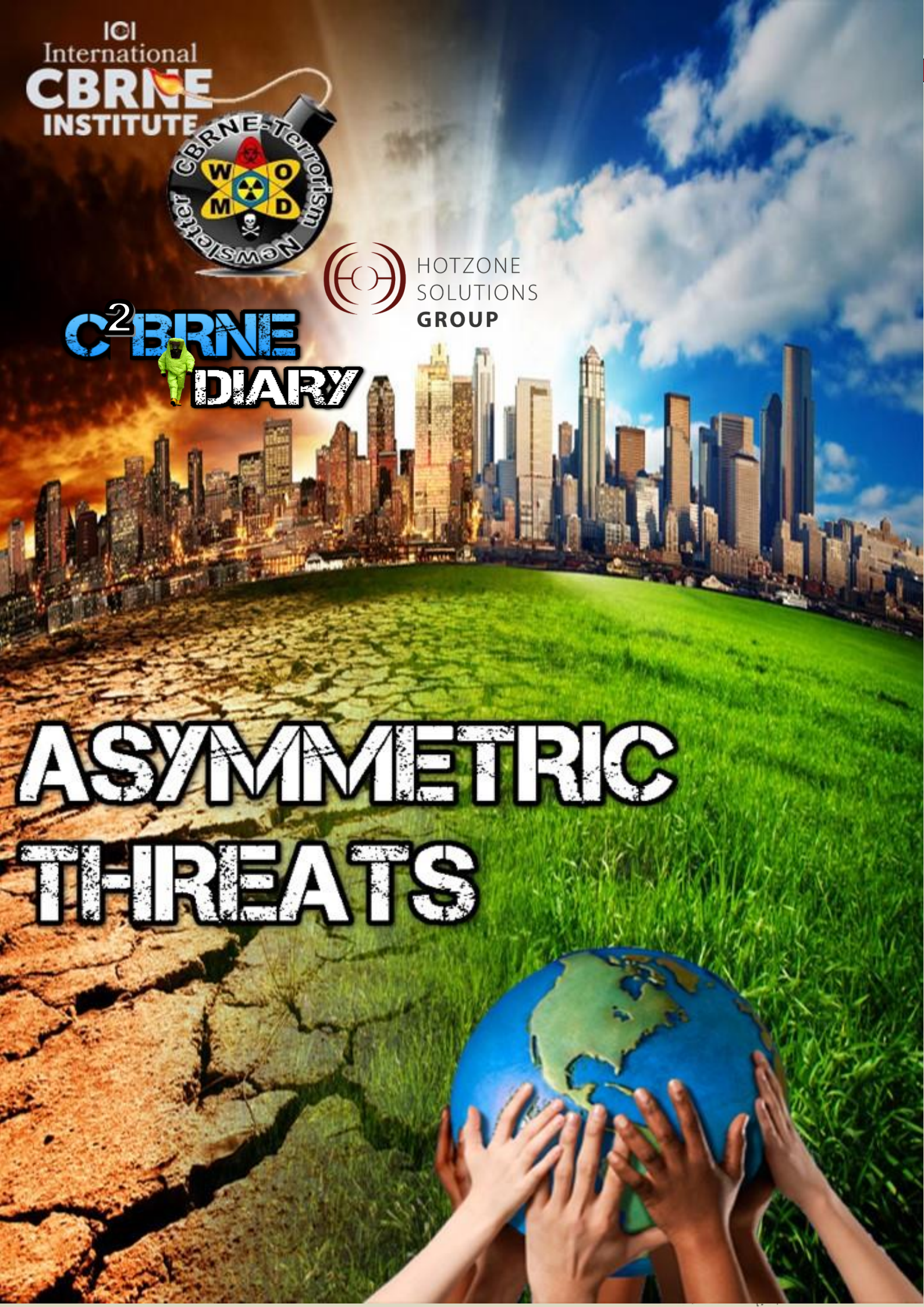
CTM takes a collaborative, multidisciplinary approach to mitigating these healthcare strains by looking at plausible as well as theoretical risks, doing risk assessments and providing solutions.

Right-wing, white supremacist and political extremist groups have been exploiting the anti-government, anti-freedom sentiments associated with the Covid-19 pandemic, not just to recruit socially or lockdown-isolated vulnerable individuals but also to openly parade their skewed narrative. And that has potentially significant implications. While the terrorists of old tended to be secretive and hidden, were usually found in developing countries, and historically relied on bombs and guns as an attack methodology, we are now seeing a new breed of terrorists

who are much more open, are much more technologically savvy and have a lot more access to a wider range of weapons.
The recent lye-poisoning attack in Florida is a good example of how rogue actors can leverage new technologies to cause harm in a way we haven't necessarily come across before. Crop-spraying drones can easily be reappropriated to deliver toxic or deadly chemicals purchased on the black market. With advanced swarm technology, they can also be preprogrammed to simultaneously strike multiple soft targets using an array of attack modalities. The use of nanotechnology in experimental weapons such as dense inert metal explosives, or DIME, is raising biotoxicity concerns and creating injury patterns previously unseen. CTM specialists need to consider how new and emerging technologies alter or create new mass-casualty scenarios that can exploit vulnerabilities in medical preparedness.
While CTM specialists spend time looking ahead at new technologies, we also need to better understand and learn from historic methodologies and the healthcare aftermath of terrorist attacks. The Tokyo sarin gas attack and the Moscow theatre siege exposed historic and ongoing deficiencies in education and training on recognising toxic syndromes, or toxidromes, in chemical weapons attacks. Law enforcement and medical personnel who responded to these attacks were not adequately prepared to deal with the effects of the toxic gases on either themselves or the initial victims.
This realisation led to the recent publication of an easy-to-use clinical algorithm for first responders to quickly identify potential chemicals deployed and provide antidotes where available. Analysis of injuries caused by both suicide and non-suicide bombings has provided insight to medical providers on blast wounds and patterns and given rise to new suggestions in blast-mitigation strategies.
While understanding past methodologies has important educational value, policymakers need to be forward-looking in anticipating the new or unexpected. The emergence of CTM as a disaster medicine subspecialty addresses the unique terrorism-related issues relating to mitigation, preparedness and response measures to asymmetric, multi-modality terrorist attacks. Healthcare facilities and medical responders are at risk of being the primary or secondary targets of attacks, and risk mitigation strategies for them also need to be reviewed and vulnerabilities addressed.
Addressing the healthcare complexities within CTM requires collaboration among specialists and experts in disaster medicine, counterterrorism, tactical medicine and law enforcement to ensure streamlined, coordinated strategies in dealing with future terrorist events.

Derrick Tin *is a senior fellow in disaster medicine at Harvard Medical School*.




ICI
International
CBRNE
INSTITUTE
CBRNE-Terrorism Newsletter
W
O
M
D
HOTZONE
SOLUTIONS
GROUP
C2BRNE
DIARY
ASYMMETRIC
THREATS

Climate change should be recognized for what it is: an issue of national security

By Rod Schoonover
Source: https://thebulletin.org/premium/2021-01/climate-change-should-be-recognized-for-what-it-is-an-issue-of-national-security/

Jan 2021 – By most accounts, President-Elect Biden looks to position climate change as a central organizing principle in his Executive Branch. Through cabinet appointments of sympathetic experts at agencies not normally at the fore of environmental policy—such as Treasury, Justice, and Transportation—Biden hopes to deliver wide-ranging wins on climate policy. The EPA, the Energy Department, and the Interior Department will be redeployed in Obama-era roles as key instruments for aggressive climate action. These would all be positive steps forward.

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

Rod Schoonover *is the founder of the Ecological Futures Group, a senior fellow at the Council on Strategic Risks, and a senior fellow at the Center for Strategic and International Studies. From 2009 to 2019 he was a senior US intelligence scientist and analyst at the National Intelligence Council and State Department. He is an adjunct professor in Georgetown University's School of Foreign Service and Emeritus Professor of Physical Chemistry at Cal Poly, San Luis Obispo, California.*

Climate Change Must Be Tackled as a Global Security Risk

By Joshua Busby, Morgan Bazilian, and Florian Krampe
Source: https://reliefweb.int/report/world/climate-change-must-be-tackled-global-security-risk

Mar 10 – When the United Nations put out emergency appeals for modest amounts of money to help Syria with the drought that preceded its civil war, they were dramatically underfunded—member states only provided a quarter of the amount requested in 2008, and a third in 2009. The United States did not contribute.
Scholars believe the displaced were among those who ultimately joined the protests and revolution that the Syrian government violently suppressed. While early intervention on its own may not have prevented the conflict in Syria, suppose small investments in drought preparedness and response could help us avoid such catastrophes in the future. Would that not be money well spent?
We live in an age of "actorless threats"—where challenges to peace and security come not only from agents intentionally trying to do us harm, but also from climate change and pandemics whose impacts are no less severe.
Climate change poses escalating risks to stability and security, with potentially far-reaching consequences, from the risks to fragile states from more volatile weather to the combined effects of rising sea levels and storm surge on the survival of island nations and coastal populations.
United States President Joseph Biden has said climate change is an "existential threat" to national security. He appointed former US Secretary of State John Kerry as special presidential envoy for climate, with a seat on the country's National Security Council. Biden has already issued a series of executive orders directing the country's intelligence agencies to assess the risks and for other parts of government to examine the links between climate change and migration.
While these are important actions, the security risks of climate change, like the broader problem itself, cannot be addressed by the US alone—nor are the solutions solely or even primarily military ones. Ultimately, the US will need partners.

Historic Opportunity to Highlight Climate Security
In March, the US will serve as the rotating president of the UN Security Council for one month. The Security Council is the right place to start, given its key role in managing peace and security in the international system. The Biden administration's new team at the United Nations has an historic opportunity to raise the profile of climate security concerns, but it needs a strategy.
In the past few years, the Security Council has paid more attention to climate security concerns. Prompted by Sweden, the UN created a small Climate Security Mechanism in 2018 to help the United Nations more systematically address climate-related security risks and devise prevention and management strategies. The Security Council also recognized the role of climate change in complicating peace operations in African conflicts, including those in Mali, Sudan, and Somalia.
In July 2020, Germany led a high-level debate on climate change and security at the Security Council and proposed several new measures to raise the profile of climate and security concerns, including creating the post of a special representative, developing an enhanced early warning system, and incorporating climate security in all peace operation mandates.

However, the administration of former US president Donald Trump quashed any hopes of a joint Security Council resolution.

Beyond Mitigation to Prevention

President Biden has an opportunity with elected members Security Council members like Ireland, Kenya, and Norway to propose new policies that would bring visibility and build capacity to address these gathering risks. These could include reviving the German proposal but going beyond them.

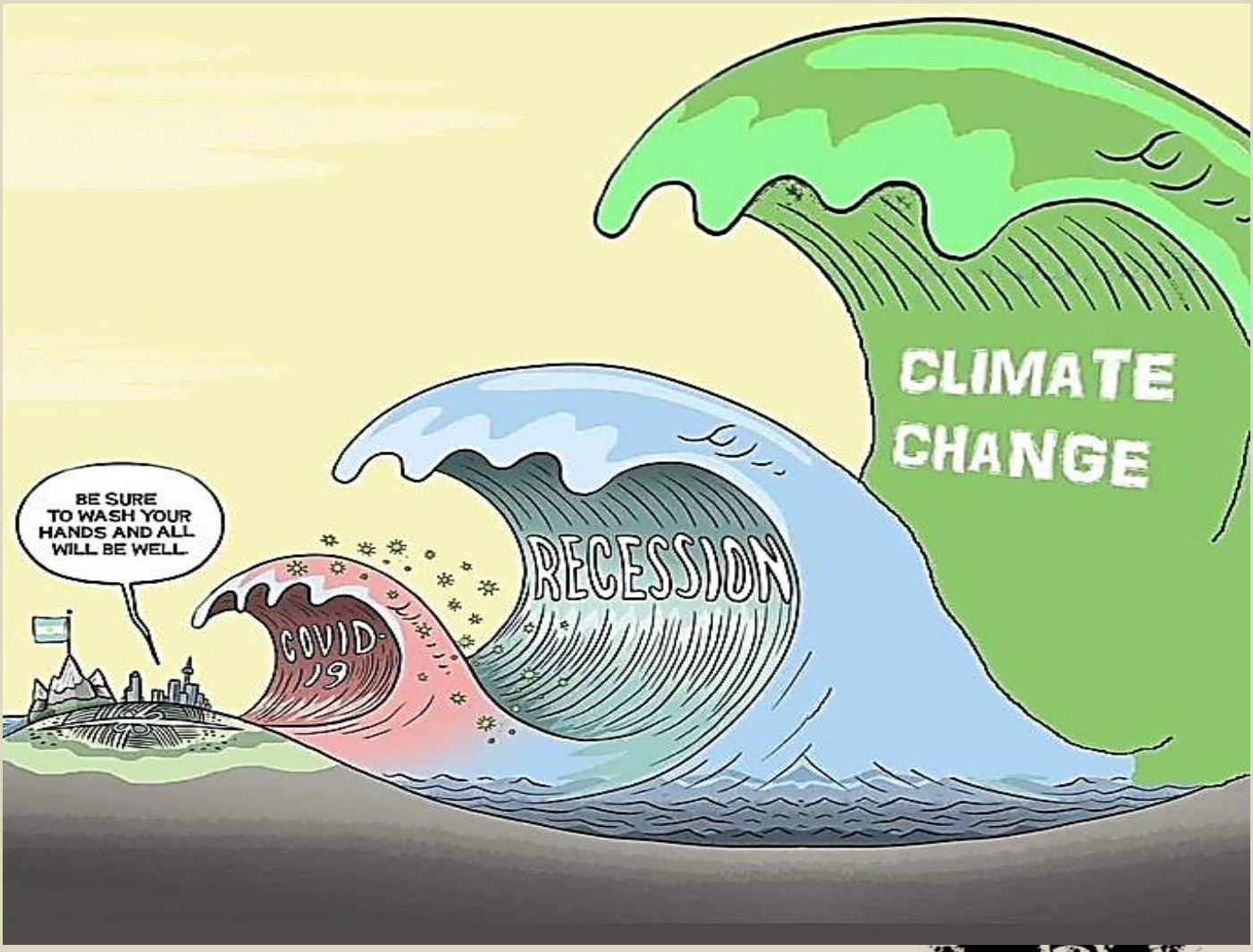
For example, the Security Council thus far has been reluctant to talk about the risks posed by climate change to low-lying island countries. The US could seek to bring that issue to the fore. Moreover, we know that climate change and wider environmental damage are increasing the risks of disease transmission from animals to humans. The United States could spur on conversation on ecological security and how to protect the basic life-sustaining functions of the planet.

To date, the Security Council has primarily focused on ongoing conflicts and how climate change might have had a role in causing or extending them. Prevention of climate-related security risks has received relatively little attention. The US should initiate a dialogue on what capacities are needed to prevent climate-related conflicts, building on the recently released strategy for the 2019 Global Fragility Act which is intended to identify problems early and diminish the risks of escalation.

While Linda Thomas-Greenfield, the US ambassador to the UN, may be chairing the Security Council's work this month, success will require building support and overcoming skepticism from Russia and China that the Council is the right place to discuss climate change at all.

Joshua Busby *is an associate professor at the Lyndon B. Johnson School of Public Affairs at the University of Texas at Austin.*

Morgan Bazilian *is director of the Payne Institute for Public Policy and a professor at Colorado School of Mines.*



Florian Krampe *is senior researcher and director of the Climate Change and Risk program at the Stockholm International Peace Research Institute.*