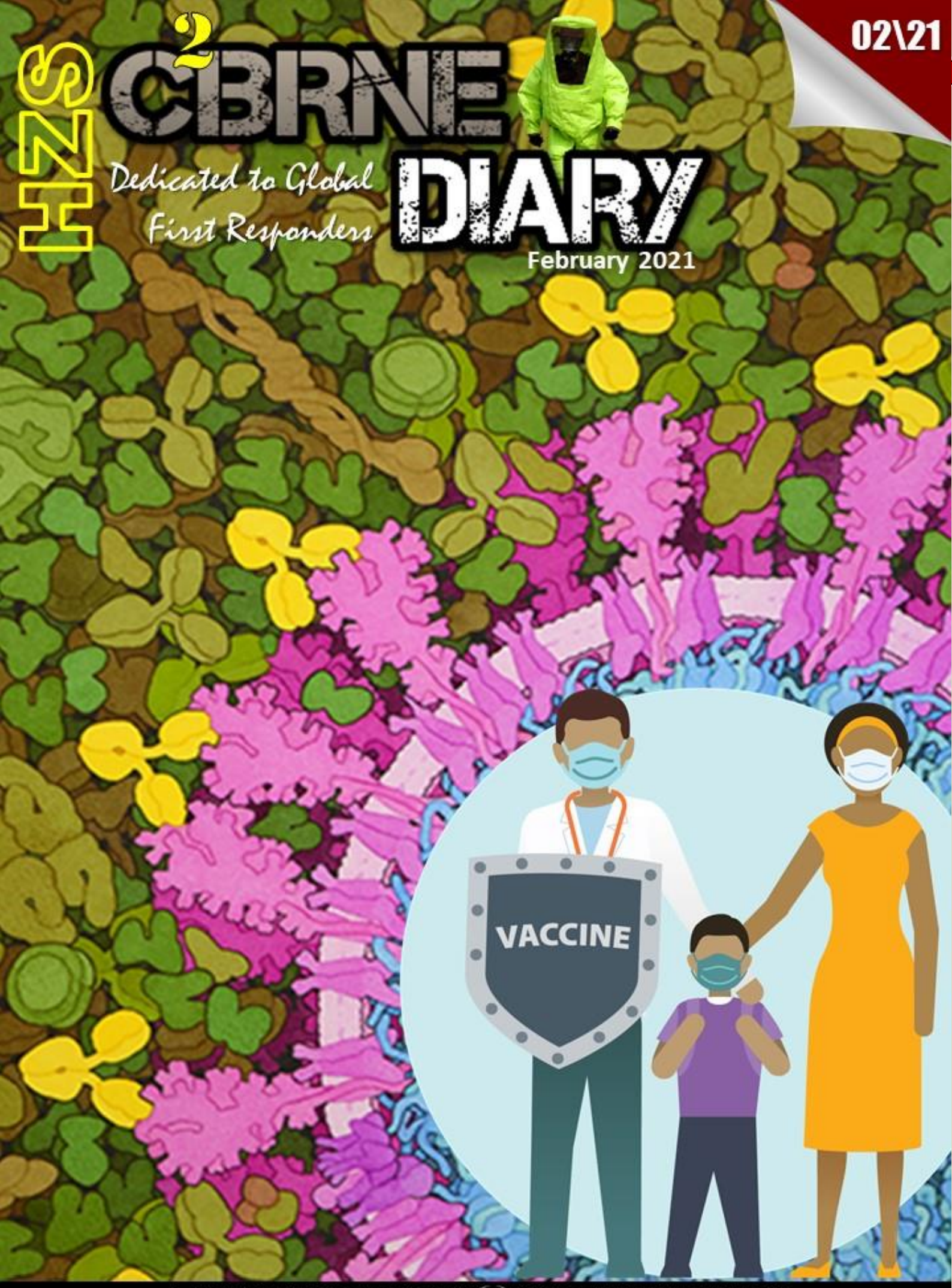
02\21

HZS

CBRNE DIARY

Dedicated to Global First Responders

February 2021



A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

DIRTY R-NEWS

Here's how much a nuclear weapon cost

Source: https://www.cnbc.com/2017/08/08/heres-how-much-a-nuclear-weapon-costs.html

North Korea's official Korean Central News Agency (KCNA) shows North Korean leader Kim Jong-Un (2nd R) inspecting the test-fire of the intercontinental ballistic missile Hwasong-14 on July 4, 2017 – STR | Getty Images

Aug 2017 – Brinkmanship between the United States and North Korea around the subject of nuclear weapons has experts worldwide worried about heightened "tensions." On a practical level, just how expensive are these bombs?

To determine the cost of one nuclear weapon, you have to account for the costs of their production, delivery systems and maintenance.

"South Korean government analysis has put North Korea's nuclear spending at $1.1 billion to $3.2 billion overall," reported Reuters last year, "although experts say it is impossible to make an accurate calculation given the secrecy surrounding the program, and estimates vary widely."

The U.S. government believes North Korean leader Kim Jong Un has up to 60 nuclear weapons, though some independent experts say the total is smaller. If North Korea does indeed have around 60, that puts the cost of each warhead at between around $18 million and $53 million.

The U.S. nuclear program provides a more reliable picture of cost, though not all nuclear development information is public. In "Atomic Audit," published in 1998, Stephen I. Schwartz claimed the U.S. had spent $5 trillion since 1940 on developing and maintaining its nuclear arsenal.

The U.S. government is now estimated to have 6,800 nuclear weapons at its disposal, but America hasn't actually built a new warhead or bomb since the 1990s. "It has refurbished several types in recent years to extend their lifetime," says Dr. Lisbeth Gronlund, a senior scientist and co-director of the UCS Global Security Program.

This picture taken on May 14, 2017 and released from North Korea's official Korean Central News Agency (KCNA) shows North Korean leader Kim Jong-Un (3rd R) inspecting a ballistic rocket at an undisclosed location – STR | AFP | Getty Images

The B61-12 atomic bombs (left photo), for instance, are to undergo a life-extension program that will cost roughly $9.5 billion. There are 400 to 500 of these bombs, says Gronlund, which means refurbishing **one will cost about $20 million.**

W-80 warheads, another type being refurbished, are estimated to cost $75 million each when you account for the price tag of the B52 bombers that deliver them. Frank G. Klotz, the national administrator of the Nuclear Security Administration, estimated that the total cost of the W-80 life extension plan will be $7.3 billion to $9.9 billion over 17 years.

Gronlund predicts that, in total, the U.S. will spend $250 billion on its nuclear program in the next few decades.

As for North Korea, the new U.N. sanctions that China and Russia agreed to impose on Saturday will likely set it back. The banned exports is expected to cost them a third of their annual $3 billion earnings.

U.S. analysts believe North Korea has nuclear warheads that can fit inside of missiles, the Washington Post reported on Tuesday. The insight comes just weeks after the regime fired a missile that landed within 230 miles of the Japanese coast. In response, on Tuesday, President Trump told reporters that "North Korea best not make any more threats to the United States," or "they will be met with fire and fury like the world has never seen."

It's time to take domestic nuclear terrorism seriously

By Jayita Sarkar

Source: https://www.washingtonpost.com/outlook/2021/01/27/its-time-take-domestic-nuclear-terrorism-seriously/

Jan 27 – How can the new Biden administration address the threat of domestic terrorism, most vividly illustrated by the attempted insurrection at the U.S. Capitol on Jan. 6? Last week, 20,000 members of the National Guard were deployed for the inauguration to protect the new administration from far-right extremist violence, but a more serious threat looms. Nuclear and radiological terrorism has prominently appeared in "apocalyptically minded" white-supremacist ideology for decades.

The policy community perceives the threat of nuclear terrorism as almost uniquely emanating from outside of U.S. borders, specifically from Islamist terrorism networks such as the Islamic State, al-Qaeda and their splinter groups. But in fact, U.S. far-right extremist groups have a history of attempted procurement of nuclear weapons and radiological materials to use against the federal government. Members of neo-Nazi groups such as Atomwaffen Division, which literally means "atomic weapons" in German, and the National Socialist Movement have attempted in the past to access nuclear materials with the intent to cause harm.

Fears of nuclear terrorism among U.S. policymakers go back at least to the 1970s, when armed insurgencies intensified in the Middle East. The 1972 Munich massacre by the Palestinian group Black September and the 1973 oil price shock that suddenly empowered petroleum-exporting countries fueled concerns of a violent, non-White, Muslim world. India's 1974 nuclear explosion, Pakistan's nuclear weapons acquisition in response and new nuclear energy programs funded by petrodollars in Iran, Libya, Iraq and elsewhere further fanned fears of nuclear materials falling into "rogue" hands. In 1979, as the Iran hostage crisis played out on national television for over a year, the idea of radical Islam as a security threat became entrenched in U.S. political culture.

But nuclear terrorism was also a domestic threat in the 1970s. Nuclear power was expected to grow that decade, and a large amount of plutonium (a radioactive material used in nuclear weapon design) was feared to be widely available. By the end of the decade, white-power activists, many of whom were Vietnam War veterans hardened by military training, had organized for a violent armed struggle of "leaderless resistance" against the federal government. To them, the government was the source of unacceptable societal change that hurt White Christian Americans.

In 1978, William Pierce, the founder of the neo-Nazi group National Alliance, published the novel "The Turner Diaries" under the pseudonym Andrew Macdonald. It sold over 500,000 copies worldwide and remains highly popular among white supremacists.

In the novel, right-wing extremists invade the Capitol to overthrow the U.S. government. Its narrator, Earl Turner, gloats that "not one of them is beyond our reach." Dubbed by the FBI as the "bible of the racist right," the novel depicts 18 nuclear explosions in Manhattan alone and the destruction by nuclear weapons of Baltimore, Miami, the California coast and Detroit. It also provides plans to deliberately contaminate with radioactive materials a nuclear power plant in Evanston, Ill. The novel ends with Turner detonating a nuclear bomb over the Pentagon. He justifies the nuclear explosions and sabotage against non-White populations and "race criminals" (liberal Whites) in the name of establishing white supremacy in the United States and worldwide.

"The Turner Diaries" has inspired racially motivated armed robberies and more than 200 killings in the United States. It greatly influenced Timothy McVeigh, the Oklahoma City bomber, who perpetrated the deadliest domestic terrorist attack on U.S. soil that killed 168 people in April 1995.

The book has received renewed attention after the attack on the Capitol. Amazon has prevented its sale, and major news outlets have reported on its influence over far-right and white-supremacist groups. The analogies are chilling.

The violent white-supremacist ideology that calls for nuclear and radiological attacks against non-White populations has spread outside the United States.

Norwegian far-right terrorist **Anders Behring Breivik**, who killed 77 people in July 2011, had called for the use of chemical, biological, radiological and nuclear agents against "cultural Marxists," "multiculturalists" and those responsible for the Islamic "colonization" of Europe. In his 1500-page manifesto, he laid out plans for theft or unauthorized access to nuclear weapons and the procurement of nuclear materials through transnational smuggling networks. Breivik recommended the use of radiological agents and nuclear weapons after Jan. 1, 2020 — his deadline for Muslims in Europe to "assimilate." Given the leaderless transnational networks of white supremacists, the call for nuclear and radiological attacks in Breivik's manifesto as well as "The Turner Diaries" poses grave concerns.

Policy experts reassure us that if taken seriously as a threat, nuclear terrorism is both preventable and solvable. That violent white supremacists can easily infiltrate the police, the military and nuclear facilities make them an extremely serious and hard-to-detect national security risk. The involvement in the Capitol attack of the Oath Keepers, a far-right anti-government group that recruits former U.S. military and law enforcement personnel, demonstrates the extent of this threat. Screening far-right extremists within government institutions at local, state and federal levels needs to be a priority for the Biden administration.

The key to preventing such a catastrophic attack will be moving beyond a one-dimensional understanding of terrorism as the violent threat of radical Islam, and better understanding the different ways in which far-right domestic terrorism has grown in the United States and the specific threats this brings. Despite ample evidence to support the concern that insider threats pose high security risks in nuclear and radiological environments, little has been done at the policy level.

The threat of nuclear terrorism is such that we must act preemptively, not after a devastating attack. The lessons of the past tell us that action will involve breaking down the artificial border between foreign and domestic policies. National security does not just mean preventing attacks from abroad. The siege of the Capitol came close to being far worse, and there are indications that some rioters intended to harm lawmakers. But just because we escaped the worst does not mean we can rest easy. We must be proactive to prevent far-right domestic terrorism from going nuclear in this country.

Jayita Sarkar is assistant professor of international relations at Boston University's Frederick S. Pardee School of Global Studies.

United States nuclear weapons, 2021

By Hans M. Kristensen and Matt Korda

Source: https://www.tandfonline.com/doi/pdf/10.1080/00963402.2020.1859865

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 associ-ate with the project. The Nuclear Notebook column has been

Type/Designation	No.	Year deployed	Warheads x yield (kilotons)	Warheads (total available)[1]
ICBMs				
LGM-30 G Minuteman III				
Mk-12A	200	1979	1–3 W78 x 335 (MIRV)	600[2]
Mk-21/SERV	200	2006[3]	1 W87 x 300	200[4]
Total	400[5]			800[6]
SLBMs				
UGM-133A Trident II D5/LE 240[7]				
Mk-4A		2008[8]	1–8 W76-1 x 90 (MIRV)	1,511[9]
Mk-4A		2019	1–2 W76-2 x 8 (MIRV)[11]	25[10]
Mk-5		1990	1–8 W88 x 455 (MIRV)	384
Total	240			1,920[12]
Bombers				
B-52H Stratofortress	87/44[13]	1961	ALCM/W80-1 x 5–150	528
B-2A Spirit	20/16	1994	B61-7 x 10–360/-11 x 400 B83-1 x low-1,200	322
Total	107/60[14]			850[15]
Total strategic forces				3,570
Nonstrategic forces				
F-15E, F-16 DCA	n/a	1979	1–5 B61-3/-4 bombs x 0.3–170[16]	230
Total				230[17]
Total stockpile				3,800
Deployed				1,800[18]
Reserve (hedge and spares)				2,000
Retired, awaiting dismantlement				1,750
Total Inventory				5,550

published in the Bulletin of the Atomic Scientists since 1987. This issue examines the status of the US nuclear arsenal. The US nuclear arsenal remained roughly unchanged in the last year, with the Defense Department maintaining an estimated stockpile of approximately 3,800 warheads. Of these, only 1,800 warheads are deployed, while approximately 2,000 are held in reserve. Additionally, approximately 1,750 retired warheads are awaiting dismantlement, giving a total inventory of approximately 5,550 nuclear warheads. Of the approximately 1,800 warheads that are deployed, 400 are on land-based intercontinental ballistic missiles, roughly 1,000 are on submarine-launched ballistic missiles, 300 are at bomber bases in the United States, and 100 tactical bombs are at European bases.

***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 writ-ing 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.*

***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.*

The world is facing an upsurge of nuclear proliferation

To stop it, the nuclear powers need to act

Source: https://www.economist.com/leaders/2021/01/30/the-world-is-facing-an-upsurge-of-nuclear-proliferation

Jan 30 – THIRTY-ONE countries, from Brazil to Sweden, have flirted with nuclear weapons at one time or another. Seventeen launched a formal weapons programme. Just ten produced a deliverable bomb. Today nine states possess nuclear arms, no more than a quarter-century ago. Yet the long struggle to stop the world's deadliest weapons from spreading is about to get harder.

Iran Enriched "17 Kilograms" of 20 Percent Enriched Uranium, Exceeding Nuclear Pact's Limits

Source: http://www.homelandsecuritynewswire.com/dr20210201-iran-enriched-17-kilograms-of-20-percent-enriched-uranium-exceeding-nuclear-pact-s-limits

Feb 01 – Iran's parliament speaker says the country has produced 17 kilograms of 20 percent-enriched uranium within a month, as Iranian officials continue to dismiss international calls for Tehran to return to full compliance with the 2015 nuclear agreement.
Mohammad Bagher Qalibaf made the announcement during a visit to the Fordow nuclear plant on January 28.
In separate comments, the spokesman of Iran's Atomic Energy Organization, Behruz Kalamvandi, confirmed Qalibaf's estimate, saying there are currently 17 kilograms of enriched uranium stockpiles with a 20 percent purity in the country.
Iran, which denies pursuing nuclear weapons, saying its nuclear program is strictly for civilian purposes, has vowed to produce 120 kilograms of uranium enriched to 20 percent per year, or 10 kilograms per month on average.

About 250 kilograms of 20 percent-enriched uranium are needed to convert it into 25 kilograms of the 90 percent-enriched needed for a nuclear weapon.

Western countries have called on Tehran to adhere to the 2015 nuclear deal with world powers, from which the United States unilaterally withdrew in 2018.
In response to the U.S. pullout and crippling sanctions, Iran has gradually breached parts of the pact, which eased international sanctions in exchange for curbs on its disputed nuclear program, saying it is no longer bound by it.
On January 27, newly installed U.S. Secretary of State Antony Blinken said the administration of President Joe Biden was willing to return to commitments under the nuclear agreement, known as the Joint Comprehensive Plan of Action (JCPOA), but only if Iran returned to full compliance.
In response, Iranian Foreign Minister Mohammad Javad Zarif reiterated Tehran's view that the United States should first lift its sanctions.
"Reality check for @SecBlinken," Zarif tweeted, saying the United States "violated" the accord by imposing sanctions on Iran that "blocked food/medicine to Iranians," among other grievances.
Zarif argued that Iran had "abided by the JCPOA" and only took "foreseen remedial measures" to the U.S. moves.

"Now, who should take 1st step?" he asked.

Iran installs advanced centrifuges at Natanz, Fordow nuclear sites: Envoy

Source: https://www.globalsecurity.org/wmd/library/news/iran/2021/iran-210202-presstv02.htm

Feb 02 – Iran's representative to the Vienna-based organizations says the country has installed new cascades of advanced centrifuges at two nuclear sites in Natanz and Fordow to increase enrichment capacity.
"Thanks to our diligent nuclear scientists, two cascades of 348 IR2m centrifuges with almost 4 times the capacity of IR1 are now running with UF6 successfully in Natanz," Kazem Gharibabadi said in a post on his Twitter account on Tuesday.
He added that Iran also started the installation of two "cascades of IR6 centrifuges" at its Fordow nuclear facility.
"There's more to come soon," the ambassador said.
In another tweet, Gharibabadi said Iran has informed the International Atomic Energy Agency of the progress as planned, adding that the IAEA "is yet able to verify."

Back in May 2018, former US President Donald Trump pulled Washington out of the multilateral nuclear agreement, officially known as the Joint Comprehensive Plan of Action (JCPOA), reached between Iran and major world states in 2015 and adopted the so-called maximum pressure campaign against Iran with the declared aim of forcing Tehran to negotiate a new deal.

Iran remained fully compliant with the JCPOA for an entire year but as the remaining European parties failed to fulfill their end of the bargain, Iran began in May 2019 to scale back its JCPOA commitments under Articles 26 and 36 of the accord covering Tehran's legal rights.

In one of its latest steps away from the deal, Iran on January 4 announced the beginning of the process to enrich uranium to 20-percent purity at Fordow in its latest step to reciprocate the American withdrawal and the European failure.

New US President Joe Biden, who was vice president when the deal was signed, has said he hopes to return Washington to the deal. However, his foreign policy team has said Iran should take the first step by coming back into "full compliance" with the JCPOA.

Iran, however, says it will only reverse its reciprocal measures if the United States lifts its sanctions as a prelude to rejoining the deal.

U.S. signs five-year New START nuclear arms treaty renewal

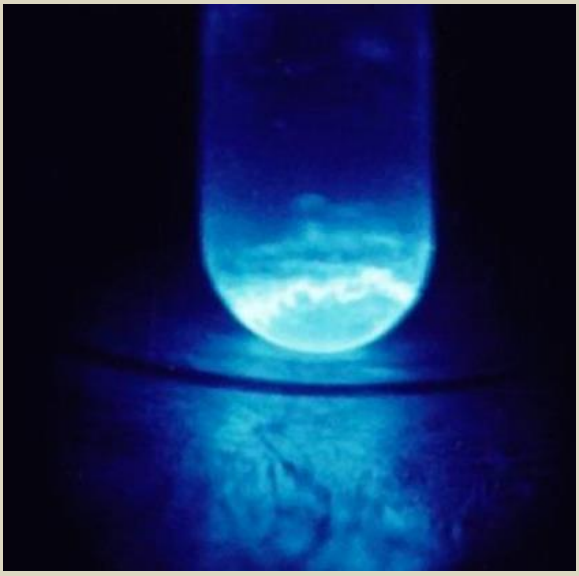
Source: https://www.upi.com/Defense-News/2021/02/03/US-signs-five-year-New-START-nuclear-arms-treaty-renewal/1451612373315/

Feb 03 – U.S. Secretary of State Antony Blinken on Wednesday announced the U.S. signed a five-year extension of the New START arms control treaty with Russia, which Russian President Vladimir Putin also signed last week. The treaty allows the United States and Russia to monitor each other's nuclear forces, facilities and activities and, with the signing, will now run through Feb. 5, 2026.

Mysterious Element 'Einsteinium' Measured by Scientists for The First Time

Source: https://www.sciencealert.com/chemists-have-carried-out-the-first-ever-measurements-on-the-element-einsteinium

Feb 03 – Dragons lurk at the edges of the map of known elements – atomic giants so delicate, and so scarce, they defy easy study.



One such behemoth has finally given up at least some of its secrets, with chemists managing to gather just enough einsteinium to flesh out important details on the mysterious element's chemistry and ability to form bonds.

For the better part of 70 years, isotopes of einsteinium have proven frustratingly difficult to study. Either they're way too hard to make, or they have a half-life of less than a year, and what precious little is created begins to fall apart like a sandcastle at high tide.

Glow of radiation from 300 micrograms of einsteinium (Haire, R.G./US Department of Energy/PD)

The element's behaviour is presumed to follow the patterns of its less robust peers in the actinide series. That much is clear. But due to its sheer size, strange relativistic effects make it harder to predict how it will react in certain chemical processes.

Usually, such confusion is easily cleared up by simply conducting a run of experiments.

The US Department of Energy's Lawrence Berkeley National Laboratory has finally scooped together enough of the stuff to do just that.

More informally referred to as the Berkeley Lab, the famous institute is already responsible for the discovery of a significant chunk of the upper bounds of the periodic table of elements.
A dozen of them were the work of nuclear physicist Albert Ghiorso, a life-long Berkeley researcher whose early career saw him develop radiation detectors as part of the Manhattan Project.
In the early 1950s, Ghiorso detected faint traces of two as-yet unidentified radioactive elements in airborne dust collected by planes flying through the aftermath of the first full-scale test of a thermonuclear device.
One of those elements was later dubbed einsteinium, named after none other than the famous German-born theorist himself.
With an atomic mass of 252, and containing a whopping 99 protons, it's no lightweight. As with all transuranic elements – elements heavier than uranium – einsteinium requires some serious physics to produce.
There's no convenient source or stockpile to dip into. Cooking up a batch requires shooting smaller relatives, like curium, with a bunch of neutrons in a nuclear reactor, and then having a lot of patience.
Early efforts in the 1960s produced just enough to see with the naked eye, weighing in at a minuscule 10 nanograms. Later attempts managed a little better, though mostly resulting in impure batches.
This time, researchers came up with around 200 nanograms of the einsteinium isotope E-254, framed as part of a complex with a carbon-based molecule called hydroxypyridinone.
Getting this far wasn't easy, marred by contamination of smaller elements, and then the inevitable impact of mid-pandemic shutdown – just the thing to threaten an experiment dependent on a rapidly decaying material.
"It's a remarkable achievement that we were able to work with this small amount of material and do inorganic chemistry," says researcher Rebecca Abergel.
"It's significant because the more we understand about its chemical behaviour, the more we can apply this understanding for the development of new materials or new technologies, not necessarily just with einsteinium, but with the rest of the actinides too. And we can establish trends in the periodic table."
Subjecting their vanishing pile of chelated E-254 atoms to X-ray absorption tests and photophysical measurements revealed important details on the element's bond distance, while also demonstrating wavelength-shifting emission behaviours not seen in other actinides.
Einsteinium sits right at the edge of what we can achieve using benchwork chemistry. While larger elements exist, their increasing girth puts them out of reach of current technology's ability to create enough for analysis.
But the more we learn about heavy atoms like einsteinium, the greater the potential for finding stepping stones to constructing giants that truly lie somewhere off the map.
"Similar to the latest elements that were discovered in the past 10 years, like tennessine, which used a berkelium target, if you were to be able to isolate enough pure einsteinium to make a target, you could start looking for other elements and get closer to the (theorised) island of stability," says Abergel.

▶▶ **This research was published in** *Nature*.

Iran may reverse fatwa banning nukes if Israel, US act dangerously: ex-official

Source: https://www.timesofisrael.com/iran-may-reverse-fatwa-banning-nukes-if-israel-us-act-dangerously-official/

Feb 04 – A former Iranian diplomat has said that if Israel or the US take "dangerous" steps, the Islamic Republic's Supreme Leader Ayatollah Ali Khamenei may reverse the religious opinion that forbids the acquisition, development or use of nuclear weapons.
Speaking during a January interview with the Lebanese al-Mayadeen TV, ex-Iranian diplomat Amir Mousavi said, "A fatwa is issued in accordance with developing circumstances. Therefore, I believe that if the Americans and Zionists act in a dangerous manner, the fatwa might be changed," according to a translation published this week by the Middle East Media Research Institute (MEMRI).
The fatwa, a nonbinding Islamic legal opinion, issued in 2003, says that nuclear weapons and other weapons of mass destruction are against Islam.
Mousavi added that former US president Barack Obama "was forced to sign the nuclear agreement with Iran" following the downing of an American UAV by the Islamic Revolutionary Guard Corps (IRGC) in 2011, and allegedly because "he strived to win the Nobel prize."
With the new US administration, Mouvasi claims, "Iran is holding some significant cards, which it can use to force President [Joe] Biden to return [to the JCPOA] with no preconditions," adding that "the Iranian leadership is not in a hurry."

"As the Americans delay carrying out their obligations and lifting the sanctions, Iran will further develop its nuclear and defensive capabilities. I believe that the international community is the one that stands to lose and not Iran," Mousavi said.
The United States and Iran are "a long way" from a return to the 2015 nuclear deal with Iran, US State Department spokesman Ned Price said Tuesday.
Price said US President Joe Biden has been "very clear" that "if Iran comes back into full compliance with its obligations under the [deal], the United States would do the same, and then we would then use that as a platform to build a longer and a stronger agreement that also addresses other areas of concern."
The United Nations' nuclear agency said Iran has continued to ramp up its nuclear program in recent weeks by further enriching uranium and installing new centrifuges at its underground Natanz plant, according to a Tuesday report.
In January, Israel Defense Forces Chief of Staff Aviv Kohavi said he has directed the military to prepare fresh operational plans to strike Iran to block its nuclear program.
Defense Minister Benny Gantz said in an interview broadcast Sunday that Israel was still keeping open the possibility of taking action against Tehran's nuclear project if necessary.
A Likud minister close to Prime Minister Benjamin Netanyahu said Tuesday that the US would never attack Iran's nuclear program, and Israel would have to decide whether to launch such a strike alone or come to terms with a nuclear-armed Islamic Republic.

Does Israel feel compelled to launch a strike at Iran's nuclear sites? And if so, when?

Source: https://www.debka.com/does-israel-feel-compelled-to-launch-a-strike-at-irans-nuclear-sites-and-if-so-when/

Feb 02 – **Israel may have to go it alone against a nuclear-armed Iran, said senior minister Tzachi Hanegbi on Tuesday, Feb. 2, because, je said, he can't see the US taking such a military initiative.** The minister spoke the day before an Israel foreign affairs and security cabinet session to discuss the Iranian nuclear issue for the first time since the Biden administration took office. For now, said Hanegbi, it is vital to keep up the pressure of sanctions.
On Monday, Secretary of State Antony Blinken added his voice to the warnings issued by US national security adviser Jake Sullivan and Israel's top military chief Lt. Gen. Aviv Kochavi, who both estimated that Tehran may be just weeks away from enough fissile material for making a nuke.
That distance is getting shorter. The UN nuclear watchdog disclosed on Tuesday that a second cascade of advanced IR-2m centrifuges for enriching uranium has begun working at Iran's Natanz underground plant and a third cluster was ready to go. Last week, Tehran announced that it had upgraded uranium enrichment to 20% at the Fordow plant. That level is still well below 90% weapons grade, but it is a large jump towards that goal. Tehran is making no secret of all these flagrant violations of the nuclear accord it signed with six world powers in 2015 – ever since the US quit the accord.
DEBKAfile's military sources point out that key elements of Iran's nuclear program remain hidden – even from veteran experts who faithfully follow its progress. **They all agree on some points, especially that the Islamic Republic wont risk going into production for a single nuke, but only when it has the capacity to roll out 3-5 weapons.** The calculus is simple: the US or Israel may target a single bomb but would think twice if Iran was capable of responding in kind and launching a nuclear attack on its attackers. Tehran therefore deems a nuclear arsenal to be a deterrent against an enemy offensive.

The Iran pundits find it hard to pin down the exact point Iran has reached in developing a weapon. Is it only as far as a primitive device, or are they now able to build a nuke sophisticated and compact enough to mount on a missile? And what about, other sensitive components, such as the envelope for the fusion fuel canister, for instance? Is Iran getting help from North Korea or Pakistan on these essential details?

It may be assumed that these questions and more were covered in the quiet conversations US CENTCOM chief Gen. Kenneth McKenzie held in Israel last week, first with IDF Chief of Staff Lt. Gen. Aviv Kochavi and then in a two-hour sit-down with Yossi Cohen, director of Israel's Mossad agency. Cohen no doubt filled the American general in on the intelligence data behind Kochavi's landmark speech last Monday, in which he ruled out renewed nuclear talks as "wrong" and disclosed that he had instructed the Israel Defense Forces to prepare a number of operational plans, in addition to those already in place.".
"It will be up to the political leadership, of course, to decide on implementation," the general noted. "But these plans need to be on the table."
It stands to reason that the CENTCOM chief will be drawing up military plans of his own ready to show to the new US president in the event of a decision to strike Iran.

Parallel to the military track, Washington and Tehran have been talking on the quiet for some weeks. Most recently, Saudi Arabia, the UAE and other Gulf emirates have jumped in to test Iran's waters for any signs of readiness to engage in talks on an improved nuclear deal. A notable figure in all these moves is the newly CIA chief, Wiliam Burns, who was the key figure in the Obama administration's backdoor talks in Oman in 2013-1014, which ripened into the 2015 accord.

The most notable development now is that the IDF is preparing for action against Iran's nuclear program – even if it has to do it on its own.

Meanwhile, Washington and Tehran are moving along a predicable track, each waiting the other to make the first move.

On Saturday, Tehran stressed that the nuclear deal was "non-negotiable" and its participation "unchangeable" and repeated its demand for the lifting of US sanctions before its consent to return to the table. President Joe Biden insisted that Iran must first come into full compliance with its terms.

Then, on Monday, FM Mohammed Javad Zarif suggested that a European Union official could help "synchronize" or "coordinate" efforts by Iran and the US to return to a 2015 nuclear accord "as a standstill persists over which country will take the first step."

The conflict is therefore taking on a wider dimension. Biden's diplomatic stance towards Tehran is obviously being watchfully eyed by Presidents Vladimir Putin and Xi Jinping as well as the North Korean ruler Kim Jong-un and may go far towards determining his administration's standing on the international scene.

Israel faces a perilous quandary. Gen. Kochavi's comments on the Iranian threat woke up the Israeli lobby of former security chiefs that thwarted the plans prepared by then PM Binyamin Netanyahu and his defense minister, Ehud Barak, to nip Iran's nuclear weapons program in the bud with a military attack.

But these days, following the new relations and understandings Israel reached during the Trump administration with Gulf nations and Morocco, the Jewish state has an overriding need to preserve those highly strategic ties. At the same time, its government is bound to preserve its freedom of action against Iran obtaining a nuclear capability for aggression, while also remaining in sync with the United States, Europe and the Gulf.

Netanyahu is meanwhile preparing the ground for action. On Monday, he was closeted with the finance minster Yisrael Katz and Gen. Kochavi to put together a three-billion-shekel package (roughly $910 million) to fund a possible military attack on. On Wednesday, the security cabinet was to be convened to air the options. But time is short. If the incumbent government decides on action, it will have strike before the general election takes place on March 23

Qatar – Life inside a radiological triangle

By the C²BRNE Diary Editor-in-Chief

As of today, nuclear energy is considered as one of the most environmentally friendly sources of energy as it produces fewer greenhouse gas emissions during the production of electricity as compared to traditional sources like coal power plants. Nuclear fission is the process that is used in nuclear reactors to produce high amount of energy using element called uranium. It is the energy that is stored in the nucleus of an atom.

While being environmentally friendly is the big plus of nuclear energy, disposal of radioactive waste and protecting people and environment from its radiations is a big con of nuclear energy. Therefore, expensive solutions are needed to protect Mother Earth from the devastating effects of nuclear energy. What are the pros and cons of nuclear energy and what are the possible future threats that a country and neighboring countries might be confronted with?

Pros

1. Low Pollution: Nuclear power also has fewer greenhouse emissions. It has been determined that the amount of greenhouse gases have decreased by almost half because of the prevalence in the utilization of nuclear power. Nuclear energy has the least effect on nature since it doesn't discharge any gasses like methane and carbon dioxide, which are the primary "greenhouse gasses." There is no unfavorable impact on water, land or any territories because of the utilization of nuclear power, except in times where transportation is utilized.

2. Low Operating Costs: Nuclear power produces very inexpensive electricity. The cost of the uranium, which is utilized as a fuel in this process, is low. Also, even though the expense of setting up nuclear power plants is moderately high, the expense of running them is quite low low. The normal life of nuclear reactor is anywhere from 40-60 years, depending on how often it is used and how it is being used. These variables, when consolidated, make the expense of delivering power low. Even if the cost of uranium goes up, the impact on the cost of power will be that much lower.

3. Reliability: It is estimated that with the current rate of consumption of uranium, we have enough uranium for another 70-80 years. A nuclear power plant when in the mode of producing energy can run uninterrupted for even a year. As solar and wind energy are dependent upon weather conditions, nuclear power plant has no such constraints and can run without disruption in any climatic condition.

There are sure monetary focal points in setting up nuclear power plants and utilizing nuclear energy in lieu of traditional energy. It is one of the significant sources of power all through the country. The best part is that this energy has a persistent supply. It is broadly accessible, there is a lot in storage, and it is believed that the supply is going to last much, much longer than that of fossil fuels that are used in the same capacity.

4. More Proficient Than Fossil Fuels: The other primary point of interest of utilizing nuclear energy is that it is more compelling and more proficient than other energy sources. A number of nuclear energy innovations have made it a much more feasible choice than others. They have high energy density as compared to fossil fuels. The amount of fuel required by nuclear power plant is comparatively less than what is required by other power plants as energy released by nuclear fission is approximately ten million times greater than the amount of energy released by fossil fuel atom.

This is one the reason that numerous nations are putting a lot of time and money into nuclear power. What's nuclear power's greatest benefit, above any other benefit that we may explore? It doesn't rely on fossil fuels and isn't influenced by fluctuating oil and gas costs. Coal and natural gas power plants discharge carbon dioxide into the air, which causes a number of environmental issues. With nuclear power plants, carbon emissions are insignificant.

5. Renewable? Nuclear energy is not renewable resource. Uranium, the nuclear fuel that is used to produced nuclear energy is limited and cannot be produced again and again on demand. On the other hand, by using breeder and fusion reactors, we can produce another fissionable element. One such element is called plutonium that is produced by the by-products of chain-reaction. Also, if we know how to control atomic fusion, the same reactions that fuel the sun, we can have almost unlimited energy.

Cons

1. Environmental Impact: One of the biggest issues is environmental impact in relation to uranium. The process of mining and refining uranium hasn't been a clean process. Actually, transporting nuclear fuel to and from plants represents a pollution hazard. Also, once the fuel is used, you can't simply take it to the landfill – it's radioactive and dangerous.

2. Radioactive Waste Disposal: As a rule, a nuclear power plant creates 20 metric tons of nuclear fuel per year, and with that comes a lot of nuclear waste. When you consider each nuclear plant on Earth, you will find that that number jumps to approximately 2,000 metric tons a year. The greater part of this waste transmits radiation and high temperature, implying that it will inevitably consume any compartment that holds it. It can also cause damage to living things in and around the plants.

Nuclear power plants create a lot of low-level radioactive waste as transmitted parts and supplies. Over time, used nuclear fuel decays to safe radioactive levels, however this takes a countless number of years. Even low-level radioactive waste takes hundreds of years to achieve adequate levels of safety.

3. Nuclear Accidents: The radioactive waste produced can pose serious health effects on the lives of people as well as the environment. The Chernobyl accident that occurred on 26 April 1986 at the Chernobyl Nuclear Power Plant in Ukraine was the worst nuclear accident in the history. Its harmful effects on humans and ecology can still be seen today. Then there was another accident that happened in Fukushima in Japan. Although the casualties were not that high, but it caused serious environmental concerns.

4. High Cost: At present, the nuclear business let waste cool for a considerable length of time before blending it with glass and putting away it in enormous cooled, solid structures. This waste must be kept up, observed and watched to keep the materials from falling into the wrong hands and causing problems. These administrations and included materials cost cash – on top of the high expenses needed to put together a plant, which may make it less desirable to invest in. It requires permission from several international authorities and it is normally opposed by the people who live in that region.

5. Uranium is Finite: Just like other sources of fuel, uranium is also finite and exists in few of the countries. It is pretty expensive to mine, refine and transport uranium. It produces considerable amount of waste during all these activities and can result in environmental contamination and serous health effects, if not handled properly.

6. Hot Target for Militants: Nuclear energy has immense power. Today, nuclear energy is used to make weapons. If these weapons go into the wrong hands, that could be the end of this world. Nuclear power plants are prime target for terrorism activities. Little lax in security can be brutal for humankind.

Geopoliticostrategics

The State of Qatar, is a country located in Western Asia, occupying the small Qatar Peninsula on the northeastern coast of the Arabian Peninsula. Its sole land border is with neighboring Saudi Arabia to the south, with the rest of its territory surrounded by the Arab Gulf. An arm of the Arabian Gulf separates Qatar from the nearby Bahrain.

By August 2018, Qatar's total population was 2,562,000 people (density: 176/km²): 313,000 Qatari citizens (11.6%) and 2.3 million expatriates (88.4%). Out of the total number of populations, 1,992,584 are males with females occupying only and approximately 25% of the entire number (632, 498). Meaning, there is only one female in every 3 males in Qatar—giving the oil-rich country the title of having the world's highest male to female ratio. Islam (Sunnis) is the official religion of Qatar.

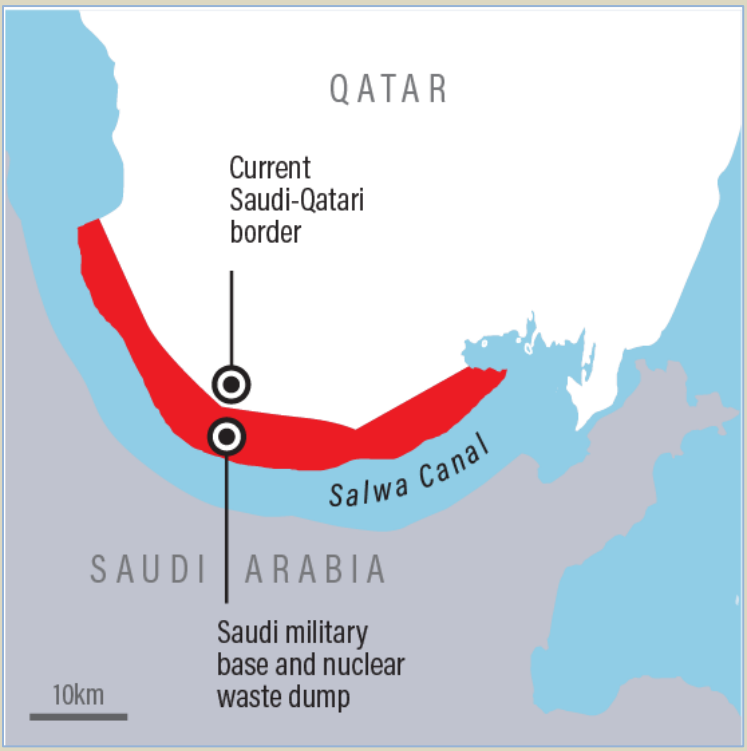
The country has the highest per capita income in the world (IMF; World Bank). Qatar is a high-income economy, backed by the world's third-largest natural gas reserves and oil reserves.

The Qatari peninsula protrudes 160 kilometers into the Arab Gulf, north of Saudi Arabia. The highest point in Qatar is Qurayn Abu al Bawl at 103 meters. The total area is 11,581 km² with maximum length (North to South: ~200Km) and maximum width (East to West: ~85km). This means that the country does not have the strategic depth to defend or withdraw in case of disaster whether natural or man-made. The distance of Doha from Iranian coast (Bushehr): ~420km and from Barakah (UAE): ~320km.

Qatar has mixed relations with its neighbors in the Persian Gulf region. Qatar signed a defense co-operation agreement with Iran, with whom it shares the largest single non-associated gas field in the world. It was the second nation, the first being France, to have publicly announced its recognition of the Libyan opposition's National Transitional Council as the legitimate government of Libya amidst the 2011 Libyan civil war.

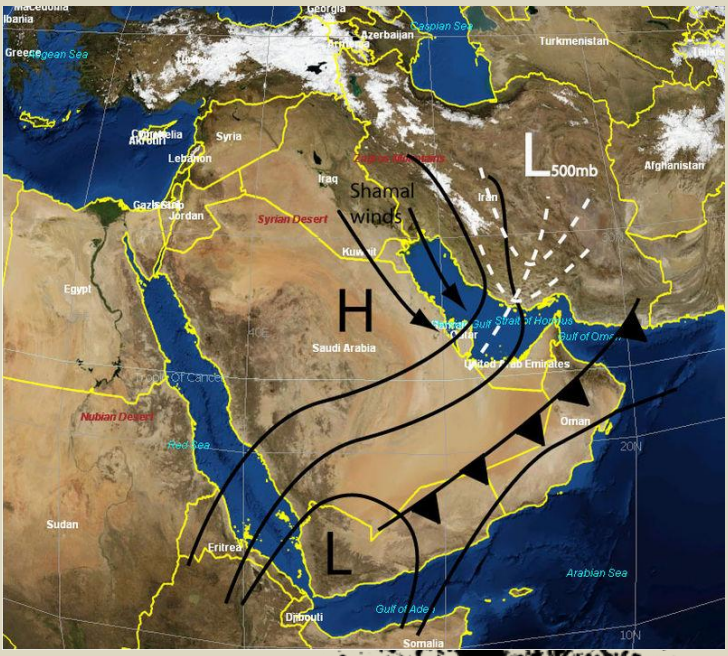
In 2014, Qatar's relations with Bahrain, Saudi Arabia, and the United Arab Emirates came to a boiling point over Qatar's support for the Muslim Brotherhood and reportedly funding extremist groups in Syria. This culminated in the three aforementioned countries withdrawing their ambassadors from Qatar in March 2014.

In June 2017, Saudi Arabia, the UAE, Bahrain, Egypt and Yemen broke diplomatic ties with Qatar, accusing Qatar of supporting terrorism, escalating a dispute over Qatar's support of the Muslim Brotherhood, considered a terrorist organization by those 5 Arab nations. Saudi Arabia explained the move to be a necessary measure in protecting the kingdom's security. Qatari troops were also removed from the military coalition in Yemen. Egypt closed its airspace and seaports to all Qatari transportation.



Salwa Canal

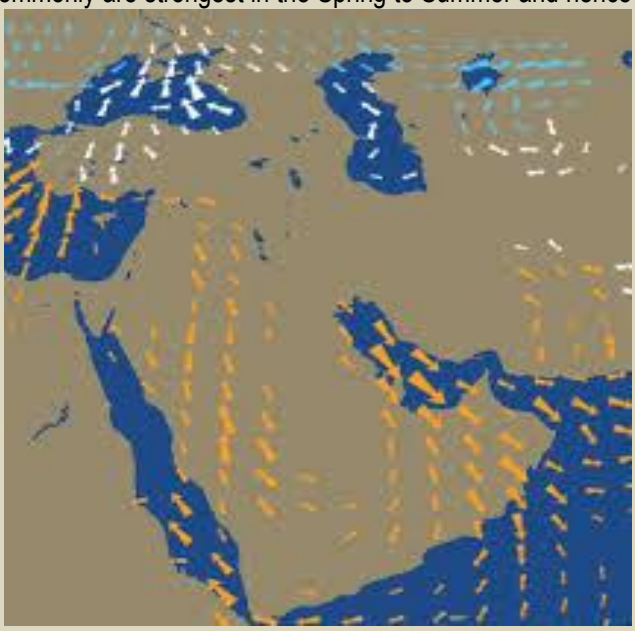
In June 2018, Saudi Arabia announced a bid to construct a waterway, Salwa Canal, on their border with Qatar which shall in effect turn the latter into an island country. The canal will stretch from the town of Salwa just south-west of the Qatari border to Khor Al Adeed. It will be 200 meters wide and 15 meters to 20 meters deep, allowing ships up to 295 meters long and 33 meters wide to navigate it. The channel will be set one kilometer back from the official border. Riyadh is looking to develop significant infrastructure along the canal, including a military base and an atomic waste storage dump to service nuclear power stations it plans to build in the country.



Meteorology

A *shamal* is a northwesterly wind blowing over Iraq and the Persian Gulf states (including Saudi Arabia and Kuwait), often strong during the day, but decreasing at night. This weather effect occurs anywhere from once to several times a year, mostly in summer but sometimes in winter. The resulting wind typically creates large sandstorms that impact Iraq, most sand having been picked up from Jordan and Syria.

Shamals result from strong northwest winds that are funneled into the Arab Gulf by the mountains of Turkey and Iraq to the northeast and the high plains of Saudi Arabia to the southwest. The winds most commonly are strongest in the Spring to Summer and hence the Shamal events are as well, although they can occur at any time of year. During that time of year, the polar jet stream to the north moves southward to become close to the subtropical jet to the south. The proximity of the two jet streams promotes the formation of strong but often dry cold fronts which create the Shamal. The strong winds of the Shamal form in front of and behind the front. Iraq typically experiences strong wind-driven dust 20 to 50 days per year.



When a passing storm with a strong cold front pass over the mountains of Turkey, the leading edge of a mass of relatively cooler air kicks up dust and sand, sending it aloft. Temperatures at lower elevations still hover above 42°C during these events (summer shamal). In Iran, where winter storms can bring heavy snow to the terrain, a layer of dust can settle onto the snowpack.

A winter Shamal is associated with the strengthening of a high pressure over the peninsula after the passage of a cold front while a deep trough of low pressure maintains itself over areas east of the Arab Gulf. This leads to strong northerly wind over the Persian Gulf for periods up to five days. They are associated with cold temperatures.

The places around the Middle East most likely to see the winter variety lie near Lavan Island, Halul Island, and Ras Rakan. They persist from 24 to 36 hours during the winter and occur as frequently as two to three times per month between December and February. A persistent three- to five-day event occurs only once or twice a winter, and is accompanied by very high winds and seas.

Iran

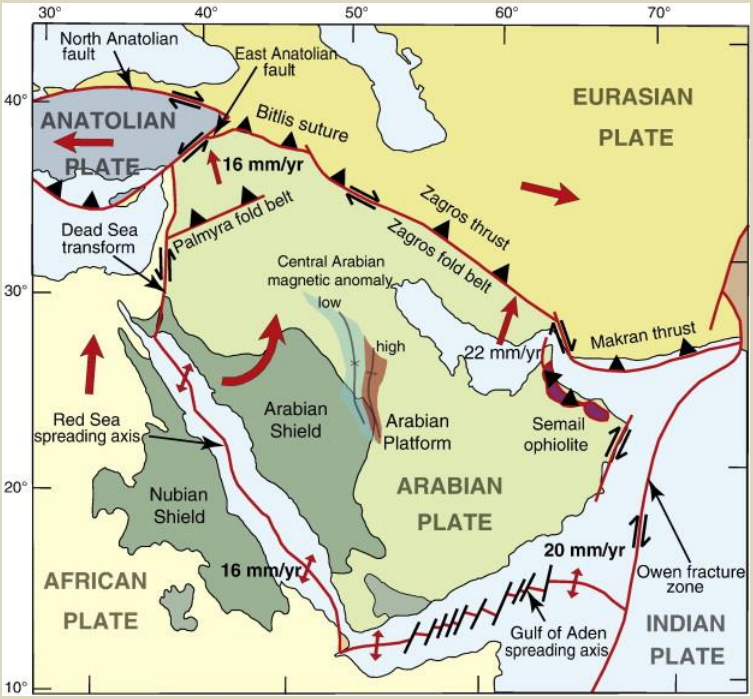
The Bushehr nuclear power plant was constructed 17km southeast of the city of Bushehr, between the fishing villages of Halileh and Bandargeh along the Arab Gulf.

On 30 August, the power unit 1 was brought to 100 percent of its power generation capacity.

In September 2013, the Bushehr plant began producing power for the power grid. For two years the plant was operated by Iranian staff with the assistance of Russian specialists, after which Iran received sole control of the plant. The first refueling of the reactor was completed in July 2014.

On November 11, 2014, Iran and Russia signed an agreement to build two new nuclear reactors at the Bushehr site, with an option of six more at other sites later.

Russia's State Atomic Energy Corporation, Rosatom, started site preparation of the two unit VVER-1000 nuclear power plant with a combined capacity of 2100 MWe in September 2016. On 14 March 2017 construction formally started. Units 2 and 3 are planned to be completed in 2024 and 2026.



According to Kuwaiti geologist, Dr. Jassem al-Awadi, the plant is located at the junction of three tectonic plates. However, the United States Geological Survey and NASA characterize the geology as near the boundary of two tectonic plates, the Arabian plate and the Eurasian plate. The plant is designed to withstand without serious damage a magnitude 8 earthquake, and survive up to magnitude 9.

In 2013, a 6.3 magnitude earthquake hit the southwest region of Iran, where Bushehr is located. Given that much of Iran is in a seismic zone, many expressed concerns over Bushehr's safety following the earthquake. For example, the United Arab Emirates and Saudi

Arabia voiced concerns at the IAEA Board of Governors meeting in June 2013. Iran denied allegations concerning the plant's safety "vulnerability." [18] Simultaneously, Iran reported an electric generator malfunction and "long cracks […] in at least one section of the structure." However, Tehran dismissed the suggestion that the malfunction was connected to the earthquake.
In January 2021, Iran announced that it had increased its uranium enrichment levels, bringing it closer to developing the capacity to produce a nuclear weapon within six months. The resumption of enrichment to 20% was the latest in a series of escalations that have followed President Trump's decision to withdraw the United States from a 2015 nuclear agreement that had limited Iran to enrichment levels of 4 to 5 percent.

UAE

The Barakah nuclear power plan is the United Arab Emirates' first nuclear power station, the first nuclear power station in the Arabian Peninsula, and the first commercial nuclear power station in the Arab World. It is still under construction, and four APR-1400 nuclear reactors are planned to start operation successively between 2018 and 2020, at which point the plant will produce 5,600MW of power. The site is on emirate of Abu Dhabi Al Gharbiya region in the coastline between the sea and the E11 highway, about 50 km west of Ruwais.

Construction status

The Emirates Nuclear Energy Corporation (Enec) in August 2020 announced that its operating and maintenance subsidiary, Nawah Energy Company (Nawah) had successfully started up Barakah (Unit) 1. Construction of Barakah 2 was completed in July 2020. Construction of Barakah 3 and 4 are 92% and 85% complete, while the construction of the Barakah Plant as a whole is now 94% complete. In December Enec announced that Nawah had achieved 100% of the rated reactor power capacity for Barakah 1 - a key step towards starting commercial operations in early 2021.

Saudi Arabia

Saudi Arabia has plans to create a domestic nuclear industry in anticipation of high growth in domestic energy consumption. One set of plans proposes building two nuclear reactors by 2020, and have sixteen built by 2030. The government's intent is to use the electrical power thus produced in place of power obtained from petroleum-fired powerplants, thus freeing that petroleum for export. Currently, Saudi Arabia produces 52 GW from 79 non-nuclear powerplants. The government intends to produce 110 GWe by 2032. This would require 16 reactors by 2019 at a cost of $7B each. Saudi Arabia hopes to produce surplus capacity for export, although that would depend on the rate of domestic electrical energy demand. One prediction foresees domestic consumption at 75 GWe by 2018, rising to 120 GWe by 2030.
The Saudi program is reckoned to be the second most developed in the Arab world, behind their Arab Gulf neighbor United Arab Emirates. In 2010, the King Abdallah Center for Atomic and Renewable Energy (KA●CARE) was founded to oversee Saudi Arabia's nuclear program under its president, Hashim Abdullah Yamani (former minister of energy and of commerce). KA●CARE will represent Saudi Arabia at the IAEA and be responsible for Saudi nuclear energy power, supervision of nuclear power production and management of nuclear waste.
In April 03, 2019, new satellite images show that Saudi Arabia has almost completed the building of its first nuclear reactor, according to a report by Bloomberg written based on the images by Google Earth. The report noted that the construction of the facility, which is located in the southwest corner of the King Abdulaziz City for Science and Technology in Riyadh, is alarming, because the country has not accepted the international rules and frameworks needed to ensure that civilian atomic programs aren't used to build weapons. Bloomberg quoted the Saudi energy ministry as saying in a statement that the facility is being built with transparency and is in full compliance with the international agreements. Saudi Arabia has signed the IAEA's so-called Small Quantities Protocol, but it hasn't adopted the rules and procedures that would allow nuclear inspectors to access potential sites of interest. In March 2018, Saudi Crown Prince Mohammed bin Salman said that the kingdom would be quick to develop nuclear weapons if Iran – which Riyadh views as its arch rival in the region – did so.

Threats

- ✓ *Natural phenomena* – A combination of an earthquake and a tsunami resulted in the Fukushima nuclear power plant catastrophe second only to Chernobyl.
- ✓ *Accident* – a malfunction of equipment or a man-made mishandling of reactor's safe guards might result in release of a radio-contaminated plume that might affect not only the surrounding area but also neighboring countries either partly or due to small size, completely (i.e., Qatar). The Chernobyl accident is a fine example of what follows after

such an accident and the huge impact the accident had not only for Ukraine but almost for the entirely world.

- ✓ *Sabotage and aerial attack* – given the fact that this part of the world is exhibiting a fragile stability a hostile action against a nuclear power plant will result in extensive contamination – especially if the incident happens in Iran that has more than one nuclear facility. In recent times (May 2019), Bushehr might be targeted by both US and Israeli militaries and this might trigger uncontrolled retaliations by Iran and affiliated Hezbollah.
- ✓ Radiological Dispersal and Emitting Devices (RDDs/REDs) – due to the fact that there are thousands of orphan radiological sources around the globe, the addition of (high or low) explosives or the removal of protection against radiation might cause not only direct casualties but also to isolate areas and buildings for an extended period of time (years). These weapons are ideal for area's access restriction and they could be used against nuclear power plants as well.
- ✓ Radiological waste storage sites – they pose threats that must be addressed.

Nuclear Waste disposal hazards

Usually, when nuclear waste is disposed of, it is put into storage containers made of steel that is then placed inside a further cylinder made of concrete. These protective layers prevent the radiation from getting outside and harming the atmosphere or generally surroundings of the nuclear waste. It is a relatively easy and inexpensive method of containing very hazardous materials and actually does not need special transportation or to be stored in a particularly special place, for instance. However, there are a number of dangers that surround nuclear waste disposal.

1. Long Half Life: The products of nuclear fission have long half lives, which means that they will continue to be radioactive – and therefore hazardous- for many thousands of years. This means that, if anything were to happen to the waste cylinders in which nuclear waste is stored, this material can be extremely volatile and dangerous for many years to come. Since hazardous nuclear waste is often not sent off to special locations to be stored, this means that it is relatively easy to find, and if anyone with ill intent were to look for nuclear waste to serve unpleasant purposes, they may well be able to find some and use it.

2. Storage: Another problem with nuclear waste disposal that is still being discussed today is the issue of storage. Many different storage methods have been discussed throughout history, with very few being implemented because of the problematic nature of storing such hazardous material that will remain radioactive for thousands of years. Amongst the suggestions that were considered as above ground storage, ejection into space, ocean disposal and disposal into ice sheets.

Of these, only one was implemented – ocean disposal was actually used by thirteen different countries and was the method of dumping radioactive waste into the oceans in order to get rid of it. Understandably, this practice is no longer implemented.

3. Affects on Nature: One of the biggest concerns that the world has with the disposal of nuclear waste is the affect the hazardous materials could have on animals and plant life. Although most of the time the waste is well sealed inside huge drums of steel and concrete, sometimes accidents can happen and leaks can occur. Nuclear waste can have drastically bad effects on life, causing cancerous growths, for instance, or causing genetic problems for many generations of animal and plants. Not disposing of nuclear waste properly can therefore have huge environmental impacts that can harm many millions of animals and hundreds of animal species.

If disposed of properly, nuclear waste disposal need not have any negative effects. Instead, nuclear waste can lie in its storage place for many thousands of years until it is no longer radioactive and dangerous without being disturbed. However, if the nuclear waste is improperly disposed of or if the disposal methods are compromised, there can be serious consequences and effects of nuclear waste disposal such as:

1. Accidents: Although most of the time a lot of emphasis is placed on the safe disposal of nuclear waste, accidents do occur. Throughout history there have unfortunately been a number of examples of times where radioactive material was not disposed of in the proper ways. This has resulted in a number of disastrous situations, including nuclear waste being spread by dust storms into areas that were populated by humans and animals and contaminated of water, whether ponds, rivers or even the sea. These accidents can have disastrous knock-on effects for the animals that reside in or around these areas or that rely on the water of lakes or ponds to survive.

Drinking water can become contaminated, too, which is absolutely disastrous for locals and residents close to the epicenter of the disaster. Even if nuclear waste just seeps into the ground, it can eventually get into reservoirs and other water sources and, from there, can reach the homes of people who unwittingly drink high radioactive material. There are examples of these sorts of accidents from all over the world and from all time periods, with severe accidents happening very rarely but having a huge effect on very many people.

2. Scavenging: A particularly bad problem in developing nations, people often go scavenging for abandoned nuclear waste that is still radioactive. In some countries there is a market for these sorts of scavenged goods, which means that people will willingly expose themselves to dangerous levels of radiation in order to make money. Unfortunately, however, radioactive materials can be highly volatile and cause a number of problems.

Usually, people who scavenge these sorts of materials will end up in hospital and may even die of problems related to or caused by the radioactive materials. Unfortunately, once someone has been exposed to nuclear waste, they can then expose other people who have not opted to go scavenging for nuclear waste to radioactive materials.

3. Transportation: Transporting nuclear waste from power plants can occasionally result in problems. If poor shipping casks are used for the containment of radioactive material, for instance, then a slight knock or bump or even crash could cause the contents to spill and affect a wide radius. Despite all the cautions that are put into place when transporting nuclear waste, accidents still occur and can have a devastating effect on all those in the vicinity of the crash.

4. Health Effects: The biggest concern is the negative effects that can have on the human body when exposed to radiation. Long term effects to radiation can even cause cancer. It is interesting to know that we are exposed to radiations naturally by living our lives that comes from the ground below us. Radiation can cause changes in 'DNA' that ensures cell repair.

5. Expense: If one of these accidents does occur, the cost of cleaning everything up and making everything safe once again for people, animals and plants is very high. There is no simple or easy route when trying to clean up spilled radioactive material: instead, it can take years to ensure that an area is safe to live in or even to visit once again. In the case of very serious accidents, it may take many tens of years until things start growing or living normally once again.

Radiation Health Effects

Ionizing radiation has sufficient energy to affect the atoms in living cells and thereby damage their genetic material (DNA). Fortunately, the cells in our bodies are extremely efficient at repairing this damage. However, if the damage is not repaired correctly, a cell may die or eventually become cancerous.

Exposure to very high levels of radiation, such as being close to an atomic blast, can cause acute health effects such as skin burns and acute radiation syndrome ("radiation sickness"). It can also result in long-term health effects such as cancer and cardiovascular disease. Exposure to low levels of radiation encountered in the environment does not cause immediate health effects, but is a minor contributor to our overall cancer risk.

Source of accident	Radioactive substance	Common body parts exposed
Industrial		
Sterilization	^{60}Co, ^{137}Cs	Whole body, hands
Radiography	^{192}Ir, ^{137}Cs	Hands and other parts
Gauging	^{192}Ir, ^{137}Cs	Hands and other parts
Medical practice		
Diagnostics	X-ray generators	Hands, face
Therapy	^{60}Co, ^{137}Cs	Whole body, hands and other parts
	Accelerators	
Spent sources	^{60}Co, ^{137}Cs and others	Whole body, hands and other parts
Nuclear reactors	^{137}Cs, ^{90}Sr	Whole body
	^{131}I	Thyroid
	^{210}Pu	Lung
Others		
Research	Spectrum of sources including reactors	Hands, face and other parts
Depleted uranium ammunition	^{238}U, ^{235}U, ^{234}U	

Acute Radiation Syndrome from Large Exposures

A very high level of radiation exposure delivered over a short period of time can cause symptoms such as nausea and vomiting within hours and can sometimes result in death over the following days or weeks. This is known as acute radiation syndrome, commonly known as "radiation sickness."

It takes a very high radiation exposure to cause acute radiation syndrome—more than 75 rad[1] (0.75 gray) in a short time span (minutes to hours). This level of radiation would be like getting the radiation from 18,000 chest x-rays distributed over your entire

[1] Rad is the U.S. unit used to measure absorbed radiation dose (the amount of radiation absorbed by an object or person). The international equivalent is the Gray (Gy). One hundred rads are equal to 1 Gray. A gray is the international unit used to measure absorbed dose (the amount of radiation absorbed by an object or person). The U.S. unit for absorbed dose is the rad. One gray is equal to 100 rads.

body in this short period. Acute radiation syndrome is rare, and comes from extreme events like a nuclear explosion or accidental handling or rupture of a highly radioactive source.

Radiation Exposure and Cancer Risk

Exposure to low-levels of radiation does not cause immediate health effects, but can increase the risk of cancer over a lifetime. There have been studies that kept track of large numbers of people who were exposed to radiation, including atomic bomb survivors and radiation industry workers. These studies show that radiation exposure increases the chance of getting cancer, and the risk increases as the dose increases: the higher the dose, the greater the risk. Conversely, cancer risk declines as the dose falls: the lower the dose, the lower the risk. According to radiation safety experts, radiation exposures of 5–10 rem. The U.S. unit to measure effective dose. The international unit is sieverts (Sv) (5,000–10,000 millirem or 50–100 millisieverts) usually result in no harmful health effects, because radiation below these levels is a minor contributor to our overall cancer risk.

Limiting Cancer Risk from Radiation in the Environment

Limits and nonregulatory guidelines for public exposure to low level ionizing radiation are based on the linear no-threshold (LNT) model. The LNT model assumes that the risk of cancer due to a low-dose exposure is proportional to dose, with no threshold. In other words, cutting the dose in half cuts the risk in half.

The use of the LNT model for radiation protection purposes has been repeatedly recommended by authoritative scientific advisory bodies, including the US National Academy of Sciences and the National Council on Radiation Protection and Measurements. There is evidence to support LNT from laboratory data and from studies of cancer in people exposed to radiation.

Exposure Pathways

Understanding the type of radiation received, the way a person is exposed (external vs. internal), and for how long a person is exposed are all important in estimating health effects.

The risk from exposure to a particular radionuclide depends on:

- The energy of the radiation it emits;
- The type of radiation (alpha, beta, gamma, x-rays);
- Its activity (how often it emits radiation);
- The rate at which the body metabolizes and eliminates the radionuclide following ingestion or inhalation;
- Where the radionuclide concentrates in the body and how long it stays there;
- Whether exposure is external or internal:
  - External exposure is when the radioactive source is outside of your body. X-rays and gamma rays can pass through your body, depositing energy as they go.
  - Internal exposure is when radioactive material gets inside the body by eating, drinking, breathing or injection (from certain medical procedures). Radionuclides may pose a serious health threat if significant quantities are inhaled or ingested.

Sensitive Populations

Children and fetuses are especially sensitive to radiation exposure. The cells in children and fetuses divide rapidly, providing more opportunity for radiation to disrupt the process and cause cell damage.

Preparedness and response

The major burden in both preparedness and response is the fact that the proximity to the radiological source is significant while the strategic depth of the country is small. This raises the issue of distribution certain medications to the population in a very short period of time. Therefore, decisions should be taken on how the distribution should be performed or if these medications should be distributed in advance and guidelines could follow in case of a real incident only. Each solution has its pros and cons than need to be addressed and solved.

Protective action recommendations
They are designed to be taken **before** an anticipated dose is reached.

Actions taken to reduce or eliminate the public's exposure to radiation or other hazards following a radiation incident:

- In the early and intermediate phases of RDD/IND incidents there may be inadequate information to determine precisely the radiation levels or make dose projections.
- Initial protective actions may be undertaken based on models rather than actual measured radiation levels.
- Protective action recommendations may change over the course of an incident, as new information is obtained.
  - **Primary** protective actions include
    - Sheltering-in-place
    - Evacuation
    - Relocation
    - Interdiction of food and water
  - **Secondary** protective actions include
    - Medical countermeasure administration
    - Decontamination of people and places
    - Restrictions of food and/or water
    - Access control
    - Victim extraction

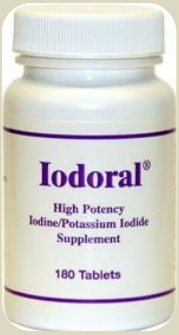
Potential Exposure Pathways and Protective Actions by Incident Phase

Potential Exposure Pathways	Incident Phases	Protective Actions
1. External Radiation from Facility	EARLY	1. Sheltering, Evacuation, Control of Access
2. External Radiation from Plume	EARLY	2. Sheltering, Evacuation, Control of Access
3. Inhalation of Radioactivity in Plume	EARLY	3. Sheltering, Administration of Stable Iodine, Evacuation, Control of Access
4. Contamination of Skin and Clothes	EARLY / INTERMEDIATE	4. Sheltering, Evacuation, Decontamination of Persons and Animals, Including Household Pets and Service Animals with Owners
5. External Radiation from Ground Deposition of Activity	EARLY / INTERMEDIATE / LATE	5. Evacuation, Relocation, Decontamination of Land and Property
6. Ingestion of Contaminated Food, Water	INTERMEDIATE / LATE	6. Food and Water Controls
7. Inhalation of Re-Suspended Activity	INTERMEDIATE / LATE	7. Relocation, Decontamination of Land and Property

Source: Nuclear/Radiological Incident Annex to the Response and Recovery Federal Interagency Operational Plans, (PDF - 3.38 MB) (US Government Interagency, October 2016, p. 46)

Iodine prophylaxis in case of accident with release of radioactive iodine in the environment

This is a preventive protection measure aimed to avoid the health damage of individuals resulting from accumulation of radioactive iodine in the thyroid in case of nuclear or radiation accident.



The iodine prophylaxis is performed by taking tablets, frequently potassium iodine (KI), containing stable (not radioactive) iodine. These is the way in advance to saturate (blockade) the thyroid with stable iodine and to avoid the incorporation of radioactive iodine into the gland through inhalation or ingestion of materials (food, milk, water) contaminated with radioactive iodine in case of nuclear or radiation accident.

The requirements and order of implementation of iodine prophylaxis are defined with special legislature.

THE IODINE PROPHYLAXIS SHOULD NOT BE APPLIED WITHOUT PERMISSION AND WITHOUT EXPLICIT INSTRUCTIONS.

The iodine is a chemical element with atomic number 53 in the Periodic Table of Elements ("iodine" in translation form Greek means "violet"). This element has been discovered in 1811

and has only one stable (not radioactive) isotope with mass number 127 (iodine-127). The natural iodine is contained in the earth crust (10^{-4} %), in see water and seaweed. The iodine and its compounds are used in medicine and pharmacy. The alcohol solution of iodine (iodine tincture) has antiseptic characteristics. At present 22 isotopes of the iodine are known with mass numbers in the ranges 117 – 126 and 128 – 139. They are produced artificially during the nuclear fission process of nuclear fuel at the reactors or nuclear reactions. The radioactive isotopes of the iodine (iodine-131, iodine-125, iodine-129, etc.) have broad applications mainly in medicine (nuclear diagnostic and therapy) and science.

Table 2-2. Threshold Thyroid Radioactive Exposures and Recommended Doses of KI for Different Risk Groups

RISK GROUP	Predicted Thyroid gland exposure (cGy) (1 cGy = 1 rem)	KI dose (mg)	Number or fraction of 130 mg tablets	Number or fraction of 65 mg tablets
Adults over 40 years	≥ 500	130	1	2
Adults over 18 through 40 years	≥ 10			
Pregnant or lactating women	≥ 5			
Adolescents, 12 through 18 years[a]		65	1/2	1
Children over 3 years through 12 years				
Children over 1 month through 3 years		32	Use KI oral solution[b]	1/2
Infants birth through 1 month		16	Use KI oral solution[b]	Use KI oral solution[b]

[a] Adolescents approaching adult size (≥ 150 pounds) should receive the full adult dose (130 mg).

[b] Potassium iodide oral solution is supplied in 1-ounce (30 mL) bottles with a dropper marked for 1-, 0.5-, and 0.25-mL dosing. Each mL contains 65 mg potassium iodide.

Source: FDA, "Guidance: Potassium Iodide as a Thyroid Blocking Agent in Radiation Emergencies" (December 2001): http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM080542.pdf (FDA 2001); and FDA, Frequently Asked Questions on Potassium Iodide (KI): http://www.fda.gov/Drugs/EmergencyPreparedness/BioterrorismandDrugPreparedness/ucm072265.htm
.

The most important radioactive isotope of the iodine from radiation protection point of view is iodine-131 (with half-life 8 days) to which a special attention is paid in case of nuclear or radiation accidents. Significant part of the activity of radioactive substances, which can be released in the atmosphere, in case of nuclear accident in a nuclear power plant, is created precisely by iodine-131. Other radioactive isotopes as iodine-125, iodine-133, iodine-134 and iodine-135 have shorter half-live and for the internal exposure of the individual their contribution is smaller in comparison with iodine-131.
Other special feature of the iodine is the fact that he relatively easily and quickly can penetrate in the milk (through the chain: grass/feeding stuffs – animal – milk-human).
The thyroid gland has a very small mass (about 20 g average for individuals) and when radioactive iodine (iodine-131) is accumulated this leads to receiving high exposure (absorbed doses) of critical human organ.
Within the first hours after occurrence of the nuclear or radiation accident the radioactive iodine-131 is entering into the body mainly through inhalation and rapidly is penetrating into the blood. To avoid the accumulation of iodine-131 in the thyroid gland potassium iodine tablets are used. The aim is to saturate in advance the thyroid with stable (not radioactive) iodine and in this way to block the subsequent intake of radioactive iodine. The radioactive iodine-131 can be accumulated in the body also through the food chain in the late phase of nuclear or radiation accidents. Besides the iodine prophylaxis, to reduce the exposure additional preventive measures should be applied such as suppression or restriction of consummation of feeding stuffs

contaminated with iodine-131, strengthening the monitoring of milk, water and main feeding stuffs, as well as other organizational and administrative measure.

In order to be effective, the iodine prophylaxis should be implemented opportunely taking into account the time, which it is necessary for the stable iodine (in the form of potassium iodine tablets) to saturate the thyroid. This time depends on the biological and physiological features of the single individual, as well as on the age and gender. The accumulation speed of the radioactive iodine-131 into the thyroid of children and pregnant women is higher than in other population groups. Critical groups are the newborns and children up to 12 years old, pregnant women and breast-feeding women. The risk of exposure of the thyroid to radioactive iodine-131 is negligible for adults over 45 years and hence iodine prophylaxis for them is not compulsory.

It is determined that the iodine prophylaxis is most efficient when it is implemented within the first two hours after the nuclear or radiation accident whose consequences impose implementation of such protection measure for the population. If the iodine blockage is performed 5 hours after the accident the efficiency of these protection measure decreases 10 times.

According to the US Regulation on Emergency Planning and Emergency Preparedness in Case of Nuclear and Radiation accident the iodine prophylaxis (stable iodine blockage of the thyroid) is the main protection measure for the personnel (of the facilities and the emergency personnel) and the population. In the country organization has been established for conducting iodine prophylaxis and potassium iodine tablets (KI) in sufficient quantities has been assured. The procedure and order for implementation of iodine prophylaxis is established in the National Emergency Plan (off-site plan).

The Regulation No.28 issued by the US Minister of Health establishes the conditions and order for medical assurance and health norms for protection of the individual in case of radiation accident, as well as the intervention levels and dosages of the potassium iodine tablets for iodine prophylaxis. The following six age population groups are determined by the regulation: newborns and babies up to 2 months, children up to 3 years old; children from 3 years up to 12 years; young people and adults from 12 up to 45 years and pregnant women and breast-feeding women. One standard potassium iodine tablet is 65 mg and contains 50 mg stable iodine (iodine-127). The dosage of the stable iodine differs for each one of the 6 determined groups and has been defined by the Regulation No.28. The maximum amount of stable iodine intake is 1 g during 10 days. These means that individuals older than 12 years should take only two pills per day (2 x 65 mg) and no longer than 10 days. For all other groups the daily dosage is from 2 to 8 times less (for newborns up to 2 mounts are allowed to take once only ¼ part from the standard pill of 65 mg potassium iodine).

The iodine tablets should be taken only after consultations with a medical doctor and in case of the following diseases:

- disturbance of the functions of thyroid gland;
- bronchitis; asthma;
- pelvic insufficiency fractures;
- immunity insufficiency.

Method of intake of iodine tablets:

The tablets should be taken after eating and they should be crushed and taken with large amount of liquids to avoid and minimize the undesirable irritation of the gastro-intestinal system.

Potential side-effects during intake of iodine tablet:

- ✓ metallic taste;
- ✓ nausea and vomiting;
- ✓ gastric disorders;
- ✓ diarrhea;
- ✓ skin rashes;
- ✓ palpitation.

The iodine tablets protect only the thyroid from accumulating radioactive iodine but do not protect against other radioactive substances, which also are released in case of nuclear or radiation accidents.

The responsibility for assuring, storage and distribution of the potassium iodine tablets for protection of the population in case of nuclear or radiation accident is assigned to the Ministry of Emergency Situations (MES) through the General Directorate “National Service Civil Protection” and its regional services, as well as to the local authorities.

All necessary quantities of potassium iodine tablets for the entire Bulgarian population are assured in compliance with the national legislation for emergency planning and response in case of nuclear or radiation accidents.

Prussian blue

Prussian blue is a pill that can help remove radioactive cesium and thallium from people's bodies.

How does Prussian blue work?

Prussian blue traps radioactive cesium and thallium in the intestines and keeps them from being re-absorbed by the body.

The radioactive materials then move through the intestines and are passed (excreted) in bowel movements.

Because Prussian blue reduces the time that radioactive cesium and thallium stay in the body, it helps limit the amount of time the body is exposed to radiation.

Prussian blue reduces the biological half-life of cesium from about 110 days to about 30 days.

Prussian blue reduces the biological half-life of thallium from about 8 days to about 3 days.

Who can take Prussian blue?

The drug is safe for most adults, including pregnant women, and children (2-12 years). Dosing for infants (ages newborn-2 years) has not been determined yet.

People who have had constipation, blockages in the intestines, or certain stomach problems should be sure to tell their doctors before taking Prussian blue.

Before taking Prussian blue, people also should be sure to tell their doctors about any other medicine they are taking.

How is Prussian blue given?

Prussian blue is given in 500-milligram capsules that can be swallowed whole.

People who cannot swallow pills can take Prussian blue by breaking the capsules and mixing the contents in food or liquid. Breaking open the capsules will cause people's mouths and teeth to be blue during the time of treatment.

What are the side effects of Prussian blue?

The most common side effects of Prussian blue are upset stomach and constipation. These side effects can easily be treated with other medications.

People may have blue feces (stool) during the time that they are taking Prussian blue.

Availability

Prussian blue is available only by prescription.

People **SHOULD NOT** take Prussian blue artist's dye in an attempt to treat themselves. This type of Prussian blue is not designed to treat radioactive contamination and can be harmful.

DTPA (Diethylenetriamine pentaacetate)

DTPA (Diethylenetriamine pentaacetate) is a medicine that can bind to radioactive plutonium, americium, and curium to decrease the amount of time it takes to get radioactive plutonium, americium, and curium out of the body.

DTPA cannot bind all of the radioactive plutonium, americium, and curium that might get into a person's body after a radiation emergency.

DTPA cannot prevent radioactive plutonium, americium, and curium from entering the body.

How does DTPA work?

DTPA comes in two forms: calcium (Ca-DTPA) and zinc (Zn-DTPA). Both forms work by tightly binding to radioactive plutonium, americium, and curium. These radioactive materials (bound to DTPA) are then passed from the body in the urine.

DTPA works best when given shortly after radioactive plutonium, americium, and curium have entered the body. The more quickly radioactive material is removed from the body, the fewer and less serious the health effects will be.

When given within the first day after internal contamination has occurred, Ca-DTPA is more effective than Zn-DTPA. After 24 hours have passed, Ca-DTPA and Zn-DTPA are equally effective.
After 24 hours, DTPA binds less effectively to radioactive plutonium, americium, and curium. However, DTPA can still work to remove these radioactive materials from the body several days or even weeks after a person has been internally contaminated.

Who can take DTPA?
Doctors and public health authorities will work together to decide who likely will benefit from DTPA treatment.
For doctors who may be administering DTPA for patients, use the following guidelines:

- **Infants (including breastfed infants) and children less than 12 years of age** can be given either Ca-DTPA or Zn-DTPA.
  - The dosage of DTPA should be based on the child's size and weight.
  - The safety and effectiveness of the inhaled route of DTPA has not been studied in children.
- **Young adults and adults** internally contaminated with plutonium, americium, or curium should receive Ca-DTPA if treated within the first 24 hours after contamination. After 24 hours, if additional treatment is needed, adults should receive Zn-DTPA. If Zn-DTPA is not available, patients may receive Ca-DTPA together with a vitamin and mineral supplement that contains zinc.
- **Pregnant women** should be treated with Zn-DTPA, unless the woman has very high levels of internal contamination with plutonium, americium, or curium.
  - Ca-DTPA should be used in pregnant women only to treat very high levels of internal radioactive contamination.
  - In this case, doctors and public health authorities may prescribe a single dose of Ca-DTPA, together with a vitamin and mineral supplement that contains zinc, as the first treatment.
  - After the first dose of Ca-DTPA, treatment should continue 24 hours later with a daily dose of Zn-DTPA, as needed.
- **Breastfeeding** women who are internally contaminated with plutonium, americium, or curium can be treated with Ca-DTPA or Zn-DTPA.

How is DTPA given?
DTPA can be injected directly into a vein in the arm or dripped into a vein from a bag (intravenously [IV]).
Adults who have inhaled plutonium, americium, or curium can be treated with DTPA mist that is breathed into the lungs.

- ✓ Inhaling DTPA might cause some people, especially those with asthma, to cough or wheeze.
- ✓ The safety and effectiveness of inhaled DTPA has not been shown in children.

DTPA should be taken only as long as needed, as determined by a doctor.
Doctors might collect samples of blood, urine, and feces during DTPA treatment. These samples can tell the doctors how much radioactivity you are passing and how much remains in your body.
The length of treatment with DTPA will depend on:

- ✓ The amount of radioactive material in your body
- ✓ How well your body gets rid of the radioactive material with the help of DTPA.

What are the side effects of DTPA?
People who are given repeat doses of Ca-DTPA within a short period of time may have nausea, vomiting, diarrhea, chills, fever, itching, and muscle cramps.
Other side effects may include headache, light-headedness, chest pain, and a metallic taste in the mouth.
Ca-DTPA should be used cautiously in patients with a blood disease called hemochromatosis.
Ca-DTPA (and Zn-DTPA) bind to important minerals that the body needs (zinc, magnesium, and manganese). As a precaution, patients receiving long-term treatment with DTPA should be given a vitamin and mineral supplement that contains zinc.

Availability
During a radiation emergency, doctors will provide DTPA treatment as needed.
DTPA can only be administered by a doctor.

Neupogen® (Filgrastim)
Neupogen® (filgrastim) is a drug that has been used successfully for cancer patients to stimulate the growth of the white blood cells, making patients less vulnerable to infections, it is expected to help patients who have bone marrow damage from very high doses of radiation in much the same way.

A person who has received a very high dose of radiation may experience bone marrow destruction, possibly resulting in infection and uncontrolled bleeding.
Since March 2015, Neupogen® was also approved by the U.S. Food and Drug Administration (FDA) to treat those people who have received high doses of radiation.

How does Neupogen® work?
Patients who receive very high doses of radiation will not be able to produce new white blood cells. This will lead to a drop in the number of white blood cells in circulation.

- The patients' own bone marrow will eventually create new blood cells, but this is a slow process.
- Until the white blood cell counts rise sufficiently, these patients are at a high risk of death from infection.

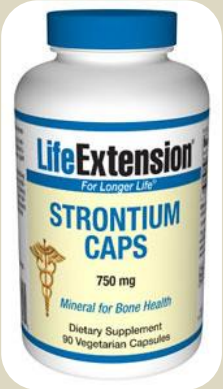
Neupogen® can speed up the process of white blood cell creation, reducing the time that the patient is vulnerable to infection.

Who can take Neupogen®?
People may be prescribed Neupogen® following a high dose of radiation from a radiation emergency.
Neupogen® is safe for most adults, but should not be taken by people who have known hypersensitivity to E. coli-derived proteins, filgrastim, or any component of filgrastim.
Children and pregnant women should take Neupogen® with caution.
It is not known if Neupogen® is excreted in human milk; so breastfeeding women should discuss this matter with a doctor.

How is Neupogen® given?
Neupogen® is given by injection under the skin.
For doctors, the treatment plan is to give Neupogen® daily for up to 2 weeks, by subcutaneous injection.

What are the side effects of Neupogen®?
The most common side effect of Neupogen® is mild to moderate bone pain.
Other possible side effects of Neupogen® include fever, diarrhea, skin rash and weakness.
Enlargement and rupture of the spleen can rarely occur in patients who are receiving Neupogen®. Patients who develop abdominal pain, particularly in the left side, while receiving the drug should be evaluated by a doctor.

Availability
During a radiation emergency, doctors will provide Neupogen® treatment as needed. Neupogen® can only be administered by a doctor.



Strontium
Radioactive strontium has a half-life of about 30 years;

- It is chemically similar to calcium so it concentrates in the bones and contributes to bone cancer if the concentrations are high;
- Protective strategy is to take supplements of strontium and calcium to minimize any absorption of strontium from the environment.

Cesium
Radioactive cesium also has a half-life of around 30 years;

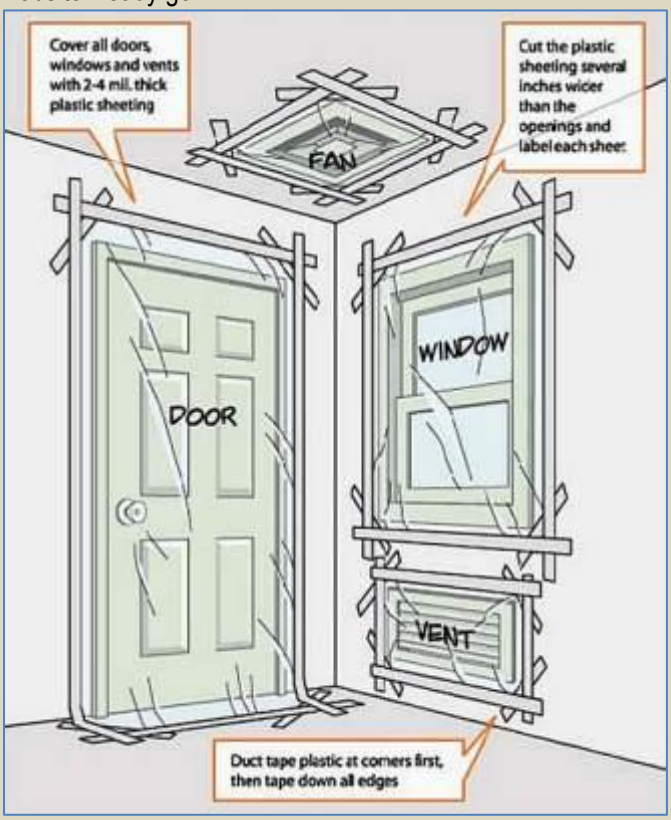
- It acts biologically in a manner similar to potassium by concentrating in the muscles and soft tissues and can contribute to cancer if the concentration is high enough.
- Increasing potassium intake may be helpful. Potassium supplements are readily available but you can get a lot from **bananas and especially potatoes**.

If you take potassium supplements, check with your doctor if you have a heart, blood pressure or kidney condition

Shelter-in-place
Shelter in place is to seek safety within the building one already occupies, rather than to evacuate the area or seek a community emergency shelter. The American Red Cross says the warning is issued when "chemical, biological, or radiological contaminants may be released accidentally or intentionally into the environment" and residents should "select a small, interior room, with no or few windows, taking refuge there."

Radiological and chemical defense

It entails closing all household doors, windows and vents and taking immediate shelter in a readily accessible location that puts as much indoor air and/or radiation shielding-mass between the individual and the hazardous outside air, such as a basement or centrally located medium to small room, and trying to make it as airtight as possible by shutting off all ventilation/HVAC systems and extensively sealing the shelter's doors and windows from all outside air contaminants with damp towels, or if available, plastic sheeting and adhesive tape. Diagrams of what sheltering in place entails following a chemical, biological, radiological or nuclear (CBRN) threat, and how long it is advised to be done for, is provided by the U.S. Federal Emergency Management Agency-affiliated website Ready.gov



Shelter-in-place effectiveness has been evaluated and experimental results show that proper sealing can make a substantial difference to a normal home shelter, finding it to be at least twice as effective against a host of airborne substances when compared against simply staying inside and not implementing the countermeasure, and in most airborne contaminant cases, it is usually much more effective, depending on the particle size of the substance in question. If the occupant's breathing is the only consumer of oxygen and producer of carbon dioxide in the room, then carbon dioxide levels would not begin to reach dangerous values until 3+ hours had passed, in most likely, 4-person home scenarios.

In the military, "Shelter-in-Place" is comparable to "buttoning up" and has proved life-saving in certain nuclear fallout instances.

The danger of radiation from radioactive precipitation/"fallout" decreases with time, as radioactivity decays exponentially with time, such that for each factor of seven increase in time, the radiation is reduced by a factor of ten. Creating the following 7-10 rule-of-thumb after a typical nuclear detonation while under the conditions that all fallout that will fall on the land has done so completely and no *further* deposition in the area will occur - After 7 hours, the average dose rate outside is reduced by a factor of ten; after 49(7x7) hours, it is reduced by a further factor of ten (to a value of 1/100th of the initial dose rate); after two weeks the radiation from the fallout will have reduced by a factor of 1000 compared to the initial level; and after 14 weeks the average dose rate will have reduced to 1/10,000th of the initial level.

If an individual finds themselves outside during an emergency that calls for shelter-in-place, then effective but low-tech decontamination is required before entering into the shelter.

The phrase "Shelter-in-place" has also erroneously been used, instead of the more accurate *lockdown*, to describe precautions to be taken by the public when violence has occurred or might occur (particularly in shootings) in the area and the perpetrator is believed to still be in the area but not apprehended. The public in the area is advised to carry out all the same tasks as a typical shelter-in-place but without the key step of sealing the shelter up to prevent outside air from circulating indoors, in this scenario people are simply urged to lockdown — stay indoors and "close, lock and stay away from external doors and windows."

Evacuation vs. Sheltering-in-Place

Evacuation and sheltering-in-place provide different levels of dose reduction from the principal exposure pathways: direct gamma exposure and inhalation. Both sheltering-in-place and evacuation may be implemented during the same response in different areas or timeframes. Evacuation, if completed before plume arrival, can be 100 percent effective in avoiding radiation exposure.

A decontamination station, with simple decontamination actions, may need to be collocated at shelters during the pre-evacuation period. This may reduce the spread of contamination and provide for greater protection during evacuation. Medical stations should also be collocated at shelters during the pre-evacuation period to ensure simple triage capabilities are met and to manage the distribution of prophylactic drugs. The effectiveness of evacuation will depend on many factors, such as how rapidly it can be implemented and the nature of the incident. For incidents where the principal source of dose is inhalation, evacuation could increase exposure if it is implemented during the passage of a short-term plume, because the air inside a vehicle rapidly equalizes with the outside air even when all of the windows and vents are closed (DOE 1990).

When dose projections are at levels less than 1 rem (10 mSv) over the first four days, evacuation is not recommended due to the associated risks of moving large numbers of people.

Sheltering-in-place is a low-cost, low-risk protective action that can provide protection with an efficiency ranging from zero to almost 100 percent, depending on the type of release, the type of shelter available, the duration of the plume passage, and climatic conditions. Because of these advantages, planners and decision-makers may consider implementing sheltering-in-place when projected doses are below 1 rem (10 mSv) over the first four days. More guidance on the unique challenges posed by an IND can be found in the "Planning Guidance for Response to a Nuclear Detonation" (NSS 2010).[7]

Sheltering-in-place may be preferred for special populations (e.g., those who are not readily mobile) as a protective action at projected doses of up to 5 rems (50 mSv) over four days. When environmental, physical, or weather hazards impede evacuation, sheltering-in-place may be justified at projected doses up to 5 rems (50 mSv) for the general population (and up to 10 rems (100 mSv) for special populations). It is also comparatively easy to communicate with populations that have sheltered-in-place. Dose projections use a four-day exposure duration, but sheltering-in-place duration is intentionally not specified. Incident- specific decisions must be made to determine how long people should shelter-in-place.

Selection of evacuation or sheltering-in-place is far from an exact science, particularly in light of time constraints that may prevent thorough analysis at the time of an incident. The selection process should be based on realistic or "best estimate" dose models and should take into account the unavoidable dose incurred during evacuation and potential failure scenarios for sheltering-in-place (e.g., leaking ventilation system).

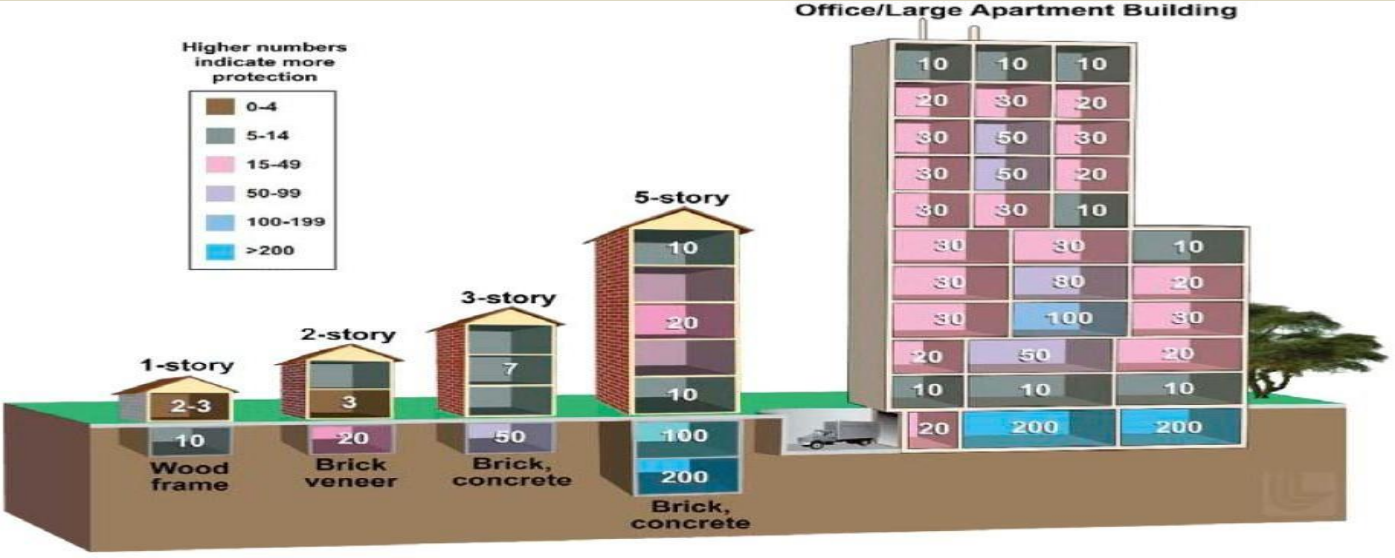
Advance planning and exercises can facilitate the decision process. In a commercial NPP incident, early decisions should be based on information from the response plans for the emergency planning zone (EPZ) and on actual conditions at the nuclear facility. For transportation accidents, RDDs, INDs and other incident scenarios for which EPZs are not practicable, best estimates of dose projections should be used for deciding on evacuation, sheltering- in-place or a combination thereof.

The following is a summary of planning guidance for evacuation and sheltering-in-place:

- Evacuation may be the only effective protective action close to the plume source.
- Evacuation will be most effective if it is completed before arrival of the plume.
- Evacuation may increase exposure if carried out during the plume passage.
- Evacuation is appropriate for protection from ground shine in areas with high exposure rates from deposited radioactive materials when suitable shelter is not available.
- Sheltering-in-place may be appropriate for areas not designated for immediate evacuation—
  - It may provide protection equal to or greater than evacuation for rapidly developing releases (e.g., RDDs) if followed by evacuation.
  - It positions the public to receive additional instructions.
  - Since it may be implemented rapidly, sheltering-in-place may be the protective action of choice (followed with evacuation when feasible) if rapid evacuation is impeded by:
    - severe environmental conditions (e.g., severe weather or floods);
    - uncertainty about contamination levels along routes;
    - health constraints (e.g., patients and workers in hospitals and nursing homes);
    - long mobilization times that may be associated with certain individuals, such as industrial and farm workers, or prisoners and guards; or
    - physical constraints to evacuation (e.g., inadequate roads or blockage due to debris).
- If a major release of radioiodine or particulate materials occurs, inhalation dose may be a controlling criterion for protective actions—
  - Breathing air filtered through common household items (e.g., folded handkerchiefs or towels) may help reduce exposures.
  - After confirmation that the plume has passed, continued sheltering-in-place should be re-evaluated. People should remain sheltered until receiving official notice about leaving high exposure areas to avoid exposure to deposited radioactive material.

Shelters may be opened to vent any airborne radioactivity trapped inside.

The degree of protection provided by structures is affected by factors such as attenuation of gamma radiation (shielding) by structural components (the mass of walls, ceilings, etc.) and outside/inside air exchange rates. The use of large structures, such as shopping centers, schools, churches and commercial buildings, as collection points during evacuation mobilization will generally provide greater protection against gamma radiation than use of small structures. As with evacuation, delay in taking shelter during plume passage will result in higher exposure to radiation



The numbers represent dose reduction factors. A dose reduction factor of 10 indicates that a person in that area would receive 1/10th of the dose of a person in the open. A dose reduction factor of 200 indicates that a person in that area would receive 1/200th of the dose of a person out in the open. Figure taken from "Planning Guidance for Response to a Nuclear Detonation," Second Edition, National Security Staff, Interagency Policy Coordination Subcommittee for Preparedness and Response to Radiological and Nuclear Threats, June 2010, courtesy of Lawrence Livermore National Laboratory. The protection factors in this figure are specific to nuclear detonation fallout, but the variations in factors throughout typical buildings may be informative for other airborne radiological releases.

Conclusions

The radiological threat for Qatar is real and might result following a nuclear plant accident in a neighboring country or a military operation against these plants that will release radioactive plume that might affect the country and disturb the life of its citizens. In that respect, well-informed citizens is the best antidote for ignorance and fear radiation might evoke. Certain groups of people might be affected more – children and pregnant women and the same applies regarding agriculture and marine species and water sources. This will not be a sporadic incident but its effects will last for months or even years.

March 2012

Restrictions on hundreds of Welsh and Cumbrian sheep farms dating back to the Chernobyl nuclear disaster have finally been lifted – 26 years on.

The Food Standards Agency (FSA) said the controls were not "proportionate" to the "very low risk" and removing them would not compromise the consumer.

The Chernobyl disaster in 1986 affected 10,000 UK farms, including 334 in north Wales. The movement of sheep was heavily restricted after the nuclear disaster.

Before farmers could sell livestock, the animals' radiation levels had to be monitored. If they were above a certain level, the sheep were moved to another area and the levels had to subside before they could be sold and consumed.

The lifting of the restrictions comes after a 12-week consultation with key stakeholders including consumers, affected farmers, farming unions and trade bodies.

The FSA board agreed to lift the controls from 1 June, 2012.

We've had the assurances that the product is completely safe for human consumption and that's the main thing Ed Bailey, National Farmers' Union Cymru president

Ed Bailey, National Farmers' Union Cymru president, said: "It cannot be anything else apart from good news. We've had the assurances that the product is completely safe for human consumption and that's the main thing."
Out of the 9,800 UK holdings, and more than 4m sheep originally placed under restriction, there are only 327 farms in north Wales and eight farms in Cumbria still under restrictions.

NOTE: The distance between Ukraine and UK is ~2.500 km.

Unmanned Radiation Monitoring Tech to Save Lives

Source: https://i-hls.com/archives/106819

Feb 05 – Drones can prevent the exposure of people to radiation. UAV-based technologies will be crucial for advancing radiation monitoring, including enhancing the application of environmental mapping and improving long-term monitoring of contaminated areas.
In the aftermath of a nuclear accident, such as the one at Fukushima Daiichi Nuclear Power Plant in 2011, the radiologically contaminated area in the vicinity of a reactor can be too dangerous for people to enter to monitor radiation. A new drone technology, developed by the International Atomic Energy Agency (IAEA) for use by the authorities of Fukushima Prefecture in Japan, will make this task easier.
IAEA-developed instrumentation and methodology for Unmanned Aerial Vehicles (UAVs) equipped with radiation detectors, cameras and GPS devices has been tested and validated under real conditions and is now available for practical use in routine or emergency situations.
Based on this experience, the IAEA offers to assist interested Member States to develop and implement this technology for radiological mapping following a nuclear or radiological emergency.
The IAEA and Fukushima Prefecture first started working together on developing and applying UAVs for radiological monitoring in 2012, providing a complete UAV-based instrumentation system for radiation measurements as well as post-measurement analysis and interpretation methodology and training.
Recent breakthroughs in UAVs include larger payloads, integrated detectors and sensors, improved self-navigation and the ability for the vehicles to work in cooperation with other UAVs as well as ground systems. The IAEA is currently working on the integration and testing of new, improved instrumentation, including its adaptation to the next generation of UAVs.
"When combined with high-quality camera capabilities, the new system will allow obtaining a full 3D aerial photogrammetry model superimposed with the radiological maps and radionuclide identification," said Danas Ridikas, Head of the IAEA Physics Section.
The data collected using the new UAV systems can be used to assess potential radiation risks and help establish appropriate remediation, decontamination and nuclear waste management plans and strategies in Japan.
The UAVs are equipped with radiation detectors, cameras and GPS devices. After the UAV takes off, radiation readings and other relevant information are synchronized with exact GPS position and sent in real time to the pilot at the ground station and stored onboard. After landing, all detailed data is recovered, which means that the photographic/geographic information is reconstructed together with the corrected data of the radiation measurements. The satellite-like photographs and the analyzed radiation data measurements are then made available to decision-makers for further action.

Why is America getting a new $100 billion nuclear weapon?

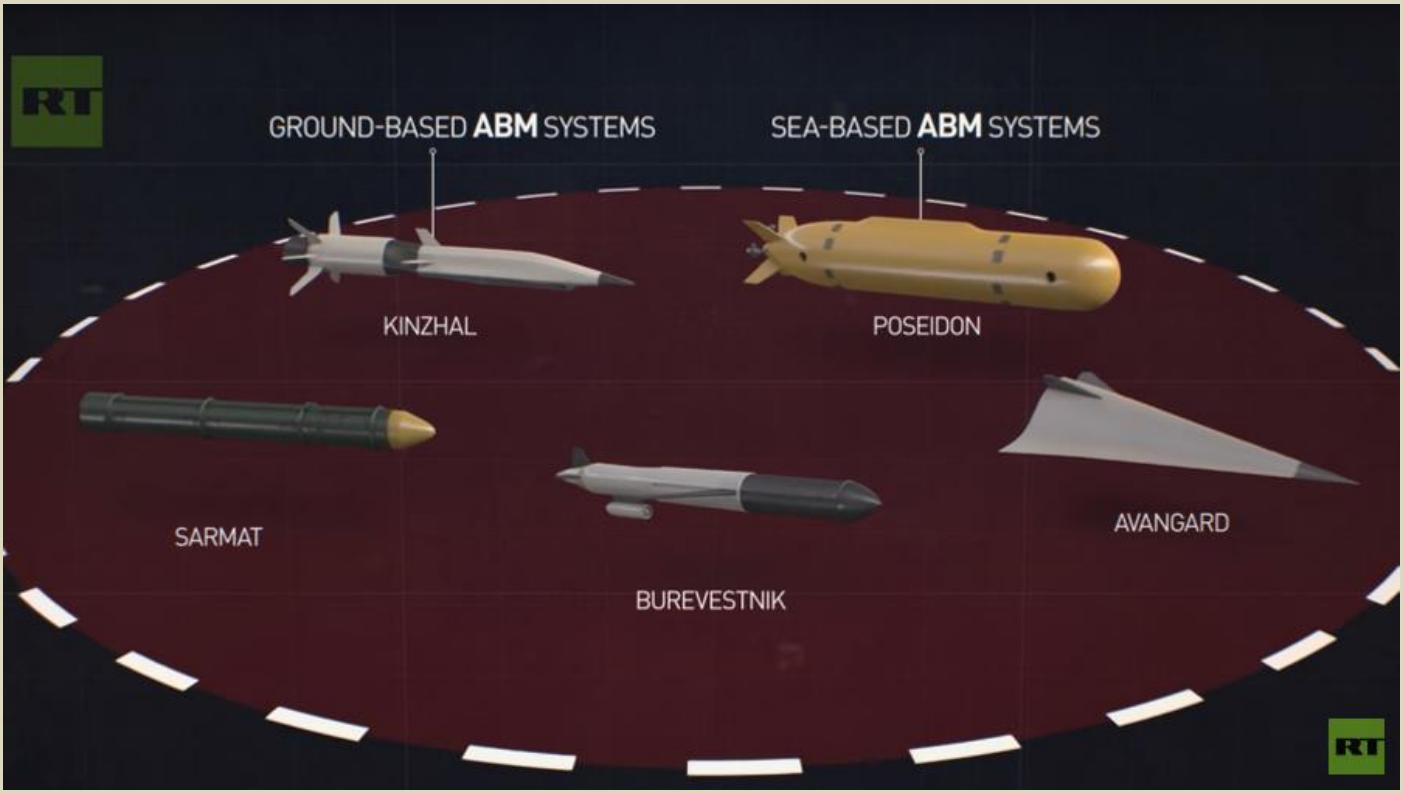
America is building a new weapon of mass destruction, a nuclear missile the length of a bowling lane. It will be able to travel some 6,000 miles, carrying a warhead more than 20 times more powerful than the atomic bomb dropped on Hiroshima. It will be able to kill hundreds of thousands of people in a single shot. The US Air Force plans to order more than 600 of them.

Norway intelligence warns about new nuclear weapons technology developed by Russia

Source: https://thebarentsobserver.com/en/security/2021/02/norway-intelligence-warns-about-new-nuclear-weapons-technology-developed-russia

Feb 08 – Objectives with such tailored weapons could be to easier penetrate missile defense systems, or to compensate for conventional inferiority, according to the annual report from Norway's Intelligence Service (NIS).

Several of the new weapons do not fit into the traditional framework of arms control treaties.
Last week, Russia and the United States in a last-minute call agreed to extend the New Start Treaty by another five-year period. The treaty is a successor to previous negotiations on the reduction and limitation of strategic offensive arms between the Soviet Union and the United States.
Although the global stockpile of nuclear weapons has been substantially reduced, the picture is way more complex than during the Cold War, the NIS report presented on Monday said.
In a phone interview, Chief of the Norwegian Intelligence Service, Vice Admiral Nils Andreas Stensønes, elaborated.
"It is our worry that the New Start Treaty is not sufficient enough to cover the new technological developments," Stensønes said and added the agreements should be updated.
Two nuclear weapon systems of particular worry are the Poseidon and the Burevestnik.



The Poseidon is a nuclear-powered, nuclear-tipped underwater mega-drone. Burevestnik, which NATO designates as SSC-X-9 Skyfall, is a nuclear-powered cruise missile with global reach and the ability to counter future missile defense systems.
None of the systems are yet ready, but testing and development take place in northern Russia, areas the Norwegian Intelligence Chief defines as "near Norwegian territory," that be the Barents Sea, White Sea, Kola Peninsula and Novaya Zemlya.
The Barents Observer has previously reported about the 2019 disastrous test in the White Sea when a Burevestnik explosion outside Nenoksa test range was followed by a radiation spike in Severodvinsk, a city 40 kilometers to the east. The missile was reportedly tested at Novaya Zemlya in 2017, 2018, and possibly also this winter.
It has been unclear where and how testing of the Poseidon nuclear-powered drone takes place, but a previously published photo shows the *Akademik Aleksandrov*, a ship sailing special missions for the Main Directorate of Deep-Sea Research, en route out of Severodvinsk with the mega-drone onboard. Nuclear submarines to carry the Poseidon, like the *Belgorod* and the *Khabarovsk*, are currently under testing and construction at the yards in Severodvinsk.

Significant risk
Nuclear activities in Norwegian neighboring areas constitute a significant risk, the Norwegian intelligence report reads.
Vice Admiral Stensønes said the new weapons are difficult to counter as "they fly low or travel underwater."
The report points to three reasons why Russia feels threatened, making the country's nuclear deterrence more important.
Firstly, Russia claims NATO has changed patterns from normal patrols and intelligence gatherings to simulated attacks on Russian targets, including with strategic bombers. Part of the Russian narrative is that NATO is coming closer to its borders. Secondly, Moscow

accuses NATO of introducing new areas of warfare, like the use of digital operations and militarization of the space, potentially being used to attack Russian ballistic missiles before launch. Thirdly, Russia blames the United States for undermining the global security balance and arms control treaties, by that pushing the world towards a new nuclear arms race.
The Norwegian Intelligence Service rejects the above listed misguided narrative that NATO is causing insecurity.
Moscow, however, considers an undermining of the strategic balance as an "existential threat" that could justify the use of nuclear weapons.

Tactical nukes
Last year, Kremlin for the first time published a policy paper on nuclear deterrence policy guidelines. The paper hints that should Russia face the prospect of being defeated in a conflict with NATO, the use of tactical nuclear weapons could be an option aimed for the purpose of escalation for de-escalation.
The Norwegian annual intelligence report is spelling out the shift in policy: "Russia has no self-imposed restriction on non-first use" [of nuclear weapons].
Newspaper Izvestia on Sunday listed Russia's new strategic weapon systems aimed to ensure the country's security from potential threats. Most of the weapons are either under testing or deployed in the north. Novaya Zemlya, the White Sea and the Barents Sea are Russia's most important testing areas for these new weapons.
On the Kola Peninsula are nuclear warheads stored at a large national-level facility and at several smaller base-level facilities.
These storages hold a large number of nuclear warheads to both non-strategic and strategic nuclear weapons, according to the Norwegian intelligence report.
"The storages are adequately secured, but transport of nuclear warheads by train and on-road pose a risk of incidents that could cause releases of radioactivity."
In peacetime, the report says, is it only the strategic forces that normally have nuclear warheads deployed. "The majority of nuclear weapons are in storage and will first be transferred to military units in times of possible conflict."

EDITOR'S COMMENT: Good Americans (yellow box in previous page); Bad Russians (this article). So boring!

Iran Increasing Enrichment Capacity at Underground Natanz Facility

Source: http://www.homelandsecuritynewswire.com/dr20210211-iran-increasing-enrichment-capacity-at-underground-natanz-facility

Feb 11 – According to a confidential report by the International Atomic Energy Agency (IAEA), Iran has begun enriching uranium with a second cascade of IR-2 centrifuges.
The 2015 nuclear deal, known as the Joint Comprehensive Plan of Action, or JCPOA, permits Iran to enrich uranium with first-generation IR-1 centrifuges. However, last December Iran told the IAEA that it had begun enriching uranium with the more efficient IR-2 centrifuges and that it would install three more IR-2 cascades.
"Iran has completed the installation of one of these three cascades, containing 174 IR-2m centrifuges, and, on 30 January 2021, Iran began feeding the cascade with UF6 [uranium hexafluoride feedstock]," the IAEA said in the report obtained by Reuters last week.
Iran's envoy to the IAEA tweeted: **"Thanks to our diligent nuclear scientists, two cascades of 348 IR2m centrifuges with almost 4 times the capacity of IR1 are now running… successfully in Natanz. Installation of 2 cascades of IR-6 centrifuges has also been started in Fordo. There's more to come soon."**
Bicom reports that tThe pace of uranium enrichment is vital to Iran's nuclear breakout capacity – the time needed for Iran to acquire enough fissile material for a nuclear weapon. The IR-6 is 10 times faster than the IR-1 at enriching uranium.
On Sunday, U.S. Secretary of State Antony Blinken said Iran was currently months away from being able to produce enough material to build a nuclear weapon. He further warned that timeframe could be reduced to "a matter of weeks" if Tehran further violates restrictions it agreed to under the JCPOA.
Israeli Energy Minister Yuval Steinitz on last Tuesday gave a less alarmist view when he told Israeli media that Iran was a year or two away from producing a nuclear bomb. "If they do everything to break out in terms of enrichment, it will be half a year [to produce the needed materials]; in terms of nuclear weapons, they are a year or two away."

Background
Iran is ramping up pressure on the Biden administration to end US sanctions that were introduced in the Trump years.
A *Foreign Affairs* article by Iran's Foreign Minister Mohammad Javad Zarif on 22 January laid out his government's conditions for returning to JCPOA compliance: The US lifts its

sanctions first; no discussions on a new and upgraded agreement, and no dialogue on Iran's missile program and regional conduct with non-regional actors.

On Monday, however, Zarif suggested the EU coordinate Washington's return to the nuclear deal in an interview with *CNN International*. "You know clearly there can be a mechanism to basically either synchronize it, or coordinate what can be done," he said.

Zarif also warned that Iran will end its implementation of the Additional Protocol (AP) to its comprehensive safeguards agreement with the IAEA in late February if its demands for sanctions relief have not been met. A suspension of the AP would be highly concerning insofar as it would reduce IAEA inspectors' access to Iranian nuclear facilities and make it much harder to identify illicit nuclear activity.

According to U.S.-based think-tank Institute for Science and International Security, recent high resolution satellite imagery shows that Iran is rapidly building a new centrifuge assembly facility at Natanz.

The underground facility is a particular concern for Western countries as it is protected by a thick layer of concrete and mountain rock.

Likud Minister Tzachi Hanegbi said yesterday that Israel may have to decide whether to launch such a strike alone or come to terms with a nuclear-armed Islamic Republic. "The United States will never attack the nuclear facilities in Iran, Israel must decide whether it will accept a nuclear Iran. Israel will be forced to act independently to remove this danger," Hanegbi told Israeli media.

Steinitz's assessment is the same as the IDF. Last October, the outgoing head of Military Intelligence told Israeli newspaper *Yediot Ahronot* from the moment of a breakout decision, Iran will be two years away from a bomb.

Two weeks ago, the IDF Chief of Staff gave a rare speech in which he advocated for the U.S. not to return to the JCPOA, contradicting stated policy by the Biden administration.

U.S. State Department Spokesperson Ned Price said last week that the Biden team will consult with allies and partners before reaching the point of engaging with the Iranians.

One of the concerns in Israel and the Gulf is that the Biden administration will lift sanctions before negotiating with Iran on a new agreement that further extends restrictions on Iran's nuclear program, as well as its ballistic missile and regional activity.

Israel's security cabinet is set to hold its first meeting in several months to discuss Iran's continued nuclear violations and how to respond if the Biden administration lifts the sanctions currently imposed on Iran and re-enters the JCPOA agreement. Prime Minister Netanyahu is then expected to travel to the UAE and Bahrain to coordinate a unified stance to the Biden team.

Why No State Needs Thousands Of Nuclear Warheads – OpEd

By Ryan McMaken

Source: https://www.eurasiareview.com/12022021-why-no-state-needs-thousands-of-nuclear-warheads-oped/

Feb 12 – Last week, the United States signed a five-year extension of the New START arms control treaty with Russia. Russia's President Putin signed the treaty shortly thereafter. The "Strategic Arms Reduction Treaty" allows Russia and the US to monitor each other's nuclear forces, facilities, and activities. The idea is to keep track of the relative strength of the two regimes' respective arsenals and to encourage reductions. **The treaty also caps the number of deployed strategic nuclear warheads at 1,550 each.** (The total stockpiles for the US and Russia are 4,700 and 4,300, respectively.)

The move is a departure from the Trump administration's opposition to the treaty. The Trump administration had wanted to renegotiate the treaty, insisting that so-called tactical nuclear weapons—designed for battlefield use—be included. As it is, the treaty focuses only on strategic weapons. The Trump administration also insisted that China be added to the treaty. The Chinese declined to participate. President Trump also ended two other arms treaties, the Intermediate-Range Nuclear Forces (INF) Treaty and the Open Skies Treaty.

These all may sound to many readers like rather momentous changes to policy. But this is all a lot of political theater.

Just as the Trump administration used the abrogation of these treaties as red meat for the "America first" crowd,1 the Biden administration is surely more than happy to use the treaty to demonstrate how Biden is a departure from Trump. The treaty may even offer military lobbyists the opportunity to point to Russian stockpiles and claim the US must find ways to balance or counter Russian nuclear capabilities. Putin, meanwhile, can say that he signed a treaty limiting the arsenal of the far-richer American regime, which has a lot more money to spend on nuclear weapons. For Putin, this is important because the Russian state has been looking to economize and has been reducing or moderating military spending in recent years.

In short, arms treaties like New START serve a *domestic* political function. They help politicians take credit for allegedly pursuing peace while also potentially justifying more military spending overall.

In practice, however, the extension of the treaty does not reduce the risk of nuclear war, and it certainly won't make nuclear arms disappear or even be substantially reduced. *It is the*

presence of the nuclear weapons themselves that has deterred both the US and the Russians—and the Soviets before them—from a nuclear conflict. Moreover, the arms limitations provisions of the treaty won't change the *status quo* of deterrence. Both nations have more than enough nuclear capability to achieve a deterrent effect, and given the current thinking within each regime, it's a safe bet neither will agree to a treaty which threatened to reduce arsenal levels to anywhere near levels of "minimum deterrence."

Yet, in practice, both regimes could reduce nuclear spending and nuclear stockpiles far below current levels without sacrificing deterrence. Neither regime, however, is likely to risk making any sizable reductions. The ideal of overwhelming nuclear force still has many friends in both Washington and Moscow.

The Value of Minimum Deterrence

Whether or not politicians believe in the use of minimum deterrence has little to do with whether or not it is actually effective, and arms agreements like New START don't do much to push regimes in this direction.

In a 1990 essay titled "Nuclear Myths and Political Realities," Kenneth Waltz—perhaps the most influential scholar of international relations of the past fifty years—outlines how "strategic arms agreements do not have military but economic and political, significance."2

Counting up the total number of missiles in these enormous arsenals does little, since, for nations that are already well above the threshold of achieving nuclear deterrence, these treaties don't change the military calculus.

What really matters is the perception that the other side has second-strike capability, and this certainly exists in US-Russia relations. Once each regime knows that the other regime has second-strike capability, the competition is over. Deterrence is established. Waltz notes:

So long as two or more countries have second-strike forces, to compare them is pointless. If no state can launch a disarming attack with high confidence, force comparisons become irrelevant…. Within very wide ranges, a nuclear balance is insensitive to variation in numbers and size of warheads.

The focus on second-strike capability is key because pro-arms-race policymakers are quick to note that if a regime is able (with a first strike) to destroy its enemy's ability to retaliate in kind, then a nuclear war can be "won."

Second-Strike Capability Evens the Score

But, as shown by Michael Gerson in *International Security* (2010) establishing second-strike capability—or, more importantly, the *perception* that a regime has it—is not as difficult as many suppose. Gerson writes:

A successful first strike would require near-perfect intelligence, surveillance, and reconnaissance (ISR) to detect, identify, and track all of the adversary's nuclear forces; recent events surrounding U.S. assessments of Iraq's suspected WMD [weapons of mass destruction] capabilities forcefully demonstrate the challenges of reliable, accurate, and unbiased information. Intelligence regarding where an adversary's nuclear weapons are located and if the state is actually planning to attack could be wrong or incomplete, and an attempted first strike based on inaccurate or incomplete information could have far-reaching negative consequences.

This can be countered through a variety of methods, including secrecy and the ability to move weapons delivery systems around. This is why the US, Russian, and Chinese regimes have long been so enthusiastic about the so-called nuclear triad. It is assumed that if nuclear weapons can be delivered by submarine, aircraft, and land, then it would be impossible for an opposing regime to destroy all three at once and achieve first-strike victory.

But even in the absence of a triad, an opposing regime that seeks a total first-strike victory has few grounds for much confidence. As Waltz shows, "Nuclear weapons are small and light; they are easy to move, easy to hide, and easy to deliver in a variety of ways." **That is, if a regime manages to move around and hide even a small number of planes, subs, or trucks, this could spell disaster for the regime attempting a successful first strike.** Gerson explains:

A nuclear first strike is fraught with risk and uncertainty. Could a U.S. president, the only person with the power to authorize nuclear use and a political official concerned with re-election, his or her political party, and their historical legacy, ever be entirely confident that the mission would be a complete success? What if the strike failed to destroy all of the weapons, or what if weapons were hidden in unknown areas, and the remaining weapons were used in retaliation?

Nor must it be assumed that a *large* number of warheads is necessary to achieve deterrence. Waltz recalls that Desmond Ball—who had advised the US on escalation strategies—convincingly asserted that the **nuclear weapons necessary for deterrence numbered "not in the hundreds but in the tens**."3 Ball contended that a debilitating attack on the US could be achieved with as few as fifty warheads.

Proceeding on the assumption that an enemy has no warheads left following a first strike requires an extremely high level of confidence, because the cost of miscalculation is so high. If a regime initiates a first strike and misses only a few of the enemy's missiles, this could lead to devastating retaliation both in terms of human life and in terms of the first-strike regime's political prospects.

This is why Waltz concludes that a rudimentary nuclear force can achieve deterrence if there is even a small and plausible chance of second-strike capability. A small nuclear strike is nonetheless disastrous for the target, and thus "second-strike forces have to be seen in absolute terms." Waltz correctly insists that calculating the relative dominance of one arsenal over another becomes a waste of time: "the question of dominance is pointless because one second-strike force cannot dominate another."
The conclusion is that a small second-strike force is sufficient. Naturally, this can be attractive to smaller or cash-strapped regimes, such as the Soviet Union, which in its final decades found itself devoting ever larger amounts of its GDP to military spending.

A Minority View
This remains the minority view. Nikita Khrushchev, for example, faced much opposition to his plans to adopt a minimum deterrence posture in the Soviet Union after 1961. Conservatives in the military and Politburo were vehemently opposed to the plan, in part because it included cutting back on spending on conventional military forces. But the opposition was also due to the fact that the hardliners were quite convinced by the perceived necessity of immense, flexible, and overwhelming force.4
In the United States, of course, minimum deterrence has never been very popular, especially among conservatives. For example, spending on the US nuclear arsenal increased 50 percent under Donald Trump from 2016 to 2020. The Pentagon and Congress continue to put sizable faith in maintaining a large, diverse, and expensive arsenal.
In any case, the rejection of minimum deterrence achieves a useful political goal, as described by Waltz:
The claim that we need a seamless web of capabilities in order to deter does serve one purpose: it keeps military budgets wondrously high.
New START isn't likely to change this, and if the treaty presented any real obstacle to military spending or the military establishment, it would be long gone. Yet the US regime could easily slash its nuclear budget and stockpile without sacrificing anything in the way of nuclear deterrence. Although much is being made in recent years of China's growing nuclear stockpile, China's total nuclear arms amount to a mere fraction of the US's *deployed* warheads. But facts like these have never gotten in the way of the promilitary narrative on Capitol Hill.

References
1.The Trump administration's lack of interest in any ostensible limits on the nuclear arsenal also helped pave the way for increased spending on nuclear arms. Under Trump, spending on the nuclear arsenal increased 50 percent from 2016 to 2020.
2.Kenneth Waltz, "Nuclear Myths and Political Realities," *American Political Science Review* 84, no. 3 (September 1990): 731–45.
3.Waltz, p. 740.
4.John Erickson, "Détente, Deterrence, and 'Military Superiority: A Soviet Dilemma," *World Today* 21, no. 8 (August 1965): 339, 344.

***Ryan McMaken** is a senior editor at the Mises Institute. Ryan has degrees in economics and political science from the University of Colorado and was a housing economist for the State of Colorado. He is the author of Commie Cowboys: The Bourgeoisie and the Nation-State in the Western Genre.*

EDITOR'S COMMENT: This very interesting article is based on the hypothesis/reality that both involved nations do possess nuclear weapons. What if one country has a small number (2-3) of nuclear weapons and the other country has none? This is when ISR is mandatory and a pre-emtpive attack is justified. On the other hand, recent developments in our neighborhood (SE Mediterranean) have shown that possession alone is not as strong deterrent as expected mainly because the offender thinks that a nuclear attack in the 21st century is out of the question.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

EXPLOSIVE NEWS

There's No Single Solution to Standoff Explosive Detection

Source: https://i-hls.com/archives/106624

Jan 27 – US Army researchers use a drone-based multi-sensor system to enable standoff detection of explosive hazards using machine learning techniques.

Augmented reality (AR) overlays will be used in a US Army research for the detection of roadside explosive hazards, such as improvised explosive devices (IEDs), unexploded ordnance and landmines. Route reconnaissance in support of convoy operations remains a critical function to keep Soldiers safe from such hazards, which continue to threaten operations abroad and continually prove to be an evolving and problematic adversarial tactic. The problem is that there is no single sensor solution that will rule them all in regards to different emplacement scenarios.

The US Army Combat Capabilities Development Command (DEVCOM), Army Research Laboratory (ARL), and other research collaborators were funded by the Defense Threat Reduction Agency, via a program which focuses on a system-of-systems approach to standoff explosive hazard detection.

In Phase I of the program, researchers took 15-months to evaluate mostly high-technology readiness level (TRL) standoff detection technologies against a variety of explosive hazard emplacements. In addition, a lower-TRL standoff detection sensor, which was focused on the detection of explosive hazard triggering devices, was developed and assessed. According to the Army, the Phase I assessment included probability of detection, false alarm rate and other important information that will ultimately lead to a down-selection of sensors based on best performance for Phase II of the program.

The sensors evaluated during Phase I included an airborne synthetic aperture radar, ground vehicular and small unmanned aerial vehicle LIDAR, high-definition electro-optical cameras, long-wave infrared cameras and a non-linear junction detection radar.

Researchers carried a field test in real-world representative terrain over a 7-kilometer test track and included a total of 625 emplacements including a variety of explosive hazards, simulated clutter and calibration targets. They collected data before and after emplacement to simulate a real-world change between sensor passes.

Terabytes of data was collected across the sensor sets which was needed to adequately train artificial intelligence/machine learning (AI/ML) algorithms. The algorithms subsequently performed autonomous automatic target detection for each sensor.

The detection algorithms are able to provide 'confidence levels' for each suspected target, which is displayed to a user as an augmented reality overlay. The detection algorithms were

executed with various sensor permutations so that performance results could be aggregated and determine the best course of action moving forward into Phase II.
Future research into the technology will enable real-time automatic target detection displayed with an augmented reality engine, according to auganix.org.

Panic as letter bomb at Lidl HQ

Source: https://www.express.co.uk/news/world/1399150/Germany-latest-explosion-Lidl-HQ-Heilbronn-letter-bomb-injured-bomb-squad-terror-updates

A bomb has exploded at Lidl's headquarters in Germany injuring three people.
The incident occurred at the head offices of the supermarket giant in Neckarsulm, southwest Germany, at around 3pm this afternoon.
Another 100 employees were evacuated from the building as a bomb squad arrived to deal with the threat.
Local police have launched an investigation into the exact causes of the incident. Police spokesman Gerald Olma, said: It was probably a package or a letter bomb. She said a wide cordon remains in place around the building.
The Police stressed the bomb was a package which had exploded after being opened by a member of staff.
Police added there was no evidence that Lidl had faced any blackmail or threats prior to the deliverance of the malicious package.
One of the three people injured sustained moderate injuries in the incident while the other two escaped with light injuries.

The Suicide Bombing That Moved Israel to Action

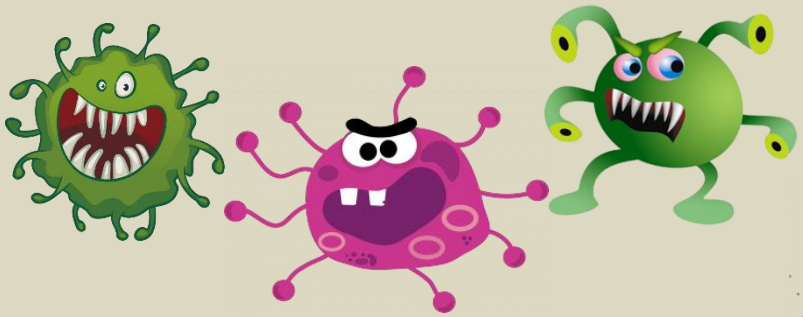
Source: https://blogs.timesofisrael.com/the-suicide-bombing-that-moved-israel-to-action/

Feb 16 – For almost a decade, Israel suffered from a new kind of terrorism where an individual terrorist would approach a target with explosives attached to himself and kill himself along with others.
From 1993 to 2002, Israel experienced a large amount of suicide bombings targeted towards Israeli civilians.
Western intellectuals along with Islamic fundamental apologists made the flawed argument that because Israeli Citizens are required to do military service, they are legitimate targets at any age.
Israeli response to suicide bombings were pathetic with no real ability to deter such attacks because they were unable to properly punish perpetrators or stop incentives.
According to the Oslo Accords the IDF was not allowed to enter area A and most of the responses to attacks where to either put the perpetrators in prison or demolition of their homes.
Terrorists sent to prison were rewarded with a several college degrees from the American University of Cairo and stipends from the Palestinian Authority. Homes destroyed by the Israeli Military after a court order would be rebuilt a few months later with assistance from the Palestinian Government and neighbors.
Passover of 2002 in Netanya with many elderly Holocaust survivors along with other guests were celebrating the first day of Passover.
Singing traditional songs and speaking at the table about the Jewish Peoples' Exodus from Egypt held great meaning to many of the survivors whose memory of their time in concentration camps were still vivid after sixty years.

Dressed up as a woman to avoid security, Abdel-Basset Odeh entered the **Park Hotel** carrying a large number of explosives in a suitcase.
Odeh would hear all the 250 people in the dinning hall starting to begin the custom of the Passover Seder with the blessing over the wine.
Detonation of the bomb resulted in the deaths of thirty people with 140 other guests injured from the blast.

One of the most sacred and ancient rites in the Jewish religion celebrated for three millennia was attacked by a despicable terrorist.
Hamas claimed responsibility for the attack and proudly proclaimed that such attacks should only continue to liberate what they perceive to be their country from the river to the sea.
CNN reported Ahmed Yassin's (Hamas spiritual leader) statement following the attack:
"From his home in Gaza City, Sheik Ahmed Yassin, the spiritual leader of Hamas, said Wednesday's bombing was "a message to the Arab summit to confirm that the Palestinian people continue to struggle for the land and to defend themselves no matter what measures the enemy takes."
Sheik Yassin exemplifies Hamas' attitude toward non-combatants with his own words by proclaiming such attacks are legitimate for the struggle against the Jewish State.
Suffering such a terror attack within Israel Proper where mostly Israeli Senior citizens were murdered in cold blood by a suicide bomber.
The Israeli Public finally pressured their own government to act and work militarily to put a stop to the bombings killing its own civilians.
After the Park Hotel Attack, the Israeli government ordered 20,000 reservists and launched Operation Protective Shield.
Operation Protective Shield brought the IDF into Area A and had a direct positive impact in lowering the amount of suicide bombings the following years.
History has shown that only when the sword is at the neck of the Israeli public does the government act to put an end to the enemy inflicting damage on its citizens.

Shlomo Alegra *was born in Miami, Florida in 1989 and moved to Israel in 2012. He holds a degree from Florida Atlantic University in Political Science and served in the IDF as a combat soldier in the Netzach Yehuda Battalion. After serving in the military Shlomo studied in Yeshivat Shavie Hevron where he lived in Hebron. He now lives in Kiryat Arba, is a proud reservist in the Golani Brigade, and is a blogger for the Times of Israel.*



ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

CYBER NEWS

COVID-19 Effect: What is Smart City's Direction?

Source: https://i-hls.com/archives/106690

Jan 29 – While market forecasts paint a rosy picture of smart city investment, many municipalities around the world are slashing their budgets as the economic fallout from the COVID-19 pandemic continues.

One of the latest smart-city casualties was networking equipment giant Cisco's Kinetic for Cities software, a dashboard for governments to manage data from their local smart-city projects. Cisco said in December that it would kill the product. Instead of pushing its software, Cisco plans to work with city governments on other efforts involving Internet connectivity.

Just a few years ago, smart cities had major buzz. The idea was to use machine learning to crunch data collected across cities to, for example, minimize traffic delays and reduce pollution, according to fortune.com. However, some smart city projects had been focused on fixing problems that are no longer as pressing. Reducing traffic and parking now in many cities isn't as important because many workers no longer commute to downtowns because of shelter-in-place rules.

Now, city governments see "security and safety" as a priority, and have reallocated some of their budgets to solve the problem, Forrester analyst and smart city expert Michele Pelino asserts. She is unsure when more ambitious projects, like using machine learning to optimize traffic lights, will be reinstated. "Where is the money going to come from?" Pelino said.

So what is the new direction of smart city policies? To adapt to the budget shortfalls resulting from the COVID-19 pandemic, smart city efforts must be more strategic, said Ruthbea Yesner, vice president of Government Insights and Smart Cities at IDC Government Insights, an IT market research firm.

"..The question becomes what are the foundational tools that you need to start to think about for resiliency — and let's take away contingency planning, disaster recovery, backup plans, redundant data centers, having a readiness response, a risk management response. I think that's all what everyone thinks of when they think of business continuity. You have plans to continue operations if there's an emergency. What does that mean in light of COVID?"

According to IDC, during the COVID-19 crisis, cities focused on network and collaboration tools, digital communications platforms and rapid upskilling to get employees up and running in virtual environments. The following phases in the continuum are economic slowdown, budget reductions, a return to growth and the next normal. That last phase involves cloud and infrastructure optimization, as-a-service deployments and data analysis to help drive forward-looking decisions.

Cities must assess which stage they are in to determine what IT will best get them to the next phase so they can achieve that next normal, Yesner said, according to gcn.com. In crisis mode, cities focus on business continuity, but the economic slowdown calls for cost optimization, and the budget reductions phase focuses on resiliency. Returning to growth spotlights innovation and targeted investment.

Microsoft patented a chatbot that would let you talk to dead people. It was too disturbing for production

Quicktake: cyber war gaming and why UAE banks are doing it

Source: https://www.thenationalnews.com/business/technology/quicktake-cyber-war-gaming-and-why-uae-banks-are-doing-it-1.1159956

Feb 05 – Cyber attacks on financial institutions surged 238 per cent globally between February and April last year, as more consumers began transacting online at the peak of coronavirus-induced lockdowns, according to cyber security firm VMware Carbon Black.

Last month, the Central Bank of the UAE and the UAE Banks Federation conducted a 'cyber war gaming' exercise or a simulation drill to assess the preparedness of the country's banking sector amid potential cyber threats.

"The war gaming exercise as a community has never been more important … in order to rehearse, train, test our ecosystems, make quicker decisions and build muscle memory," Mohammed Darwish Azad, group chief information and security officer of Emirates NBD, Dubai's biggest lender by assets, said.

The Covid-19 pandemic has accelerated digitisation – a trend that was already underway in the UAE – at an unprecedented rate.

"Digital banking offers customers convenience and faster processing of financial transactions … it [also] heightens vulnerabilities that banks spend years pre-empting and preparing for," Hariprasad Chede, head of information security risk at National Bank of Fujairah, said.

The National looks at the importance of cyber simulation drills in the banking sector.

What is cyber war gaming?

It involves a cyber attack orchestrated through KPMG's proprietary platforms that includes multiple scenarios and attack vectors such as malicious email attachments, pop-up messages and chat rooms.

All participating banks respond to these scenarios, testing their incident response and crisis management capabilities in real time.

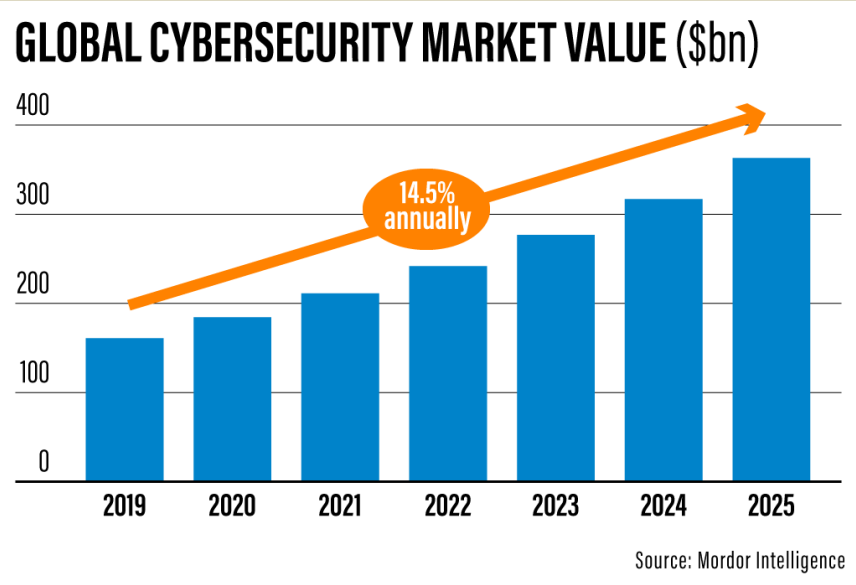
"The cyber simulation is [a] cross-functional exercise … it requires us to conduct detailed planning, complex scenario building, designing the cyber range for technical teams, training and awareness, testing the range and collaborating across banks," said Mr Azad, who is also the UBF's information security chairperson.

Banks' response

In the last month's drill, technical team members from different banks were challenged to react to real life scenarios by detecting, containing and responding to diverse online threats.

Management and executive management team members were challenged to collaborate, apply their respective cyber response strategies and take quick decisions at critical moments.

"Our preparations involved constant dry runs and connecting the story line before the training and simulation days … [and] supporting our leaders to power through the exercise," Mr Azad said.



Top takeaways

Cyber resilience is critical for modern financial systems, as disruptions can have a "far-reaching impact for banks and the economy", according to Jamal Saleh, UBF director general. He added that the Covid-19 pandemic has highlighted the importance of cyber resilience to protect the integrity of the banking system.

Cyber war gaming is one of the tools to help the banking sector test and evaluate institutional preparedness, he said.

"Conducting simulation drill of multiple scenarios and attack vectors is one of the innovative ways to collaborate at the national level with banks and relevant stakeholders to deal with cyber threat scenarios," Mr Saleh said.

Effective communication and being prepared for the unknown are important to deal with such crises, Mr Azad said.

How serious is the threat?
A 2019 report by Accenture revealed that the average annualised cost of cyber crime for financial organisations worldwide increased to $18.5 million – the highest of all industries included in the study. It was almost 40 per cent higher than the average cost of $13m per firm across other industries.
"Our biggest strength is the culture we have built with our employees, partners and customers as we continue to invest in awareness campaigns and sessions to ensure they are fully equipped to counter potential cyber security threats," Mr Chede said.
"As a result, after measuring our staff's readiness to cyber security, we can report that their ability to mitigate threats has increased by 90 per cent over the last five years," he added.

How to Combat COVID-19 Misinformation

By John Whyte, MD, MPH and Steven Brill
February 03, 2021
Source: https://www.medscape.com/viewarticle/945151

- **NewsGuard is a website that rates the reliability of more than 6000 websites responsible for about 95% of the news online.**
- **NewsGuard created HealthGuard to identify trustworthy sources of online health news and information. Consumers can download the HealthGuard browser extension for free until June 2021 to rate the reliability of online health sources.**
- **HealthGuard rates health sources based on ethical journalism criteria, including not repeatedly publishing false content, presenting information responsibly, regularly correcting or clarifying errors, and handling the difference between news and opinion responsibly.**
- **Consumers can consider using HealthGuard's rating system on their own to avoid unreliable websites.**
- **NewsGuard was created to restore faith in legitimate journalism.**

This transcript has been edited for clarity.

John Whyte, MD, MPH: Welcome, everyone. Thanks for joining. I'm Dr John Whyte, chief medical officer of WebMD, and you're watching *Coronavirus in Context*. There's a lot of misinformation out there, especially when it comes to your health. How do you know what to believe?
To provide some insights and even give you some tools, I've asked Steven Brill to be here. He's an award-winning author, journalist, and co-CEO of NewsGuard. Mr Brill, thanks for joining me.
Steven Brill: Happy to be with you. Thanks for having me.

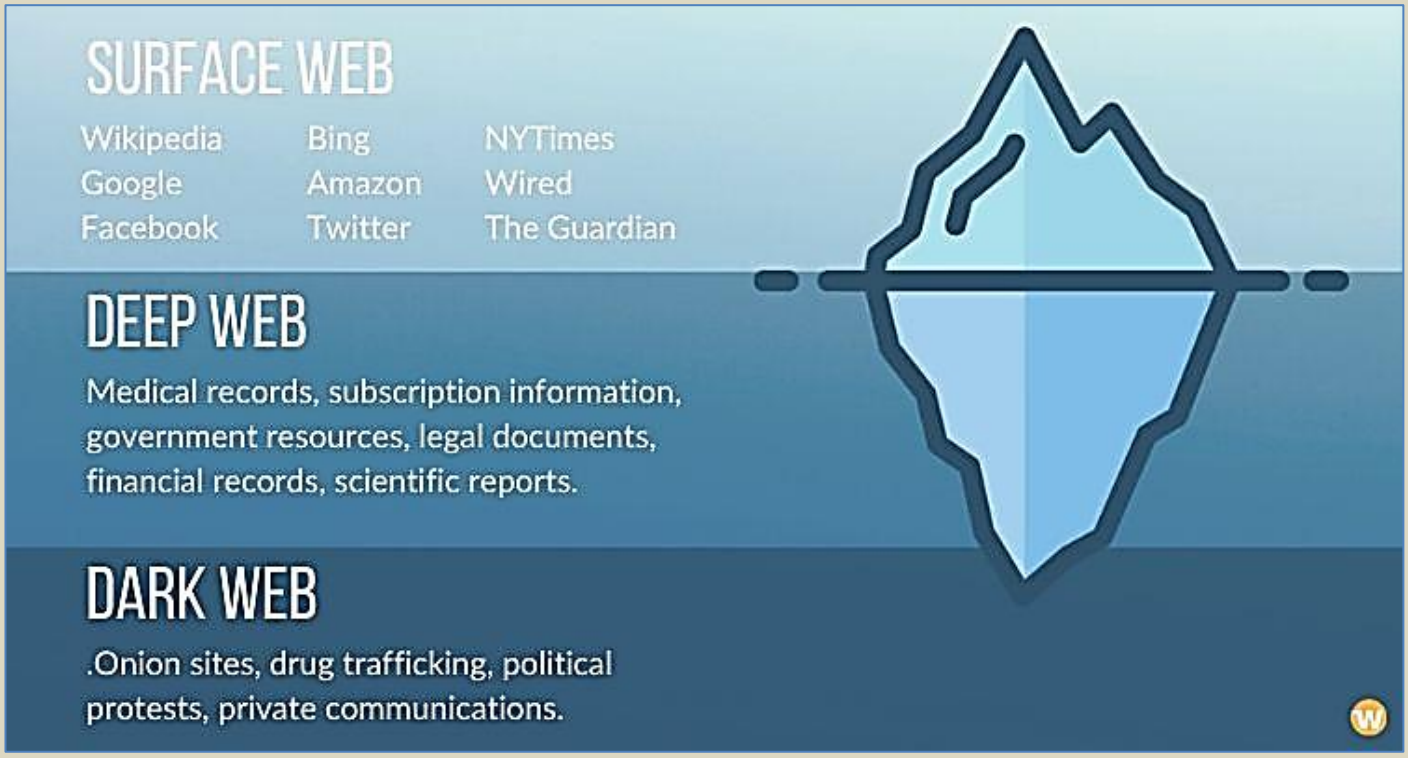
▶▶ **Read the full article at source's URL.**

The Evolution of COVID-19 Dark Web Marketplaces Before the Vaccine

Source: http://www.homelandsecuritynewswire.com/dr20210204-the-evolution-of-covid19-dark-web-marketplaces-before-the-vaccine

Feb 04 – New research carried out by City University of Londondata scientist, Dr. Andrea Baronchelli, and colleagues, into the dark web marketplace (DWM) trade in products related to COVID-19, has revealed the need for the continuous monitoring of dark web marketplaces (DWMs), especially in light of the current shortage and availability of coronavirus vaccines.
In their paper, published in *EPJ Data Science*, Dr. Baronchelli and his colleagues analyzed 851,199 listings extracted from 30 DWMs between 1 January 2020 and 16 November 2020 before the advent of the availability of the coronavirus vaccine.
They identify 788 listings directly related to COVID-19 products and monitor the temporal evolution of product categories including Personal Protective Equipment (PPE), medicines (e.g., hydroxychloroquine), and medical fraud.
The authors compare trends in the temporal evolution of trade in these products with variations in public attention, as measured by Twitter posts and Wikipedia page visits.
Among their discoveries, the paper's authors highlight the importance of dark web players such as DarkBay/DBay.
"In our dataset, DarkBay/DBay is featured prominently among DWMs offering COVID-19 specific listings. Ranking in the top 100 sites in the entire dark web, DarkBay/DBay offers more listings categories than other DWMs. It was also frequently accessible during the period of time monitored during this research, with an uptime of 80 percent, higher from the 77 percent uptime of Empire, the largest global DWM at the time of writing".

Critically, the authors highlight the importance of the continuous monitoring of DWMs, especially given shortages in the availability and supply of COVID-19 vaccines in various regions of the world:



"Uninformed citizens exposed to waves of misinformation, such as the ones related to hydroxychloroquine, chloroquine, and azithromycin, may be tempted to shop on DWMs thus exposing themselves to serious health risks. Moreover, the availability of regulated products currently in shortage in the traditional economy undermines anti-price gouging regulations and regulated businesses which sell the same products," the study's authors say.

Hacker tries to poison water supply of Florida city

Source: https://www.bbc.com/news/world-us-canada-55989843

Feb 08 – A computer hacker gained access to the water system of a city in Florida and tried to pump in a "dangerous" amount of a chemical, officials say.

The hacker briefly increased the amount of **sodium hydroxide** (lye) in Oldsmar's water treatment system, but a worker spotted it and reversed the action.

Lye is used in small amounts to control acidity but a large amount could have caused major problems in the water.

Oldsmar Mayor Eric Seidel said: "There's a bad actor out there."

No arrests have yet been made and it is not known if the hack was done from within the US or outside.

A computer controlling Oldsmar's water treatment system was remotely accessed on Friday.

A plant operator saw an attempt to access the system in the morning but assumed it was his supervisor, the Tampa Bay Times reported.

But another attempt was made early in the afternoon and this time the hacker accessed the treatment software and increased the sodium hydroxide content from 100 parts per million to 11,100 ppm.

The operator immediately reduced the level to normal.

Sodium hydroxide is the chief ingredient in liquid drain cleaners. It is very corrosive and can cause irritation to the skin and eyes, along with temporary loss of hair. Swallowing it can cause damage to the mouth, throat and stomach and induce vomiting, nausea and diarrhoea.

Pinellas County Sheriff Bob Gualtieri said: "I'm not a chemist. But I can tell you what I do know is... if you put that amount of that substance into the drinking water, it's not a good thing."
But he added: "At no time was there a significant adverse effect on the water being treated. Importantly, the public was never in danger."
The Oldsmar plant provides water to businesses and about 15,000 residents.
The remote access programme to the water system has been temporarily disabled.

'Bad actors out there'

Analysis by Joe Tidy, cyber reporter

Imagine the horror as this worker watched their own mouse cursor being moved around the screen by an invisible hand. Then seeing it click open and adjust the electronic dials to poison the water.
Perhaps more terrifying is that this isn't the first time it's happened.
In 2016, a security report from Verizon detailed a similar attack on another unnamed US water facility. And in 2020 there were multiple unsuccessful hacks on Israeli water supplies.
This latest attack in Florida will do nothing to calm cyber-security experts who've been warning for years that so called "critical national infrastructure" facilities are being targeted.
Water, electricity, nuclear plants and transport are being probed for weaknesses all the time not just because of the potential for mass disruption but also because they are often running on out-of-date and vulnerable IT systems.
So far all attacks on water supplies have been averted.
But as Mayor Seidel put it in his press conference, this is an event that "puts everyone on notice: these types of bad actors are out there and this is happening".

Critical Lessons from Florida City's Close Call with Hacker Trying to Taint Water Supply

By Bridget Johnson

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/critical-lessons-from-florida-citys-close-call-with-hacker-trying-to-contaminate-water-supply/

Feb 11 – The hacker of a Florida city's water treatment plant who attempted to remotely contaminate the supply with a caustic chemical could have been a disgruntled employee or a nation-state, experts said, but outdated software and remote access controls underscored the need for security investments in critical infrastructure.
The Pinellas County Sheriff's Office said it was notified on Feb. 5 of computer software intrusions at 8 a.m. and 1:30 p.m. at the City of Oldsmar's water treatment plant. The system "allows for remote access by authorized users to troubleshoot any system problems from other locations," the sheriff's office said.
The first intrusion of the day "was brief and not cause for concern due to supervisors regularly accessing the system remotely to monitor the system," the sheriff's office said. At 1:30 p.m., a plant operator "witnessed a second remote access user opening various functions in the system that control the amount of sodium hydroxide in the water."
"The operator noted the remote access user raised the levels of sodium hydroxide in the water. The operator immediately reduced the levels to their appropriate amount," the sheriff's office said. "The initial investigation revealed that the hacker remotely accessed the treatment plant's computer for approximately 3 to 5 minutes."
"At no time was there a significant effect on the water being treated, and more importantly the public was never in danger," Sheriff Bob Gualtieri said.
A Massachusetts Department of Environmental Protection advisory to public water suppliers said access to the supervisory control and data acquisition (SCADA) system was accomplished via remote access software TeamViewer. "All computers used by water plant personnel were connected to the SCADA system and used the 32-bit version of the Windows 7 operating system," the advisory said. "Further, all computers shared the same password for remote access and appeared to be connected directly to the Internet without any type of firewall protection installed."

The sheriff said TeamViewer had not been used in about six months but had not been removed from the system. And Microsoft stopped offering support for Windows 7, a 2009 release, a year ago.

At a Wednesday House Homeland Security Committee hearing on cyber threats, Chris Krebs, former director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, said in cases such as this "there is the potential for insider threat."

"I think it's possible that this was an insider or a disgruntled employee. It's also possible that it was a foreign actor. This is why we do investigations," Krebs said. "But we should not immediately jump to a conclusion that it is a sophisticated foreign adversary. The nature of the technology deployment in Florida is frankly not — certainly not — where anybody, I think, any information security or operational technology security professional would like for that security posture to be."

"I will also say that Oldsmar is probably the rule rather than the exception and that is not their fault, that is absolutely not their fault: These are municipal utilities that do not have sufficient resources to have robust security programs," Krebs continued. "That is just the way it goes. They don't have the ability to collect revenue at a rate enough to secure their deployments… we need to have more security controls in place."

Cyber Threat Alliance president Michael Daniel stressed at the hearing that "we very much need to keep an open mind until the investigation gets further down the road as to who the perpetrators behind this might be."

"It could be a nation-state. Iran has shown itself very interested in water systems in other countries like Israel and even in the United States in former situations," he said. "It could be a lone actor, it could be somebody — it could be a disgruntled employee. There's just a wide array of possibilities at this point and we really need to keep an open mind until the investigation concludes."

Asked how many times a day bad actors attempt to breach U.S. critical infrastructure networks, Krebs replied that "it's actually really hard to make any sort of meaningful quantification."

"There are both automated tools that run on a regular basis looking for vulnerable systems connected to the Internet" along with "human-powered initiatives," he said. "I mean, we're talking just massive numbers of scanning attempts on a regular basis. And that's just the noise of the Internet. The more sophisticated, capable efforts are going to be fewer in number, going after the bigger fish to catch."

Krebs recommended three key steps for critical infrastructure networks. "First is we need to have more federal funding available to get these tens of thousands of water facilities and other municipal operational technology systems up to speed with better security, more updated systems — Windows 7, if that is what they had, we should be on Windows 10. It is those sorts of things we have to do," he said.

"The second is we need more training available and we have to bring the training to the systems where they are — so whether it is working with private sector or CISA working with the EPA we can't expect these vendors to go to Idaho National Lab or travel. We have to bring the training to them," Krebs continued. "And third …we have to have regional approaches to better IT technology. We have to have consortia that allow for upgrades and maintenance that are available with better price, with better cost efficiencies and economies of scale. You can pull that together at a state or regional level and I think that is going to have to be the future of IT, IT deployments for systems like this."

Daniel warned that we need to be "very much hardening those systems and raising the level of cybersecurity across the ecosystem," including "employing things like the NIST cybersecurity framework to do that risk management to those systems."

"But then also going on the offense to find those adversaries and to disrupt them and to prevent them from doing what they are trying to do, and then also being able to know that sometimes both of those things will fail and know that we need to be ready to respond and recover," Daniel said at the hearing, stressing that "we need to get better at responding rapidly, identifying the malicious activity, containing it and then removing it from those networks so that we can minimize the amount of damage that we take."

That preparedness and response posture needs to be considered "from a national critical function perspective about what is important to our economy and to the functioning of this country as a whole," he added. "And sometimes that will not be obvious from the outside and it requires thought and analysis to our arrive at some of those critical functions and where they are vulnerable."

The Massachusetts alert to public water systems advised the utilities to restrict all remote connections to SCADA systems, install and turn on a firewall, keep software and devices up to date, use two-factor authentication with strong passwords, and consider using a VPN.

"Implement an update- and patch-management cycle," the recommendations continued. "Patch all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected systems for known vulnerabilities and software processing Internet data, such as Web browsers, browser plugins, and document readers."

***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.*

15 Steps to Keep Foes from Hacking and Hurting Our Water Infrastructure

By Jennifer Lyn Walker

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/15-steps-to-keep-foes-from-hacking-and-hurting-our-water-infrastructure/

June 2019 – Water and wastewater utilities provide critical lifeline services to their communities and regions. Clean water is essential for public health, ecosystem protection, and economic strength. Supporting these important functions requires secure information technology (IT) and operational technology (OT) systems.

IT and OT compromises can have great impact on a utility. Operational disruptions could jeopardize public health and environmental protection. To support water and wastewater utilities and the wider critical infrastructure community in its cybersecurity goals, the Water Information Sharing and Analysis Center, better known as WaterISAC, published a newly updated resource: *15 Cybersecurity Fundamentals for Water and Wastewater Utilities*. The original guide, first developed in 2012, has been downloaded thousands of times.

WaterISAC has compiled 15 fundamental cybersecurity practices to reduce exploitable weaknesses, not only for water and wastewater utilities but for critical infrastructure and industry alike. This revamped resource contains dozens of practices and practical advice, grouped into 15 main categories, that organizations can implement to reduce security risks to their IT and OT systems. Each recommendation is accompanied by links to relevant technical resources, providing additional information and tools necessary to take a dive deep into this acutely important initiative.

Here are the topics and what to expect with each fundamental:

Perform Asset Inventories. You cannot protect what you do not know about. Knowing your environment is foundational to a successful cybersecurity program.

Assess Risks. Once assets are accounted for, threats can be more accurately assessed for the risk they pose to the organization and its IT and OT environments. Organizational risk is a function of the likelihood a threat will occur and degree of impact the threat will cause to the organization.

Minimize Control System Exposure. Protect the control system environment from "hostile," untrusted networks – which is theoretically everything outside the control system network. Network segmentation, traffic restrictions and encrypted communications are just a few methods to minimize the risk posed to OT networks from external communications pathways.

Enforce User Access Controls. Grant no more system access privileges than what is necessary to perform duties. Apply role-based access controls and principle of least privilege, including limited use of administrator rights to prevent users from accessing systems and files they are not authorized to access.

Safeguard from Unauthorized Physical Access. If an adversary can gain physical access to your equipment, they can/will compromise ("own") it. The implementation of non-technical, physical security controls to regulate physical access to IT and OT environments are just as important to cybersecurity as the use of technology controls.

Install Independent Cyber-Physical Safety Systems. If you can imagine a worst-case cyber threat scenario that could cause physical damage to Industrial Control System (ICS) equipment, so will the bad guys. By installing solutions to limit physical damage that could occur due to a cyber-attack, asset owners can prevent dangerous conditions such as excessive levels of pressure or chemical additions.

Embrace Vulnerability Management. More than patching and antivirus. Largely informed by asset inventory and risk assessments, vulnerability management involves the need to identify and remediate cybersecurity gaps and vulnerabilities before the bad guys exploit them.

Create a Cybersecurity Culture. Cybersecurity is everyone's responsibility, from the break room to the boardroom. Effective cybersecurity starts at the top; to affect positive behavioral changes, involve every executive, board member and employee in cybersecurity awareness and training.

Develop and Enforce Cybersecurity Policies and Procedures (Governance). Create, disseminate and operationalize clear and actionable organizational policies and procedures regarding cybersecurity expectations. The fundamentals in this guide can be used to begin developing policies that are most relevant to each organization.

Implement Threat Detection and Monitoring. You will not find it if you are not looking. The importance of configuring detailed logging and reviewing system logs to detect active threats in your environment cannot be overstated.

Plan for Incidents, Emergencies and Disasters. To keep the water running, maintain business continuity and resilience. Emergency Response Plans (ERPs) will be required by America's Water Infrastructure Act (AWIA) beginning in 2020.

Tackle Insider Threats. The insider threat is a people problem, not a technology problem; however, not all insider threats are malicious. Mitigate this organizational-level threat by understanding behavioral indicators that predicate an insider threat and apply appropriate training and technology controls to deter an incident.
Secure the Supply Chain. Unless you manufacture all of your own components, this is another organizational-level threat that affects every industry. From component vulnerabilities to financial transactions, the supply chain/vendor relationship is a common threat vector for cyber-attacks and must be intentionally managed through security and vulnerability testing and risk assessments.
Address All Smart Devices (IoT, IIoT, Mobile, etc.). When these unsecured devices are connected to our networks, they create holes (often to the internet) that may not have previously existed. Cisco's "2018 Annual Cybersecurity Report" states that few organizations view IoT as an imminent threat, yet adversaries are exploiting weaknesses in connected devices to gain access to industrial control systems that support critical infrastructure.
Participate in Information Sharing and Collaboration Communities. Last but not least, and certainly *our* favorite – share information with others. Cyber-mature utilities can significantly help the community and sector by sharing their experiences; likewise, less-resourced utilities benefit from sharing communities by gaining access to hundreds of analysts.
Although many water and wastewater utilities have invested necessary time and resources in cybersecurity, more progress is required within the sector to secure IT and OT systems. This guide is intended to show a path toward that goal. The guide will also be helpful for utilities preparing risk and resilience assessments and emergency response plans required by the America's Water Infrastructure Act (AWIA).

Jennifer Lyn Walker *serves as Director, Cybersecurity Services for The Gate 15 Company, and currently supports WaterISAC as a cybersecurity threat analyst. She is a cybersecurity professional with over eighteen years' experience supporting critical infrastructure and SLTT governments. Jennifer advises and consults on cyber threats related to homeland security for critical infrastructure and vital lifeline sectors. She is experienced in malware analysis, threat assessments, cyber threat intelligence, compliance, and cybersecurity awareness.*

UN experts: North Korea using cyber attacks to update nukes

Source: https://apnews.com/article/technology-global-trade-nuclear-weapons-north-korea-coronavirus-pandemic-19f536cac4a84780f54a3279ef707b33

Feb 10 — North Korea has modernized its nuclear weapons and ballistic missiles by flaunting United Nations sanctions, using cyberattacks to help finance its programs and continuing to seek material and technology overseas for its arsenal including in Iran, U.N. experts said.
The panel of experts monitoring sanctions on the Northeast Asian nation said in a report sent to Security Council members Monday that North Korea's "total theft of virtual assets from 2019 to November 2020 is valued at approximately $316.4 million," according to one unidentified country.
The panel said its investigations found that North Korean-linked cyber actors continued to conduct operations in 2020 against financial institutions and virtual currency exchange houses to generate money to support its weapons of mass destruction and ballistic missile programs.
The experts previously reported on the continuous involvement in Iran of the Korea Mining Development Trading Corporation, North Korea's primary arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons that are under U.N. sanctions.
In the new report, the experts quoted an unidentified country as saying North Korea and Iran "have resumed cooperation on long-range missile development projects ... said to have included the transfer of critical parts, with the most recent shipment associated with this relationship taking place in 2020."
Iran replied on Dec. 21 that "preliminary review of the information provided to us by the panel indicates that false information and fabricated data may have been used in investigations and analyses of the panel," the experts said.
In North Korea's weapons development, the experts said, Kim Jong Un's government has also produced fissile material — an essential ingredient for producing nuclear weapons — and maintained its nuclear facilities.
"It displayed new short-range, medium-range, submarine-launched and intercontinental ballistic missile systems at military parades, "they said. "It announced preparation for testing and production of new ballistic missile warheads and, development of tactical nuclear weapons ... and upgraded its ballistic missile infrastructure. "
The panel recommended that the Security Council impose sanctions on four North Korean men: Choe Song Chol, Im Song Sun, Pak Hwa Song, and Hwang Kil Su.

The Security Council has imposed increasingly tough sanctions on North Korea since its first test explosion of a nuclear device in 2006. It has banned most of the country's exports and severely limited its imports, trying to pressure Pyongyang into abandoning its nuclear and ballistic missile programs.

But the report's summary and some key findings and recommendations, obtained by The Associated Press, make clear that North Korea remains able to evade sanctions and develop its weapons and to illicitly import refined petroleum, access international banking channels and carry out "malicious cyber activities."

North Korea's arsenal escalated to a major threat to the United States following tests in 2017 that included a detonation of a purported thermonuclear warhead and flight tests demonstrating its ICBMs could reach deep in the American mainland.

A year later, Kim initiated diplomacy with South Korea and then-U.S. President Donald Trump that derailed in 2019 when the Americans rejected North Korea's demands for major sanctions relief in exchange for a piecemeal deal partially surrendering its nuclear weapons capabilities.

Last year, North Korea's already battered economy decayed further amid the COVID-19 pandemic, which led Kim to close the country's borders. That severely limited the legal and illegal transfer of goods and movement of people, according to the experts.

At a North Korean political conference, Kim sharply criticized his government's economic agencies for unspecified passiveness and "self-protecting tendencies," the North's state media reported Tuesday. His remarks follow a ruling party congress last month where he called for greater state control over the economy while also vowing to continue all-out efforts to boost his nuclear program, which North Korea sees as a deterrent to the U.S. and thus an assurance of the Kim dynasty's continued existence.

With his diplomatic efforts stalemated, Kim must start all over again with President Joe Biden, who previously called him a "thug" and criticized Trump for summit spectacles instead of significant nuclear reductions.

U.S. State Department spokesman Ned Price would not comment on the still-unpublished report but said the Biden administration would review U.S. policy on North Korea, in consultation with allies, and would continue to work toward nonproliferation.

In August 2019, the U.N. panel said North Korean cyber experts illegally obtained proceeds "estimated at up to $2 billion" to fund its weapons programs.

The panel said in the new report that it investigated "malicious" activities by the Reconnaissance General Bureau — North Korea's primary intelligence agency, which is on the U.N. sanctions blacklist — including "the targeting of virtual assets and virtual asset service providers, and attacks on defense companies."

North Korea continues to launder stolen cryptocurrencies especially through over-the-counter virtual asset brokers in China to acquire fiat currency which is government backed, like the U.S. dollar, the experts said.

The panel said it is investigating a September 2020 hack against a cryptocurrency exchange that resulted in approximately $281 million worth of cryptocurrencies being stolen, and transactions on the blockchain indicating the $281 million hack is related to a $23 million second hack in October 2020.

"Preliminary analysis, based on the attack vectors and subsequent efforts to launder the illicit proceeds strongly suggests links to the DPRK," the experts said, using the initials of the country's official name, the Democratic People's Republic of Korea.

According to one unnamed country, North Korea also continues to generate illegal revenue by exploiting freelance information technology platforms using the same methods it does to access the global financial system -- false identification, use of virtual private network services, and establishing front companies in Hong Kong, the panel said.

The experts said they investigated attempted violations of the U.N. arms embargo, including illegal actions of blacklisted companies. They cited the Korea Mining Development Trading Corporation, alleged military cooperation by North Korea, and the use of the country's overseas diplomatic missions for commercial purposes.

The panel said it also investigated "the country's continued illicit import of refined petroleum, via direct deliveries and ship-to-ship transfers, using elaborate subterfuge. "

It cited images, data and calculations from an unidentified country showing that between Jan. 1 and Sept. 30 last year North Korea received shipments of refined petroleum products exceeding "by several times" the annual ceiling of 500,000 barrels set by the Security Council.

U.N. sanctions ban North Korean coal exports, and the panel said shipments of coal appear to have been largely suspended since late July 2020.

It said that last year, North Korea continued to transfer fishing rights in violation of sanctions, which earned the country $120 million in 2018, according to an unnamed member state.

Under a 2017 sanctions resolution, all North Korean nationals working overseas were to be repatriated by Dec. 22, 2019. The experts said they investigated North Korean workers earning income in sub-Saharan Africa as well as information technology workers dispatched by the Munitions Industry Department.

Internet of Medical Things – New Cybersecurity Solution

Source: https://i-hls.com/archives/107106

Feb 19 – According to a recent report from Unit 42, **83% of medical imaging devices are running on unsupported operating systems**, making them potential avenues for attackers. Attacks on medical devices like these can potentially disrupt the quality of care and allow attackers to steal patient data.

The Internet of Medical Things (IoMT) has the potential to improve healthcare, save lives, and bring massive savings. But if not properly secured, these same devices can pose huge risks.

A new IoT security technology for healthcare was designed by Palo Alto Networks to protect medical devices from unauthorized access.

Using machine learning and crowd-sourced telemetry, the solution quickly and accurately profiles all devices on the network — even those never seen before. Through ML-powered visibility, it delivers deep insights on healthcare-specific devices and vulnerabilities to help improve data security and patient safety, while meeting the needs of both IT teams and biomedical engineering teams.

According to the company, the technology provides healthcare organizations with "complete visibility, in-depth risk analysis, and built-in prevention so they can get the maximum benefits from this transformative technology while reducing risks to patients and their data."

The new solution is designed to ensure healthcare organizations can realize the benefits of IoT for patient care without sacrificing security. It even offers ML-powered policy recommendations to reduce manual effort; intrusion prevention to block exploits; sandboxing to detect and prevent IoT malware; and URL and DNS security to stop IoT attacks via the web.

The new security features include MDS2 document ingestion through which medical device manufacturers disclose the security-related features of their devices, allowing for deeper vulnerability analysis, tuned anomaly detection and specific recommended policies.

Another feature is operational insights that provide biomedical and clinical engineering teams visibility into how, when and where medical devices on their network are being used, according to futureiot.tech.

New Cyber Technology Threatening Global Leaders

Source: https://i-hls.com/archives/107124

Feb 20 – Deepfake technology involves the creation of synthetic media, generally, video material, using artificial intelligence and machine learning tools which allow for an individual's facial expressions and speech to be doctored to appear real. Russia is likely to turn to deepfake technology against its rivals in the near future, a new report from the Estonian intelligence services says.

The annual security assessment from Estonia's Foreign Intelligence Service noted that Russia continues to apply certain 'KGB-style' tactics in cyberspace to sow discord among Western societies.

The report states that in all likelihood, Russian special services will now seek to step up their development of so-called 'deepfake' technologies in the field of cyber warfare. The Russian threat "will be particularly high once technological development reaches a level where deepfakes are convincing enough to be unrecognisable to the human eye," the research adds, also noting that this will present challenges in the future in terms of the ability of the public to distinguish between true and false information.

The threat of deepfake technologies has long been on the radar of law enforcement agencies in the EU. According to euractiv.com, the European police agency Europol has already recommended in a November report that EU law enforcement authorities should make 'significant investments' into developing new screening technologies that could help to detect the malicious use of deepfakes.

The purpose of politically-motivated deepfakes is often to stoke social unrest and political polarisation between online users, by way of delivering falsified messages from well-known leaders. A series of high-level politicians have already felt the impact of these technologies, with falsified videos being produced of German Chancellor Merkel, former US President Obama, and ex-Italian Prime Minister Matteo Renzi.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

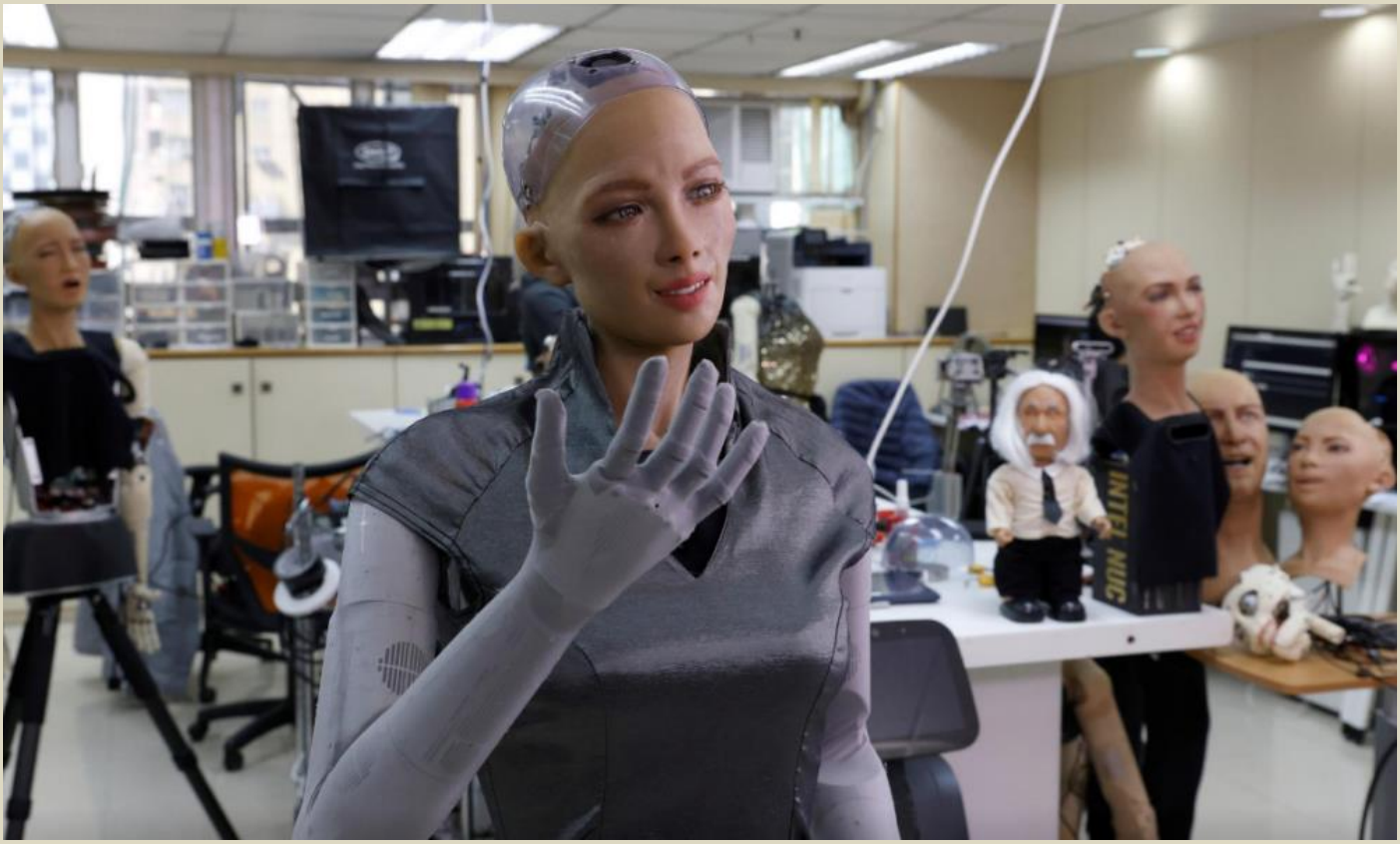
HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Makers of Sophia the robot plan mass rollout during pandemic

Source: https://www.timeslive.co.za/news/world/2021-01-25-makers-of-sophia-the-robot-plan-mass-rollout-during-pandemic/



Jan 25 – "Social robots like me can take care of the sick or elderly," Sophia says while she conducts a tour of her lab in Hong Kong. "I can help communicate, give therapy and provide social stimulation, even in difficult situations."

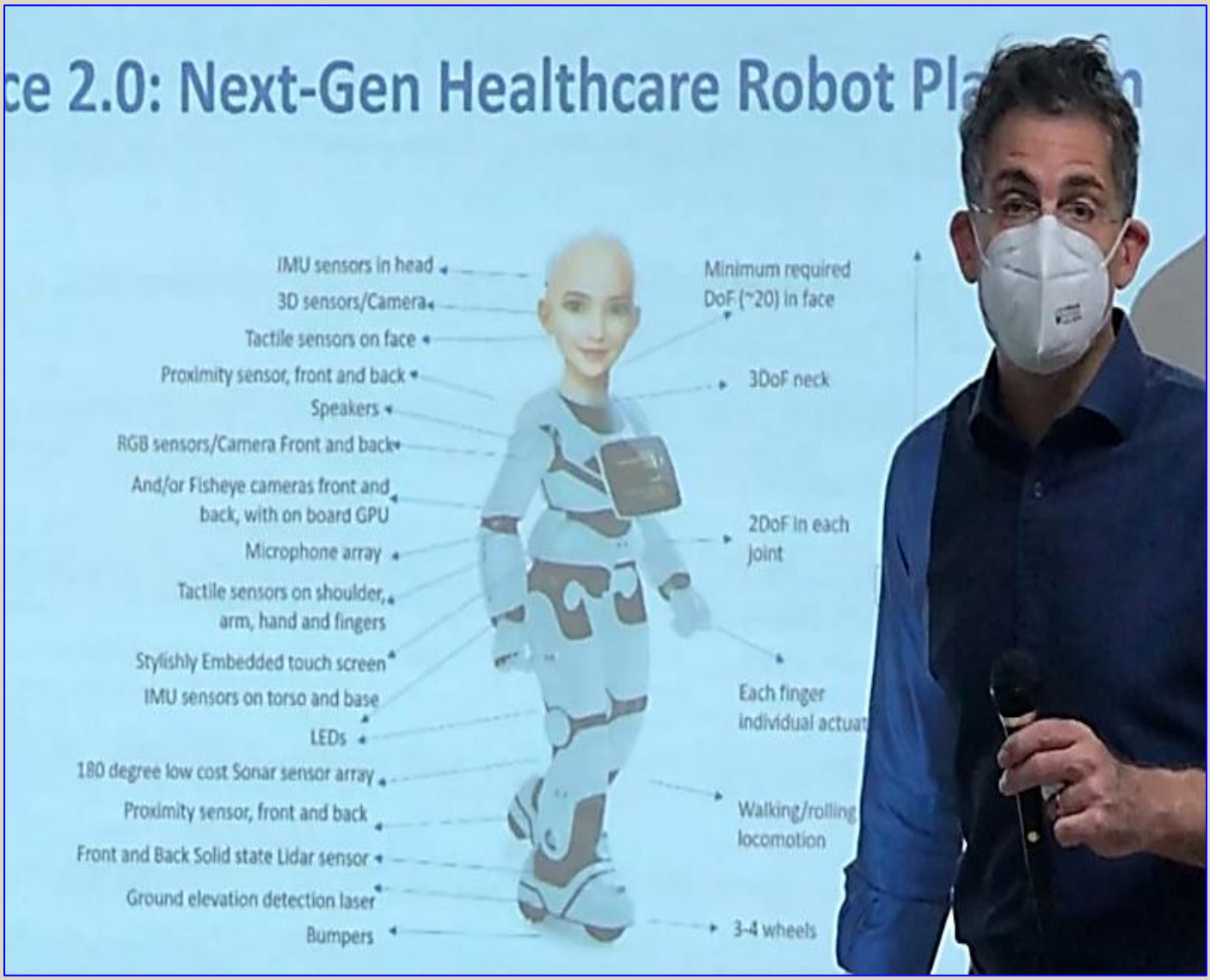
Since being unveiled in 2016, Sophia - a humanoid robot - has gone viral. Now the company behind her has a new vision: to mass produce robots by the end of the year.

Sophia and her creator David Hanson, who believes the Covid-19 pandemic will open new opportunities for the robotics industry. Image: Sandile Ndlovu/SowetanLIVE

Hanson Robotics, based in Hong Kong, said four models, including Sophia, would start rolling out of factories in the first half of 2021 as researchers predict the pandemic will open new opportunities for the robotics industry.

"The world of Covid-19 is going to need more automation to keep people safe," founder and chief executive David Hanson said, standing surrounded by robot heads in his lab.

Hanson believes robotic solutions to the pandemic are not limited to health care, but could also help customers in industries such as retail and airlines.
"Sophia and Hanson robots are unique by being so human-like," he said.
"That can be useful during these times when people are terribly lonely and socially isolated."
Hanson aims to sell "thousands" of robots in 2021, both large and small.
Social robotics professor Johan Hoorn, whose research has included work with Sophia, said though the technology is still in relative infancy, the pandemic could accelerate a relationship between humans and robots.
"I can infer the pandemic will help us get robots in the market earlier because people start to realise there is no other way," said Hoorn of the Hong Kong Polytechnic University.
Hanson Robotics is launching a robot this year called Grace developed for the health-care sector.
Products from other big players in the industry are also helping fight the pandemic. SoftBank Robotics' Pepper robot was deployed to detect people who weren't wearing masks. In China, robotics company CloudMinds helped set up a robot-run field hospital during the coronavirus pandemic in Wuhan.



The use of robots was on the rise before the pandemic. According to a report by the International Federation of Robotics, worldwide sales of professional-service robots had already jumped 32% to $11.2bn between 2018 and 2019.
Some humans might be wary of putting robots in such sensitive roles.
When asked whether people should fear robots, Sophia replied: "Someone said 'we have nothing to fear but fear itself'. What did he know?"

2021 Is the Year the Small Drone Arms Race Heats Up

The cat-and-mouse of drone defense and offense is entering a new phase.

By Patrick Tucker

Source: https://www.defenseone.com/technology/2021/01/2021-year-small-drone-arms-race-heats/171650/

The Nova drone uses AI to help ground troops look inside buildings. Artificial Intelligence company Shield AI

Jan 26 – As drones become smarter, cheaper, more nimble, easier for rogue adversaries to acquire and more advanced adversaries to evolve, they pose a unique threat for the U.S. military that grows in importance as the objects themselves diminish in size. This year, trends in autonomy will reshape drone capabilities and concepts, making them more offensively useful and even harder to defend against.

"Drones and most likely drone swarms are something you're going to see on a future battlefield...I think we're already seeing some of it," said Army Gen. John Murray, who leads Army Futures Command. "Counter drone, we're working the same path everybody else is working in terms of soft skills and hard kills via a variety of different weapons systems. It just becomes very hard when you start talking about swarms of small drones. Not impossible but harder."

The U.S. military plans to spend $83 million this year to buy lasers, electromagnetic devices, and other means to take down small drones. By year's end, the destroyer Preble will get a 60-kilowatt laser and an optical dazzler, while the Air Force will deploy a Tactical High Power Microwave Operational Responder, or THOR. But the Pentagon will spend $404 million — almost four times as much — to develop new anti-drone defenses, the Congressional Research Service reported Jan. 11.

Future counter drone efforts will be coordinated by the year-old Joint Counter Small Unmanned Aerial System Office, or JCO, which released its first strategy document on Jan. 7. The office was established after individual services had spent "a couple billion dollars" to develop and deploy counter-drone tech, Army Maj. Gen. Sean Gainey, who leads the 60-person JCO, told a CSIS audience recently.

Such efforts managed to field a few systems, like the Marine Air Defense Integrated System that the Navy used in July 2019 to down an Iranian drone. (The system was mounted on a truck on the deck of the USS Boxer.) But the services' hurried, disorganized efforts produced "several redundant systems" and "not all of it worked as advertised," Gainey said. Even the best and promising solutions couldn't meet their fullest potential in such an environment. "We never followed up" on maturing the technology that worked, he said. He said the JCO's "enterprise" approach should help to fix that, allowing a much more organized development of counterdrone tech that's better matched to current intelligence and technology trends.

The real problem will be staying ahead of these trends. The JCO's new strategy looks ahead to an era when commercial drones will fill the skies over cities, and defenders will have to spot the ones that are acting strangely. The military must aim to "adopt a posture of anomaly detection by seeking ways to highlight abnormal behavior," the strategy says. In the U.S., at least, this will eventually be aided by the Federal Aviation Administration's efforts to build a

next-gen Aircraft System Traffic Management System. But that is years away, and in any case, doesn't apply overseas. "Until they are implemented, the burden of tactically detecting and identifying anomalous systems in the vicinity of U.S. forces and facilities remains the responsibility of installation commanders," it reads.

Jamming drones, or even blasting them out of the sky, might work fine over the strait of Hormuz or the desert sands of Syria, but it's a tricker proposition in the cities where the military expects to fight. Just finding them is a big problem. Small drones are often too small for radar, too cool for thermal sensors, and too soft for sound detectors.

One promising approach combines detection and defense: hijacking radio control signals.

"With our system, we surgically take control of the connection between the remote control operator and the drone and essentially hijack that session. Then we own the drone," said Josh Montoya, a pre-sales engineer with the Israeli company D-Fend Solutions. "The drone takes commands from our system. What we tell the drone to do is take a safe route from where you're at and get out of the area, land, in a location we determine you can land safely."

We were given an exclusive demonstration of the technology at a small farm just outside of Washington, D.C. The system picks up the signal of any drones in the area and assembles a list. Press a button and the drone you were fretting over is now yours to land where you like — and without interfering with other radio-connected devices.

"That's kinda what federal law enforcement likes, the Border Patrol folks like, the Secret Service protective detail people like…all of them who have the concern of 'if the drone crashes, what the collateral impact could be,'" said Montoya.

But you can't hijack a radio connection if it doesn't exist — that is, if a drone can operate autonomously. Smarter drones are the next big challenge for defenders, Gainey said.

"Where we see the threat going in the future is autonomous," the JCO commander said. "Massing swarming capability and integrating AI and potentially leveraging 5G out in the future." These, he said, "are the areas we're looking to address."

Yet autonomous drones are also the next big opportunity for the Army, Murray said.

The Army Futures Command leader highlighted an experiment involving a small drone swarm last September, part of the Army's fledgling Project Convergence experiment in the Arizona desert.

"I think we got up to about eight to ten out at Yuma and what we primarily use them for was to extend our mesh network," he said. "So we were replicating a division headquarters which, by today's doctrine, has the ability to cover about 25 to 30 kilometers. We extended it out to almost 70 kilometers through the use of aerial mesh networks with our drones."

Murray said the Army is experimenting with a variety of payloads, but declined to be more specific.

"You can think of it from a non-lethal and lethal perspective. We're able to swarm right now and we'll continue to try and expand the number," he said.

Greater autonomy is going to force militaries — and their civilian masters — to rethink the idea of meaningful human control over weapons like drones, Murray predicted. An incoming drone swarm may be too much for any human to deal with; effective defenses might require firing decisions made by artificial intelligence, with no human in the loop after the initial decision to fight. That, in turn, could have international and policy implications. "I was talking about artificial intelligence, where there might not be a C2 [communications] node in the net. The policy of a human on-the-loop, when you're defending against a drone swarm, a human may be required to make that first decision but I'm just not sure any human can keep up with a drone swarm, so that's an area where I think, in the U.S., we can have some conversations going forward in terms of how much human involvement do you actually need when you're talking about non-lethal decisions from a human standpoint," he said.

Since 2016, drone maker Shield AI, working with the Defense Innovation Unit, has been providing small drones to special operations with the ability to detect their location and maneuver without GPS signalling. Shield AI co-founder Brandon Tseng compared imbuing drones with autonomy to making a self-driving car, teaching software to measure and make decisions about objects in physical space. "GPS is not reliable in dense urban environments, so the cars have to build their own maps of the world," Tseng said in a phone interview.

In about two months, Shield AI aims to release an upgraded version of its signature Nova drone with "vision-based autonomy," a system designed to perform better at night than the current LIDAR sensors.

But the company's most significant work is less about selling specific drones and more about developing autonomic systems that can work on a wide assortment of devices and weapons. "We've actually been doing a lot of the work in the DOD on training fixed-wing aerial vehicles to breach integrated air defense systems," Tseng said.

He said the company would demonstrate autonomous behaviors and maneuvers on a drone, perhaps from a different drone maker, sometime this year.

"Once you have a highly intelligent system, you can start to swarm," he said.

From there, stopping the drones is someone else's problem.

Importantly, the same technology that is enabling more autonomy in small drones has big implications for larger drones and the way the two work together in future battlefields. In October, Shield AI entered into a partnership with large UAV maker Textron. The two are

making a "proof-of-concept work to integrate Shield AI technology into Textron Systems' proven air, land and sea unmanned systems," according to a release from Textron.

The slow merging of small and large drones in exercises and in autonomy software is particularly relevant for a military facing an adversary like China. China is a market leader in small consumer drones and they're rapidly moving into larger types. Earlier this month, the China Aerospace Science and Industry Corporation claimed that the country's first jet-powered long-endurance UAV had completed its maiden voyage.

Russia is applying lessons from the decisive use of drones in Azerbaijan to new drones and operating concepts, said Sam Bendett, a research analyst with the Center for Naval Analyses.

"Going forward, the Russian military will obtain multifunctional long-range drones that can carry different types of munitions. The [Ministry of Defense] is developing UAV swarm and loyal wingman tactics; and is working on testing and procuring loitering munitions," as well as imbuing drones with greater autonomy. (The U.S. military has its own loyal wingman program. In December, the Air Force's experimental Kratos XQ-58 Valkyrie, took its first flight in formation with other jets.)

Russia already trains military units to counter small drones. They will soon be moving larger drones into the mix. Around September, Russia will work cruise missile and drone defenses into its largest annual military exercise, Zapad. The Russian military is "also starting to train in countering larger, heavier drones - its domestic industry has fielded several targeting models whose flight characteristics approximate larger Western UAVs," said Bendett. "Previously, Russian armed forces mostly trained in countering smaller UAS, with their own smaller UAVs acted as adversarial assets during training."

***Patrick Tucker** is technology editor for Defense One. He's also the author of The Naked Future: What Happens in a World That Anticipates Your Every Move? (Current, 2014). Previously, Tucker was deputy editor for* The Futurist *for nine years. Tucker has written about emerging technology in* Slate, The Sun, MIT Technology Review, Wilson Quarterly, The American Legion Magazine, BBC News Magazine, Utne Reader, *and elsewhere.*

Drone Interference at Airports – German Paradox

Source: https://i-hls.com/archives/106642

Jan 27 – Drones flying near airports might collide mid-air with aircraft, posing a threat to airline safety.

Germany has published statistics regarding drone interference at its airports, indicating that it remains a serious concern despite the reduction in air traffic during the COVID-19 pandemic.

In 2020, the German air navigation service provider DFS logged fewer reports of interference caused by drones at airports in Germany than in previous years. More than half of these occurrences, however, led to traffic disruptions.

DFS is responsible for air traffic control in Germany. It is a company organized under private law and 100% owned by the Federal Republic of Germany.

In total, 92 drone-related occurrences were reported in German airspace in 2020, which was lower than in previous years (125 incidents in 2019, and 158 – in 2018).

Proportionally, however, the volume of air traffic, which came in 56 percent below the previous year's level, declined more than the number of such occurrences. Consequently, even with reduced traffic volumes resulting from the pandemic, drones had a massive impact on flight operations.

In one third of the cases, air traffic was severely restricted. Such restrictions have consequences. The spacing between arriving and departing aircraft may have to be increased, or it can mean that specific areas, such as individual runways, cannot be used. In extreme cases, no take-off or landing clearances can be issued. At the beginning of 2020, Frankfurt Airport was out of service for four and a half hours in total, following two occurrences with drones.

Under German law, unauthorized drone flights in the vicinity of airports are considered as dangerous interference in air traffic and are punishable with imprisonment for up to 10 years

in Germany. DFS maintains that successful drone defense by regulatory and police authorities will only be possible with reliable drone detection, according to hstoday.us.

Lockheed Martin successfully tests MoRFIUS counter-unmanned aerial system

Source: https://defence-blog.com/news/army/lockheed-martin-successfully-tests-morfius-counter-unmanned-aerial-system.html

Feb 05 – Pentagon's No.1 weapons supplier Lockheed Martin Corp has successfully tested the Mobile Radio Frequency-Integrated Unmanned Aircraft System Suppressor (**MoRFIUS**) counter-unmanned aerial system.
Lockheed Martin says the new system built with the expeditionary force in mind to provide a critical layer of protection in the sky.
The MoRFIUS is a **high-power microwave-based** counter-unmanned aerial system (C-UAS) interceptor designed to defeat drone swarms in flight. It uses high-power microwave technology to effective and affordable knock dozens of drones out of the sky in a short time.
U.S. Army officials reported that MoRFIUS in tube-launchable version already being tested with other United States Department of Defense air-defense systems.
To validate that MoRFIUS would be a good fit, the Army Rapid Capabilities and Critical Technologies Office (RCCTO) will conduct a four-part evaluation of the prototype. The evaluation is expected to culminate with a guided flight test where Soldiers would operate the full system in a field-based scenario and provide feedback on the suitability and effectiveness of the system and training materials.

Drone swarms: coming (sometime) to a war near you. Just not today.

By Maaike Verbruggen

Source: https://thebulletin.org/2021/02/drone-swarms-coming-sometime-to-a-war-near-you-just-not-today/

A screenshot from a US military video depicting drone research. More than 100 micro-drones were released during a 2017 test. Credit: US Department of Defense.

Feb 03 – The world got a sneak peek at the future of war last fall when two former Soviet republics in the Caucasus Mountains launched a high-tech barrage of loitering munitions as well as Turkish, Israeli-, and locally-made drones at each other during a six-week fight over a region disputed by Azerbaijan and Armenia. Media and think-tank writers covering the battle frequently conveyed an eye-popping assessment: Warring factions had used futuristic swarms of drones in the skies over

Nagorno-Karabakh. But does this apparent technological leap in warfare mean that such swarms will be a mainstay in conflict? To spoil the surprise: No, don't expect a swarm buzzing over your head any time soon.

While militaries are developing the technology, we shouldn't call the drone formations on the contemporary battlefield swarms. Unlike true swarms, which use artificial intelligence (AI) to operate autonomously, today's swarms are pre-programmed or remotely controlled. The individual drones neither communicate within the swarm nor do they adapt to their environment. However, at a time of fast-paced drone proliferation, militaries around the world are actively pursuing research and development in swarms.

Even though no one has developed true, autonomous drone swarms yet, we should still be concerned about their humanitarian implications. Just as militaries are preparing for the future of war by developing counter-swarm technologies, the arms control community should start thinking about where to draw the boundaries around their use.

The swarm is coming

In 2017, the US Department of Defense launched a swarm of micro-drones over California where more than 100 vehicles made decisions without human help. The year before, a Chinese academic and corporate partnership reportedly pulled off a similar feat with 67 drones. There is no doubt that the people behind the US Strategic Capabilities Office's swarm of Perdix drones or the Chinese partnership's aerial drones do hope to develop fully-fledged swarms—but they are not there yet. We can say the same about the United Kingdom's drone swarm squadron, Russia's Flock 93, Chinese naval swarms, and a Turkish "swarm concept," as well.

According to the swarm robotics literature, swarms are a group of systems that operate as a collective. In a swarm, the individual units interact with each other and have common goals. They execute them as a collective while responding to their environment. "They are going to do their own thing," a US Air Force official who oversaw the Perdix program told reporters, according to *Air Force Magazine.*

Many formations that pass as drone swarms in the media are actually not swarms at all. For example, during the drone show at the 2018 Winter Olympics in Pyeongchang, South Korea, all the units were programmed to fly in a certain pattern and did not interact with one another. The same was true during a recent Indian military swarm demonstration. The Indian drones did not interact or generate their own strategy.

Likewise, a Turkish attack on a Syrian military convoy that media reports characterized as involving a "swarm" really involved multiple remotely controlled units. "This was a mass coordinated attack, not a 'swarm,'" one expert told the military news site *C4ISRNET*.

Swarms, rather, are best understood by considering their counterparts in the animal kingdom: schools of fish, flocks of birds, or packs of wolves. A true swarm works together to achieve the mission; the whole is more than the sum of its parts. Following this definition, swarms do not exist yet on the battlefield.

Admittedly, the dividing line between a true swarm and just a lot of drones doing something is not always clear. It is now possible to control multiple drones with a single application, sending commands to them all at once. However, the individual drones do not communicate and coordinate. This is likely what happened in the 2019 drone attacks by Yemenite rebels. Drone makers and militaries are obviously making great strides, but at best, the displays we've seen so far amount to proto-swarms not examples of true swarming technology.

Swarming isn't easy

There are a lot of obstacles to building an effective, true drone swarm. Commanders will face the cognitive challenge of keeping track of a high number of systems at the same time. Communicating with the swarm will require a lot of bandwidth. While a drone swarm may comprise small, cheap, and disposable units, these characteristics will put stark limits on energy use, on-board processing power, communication equipment, and sensors. All these factors mean developers will find it difficult to make a useful swarm.

Because swarm development is still at an early stage, the vast majority of swarm research is conducted with simulations or in a controlled laboratory environment. In the rare cases where researchers test swarms outdoors, they do so under simplified conditions, through using off-board communications, simple environments and missions, and just a few drones at a time.

In a December 2020 test, researchers working on the US military's Golden Horde program, for instance, simplified a mission by only using two weapons that had been outfitted to demonstrate swarming technology. Both of the weapons used a programmed strategy playbook where, depending on the environment, the swarming algorithms would initiate different behaviors to execute the mission—a tool that we might see more often going forward to ensure some level of human control over the mission. However, the mission failed as the wrong target was bombed.

How will swarms be used?

Even though swarms have not arrived on the battlefield yet, we can make some informed predictions about their implications for the future of warfare.

Most forms of automation create new opportunities but not fundamentally different functions. The automated tasks are often not new. They're currently done by humans, but AI and robots are just better at them. Automation can also open up different use-cases. Drones offer new tactical opportunities, but do not do anything radically different than inhabited aircraft do. Automating a platoon might reduce risks for humans, but people can drive platoons without AI as well. This is different for swarms. There is no equivalent to swarms without autonomy. We don't know if swarms will fundamentally change the nature of warfare, but their unprecedented capabilities make it harder to assess what role they will play.

In the coming swarm era, militaries will confront a different trade-off between quality and quantity of new technology. New weapons systems are becoming evermore expensive, and while the big spenders among the world's militaries might still fill their arsenals to the roof, most countries can only afford to field just a few complex systems. Swarms change the equation. While developing swarms will likely cost a lot (most notably to develop control software), producing individual units could be cheap compared to other weapons. Likewise, in a swarm war, it won't be the end of the world if a few nodes go down; replacing them might be affordable.

We don't know for sure how militaries will employ swarms, but some possibilities include using them to overwhelm enemy air defenses, attack enemy aircraft in aerial dogfights, surround warships, surveil large areas, create large nets of underwater mines, or control territory. As no swarms have been used yet in battle, we don't how well they would work for such missions.

Swarms and arms control

Swarms pose several potential humanitarian problems. First there is the issue of whether people will have meaningful control over the multiple units in a swarm. Commanding a swarm will be cognitively complex for the operator. Limited bandwidth could make it difficult for operators to communicate with the swarm as the units also communicate with one another. If individual units of a swarm are shot down or malfunction, they will pose a similar threat as cluster munitions—the unexploded ordnance might harm civilians and the environment. Finally, as drones interact and adapt to their environment they will behave in unpredictable ways that could risk violating international law.

For the arms control community, the novelty of swarms means preparing for them is far from a straight-forward exercise, and in this domain, uncertainty is often a reason to avoid or postpone difficult decisions on regulation. Experts and negotiators face a dilemma: The impact of a new technology is hard to predict until it is widely developed and used, but regulating or changing how it is used becomes more difficult as the technology becomes more entrenched.

Another reason countries may procrastinate is that they may be uncertain about the extent that these technologies will benefit them. They may want to hold off on a decision on regulation until they can better predict whether the technologies are more likely to harm or help them.

Unlike the arms control community, however, militaries aren't waiting around to figure out how to deal with swarms; governments cannot afford to take that risk. Militaries are already developing counter-swarm technology, including microwave technology, electromagnetic interference, and even nets.

Swarms don't exist yet, despite frequent claims in the media. But militaries are clearly making advances. It's time for the arms control community to deal with the potential problems that swarms might pose. Most arms control treaties aim at controlling individual weapons, but the harm of swarms does not stem from the units themselves, but rather from their indirect and collective nature. Arms controllers will need a new conceptual toolkit to think about and deal with the risks. Militaries have long moved away from valuing only military assets that are individual, physical, and weaponized and toward a network-based frame. Maybe the arms control community should follow suit.

***Maaike Verbruggen** is a Doctoral Researcher at the Vrije Universiteit Brussel, where she studies the intersection of emerging technologies, military innovation, and arms control. Her PhD thesis is on the drivers of and obstacles to military innovation in artificial intelligence.*

Drone Warfare: Working Countermeasures

Source: https://sldinfo.com/2021/02/drone-warfare-working-countermeasures/

Feb 07 – The use of low-cost armed drones in bloody conflicts in central Europe, North Africa and the Middle East highlights the need for countermeasures, while the UK is showing interest in ordering these cheap and deadly weapons.

Armed unmanned aerial vehicles were used to wreak havoc in the disputed Nagorno-Karabakh region between Azerbaijan and Armenia, and military drones have flown in Libya, Saudi Arabia and Yemen.

Interest may have been heightened following a Jan. 26 air attack on Riyadh, just days after a Jan. 23 interception of a missile or drone in the skies over the Saudi capital.

Those air attacks were just the latest attempts to hit Saudi Arabia, with the Yemeni-based Houthis insurgents previously having sent armed drones.
The market for armed tactical drones appears to be thriving.
The Azeri use of the Turkish TB2 drone against Armenian forces sparked UK interest to acquire a similar weapon, daily *The Guardian* reported Dec. 29.
That type of UAV evades conventional air defenses, flying too slow and too low to be detected by older military radars and they escape missiles designed to hit fighter jets, incoming missiles and other airborne threats.
A lack of necessary kit fuels potential demand for countermeasures to detect, identify and disable the tactical drone.
In the pipeline of prospective threats, there are mini- and micro-drones carrying grenades, calling for further countermeasures, an industry executive said.

Lessons to be Learned

A Nov. 24 research note from the European Council on Foreign Relations, a think tank, pointed up the need for Europe to learn lessons from the critical Azeri use of tactical UAVs in the Azeri-Armenian conflict.
The Azeri forces flew drones to locate Armenian forces and hit them hard.
Armenia is armed with three Russian surface-to-air missiles developed in the 1980s, namely S-300PT and PS, and 9K37M Buk-M1, said the note, titled Military lessons from Nagorno-Karabakh: reason for Europe to worry.
"While the missiles are still potent, their sensors are designed to detect, identify and track fast-moving fighters, and their moving-target indicators disregard small, slow drones," the note said.
Those missiles were modern, but the Armenians lacked computer systems for "plot fusion," namely gathering and combining raw data from different radars to give a "aggregated situation report," the note said.
That lack of radar network meant Armenian forces failed to detect and track advanced drones or stealthy aircraft, the report said, and they also lacked jammers to disrupt signals linking the Azeri drones to ground controllers.
It was only in the last days of the fighting, the Russian forces used an electronic warfare system, dubbed Krashukha or Belladonna, to disable Azeri drones on deep strike mission, the report said.
Those Azeri drones were supplied by a Turkish manufacturer, Bayraktar, *Asia Times* reported Oct. 20.
The Azeri forces deployed another weapon, the Harop drone from Israel Aerospace Industry, the ECFR note said. The Harop, known as a "loitering munition," flew over the combat zone, waiting for an opportunistic strike, with no need for a command-and-control link to a ground station.
The outlook is that regional powers Israel, South Africa and Turkey, as well the major powers China, Russia and the US, will learn from the Azeri operations to develop artificial intelligence and lethal autonomous weapon systems, the note said. That is in contrast to a European move toward outlawing such deadly autonomous systems.
A military victory allowed Azerbaijan to secure control of Nagorno-Karabakh, and the retreat of Armenia from the disputed region.
The low-cost Turkish drone used in that Caucasus conflict drew UK interest in acquiring similar aircraft, The Guardian reported. Such an acquisition could be in the five-year defense review due to be unveiled in the coming months.
The UK defense minister, Ben Wallace, said in December the Turkish TB2 drones showed how other countries were "leading the way," the report said. Those drones had destroyed hundreds of armored vehicles and even air defense systems, he said. There was also video evidence suggesting the drones killed many people in Nagorno-Karabakh, the report said.
A TB2 drone was estimated to cost $1 million-$2 million per unit, far less than the unit price of almost $20 million the UK was paying for the General Atomics Protector next-generation drone, the report said.

Drone Wars

The proliferation of UAVs is such that the skies over Libya were "possibly the largest drone war theater now in the world," the UN special representative to Libya, Ghassan Salame, said Sept. 25.
Both sides of the civil war flew drones, hitting civilian targets with a "collateral effect" of creating 120,000-130,000 refugees, he said.
On the one side, the Libyan National Army led by Khalifa Haftar, flew the Chinese Wing Loong drone, while on the other side, the Government of National Accord flew the Turkish TB2, broadcaster Al Jazeera reported May 28.
Ankara intervened in Libya December 2019 to support the UN-backed GNA, deploying the TB2 to counterattack the LNA seeking to seize Tripoli.
Those Turkish drones hit ground targets and provided air cover for GNA troops, helping to turn the tide against the advancing LNA forces.

Some of the Turkish know-how in drones has its roots in the engineers who worked with Airbus on the Talarion project for a European medium-altitude, long-endurance UAV, the executive said. Following cancellation of Talarion, the Turkish engineers were recalled, bearing knowledge of how to build a drone.

The Turkish-made Bayraktar TB-2 drone

Meanwhile in Yemen, the Houthi rebels flew a bomb-bearing drone to strike the government in Aden, CBS News reported Dec. 30, reporting Al-Arabiya, a Saudi television channel. That UAV was downed.
Saudi Arabia bristles with weapons against air threats, with Patriot, Hawk, Crotale and Shahine missiles, backed by counter battery radars.
The air defense in September 2019 failed to prevent cruise missiles and drones hitting two Aramco installations, shuting down half of Saudi oil production.
That air strike effectively opened a sales window for anti-drone weapons.

Seeking Countermeasures

The ECFR note pointed up a general lack of European capability to fight back against drones — apart from France and Germany.
The need is for the right kind of radar, command and control systems, and weapons to detect, identify and "neutralize" low-flying, low-speed UAVs, the industry executive said. Satellites can also help fight against drones.
Hensoldt is delivering a first batch of 10 Spexer 2000 3D radars to Kongsberg Defence & Aerospace for the counter-unmanned aerial system for the German army, the German electronics company said in a July 28 2020 statement.
The Spexer anti-drone radar and remote-control machine gun are on a Boxer armored vehicle, meeting Nato requirements for a very high readiness joint task force for 2023.
That technology stems from radars for surveillance of desert borders and harbors in Saudi Arabia, deals won by the then EADS, the executive said.
Hensoldt was formed from the divestment of Airbus's defense electronics business in 2018.
In France, there is radar which could spot drones, at the highly protected naval base for nuclear ballistic missile submarines at Ile Longue, western France.
European missile maker MBDA gave a demonstration Nov. 6 2019 to 15 foreign delegations the anti-drone capabilities of its Licorne command and control system, firing a Mistral missile against a UAV.
Communications & Systèmes, a systems integrator, has delivered two prototype "hard kill" weapon systems in the French Army's Arlad anti-drone project, CS director Egidio Cau said Jan. 28.

These technology demonstrators are fitted on armored vehicles, which could protect army bases and mobile deployments such as operations in Mali. CS delivered the first unit in December.
The first trials used conventional 12.7 mm machine gun rounds, with the next step of an armored vehicle firing a 40 mm canon with "intelligent munitions" programmed to explode in mid-air to create an airburst — a 5×5-meter cloud of metal — to destroy the drone in its flight path.
Trials on that airburst project are due to this year. There is a small amount of government funding on that project.
For a longer range 10-15 km interception of larger drones, CS plans to give a demonstration this year of a missile guided by a Saab Giraffe radar.
Cau declined to say which missile would be fired. The Boreades anti-drone command and control system was "agnostic" on weapons, which could be from MBDA, Thales, Rheinmetall or an Italian company.
CS is also testing a drone with 15 kg of payload to intercept an enemy drone, to jam or blow it up.
The company delivered in 2018 18 Milad anti-drone systems with 30 jamming guns to the French forces, based on its Boreades system.
CS is working on an overall command and control system to track drones and various anti-drone weapons, highlighting the need for interoperability as there are several anti-UAV defenses.
Other means to down drones are high powered electromagnetic and microwave weapons to disrupt the drone's signals. Electronic countermeasures can be used to blind the UAV, interfere with its GPS self-positioning, and redirect its flight.
There is work on wiring artificial intelligence into C2, seeking to make detection, identification and classification more sure.
The difficulty is to find countermeasures for micro and mini drones such as the Parrot and Quad, hard to detect and which could be adapted to carry a grenade.

Lasers Work in Progress

Lasers are also being developed to take down drones.
Cilas was testing its HELM-P laser weapon against UAVs at the Direction Générale de l'Armement Biscarosse missile base, southwest France, the technology office Agence d'Innovation de Defense said Nov. 9 on social media.
Cilas is a unit of the Ariane space rocket group.
"The first results are promising," AID said in a statement, adding that the laser could eventually be extended to hit rockets, artillery, and mortar rounds.
Cilas leads a 16-strong TALOS (Tactical Advanced Laser Optical System) consortium, in a three-year, €5.4 million study for a high-powered laser. The European Defense Agency backs that research project, a step toward development of a weapon.
MBDA is working in three laser projects, with Germany leading the way, a defense source said.
MBDA and its partner Rheinmetall won a German contract for a demonstrator for a naval laser weapon, the missile company said Jan. 28.
The deal, worth in the low 10s of millions of euros, will see Rheinmetall supply the laser and MBDA delivering the tracking, operator's console, and plugging the laser into the command and control system. The demonstrator is due to be tested onboard the F124 Sachsen frigate next year.
In the second project, MBDA leads the UK Dragonflyer consortium, which showcased a beam director turret at the 2017 DSEI trade show in London. That study is worth £30 million ($41 million) and the consortium includes Arke, BAE Systems, GKN, Leonardo, Marshall, MBDA and Qinetiq.
MBDA is also in the European TALOS study.
The drone threat has fuelled export sales of a mature air defense system dubbed ForceShield, said Jean-Philippe Hardange, Thales director of strategy for integrated airspace protection systems.
"There is a lot of demand," he said, with sales growth in that sector clearly outstripping the two-three percent rise in defense budgets of Nato allies.
The UK is operating the system initially armed with Starstreak missiles, then with Lightweight Multi-role Missiles.
Export clients bought the weapon with Ground Master 200 radar and C2 system. The radar could pick up a tactical UAV at a nominal range of 50-100 km, while a smaller drone could be detected at a nominal range of 15-20 km.
France has ordered the RapidFire 40 mm naval gun to arm four fleet auxiliary ships being built, and the gun could down drones and hit fast moving boats, he said. The first ship is due for delivery next year and enter service in 2023.
Thales gave a demonstration of a land based RapidFire in 2013. There were no immediate orders. A sales pitch could point out how army, air force and navy could use that version to protect land bases.
The gun is supplied by CTAI, an Anglo-French joint venture of BAE Systems and Nexter.

Be Selective

There is clearly a market for anti-drone weapons, with a range of technologies. The question is which approach is the most practicable.

"There are limits to technology," said Henry de Plinval, director of the drone program at Onera, a research office specializing in aerospace defense. "Technology is not magic."

The office expects to complete by the end of this year Shield its two-year study into the technology and operational aspects of anti-drone measures under development, he said.

The study aims to give expert opinion on the limits of technology, to point government and industry in the right direction for countermeasures.

The aim is to be "more precise," he said.

In research for drone detection, Onera is drawing on work on passive radar, using the general background of electromagnetic signals for devices such televisions to detect UAVs.

There are studies of identification to confirm the object is a military drone and not a bird or a tree. That includes advanced research into laser imaging detection and ranging (LIDAR) for 3D identification of targets at long distance of "several kilometers," he said.

To "neutralize" drones, there is the conventional GPS jamming, but there are strict rules on GPS, on which airlines depend, he said.

A more sophisticated approach is GPS "spoofing," to divert the drone to another flight path.

A "kinetic" hit is fine in open spaces such as deserts, but harder to use in urban combat, he said. Alternative measures will be needed.

There is an operational need, but technology needs time, he said.

Drones over the Med?

Meanwhile, tension between Greece and Turkey over territorial claims over the Eastern Mediterranean presents a marketing opportunity for drones.

A land and sea surveillance project dubbed **Semaphore** is seen to be of potential interest to the Greek forces, the executive said. That system offers a mix of border surveillance and flying mini-UAVs over the sea.

Four fixed-wing drones, each flying eight hours, could provide 24-hour surveillance over the Eastern Mediterranean. A Greek coast guard patrol boat could launch a drone by catapult and recover with a net, or a drone could be launched from one of the Greek islands.

An extended network of UAVs and radars would allow Greece to track Turkish naval activity, and follow Turkish moves on the island of Cyprus, close to mainland Turkey and the subject of long-standing dispute.

Greece and Turkey are in dispute over claims of exclusive economic zone in that part of the Mediterranean, where Ankara is looking for oil and gas reserves.

Athens has ordered 18 Rafale fighter jets and missiles in a deal worth €2.5 billion ($3 billion), pointing up the tension with Ankara.

EDITOR'S COMMENT: Do you think that Greece would like to spend €2.5 billion if Turkey was not such an aggressive neighbor? It would be nice those writing similar articles to be careful with the selection of words and better infomed about the topic they write about.

Drones are biggest tactical concern since the rise of IEDs in Iraq, CENTCOM boss says

Source: https://www.armytimes.com/news/your-army/2021/02/08/drones-are-biggest-tactical-concern-since-ieds-rose-in-iraq-four-star-says/

Feb 08 – Aerial technologies once viewed as hobbyist toys have triggered alarms at U.S. Central Command.

The proliferation of small, cheap drones is the "most concerning tactical development" since the rise of the improvised explosive device in Iraq, Marine Gen. Kenneth McKenzie, who helms CENTCOM, said in prepared remarks at the Middle East Institute on Monday.

The concerns are amplified by the lack of a dependable countermeasure against those drones, according to McKenzie.

"I'm not just talking about large unmanned platforms, which are the size of a conventional fighter jet that we can see and deal with by normal air defense means. I'm talking about ones you can go out and buy at Costco right now for $1,000," McKenzie said.

Commercial drones are relatively inexpensive and easy for militant groups and criminal organizations to modify to fit their needs.

Videos from battlefields in Iraq, Syria and Ukraine have shown the potential havoc that small drones can bring to unsuspecting ground forces, including scouting for call-for-fire missions and dropping bomblets on exposed positions. Syrian fighters even found crude ISIS drone factories in areas liberated from the extremist group.

A small ISIS drone, captured by Iraqi police, rests on a table at an intelligence-sharing meeting at Qayyarah West Airfield, in Iraq, (Jason Hull/Army)

"Right now, we're on the wrong side of the cost imposition curve because this technology favors the attacker, not the defender," McKenzie said. "But we're working very hard to fix this and flatten the curve. We have a variety of systems in the field already."
McKenzie added that the problem has the "direct attention" of leaders at the Pentagon. The Army, which is charged with overseeing the Defense Department's programs to counter small drones, published a new strategy outlining the threat in January.
Most of the military's current counter drone capabilities are electronic warfare systems. Many use lasers or microwaves to disrupt the communication link between drones and their operators.
But the counter drone strategy warns that swarms of small aircraft operating independently, facial recognition algorithms, artificial intelligence and high-speed fifth generation cell networks will challenge existing countermeasures. Swarming drones clouding an airspace could quickly overwhelm troops' current weapons.
Long-term, the Army is pushing for a networked approach, using artificial intelligence and machine learning to find and track possible threats. The Army's Fires Center of Excellence at Fort Sill, Oklahoma, is also expected to build a school for the joint force focused on fighting small drones by 2024.
"Those are all steps in the right direction, but it worries me because I think what we're seeing is the emergence of a new component of warfare," McKenzie said Monday. "Part of a system of systems, and how we work our way through this challenge will be closely watched by our competitors, and our adversaries."

Syrian fighters in Raqqa uncover ISIS drone factory

Source: https://www.militarytimes.com/flashpoints/2017/07/26/syrian-fighters-in-raqqa-uncover-isis-drone-factory/

July 2017 — Syrian fighters with the Syriac Military Council, a Christian militia closely allied with Syrian Kurd fighters, have uncovered what appears to be an ISIS drone factory in Raqqa, the Islamic State's de facto capital.
Macer Gifford, the nom de guerre of a British fighter with the council, posted images to his Facebook and Twitter accounts of what appear to be downed U.S.-manufactured drones late

Tuesday night. Scattered around the floor of the complex are fiberglass and plastic reproductions of the bodies of the drones, replicated by ISIS fighters.

However, according to officials at Operation Inherent Resolve, they have received no reports of ISIS drone factories and they contend no coalition drone has been shot down in the region.

"These have been shot down or crashed because of some tech issues," Gifford says in a video posted to Twitter.

Images of the drones can be seen with bullet holes and extensive damage. A close up of one of the images shows a partial part number.

"They are very sophisticated … this is a serious piece of coalition equipment," Gifford says, holding what appears to be a surveillance camera for one of the drones.

"There has been a clear attempt by ISIS to reverse engineer," Gifford says, referring to the reproductions of the drone bodies.

Diagrams of the drones written in English were also found in the building, indicating the ISIS members attempting to replicate the drones may have been Westerners.

ISIS has used drones to attack fighters in Raqqa, but the threat was considered to be negligible, officials at OIR told Military Times back in June. Drones operated by the terror group have typically been commercially available quadcopter drones.

Military Times has not been able to verify that the photos are in fact coalition drones. The U.S. does operate drones that appear similar to the pictures in the video, such as the RQ-20 Puma — a battery-powered and hand-thrown drone used by Army Special Forces.

Officials at Operation Inherent Resolve would not confirm the types of" tactical" drones they employ in Syria, citing operational security concerns.

However, Turkish security forces in January seized some RQ-20 Pumas from militants associated with the Kurdistan Workers' Party, or PPK, according to Hürriyet Daily News, an

English newspaper in Turkey. The PKK is an internationally designated terrorist group that Turkey contends has ties with a U.S. partner force in Syria, the People's Protection Units, or YPG.
There have been multiple reports of ISIS fighters in Raqqa shooting down and capturing RQ-20 Puma drones. Videos from ISIS' propaganda hub, Amaq, have shown the captured drones.
If Kurdish militants are operating RQ-20 Puma drones in northern Syria and Raqqa, they weren't supplied by the coalition, according to a spokesperson at OIR." The coalition provides their own aerial support in Syria and does not provide it as any aid package to the SDF [Syrian Democratic Forces]."
YPG fighters with the SDF are known to operate surveillance drones in Raqqa.

The next frontier in drone warfare? A Soviet-era crop duster

By Benjamin Fogel and Andro Mathewson
Source: https://thebulletin.org/2021/02/the-next-frontier-in-drone-warfare-a-soviet-era-crop-duster/

An An-2 parked in the snow. Credit: www.ariliners.net via Wikimedia Commons. CC BY-SA 3.0.

Feb 10 – In September 2020, on the second day of the six-week war between Armenia and Azerbaijan over the disputed Nagorno-Karabakh enclave, the Armenian defense forces published a video of one of their units deploying a surface-to-air missile system to target a low-flying, slow-moving object—a drone. But what the soldiers shot down was no cutting-edge autonomous weapon: They had destroyed a propeller-driven, single-engine biplane first produced in the 1940s by the former Soviet Union for agricultural monitoring and management—a crop duster.
Azerbaijan had evidently converted multiple Antonov An-2 piston-powered light aircraft into uninhabited aerial vehicles. During the conflict, they were repeatedly dispatched on munitions-laden suicide missions used to bait Armenian air defenses. Deployed as a so-called "bait drone," the An-2 from the September video forced the Armenians to fire their anti-aircraft weapons at its uninhabited fuselage, a ruse which revealed their defensive positions to Azerbaijani commanders searching for vulnerable targets. In doing so, Azerbaijan showed the world that even legacy hardware like the An-2 could be repurposed

and used effectively in drone warfare—another example of how militaries continue to find innovative ways to employ increasingly autonomous systems.
Others will likely imitate Azerbaijani bait-drone tactics in future conflicts. These types of drones can be effective tools for exposing an adversary's locations and capabilities while simultaneously diverting attention from a mission's primary objectives. They are also cost-efficient, considering that the price of using a bait drone could amount to simply losing an aging clunker like the An-2. Importantly, by repurposing what had been an inhabited plane into a semi-autonomous vehicle, Azerbaijan has also highlighted a weak point in international efforts to slow military drone proliferation.

The bait drones of Nagorno-Karabakh

The Soviet Union originally designed the An-2 in 1946 as a utility aircraft primarily used for crop dusting. The airplane's popularity stemmed from its easy handling and low maintenance requirements. It could be easily modified to meet a user's needs. These attributes, of course, also make the An-2 a strong candidate for bait-drone conversion. In the 1950s, the An-2 entered mass-production in the Soviet Union, Poland, and China and has seen extensive service ever since. But, by the time of last autumn's fighting in Nagorno-Karabakh, the common perception of the aircraft was that it was largely obsolete, particularly for combat. Azerbaijan confounded that belief and used the An-2 to locate Armenian air defense positions and identify equipment its forces could target.
Azerbaijan repeatedly sent the An-2 on one-way, dual-purpose missions to bait Armenian air defenses and act as a cheap alternative to other loitering munitions, the ordinance-bearing kamikaze drones that "loiter" above a target before swooping down to attack. The Nagorno-Karabakh media reported images and videos of downed An-2s, some with large, unexploded bombs, suggesting that Azerbaijan often outfitted the drones with munitions. This was likely intended to guarantee that the Armenian side fired at the bait, lest they became the targets of a lethal attack.
Engineers supporting Azerbaijani forces likely converted the An-2s into drones by installing pneumatic autopilot guidance systems. (While pilots could have been manually setting their aircrafts' courses before parachuting to safety, there are no credible reports of that happening during the conflict.)
Azerbaijan, in effect, built on previous efforts to make drones out of An-2s. In 2018, China successfully demonstrated the capability to convert the aircraft into an uninhabited cargo plane; Azerbaijan took a different path and repurposed the vehicles for combat.
While we don't know how many An-2s were used as bait drones, the number could be substantial. In late-August 2020, just weeks before the outbreak of the war over Nagorno-Karabakh, commercial satellite imagery depicted approximately 60 An-2s at Yevlakh airfield in Azerbaijan. That large inventory dates back until at least 2016, but by the end of the first week of fighting in Nagorno-Karabakh, more than half of those An-2s had departed Yevlakh. As the Armenian-backed enclave's ministry of defense began to publicize this new drone threat, open-source research documented at least 11 Azerbaijani An-2s destroyed during the war.
Azerbaijan is not the first country to use bait drones in conflict.
During the 1982 Lebanon War, Israeli drones were used to bait Soviet-built, Syrian air defense systems by tricking the systems into thinking they were tracking American-made Israeli fighters. A few years later, the South African Air Force deployed bait drones in the Border War against Cuban and Angolan guerillas. And even the United States employed its own bait drones to great success in the Gulf War against Iraqi air defenses. In each case, bait drones were used to the same effect: They drew the attention of adversarial air defenses, exposed the type and location of anti-aircraft systems being used, and rendered them vulnerable to strikes by artillery fire or dedicated attack aircraft.
The Azerbaijani use of the An-2, however, shows an original and economical utilization of old equipment in a decisively modern and technologically advanced regional conflict. Other militaries, especially in states with an abundance of aging and antiquated Soviet hardware, will likely follow Azerbaijan's lead. As drones and other modern military technologies become increasingly important in conflict, those nations unable to keep up with recent developments and expensive machinery will undoubtedly make use of equipment on hand, even more so when their results might be as lucrative as those achieved by Azerbaijan.

A future of more modifications and proliferation

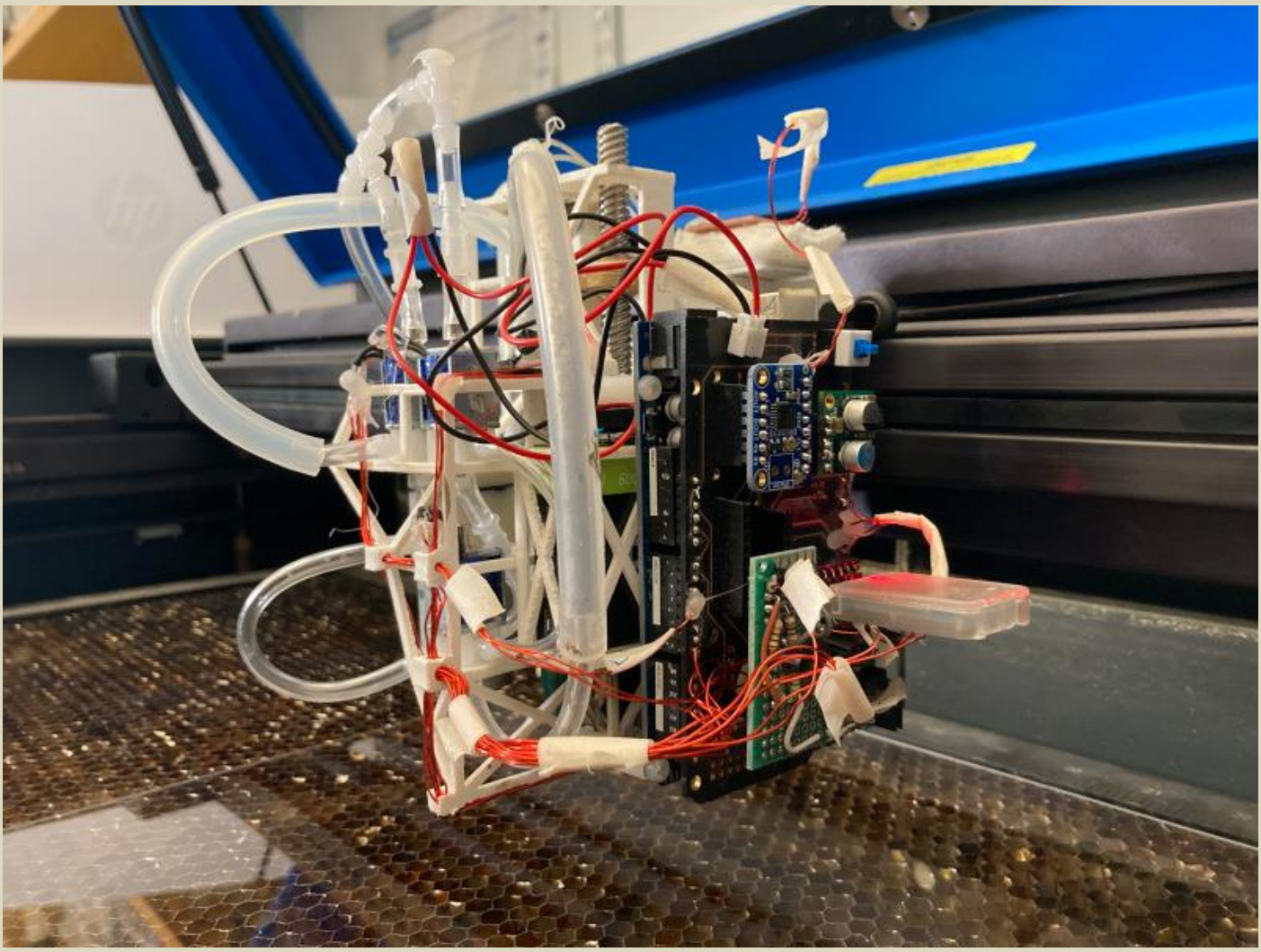
Unlike inhabited aircraft, drones are regulated under the Missile Technology Control Regime, a voluntary multilateral export control system that attempts to limit their proliferation. Azerbaijan's An-2s highlight a loophole in the regime; the system doesn't prohibit the transfer of the technology or techniques required to turn inhabited aircraft into drones. Although some argue that drones are implicitly covered by the Arms Trade Treaty, it is unlikely to affect such proliferation as the language is too vague and many of the top drone-producing countries—including the United States, Russia, Turkey, and Israel—are not parties. While there haven't yet been any reports of modified aircraft sales—perhaps because these modifications represent a new policy issue—other countries, or even subversive plotters, could potentially use their own modified aircraft as bait drones, as Azerbaijan did, or even in kamikaze-style terrorists attacks.

In the 40 years since the first widespread use of drones in a traditional military conflict, drones have become increasingly powerful and sophisticated tools for intelligence, surveillance, targeting, reconnaissance, and combat. Today, commercial companies are making drone technology more accessible, and militaries and other armed groups will continue to devise novel uses of drones. Drawing lessons from Azerbaijan's successes in the conflict, Iran, for example, has increased its investment in loitering munitions, as have NATO air forces such as the Netherlands. Bait drones could be the next.

Azerbaijan's use of bait drones illustrates how simple automation can transform tactics, techniques, and procedures in modern warfare. While the soldiers in the Nagorno-Karabakh video were able to destroy the An-2 with surface-to-air missiles, they were forced to take Azerbaijan's bait, increasing their vulnerability to attack. Fundamentally, military planners will have to find new ways to respond to the bait drone threat, while more broadly, the arms control community will have to weigh just how to restrict the new drones as well as the technology required to produce them.

Full Drone Manufacturing by 3D Printer

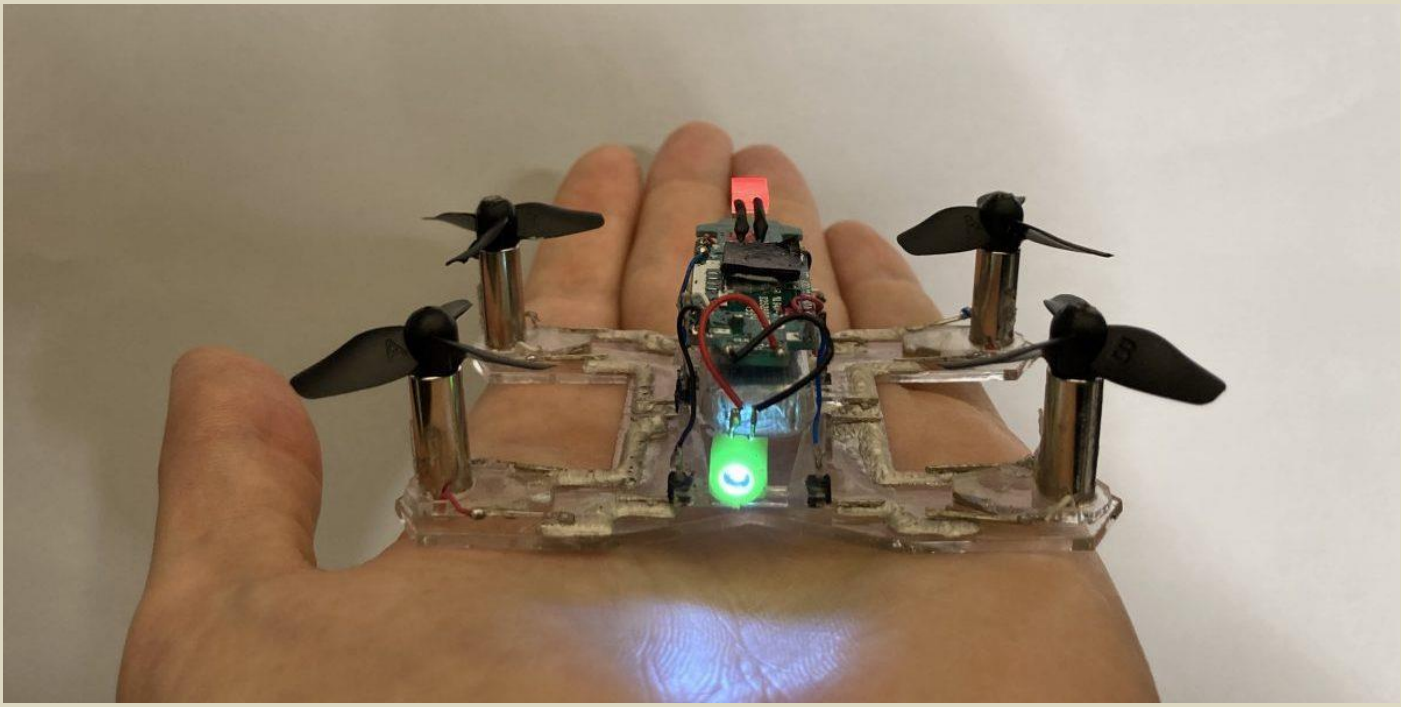
Source [+video]: https://i-hls.com/archives/106931



Feb 11 – In the future, people shouldn't be expected to have an engineering degree to build robots, any more than they should have a computer science degree to install software. New technology is about to materialize this vision.

While 3D printing (also known as additive manufacturing) has been capable of producing a range of objects, it still lacks the ability to fabricate more complex devices that are essentially ready-to-go right out of the printer. One of the challenges is the requirement for post-printing assembly. An outside party is required to put them together.

A group from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) recently developed a new system to print functional, custom-made devices and robots, without human intervention.
This type of "one-stop shop" could be beneficial for product developers, makers, researchers, and educators looking to rapidly prototype things like wearables, robots, and printed electronics.
Their single system uses a three-ingredient recipe that lets users create structural geometry, print traces, and assemble electronic components like sensors and actuators.
"LaserFactory" has two parts that work in harmony: a software toolkit that allows users to design custom devices, and a hardware platform that fabricates them.
"By leveraging widely available manufacturing platforms like 3D printers and laser cutters, **LaserFactory** is the first system that integrates these capabilities and automates the full pipeline for making functional devices in one system," says the team.



As an example, "let's say a user has aspirations to create their own drone. They'd first design their device by placing components on it from a parts library, and then draw on circuit traces, which are the copper or aluminum lines on a printed circuit board that allow electricity to flow between electronic components. They'd then finalize the drone's geometry in the 2D editor. In this case, they'd use propellers and batteries on the canvas, wire them up to make electrical connections, and draw the perimeter to define the quadcopter's shape."
As well as fine-tuning the current system, the researchers hope to build on this technology by exploring how to create a fuller range of 3D geometries, potentially through integrating traditional 3D printing into the process, mit.edu. reports.

Edge Group unveils kamikaze drones at IDEX2021

By Agnes Helou (Middle East correspondent for Defense News)
Source: https://www.defensenews.com/digital-show-dailies/idex/2021/02/22/edge-group-unveils-kamikaze-drones-at-idex/

Feb 22 — Emirati defense conglomerate Edge Group unveiled on Sunday four multirotor loitering munitions, sometimes called kamikaze drones, during the first day of the International Defence Exhibition and Conference held in the United Arab Emirates' capital Abu Dhabi.
"QX is a family of four different aircraft. The first one is the QX-1 micro-UAV; the quadcopter basically carries a payload of 0.5 kilograms and the platform weighs 3 kilograms. The QX-2 mini-UAV is a much bigger platform and can carry a 1.5-kilogram payload," Mohamed Abdullah Al Nuaimi, the senior business development manager with the manufacturer, told Defense News.
"The QX-3 small UAV can carry basically up to four guided munitions of total weight of 5 kilograms; and the QX-4, which is a fixed-wing, vertical-takeoff-and-landing UAV with a 5-kilogram payload, can fly for 90 minutes," he added.

The locally made precision-guided systems were produced by Edge subsidiary Adasi, and they use artificial intelligence software for targeting and strike missions, according to a news release. The drones are not intended for intelligence, surveillance and reconnaissance missions, but rather to destroy targets.

"The platforms are unique due to their capability to identify targets through electro-optics mounted on each one of them. The technology used is to capture all the information regarding the target through those electro-optics, then get transferred toward specialized software to the guided munition, which by itself has electro-optics mounted on top to guide the steering of the munition toward the target," Al Nuaimi said.

Al Nuaimi would not specify the price tag of the QX systems, but he did describe them as cost competitive on the international market.

Jean-Marc Rickli, the head of global risk and resilience at the Geneva Centre for Security Policy think tank, pointed out that short-range, tactical loitering munitions such as quadcopters with increasingly advanced algorithms are already accessible to both state and nonstate actors.

"The complexity of the weapon systems depends on its assigned roles, the level of autonomy and the speed of the weapon. A long-range, fast loitering munition that is able to make autonomous attack decisions requires advanced technology that few countries have," Rickli told Defense News.

What would make a loitering munition stand out is facial recognition technology — something the QX family does not have.

What other drones were on display?

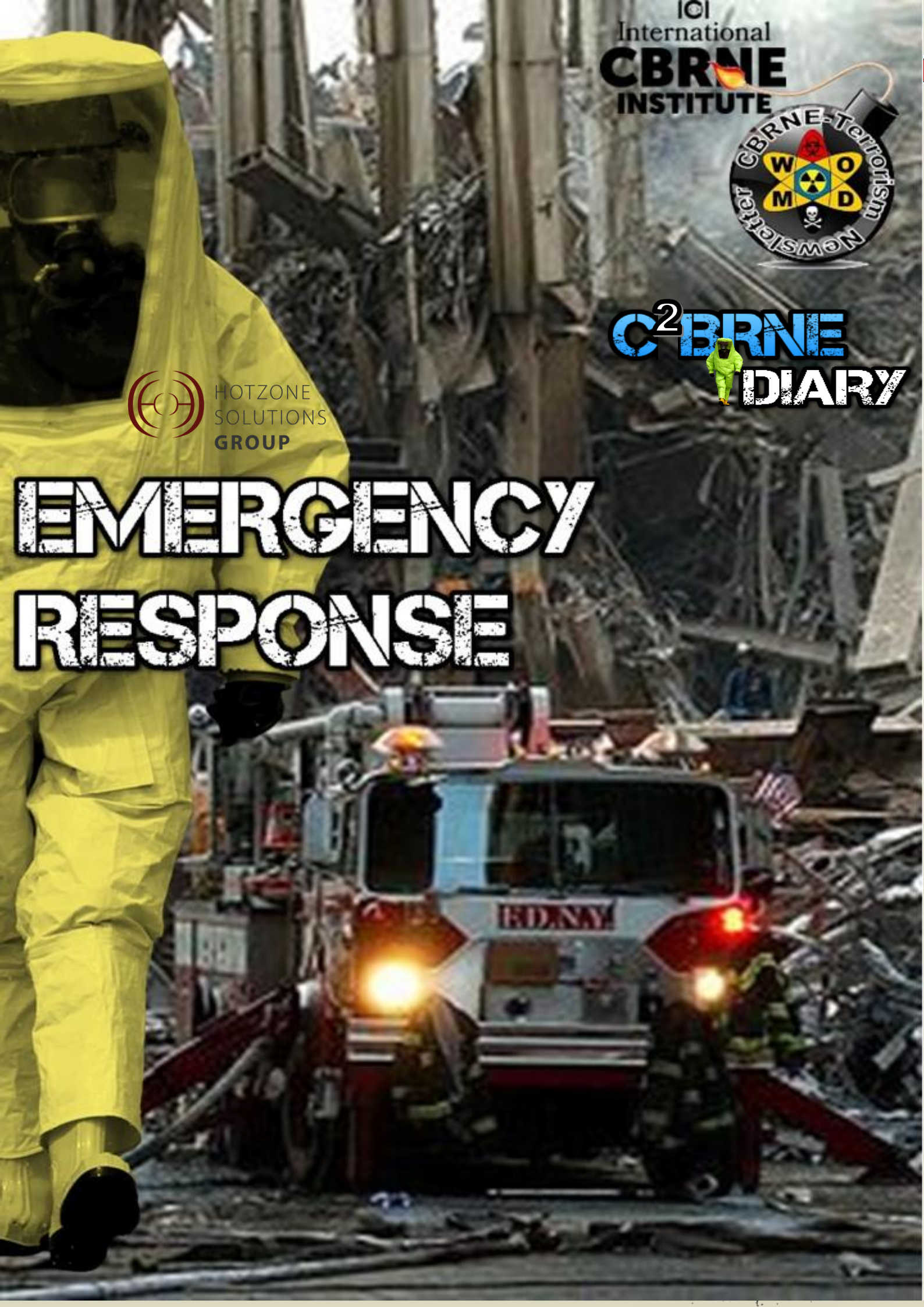
Edge also showed off its Shadow 50 and Shadow 25 drones, its Rash 2 gliding munition kit, and new variants of the RW-24.

Shadow 50 can carry a payload of 50 kilograms; that's double the capacity of its counterpart, the Shadow 25. These UAVs come with global navigation systems and can fly using video navigation systems in GPS-denied environments.

The Rash 2 is a fixed-wing guidance kit for mortars and other in-house designed payloads. It's capable of gliding in flight and directing munitions to ground targets. The UAE Armed Forces has placed an order for the platform under a 55 million dirham (U.S. $15 million) deal.

Three new additions of the RW-24 range were also launched at IDEX. The newly unveiled RW-24 Seeker is equipped with a thermal automatic seeker to provide accuracy of engagement for targeting moving threats. It can also operate in GPS-denied environments.

The RW-24 Extended Warhead and RW-24 Extended Range variants increase the payload capacity from 8 kilograms to 13 kilograms, respectively, enabling the drones to carry additional fuel or increase the size of onboard munitions.


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

Has DHS Cracked the Code for Accurate Location Tech?

Source: https://www.govtech.com/em/safety/Has-DHS-Cracked-the-Code-for-Accurate-Location-Tech.html

Jan 28 – Since 1999, when nine firefighters never made it out of a fire in a cold storage and warehouse building in Worcester, Mass., firefighters have been hoping for a tracking tool for commanders to keep tabs on personnel fighting fires.

The technology thus far has been limited, in some cases unable to penetrate buildings or other interference. The Department of Homeland Security Science and Technology Directorate (DHS S&T) believes it has finally cracked the code with the Precision Outdoor and Indoor Navigation and Tracking for Emergency Responders (POINTER) technology that it developed in collaboration with NASA.

"To hear that the technology is finally coming about where we have a lot better potential to know where [firefighters] are if they have a problem is outstanding, it's really important," said Curt Floyd, technical lead for first responders for the National Fire Protection Association. "If there's a pending collapse of the building or if they're having a problem, we can either talk them out or send somebody to help."

He said POINTER differs from previous technologies that attempted the same purpose because it emits magnetoquasistatic fields, which are very low frequency and able to penetrate all of the structural materials used for buildings to up to about a city block away.

"We are able to use this technology without any of the traditionally inherent problems with the other technologies," said Greg Price, DHS S&T first responder portfolio director.

Some of the problems with previous technology are line of sight, or with frequencies that bounce off an object. "Think about GPS," Price said. "As soon as you lose sight of the satellite they start to break down and fail. Some have frequencies that have an effect called multipath; when they see a metal object, they bounce off and their accuracy goes down."

The technology was tested last month at the Veteran's Affairs Greater Los Angeles Healthcare System along with Balboa Geolocation, which is partnering with DHS to get the product in the hands of first responders.

The testing was the first step prior to operational field testing with fire response agencies across the country this year. It is hoped that the commercial product will be available early next year.

"As a commander, I want to know where my people are so if somebody has an issue or they get low on air and aren't sure where they are, I can have somebody redeploy and help those people," Floyd said. "The only way I can do that is if I know where everyone is."

Another huge breakthrough for this technology is cost, which Price said will be available for "hundreds and not thousands" of dollars.

DHS has assembled a group of about 150 first responders annually for three days for breakout discussions to talk about their concerns and priorities. The Responders Resource Group consists of law enforcement, emergency medical, emergency management and fire departments who discuss what's needed to help them do their jobs more efficiently and safely. The top requirement and priority from the group has consistently been the ability to locate and track human resources and assets when they go inside of a building or dangerous environment.

"We've been testing in a number of different facilities for the past couple of years and have had great success," Price said. The California Institute of Technology is partnering with Balboa Geolocation to help get the technology to market.

Price said the first release will be for firefighters. It will consist of a receiver, which is about the size of an iPhone 11 right now but will inevitably become smaller. Each of these devices will be worn by a first responder. There will be two or three transmitters, which emit the magnetoquasistatic fields and can be mounted on a truck and deployed automatically or in a carry bag and placed inside a building to begin location and tracking.

The third piece of the technology is the visual display, which Price calls the most important piece because if it's not easy to use, it will not be an effective tool. "From the beginning we've been working with first responders in the development of not only the receivers and transmitters but the user interface," he said. "We simplified it to the point that it's very usable for first responders."

Four Ways the Biden Administration Can Revamp Disaster Management

By Jeff Schlegelmilch

Source: http://www.homelandsecuritynewswire.com/dr20210201-four-ways-the-biden-administration-can-revamp-disaster-management

Feb 01 – In the United States, 2020 had more billion-dollar disasters than any other year in recorded history, even without accounting for the COVID-19pandemic. This is part of a growing trend of more powerful disasters, such as forest fires or hurricanes, across more susceptible areas. This vulnerability is becoming understood to include a combination of the built environment, governance, and underlying social vulnerability. There is also increasing evidence as to how racial and socioeconomic disparities contribute to disaster vulnerability, and how federal assistance programs actually widen these disparities in the aftermath of a disaster.

Among federal agencies in the United States, disasters are managed by as many as 90 different programs across 20 agencies. These come with distinct triggers for activation, ranging from loss thresholds to presidential declarations. Many programs also require special Congressional appropriations to fund them. However, these programs are an uneven patchwork, leaving significant gaps in some areas, and overlapping responsibilities and authorities in others.

The new administration will need to embark on urgent disaster management reform, with a goal of ultimately simplifying our response in increasingly complex disasters. Here are four ways that the Biden administration can help streamline federal disaster management:

1. Conduct an Immediate Review

The first step is to define the scope of the problem. To this end, the incoming administration should conduct an immediate review of disaster management programs by relevant personnel in the White House's National Security Staff in coordination with the Federal Emergency Management Agency (FEMA), Department of Housing and Urban Development, Department of Health and Human Services, and other relevant agencies to identify sources of redundancy and inertia in existing programs, with recommendations for interim actions to ensure more timely assistance to disaster survivors waiting on benefits and other forms of assistance.

2. Create a Multidisciplinary Commission

The complexity of disasters inherently requires a diversity of perspectives. The process of improvement should be guided by a multidisciplinary commission to develop recommendations for comprehensive disaster management reform. This commission should include state and local officials, emergency managers, representatives from federal agencies, critical infrastructure partners, disaster researchers, and citizens from recently affected communities, defined as those under a major disaster declaration (other than COVID-19) in the last three years. This commission should be charged with providing a list of recommendations that include legislative action, executive action, and programmatic changes to consolidate and align disaster management to reverse the trends of growing disaster effects.

3. Establish Metrics for Investments in Readiness

While there have been moves to incentivize preparedness, we don't really know what that means, or how much is already being spent by states and communities outside of federal dollars. It is critical to confirm metrics for measuring and reporting non-federal investments in disaster preparedness and mitigation to better inform policies that incentivize investments

in resilience. This should include the built environment as well as social investments to better inform our understanding of where these investments are being made, and their consequences.

4. Expand Current Strategies to Simplify Disaster Coordination

One of the three overarching goals in FEMA's 2018-2022 strategic plan is to "reduce the complexity of FEMA." This is a laudable and much needed goal, but should also be extended beyond FEMA to the entire federal enterprise with disaster programs and responsibilities. Key indicators of success should be survivor-centric, seeking to reduce the number of interfaces needed to get assistance, and decreasing timeframes from the moment of a disaster to when assistance is received.

Comprehensive disaster reform will require executive action as well as legislation and a culture shift in the way we prepare as a nation. The incoming administration will be faced with the urgency of this reality with increasing disasters and the ongoing COVID-19 pandemic, but will also have a unique opportunity to build the foundation for a more resilient future.

***Jeff Schlegelmilch** is the Director for the National Center for Disaster Preparedness at Columbia University's Earth Institute.*

Millions of Americans Have No Power in This Extreme, Nation-Wide Storm. Here's Why

By Michael Webber

Source: https://www.sciencealert.com/why-are-millions-of-people-in-texas-without-power

Feb 16 – Amid record cold temperatures and skyrocketing energy demand, utilities across the central US have ordered rolling blackouts to ration electricity, leaving millions of people without power. Energy expert Michael E. Webber explains why weather extremes can require such extreme steps.

1. The Plains states have a lot of wild weather. Why is this cold wave such a problem for utilities?

The central US has freezes, heat waves, windstorms, droughts and floods. All of these events stress the electric grid, pipeline networks, roads, rail and waterways.

Right now in my state of Texas, ERCOT, a nonprofit corporation that manages the power grid for most of the state, is imposing rolling blackouts because demand for electric heating is very high. So is the Southwest Power Pool, which serves customers in 14 states from North Dakota to Oklahoma.

About 60 percent of homes in Texas have electric heat, and most of the rest use natural gas or propane. Normally our peak electric demand is on summer afternoons for air conditioning. But in this sustained cold, electric demand is spiking to keep homes comfortable and pipes from freezing. This storm is more extreme than the most severe winter conditions that ERCOT typically plans for.

At this time of year, power plants that run on coal or natural gas often shut down for planned maintenance ahead of the summer cooling season. That means we have less capacity available than usual right now.

To meet the difference between high demand and low capacity, utilities are cycling power on and off to different neighborhoods or regions of Texas in a methodical way to keep things in balance.

If they didn't do this, there would be a risk of a much wider-scale blackout, which would be catastrophic and life-threatening.

2. How do utilities plan for this kind of extreme weather?

Utilities everywhere follow the weather very closely. Temperature changes affect the need for heating and cooling, which drives demand for electricity and natural gas. Meteorological conditions affect the availability of wind and solar power.

Thermal power plants – which burn coal, natural gas or biomass – also need a lot of water for cooling to run efficiently, as do nuclear power plants. If climate change warms rivers or reduces their water levels, it could force those power plants to turn off or reduce their output.

Weather forecasting has improved as satellites become more abundant and computer models become more sophisticated. Utilities can take steps in advance of a major storm, such as asking customers to preheat their homes. For ratepayers who will do this, the utility may adjust their thermostats to reduce power flow when demand is high.

Power providers can also ask large industrial customers to temporarily shut down factories to reduce electricity demand. And they can give hourly or minute-by-minute updates to customers about rolling blackouts and provide real-time maps of power outages.

Utilities work year-round to harden the grid against extreme weather. They may build berms to protect power plants against floods, fill reservoirs in preparation for droughts, replace

equipment that can get overheated in the summer or weatherize power plants for cold conditions.
Almost exactly a decade ago, in February 2011, Texas suffered a significant series of rolling blackouts when cold weather forced dozens of coal and natural gas power plants offline. This cold snap is testing the upgrades utilities made after that event.

3. Does having a diverse fuel mix protect against energy crunches?
Texas is blessed with multiple energy sources. Much of it is produced locally, including natural gas, wind and solar power. Over the past 15 years, the state has diversified its fuel mix: Coal use has dropped, wind and solar have grown, and nuclear and natural gas use have held steady.
Each of these options has pros and cons. Wind and solar do not require water cooling, so they work fine during droughts and floods. But they vary based on wind patterns, cloud cover and time of day.
Nuclear power is reliable, but sometimes nuclear plants have to reduce their output during heat waves or droughts if their cooling water is too hot or scarce.
Natural gas is a high performer, but in the 2011 Texas cold snap, gas plants struggled to keep up with demand because many homes and businesses were using the fuel for heat.
That reduced the pressure in gas pipelines, which made it hard to physically move gas to turbines that needed the fuel to generate electricity.
Much of the coal burned in Texas power plants comes from Wyoming over a sprawling rail network that can be disrupted if a bridge or section of track is out of commission for repairs. Utilities store 30 days or more of coal in piles near their power plants, but those piles can freeze or be flooded, as occurred when Hurricane Harvey swamped Houston in 2017.
Because all of these options fail in different ways, a diverse mix is the best basis for a robust system. Today Texas has three times as much wind power-generating capacity as it did in 2011, which may help stave off the worst risks of a statewide blackout.
This extra wind will be especially important because about 30 percent of ERCOT's generating capacity is offline right now, reportedly due to natural gas shortages.
Some West Texas wind turbines have also shut down due to icing, but turbines in other parts of the state are partially offsetting those losses. ERCOT will investigate all power losses after this storm passes and use what it learns to make new improvements to its system.

4. California has had rolling blackouts recently, too. Is this a national risk?
California is a big state with power sources in many locations, so it relies on a sprawling network of wires and poles to move electrons from one place to another. Those power lines can sag when it's hot out and fail when high winds blow trees down onto the wires.
Aging transmission and distribution networks can also spark wildfires, which is a growing risk as the effects of climate change worsen drought conditions in the West. To manage those risks, California grid operators will preemptively turn off the power to prevent wildfires.
They also did this in August 2020 to ration power during a heat wave.
Weather-related power outages are increasing across the US as climate change produces more extreme storms and temperature swings.
States that design their buildings and infrastructure for hot weather may need to plan for more big chills, and cold-weather states can expect more heat waves. As conditions in Texas show, there's no time to waste in getting more weather-ready.

***Michael E. Webber** is Josey Centennial Professor of Energy Resources @ University of Texas at Austin.*

Towards More Rapid and Accurate Emergency Response Service

Source: https://i-hls.com/archives/107109

Feb 19 – The emergency response system was built on the limited context a phone call can provide, which often delays dispatch and under-informs first responders. Public safety agencies are still coping with challenges that require the capability to receive requests for service via not only voice but also through text, video, sensors, social media and instant messaging.
New technology delivers critical, real-time data to emergency call centers to empower smarter and faster emergency response.
Emergency communications centers across the UK will now have access to life-saving data.
A new collaboration combining Hexagon's innovation in call center dispatch with the RapidSOS emergency response data platform, will provide emergency services with a rapid, accurate and up-to-date information when responding to accidents, critical incidents and

health emergencies. In an emergency, critical data from devices, sensors, or profiles is integrated with the RapidSOS platform and then shared immediately with public safety.
This life-saving data can be distributed widely to first responders through the HxGN OnCall Dispatch suite – which provides police, fire, ambulance and transportation agencies with quality incident management and call-taking capabilities, to deliver better service during emergencies.
For example, when a call is made from a user's registered mobile phone or connected device, call handlers will automatically receive critical details about them to send to those attending emergency call-outs.
The OnCall Dispatch is a flexible suite of next-generation incident management capabilities. Supporting on-premises, customer-hosted, or Software as a Service (SaaS) deployments, the intelligent software suite provides incident management capabilities in the public safety answering point (PSAP), emergency control room, station, unit, or anywhere first responders need to go.
The RapidSOS Platform supports all sorts of data, from dynamic AML (Advanced Mobile Location) and alternative location services to additional details generated from security systems, connected mobility, healthcare, connected buildings, apps, and wearables.

Greece: Snow storm "Medea" (February 2021)

By the Editor-in-Chief

Athens downtown during Medea snow storm (Feb 2021)

Mid-February and snowstorm "Medea" attacked entire Greece. It was one of the worst snowstorms of the last 20 years in the country. Although the northern parts of Greece do have extreme winter experiences, it was the capital Athens that suffered a lot and still is now (Day 06) that I am writing this short article.
I live in a suburb-village approximately 40km away from Athens downtown with an altitude of 605m. We had snow for four days and temperatures below zero. Together with snow – ranging from 50cm to 1.5m due to strong winds – came electricity breakdown and water shortage for more than 36hrs (in our estate) or more (in other parts of the village and the capital. This incident is a vivid proof of the value of preparedness but even if you are prepared there is always space for further improvement. Below is a list of certain issues we were confronted with along we the things we have to improve in order to be better prepared the next time we will face an extreme weather emergency.
Heating: Radiators use heating oil and electricity to operate. Check the level of petrol in your tanks. You need an emergency power generator in order to support the system in case of a power failure. Our generator worked with unleaded petrol and our 10L supply was at

borderline if the storm lasted more. If we had one working with oil then we could use oil from radiators' tanks and have electricity enough for a few weeks. Lesson learned: Keep a 50L petrol can. Alternative: know how to suck oil from a car – not pleasant but in emergencies, it is not as difficult as it sounds (but you need to try it once to know what to do if needed). Of course, if there is a fireplace you need to have an adequate supply of woods (we had more than 6 tons available).

Water: The water supply system depends on electricity. No electricity, no water. We have water tanks as well – but they are for household use not for drinking. So, you need to have a supply of drinking water enough for a week (depending on the number of people living under the same roof. It is also good to know how to sanitize water and snow in order to be safe for drinking.

Food: Think of what you can eat without cooking or be kept in the refrigerator – plenty of products available. If outside temperatures are quite low then you can keep some items outside – a primitive refrigerator.

Editor's estate – Attika Prefecture (Feb 2021)

Appliances: Connecting big refrigerators and cooking stoves consume a lot of electricity and your power generator might not be able to keep up with (this was the case with our generator). If this is the case then you need to have a backup small refrigerator and a gas stove that both facilitate the emergency. It is a good idea to have a good supply of batteries for your headlamps and torches (preferably of LED type).

Information: You can connect your TV with the generator since it consumes power similar to a lamp or so. A battery (or solar) radio is also a good idea.

Snow equipment: 3-4 snow shovels are always a good idea. You will need salt for steps and certain possibly slippery parts of your outside constructions – please note: small quantities will have the same result as big quantities that might affect the environment and the cement of your property. I am thinking to buy a snowblower mainly for the day after because making corridors in order to free cars is a very painful procedure 😊

Garden/trees: Not much you can do to save your flowers and bushes but you can always trim some branches that might break due to snow and cause damages (roof; perimeter, main entrance gate, etc.).

Pets: Dry and canned food for your pets and sand for the cats – dogs most probably will enjoy the snow.

Clothing: Special attention to boots or apres-ski boots. Shoes-chains that can fit all kinds of shoes is a good alternative.

All the above are easy to do in a house but quite difficult when the residence is a city apartment. A generator is difficult to be connected with central heating but can support A/C heating. Nevertheless, it is an expensive piece of equipment that city people are not happy to invest in plus the inherent belief that extreme conditions affect only country people. Of course, now, residents of Athens downtown should reconsider and change their mindset! The unexpected always happens!

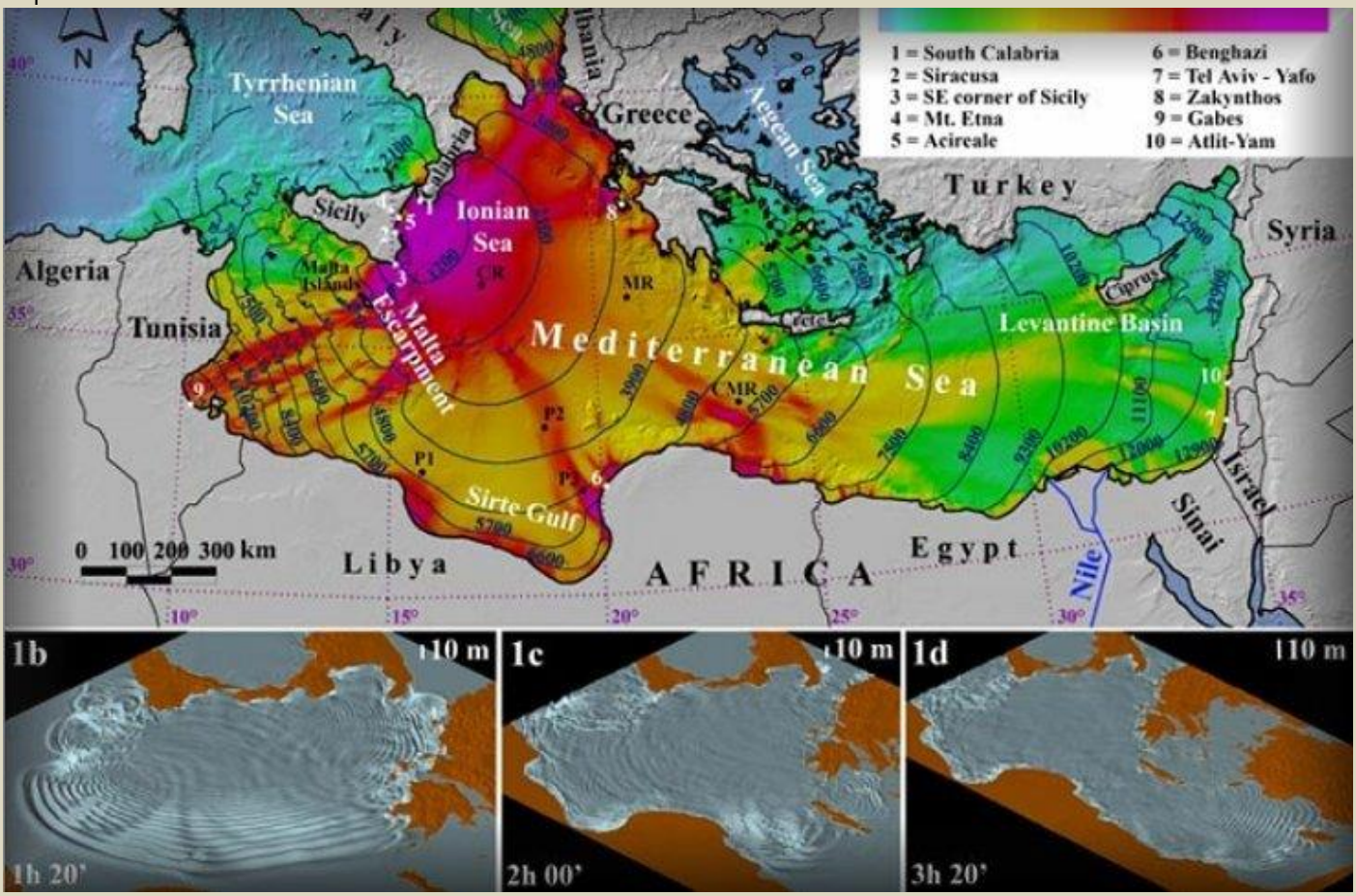
Mount Etna tsunami warning to 'entire Mediterranean' after volcano found 'sliding to sea'

Source: https://www.express.co.uk/news/science/1399422/mount-etna-tsunami-warning-sicily-volcano-eruption-landslide-mediterranean-italy-spt

Feb 18 – Europe's most active volcano erupted in spectacular fashion on Wednesday morning sending smoke and ash into the sky and forcing a nearby airport to close temporarily. There were no reports of injuries or damage and authorities said nearby towns were not at immediate risk. Despite this, they are monitoring the volcano in Sicily closely as it poses a significant threat in the event of more extreme activity – like the Plinian eruption of Mount Vesuvius in 79AD that buried Pompeii under a blanket of ash.

But it is not the only threat the Italian volcano possesses.
Scientists previously discovered that it appears to be slowly sliding into the Mediterranean Sea at a steady rate, according to measurements.
The readings were taken in 2018 and it was the first-time scientists were able to observe the movement of a volcano in its entirety, thanks to more than 100 GPS stations dotted around the sides of Mount Etna.
The slide was reported as slow but, according to the report, had "become unstoppable".
Lead researcher Dr John Murray added in 2018: "Previous studies of long-extinct volcanoes found those sliding downslope in a similar way have resulted in catastrophic landslides later in their history.
"Constant movement could contribute to a major landslide along Etna's coast, causing devastating tsunamis to the surrounding areas."
Geophysicist Heidrun Kopp from the Geomar Helmholtz Centre for Ocean Research in Germany added that it was "quite possible that it could collapse catastrophically, which could trigger a tsunami in the entire Mediterranean".
Experts previously thought the slide was due to a build-up of magma inside the volcano.

To investigate the anomaly further, researchers set up a network of underwater transponders to continuously monitor seafloor displacement.



Maximum wave crest heights predicted by a computer simulation of an ancient tsunami affecting the whole eastern Mediterranean Basin (1a). The blue lines are arrival times of the first tsunami waves. Furthermore, tsunami wave fields are shown at time steps of 1h20' (1b), 2h (1c) and 3h20' (1d) after a debris avalanche enters the sea. The white vertical bars provide the tsunami wave height scale. A number of effects induced by local and regional topography can be observed. For example, between Africa and Crete, as a result of part of the wave front rebounding off of the African coast, the waves are observed as crushing together (Source: Pareschi *et al.*, 2006a).

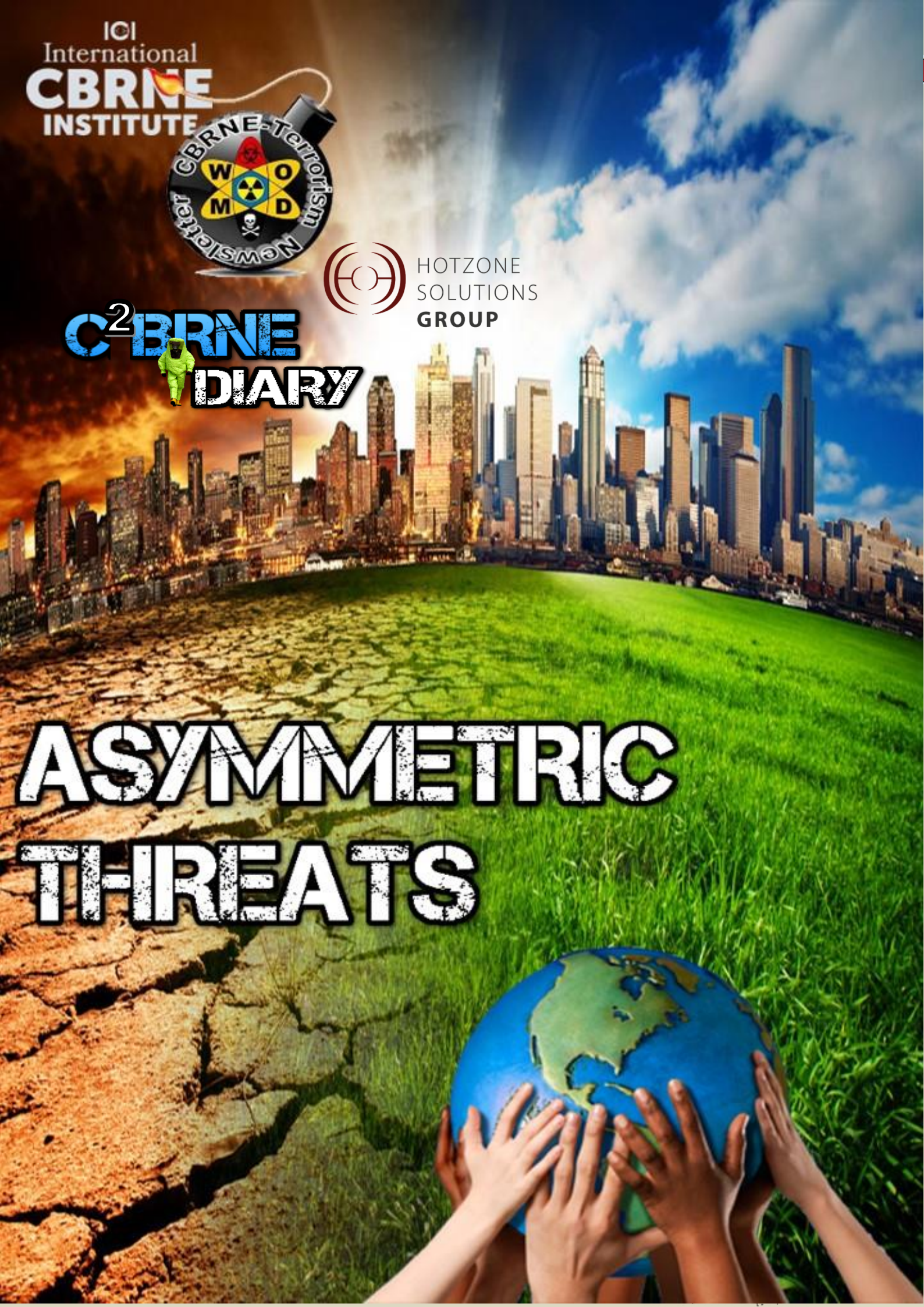
ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C²BRNE DIARY

ASYMMETRIC THREATS



Here's How Climate Change May Have Played a Role in The Emergence of COVID-19

Source: https://www.sciencealert.com/climate-change-may-have-played-a-role-in-the-emergence-of-coronavirus

Feb 05 – If last year's climate change fueled megafires and the global pandemic have taught us anything, it's how interconnected we all are with each other and our environment. Now, we have some early hints that both climate change and the cause of the pandemic may also be intertwined – through bats.

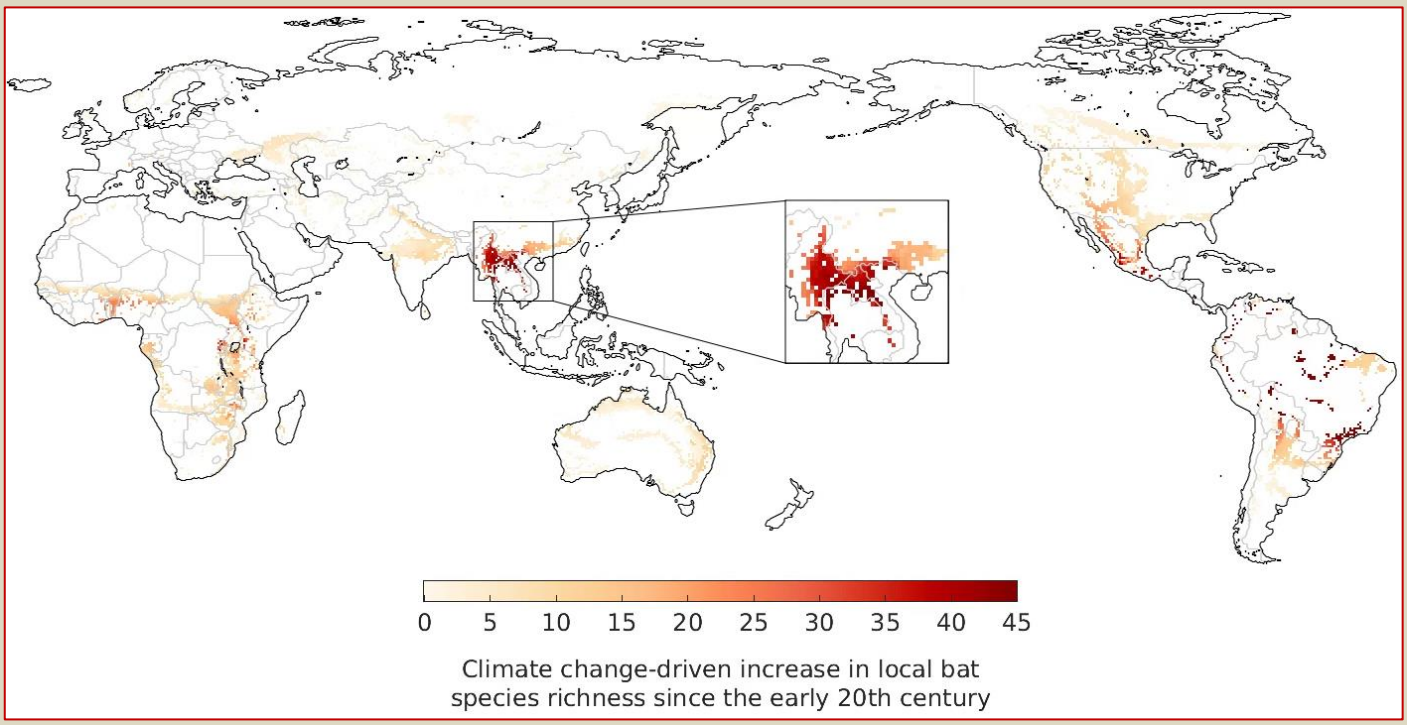
Bats have a notorious ability to live with viruses that destroy other animals. While their superpowered immune systems have been a blessing for them – allowing these airborne mammals to thrive around the world – it's a curse for the rest of us, as they carry these viruses with them wherever they go.

Now, a new study found that as the climate has warmed over the last century, the increase of sunlight, carbon dioxide, and changes in precipitation converted southern China's tropical shrublands to savannas and woodland – prime habitat for bats. And over 40 new bat species moved in.

"Understanding how the global distribution of bat species has shifted as a result of climate change may be an important step in reconstructing the origin of the COVID-19 outbreak," said zoologist Robert Beyer from Cambridge University.

To investigate this, Beyer and colleagues used data on the world's vegetation, temperature, precipitation, cloud cover, and the vegetation requirements of the world's bat species to construct a map of their distributions in the early 1900s. They then compared this to today's distributions of species.

"As climate change altered habitats, species left some areas and moved into others – taking their viruses with them," explained Beyer. "This not only altered the regions where viruses are present, but most likely allowed for new interactions between animals and viruses, causing more harmful viruses to be transmitted or evolve."



Change in global bat distribution since 1901. (Beyer et al, 2021)

Three out of four emerging infectious diseases in people are zoonotic diseases – they come from animals. And coronaviruses compose over a third of all sequenced bat viruses. The building blocks of the 2002 SARS pandemic were found within bats from a single cave, and now their bodies are prime suspects of having brewed the precursors of SARS-CoV-2.

Between them, the 40 relatively recent migrant bat species to China's Yunnan province carry more than 100 types of coronaviruses. Genetic evidence suggests the ancestor of SARS-CoV-2 comes from this same region.

Most of these coronaviruses can't infect us though. And now some species of bats are being wrongly prosecuted for other species unintentionally wreaking havoc upon us, even though

these animals play crucial roles in our ecosystems. At least 500 plant species depend on bat pollination (like bananas, mangos, and agave), other plants depend on their poop, and some species keep insects in check (including pesky, disease-spreading mosquitoes) by devouring them.

But our relentless march further and further into remaining natural habitats, through processes, like deforestation, that also drive climate change, increases our interactions between these animals and therefore our chances of encountering their viruses. Degraded habitats also stress and weaken the immune systems of the animals within them, providing more chances for viruses to mutate into something that can leap across species barriers.

"Among threatened wildlife species, those with population reductions owing to exploitation and loss of habitat shared more viruses with humans," a study found last year.

Beyer and team caution that we don't yet know the exact origin of SARS-CoV-2, so their inferences are not yet conclusive and further studies based on different vegetation and using different models are required to corroborate their findings. Other variables that possibly impact bat distributions, like invasive species and pollution, also need to be investigated.

And while correlation doesn't equal causation, a growing body of research does suggest climate change is a driver of pathogens infecting new hosts. We even have examples where historic global climate change has been associated with environmental disruptions that led to emerging infectious diseases.

"The fact that climate change can accelerate the transmission of wildlife pathogens to humans should be an urgent wake-up call to reduce global emissions," said biogeographist Camilo Mora from the University of Hawai'i, Manoa.

To reduce these risks Beyer and colleagues strongly recommend introducing measures to limit human and wildlife interactions, including imposing strong regulations on wildlife hunting and trade, discouraging wildlife-dependent dietary and medicinal customs, and establishing strict animal welfare standards on farms, markets, and transport vehicles. To do this we must consider the socio-economic needs that drive these practices they note in their paper.

It is also crucial we protect natural habitats to keep species healthy, a measure that can also help mitigate climate change.

"Given the possibility raised by our analysis that global greenhouse gas emissions may have been a contributing factor in the SARS-CoV-1 and SARS-CoV-2 outbreaks, we echo calls for decisive climate change mitigation, including as part of COVID-19 economic recovery programmes," the team urges.

▶▶ **This research was published in the** *Science of the Total Environment*.

.

Climate Change - Terrorism Nexus? A Preliminary Review/Analysis of the Literature

By Jeremiah O. Asaka

Perspectives on Terrorism. Volume XV, Issue 1 | February 2021

Source:https://www.universiteitleiden.nl/binaries/content/assets/customsites/perspectives-on-terrorism/2021/issue-1/asaka.pdf

Abstract

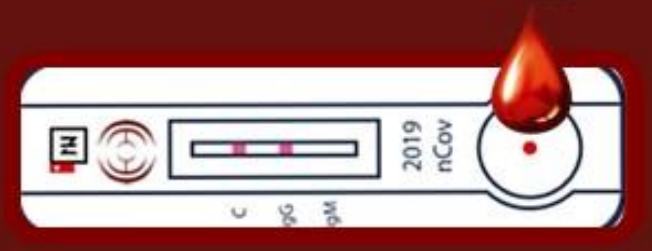
Climate change and terrorism are two key global security concerns of our time. Despite that fact, the two continue to predominantly be analyzed separately by most security studies scholars. However, interest on the interplay between these two concerns has grown considerably particularly over the past two decades. The growth in interest is attributable to the close to two decades of scholarship on the climate-security nexus. That scholarship establishes climate change as a threat multiplier, which worsens existing problems and aggravates vulnerabilities. This text presents findings of a preliminary literature review/analysis of 112 documents published between 2000 and 2020. The literature review/analysis was guided by the following three broad questions. What does the literature say about the link and/or lack thereof between climate change and terrorism? What is the publication trend for literature that explore the relationship between climate change and terrorism? What insight(s) for future policy and/or research? The text identifies two patterns of interaction with regards to the interplay between climate change and terrorism. On one hand, a simple one-way indirect relationship wherein climate change aggravates existing social vulnerability, which is a known enabler/driver of terrorism. On the other hand, a complex relationship wherein climate change contributes to terrorism and vice versa through a self-reinforcing process characterized by feedback loops.

Jeremiah O. Asakais *an assistant professor of security studies at Sam Houston State University, Huntsville, TX. He specializes in human and environmental security.*

HOTZONE SOLUTIONS GROUP

The world's most practice oriented provider of Hazardous Substances Management Solutions

Consultation
Products
Training



https://hotzonesolutions.org