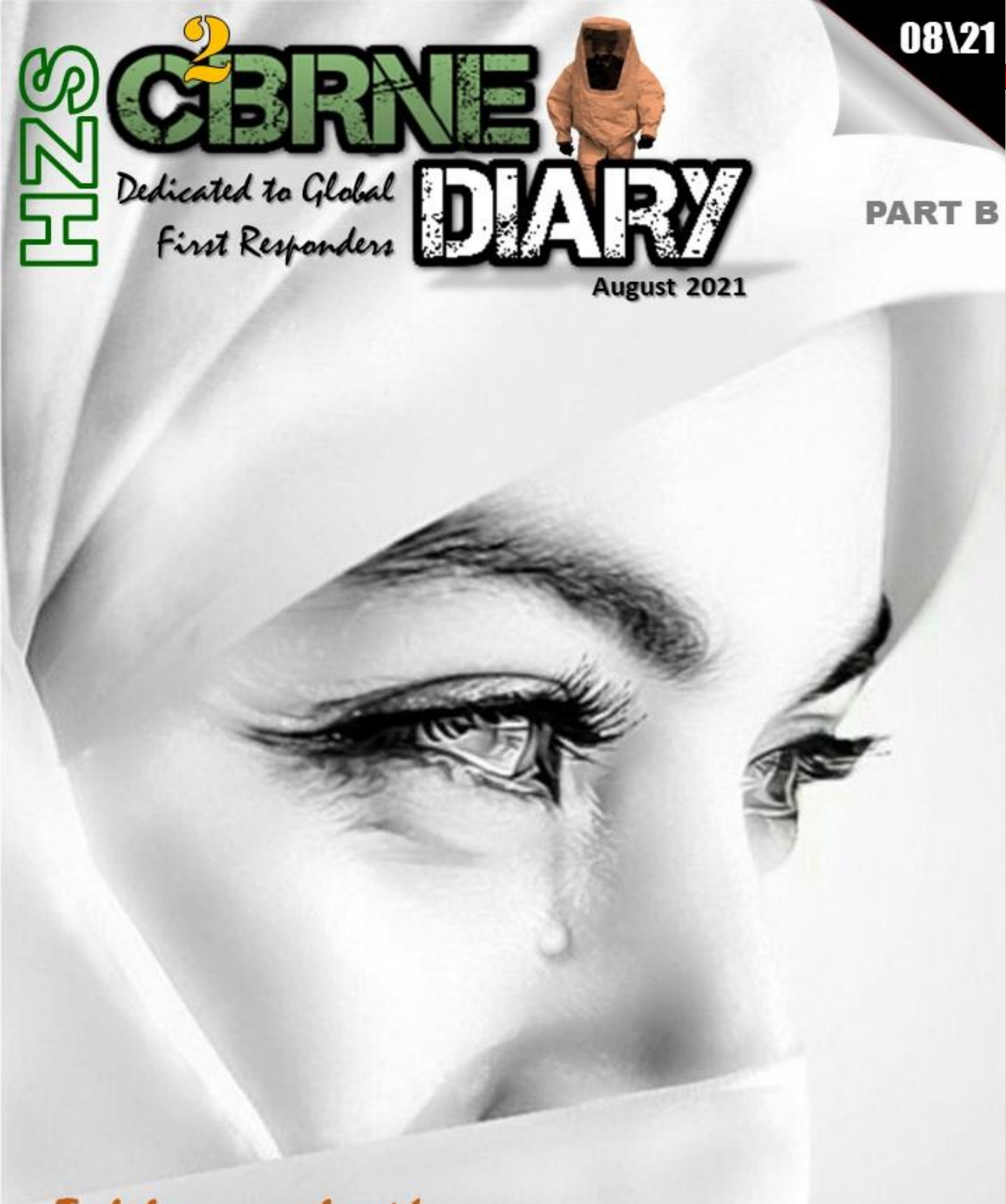
08\21

HZS C²BRNE DIARY

Dedicated to Global First Responders

PART B

August 2021



Taliban are back!

A HOTZONE SOLUTIONS GROUP PUBLICATION

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DIRTY R-NEWS

Are American Actions Pushing Japan And China Closer To Nuclear War?

By Marc Pilisuk

Source: http://www.blackstarnews.com/global-politics/asia/are-american-actions-pushing-japan-and-china-closer-to-nuclear-1

July 24 – After a war has ended, historians, elected officials, and faith leaders, no less than the people involved, often raise doubts over whether the outcomes were worth the many horrific costs.

But mourning diminishes over time and life for the survivors goes on.

Such a recovery from destruction is no longer assured or even likely in the age of nuclear weapons. World leaders, however, continue to play the game of war in ways that risk the war that could end life on earth.

Recent US actions in Asia are bringing us closer to such a war. The US has long held agreements with many countries, including South Korea, permitting launch facilities for nuclear missiles. Now the US is engaging in a program of assisting Japan in the development of missiles capable of launching nuclear warheads.

The Japanese constitution bans the development and deployment of such weapons. But the escalation of threats by the US and Chinese officials may threaten this longstanding policy.

This potential for Japan to launch weapons of mass destruction comes at a time of increasing the presence of US warships in the South China Sea. China was cruelly devastated by Japan in WW II, something effectively forgotten in the US but not in China. Indeed, a Chinese Communist Party video, still not confirmed as Chinese policy, threatens repeated nuclear attacks on Japan in response to anticipated military provocations.

This would amount to a departure from China's long-term policy of "no first use" (of nuclear weapons). Incredibly, the US has not yet committed itself to a "no first use" policy and has expanded its own nuclear weapons development programs. The recognition of potential danger from such development was clearly visible in the multi-lateral agreement preventing such activity in Iran. The US withdrew its treaty obligations under the Trump administration and has still not been able to revive the agreement.

History in the atomic era contains several examples in which deficiencies in communication during periods of hostility and threats almost led us inadvertently into the launch of a nuclear war.

The atomic scientists who monitor the level of risk have moved the nuclear doomsday clock closer to midnight. Massive expenditures for nuclear weapons development have produced tactical weapons more likely to be used and high yield weapons with destructive capacity far exceeding those used to destroy Hiroshima and Nagasaki.

These weapons continue to provoke adversaries, making us less secure. US military policy, resulting in 800 military bases in 80 countries, has not brought us security.

We live in a world in which the other greatest threats to life come from global warming and pandemic illness. To combat these threats international cooperation is needed.

We have developed a framework for such cooperation through the World Health Organization and other agencies of the UN. They have not been perfect but strengthening international collaboration in defeating pandemics and in radically reducing climate chaos may prove to be an insurance policy against falling into a nuclear war. When the reach of weaponry is global the reach of our relationships must be too.

This is far better than relying upon military powers to demonize competitors and continuing to see threats and force as a way that supposedly sane leaders can vie for competitive advantage. Building back better should mean the goods of life, not the instruments of death.

An appropriate agenda would start with rejecting the first use of nuclear weapons, ending the budget for nuclear weapons, ending the idea that wars are ever moral alternatives to peaceful conflict resolution, and demanding that our government rise to a level of mature diplomacy with all nations.

Negotiations toward zero nuclear weapons should be underway already, something that inspection technology makes practical and doable. We should lead and should incentivize all nuclear powers to join. This is literally a mortal threat to humankind.

Well-meaning military strategists are mired in a very dangerous game. They must be reminded that destroying our planet in a nuclear war would be a betrayal of everything we hold dear.

Dr. Marc Pilisuk is Professor Emeritus at the University of California, a faculty member at Saybrook University, and the co-author of The Hidden Structure of Violence.

EDITOR'S COMMENT: Apart from the obsession of Americans and NATO with Russians, there is a second obsession with China. As if there are no better things to pursue in life. Can you imagine a nuclear war in 2021?

'Unusual Warning': Israel Reportedly Tells US That Iran Is One Step Away From Obtaining Nukes

Source: https://sputniknews.com/middleeast/202107251083460417-unusual-warning-israel-reportedly-tells-us-that-iran-is-one-step-away-from-obtaining-nukes/

July 25 – Israel has long been sounding the alarm about Iran allegedly working to develop nuclear weapons. However, the Jewish State itself is widely believed to have obtained weapons of mass destruction a long time ago, with reports saying it could have at least 90 warheads at its disposal.

Israeli officials have told the United States that Iran is allegedly on the threshold of acquiring nuclear weapons, Israeli media reported Sunday.

According to The Times of Israel, which cited a Sunday report by Kan News, the country's foreign minister Yair Lapid, defense minister Benny Gantz and other senior officials issued an "unusual warning" to Washington: "This 'limbo' cannot be a time when Iran is quickly advancing toward becoming a nuclear threshold state," a senior diplomat told the Israeli news channel, reportedly referring to the ongoing Vienna talks on reviving the Iran nuclear deal.

Since April, Vienna has been hosting sessions of the JCPOA joint commission, as well as informal meetings in different formats aimed at preventing the Iran nuclear deal from falling apart after the US pullout. Trump unilaterally withdrew Washington from the agreement in 2018, slapping Tehran with harsh sanctions under the so-called "maximum pressure" campaign.

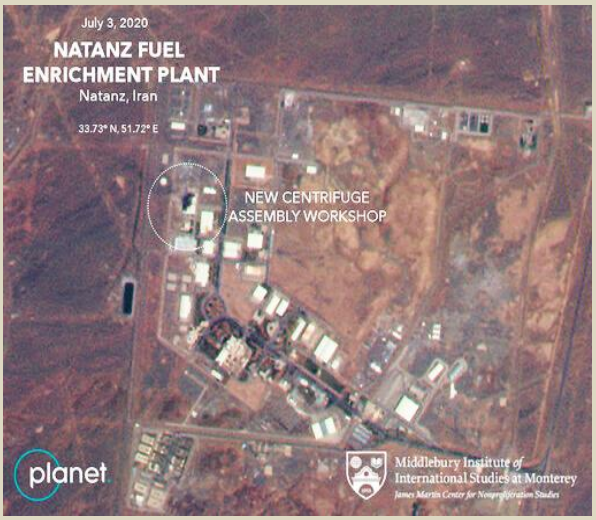
Iran has repeatedly insisted that sanctions must be lifted in the first place. Economic pressure has undermined the lives of ordinary citizens in Iran, especially during the pandemic.

This also comes along with the news that Israeli premier is reportedly to meet US President Joe Biden next month. In late June, Biden received the now-ex president of Israel Reuven Rivlin, where he claimed that under his watch, "Iran will never get a nuclear weapon".

Last week, the Israeli defense minister urged the government to prepare more carefully for a scenario in which Iran could obtain nuclear weapons, in the light of earlier reports of the IDF requesting more military spending for the sole purpose of preparing for a large-scale attack on Iran's nuclear program.

(enlarge the page to read the notes)

Tensions soared between Iran and Israel following the assassination of Iranian top nuclear physicist Mohsen Fakhrizadeh in autumn last year. Tehran attributed the killing to Israeli spy agency Mossad, while Israel refrained from either confirming or denying its alleged involvement.



The escalation was also driven by a series of "sabotage" attacks, attributed to Israel, at Iran's nuclear facilities, including the Natanz incident. In a scandalous recent interview given by ex-Mossad chief Yossi Cohen, it was hinted that Israel could have been involved both in the Natanz incident and in the operation to assassinate the nuclear scientist, stating that individuals who are considered to pose a threat to Israel should be eliminated.

Back in 2018, outgoing Israeli Prime Minister Benjamin Netanyahu claimed the scientist had headed a secret unit within the Iranian military allegedly working to develop nuclear weapons.

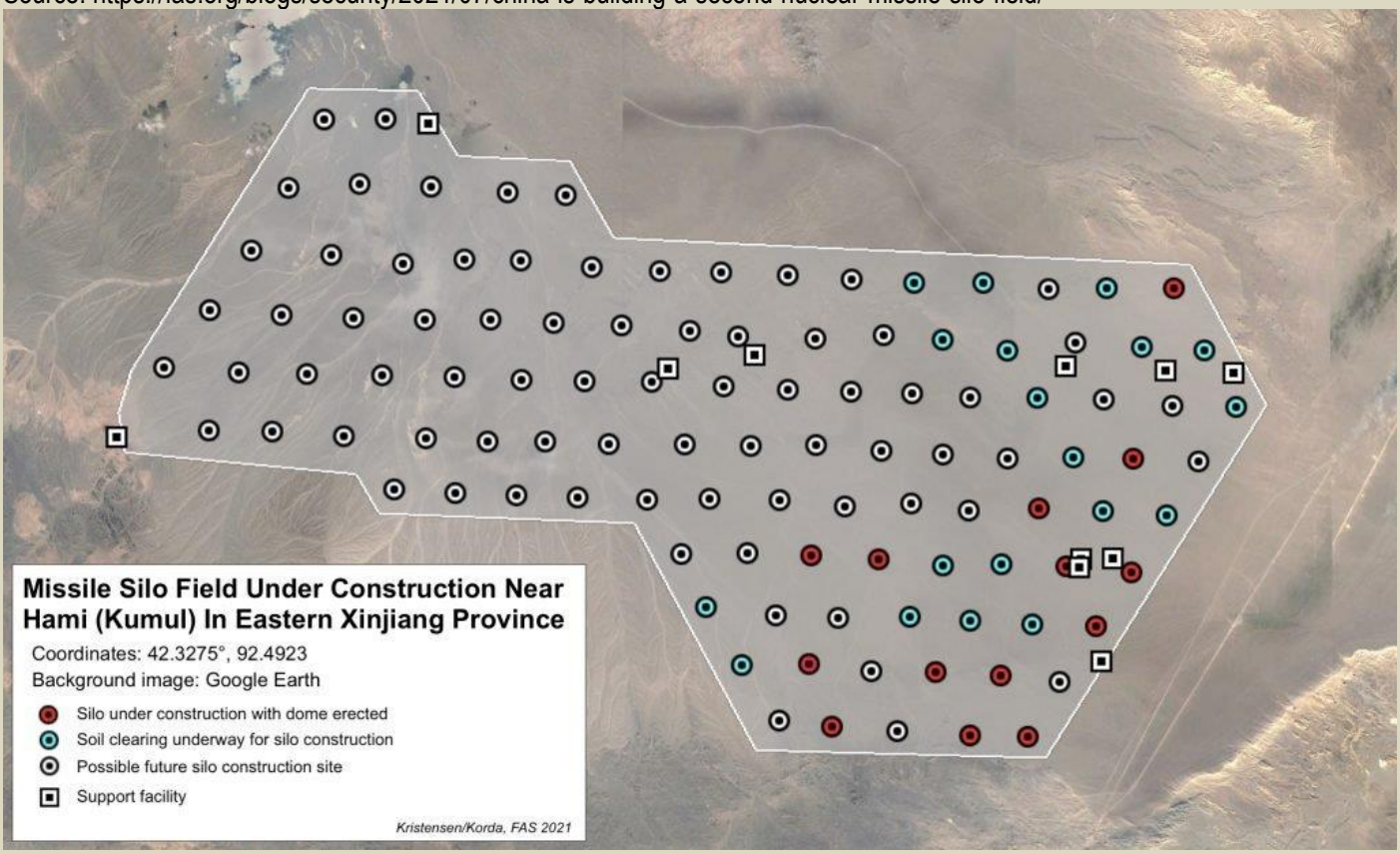
Iran has repeatedly accused the West of hypocrisy regarding its nuclear program, pointing to various reports suggesting Israel acquired the weapons of mass destruction long ago.

According to the Center for Arms Control and Non-Proliferation, Israel could possess at least 90 plutonium-based nuclear warheads and has reportedly produced enough plutonium for 100-200 nukes. Some speculate that the Jewish State might have conducted a successful nuclear test as early as 1979, referring to the Vela incident in South Africa.

China Is Building A Second Nuclear Missile Silo Field

By Matt Korda and Hans Kristensen

Source: https://fas.org/blogs/security/2021/07/china-is-building-a-second-nuclear-missile-silo-field/



The Hami missile silo field covers an area of about 800 square kilometers and is in the early phases of construction.

July 26 – Satellite images reveal that China is building a second nuclear missile silo field. The discovery follows the report earlier this month that China appears to be constructing 120 missile silos near Yumen in Gansu province. The second missile silo field is located 380 kilometers (240 miles) northwest of the Yumen field near the prefecture-level city of Hami in Eastern Xinjiang.

The Hami missile silo field is in a much earlier stage of development than the Yumen site. Construction began at the start of March 2021 in the southeastern corner of the complex and continues at a rapid pace. Since then, dome shelters have been erected over at least 14 silos and soil cleared in preparation for construction of another 19 silos. The grid-like outline of the entire complex indicates that it may eventually include approximately 110 silos.

The Hami site was first spotted by Matt Korda, Research Associate for the Nuclear Information Project at the Federation of American Scientists, using commercial satellite imagery. Higher resolution images of the site were subsequently provided by Planet.

The silos at Hami are positioned in an almost perfect grid pattern, roughly three kilometers apart, with adjacent support facilities. Construction and organization of the Hami silos are very similar to the 120 silos at the Yumen site, and are also very similar to the approximately one-dozen silos constructed at the Jilantai training area in Inner Mongolia. These shelters are typically removed only after more sensitive construction underneath is completed. Just like the Yumen site, the Hami site spans an area of approximately 800 square kilometers.

Impact on the Chinese nuclear arsenal

The silo construction at Yumen and Hami constitutes the most significant expansion of the Chinese nuclear arsenal ever. China has for decades operated about 20 silos for liquid-fuel DF-5 ICBMs. With 120 silos under construction at Yumen, another 110 silos at Hami, a dozen

silos at Jilantai, and possibly more silos being added in existing DF-5 deployment areas, the People's Liberation Army Rocket Force (PLARF) appears to have approximately 250 silos under construction – more than ten times the number of ICBM silos in operation today.

The number of new Chinese silos under construction exceeds the number of silo-based ICBMs operated by Russia, and constitutes more than half of the size of the entire US ICBM force. The Chinese missile silo program constitutes the most extensive silo construction since the US and Soviet missile silo construction during the Cold War.

The 250 new silos under construction are in addition to the force of approximately 100 road-mobile ICBM launchers that PLARF deploys at more than a dozen bases. It is unclear how China will operate the new silos, whether it will load all of them with missiles or if a portion will be used as empty decoys. If they are all loaded with single-warhead missiles, then the number of warheads on Chinese ICBMs could potentially increase from about 185 warheads today to as many as 415 warheads. If the new silos are loaded with the new MIRVed DF-41 ICBMs, then Chinese ICBMs could potentially carry more than 875 warheads (assuming 3 warheads per missile) when the Yumen and Hami missile silo fields are completed.

It should be emphasized that it is unknown how China will operate the new silos and how many warheads each missile will carry. Regardless, the silo construction represents a significant increase of the Chinese arsenal, which the Federation of American Scientists currently estimates includes approximately 350 nuclear warheads. The Pentagon stated last year that China had "an operational nuclear warhead stockpile in low-200s," and STRATCOM commander Adm. Charles Richard said early this year that "China's nuclear weapons stockpile is expected to double (if not triple or quadruple) over the next decade." The new silos could allow China to accomplish this goal, if it is indeed the goal.

Although significant, even such an expansion would still not give China near-parity with the nuclear stockpiles of Russia and the United States, each of whom operate nuclear warhead stockpiles close to 4,000 warheads.

The Hami missile silo field domes are identical to silo domes seen at the Yumen missile silo field and the Jilantai training area.

Chinese motivations

There are several possible reasons why China is building the new silos. Regardless of how many silos China ultimately intends to fill with ICBMs, this new missile complex represents a logical reaction to a dynamic arms competition in which multiple nuclear-armed players—including Russia, India, and the United States—are improving both their nuclear and conventional forces as well as missile defense capabilities. Although China formally remains committed to its posture of "minimum" nuclear deterrence, it is also responding to the competitive relationship with countries adversaries in order to keep its own force survivable and capable of holding adversarial targets at risk. Thus, while it is unlikely that

China will renounce this policy anytime soon, the "minimum" threshold for deterrence will likely continue to shift as China expands its nuclear arsenal. The decision to build the large number of new silos has probably not been caused by a single issue but rather by a combination of factors, listed below in random order:

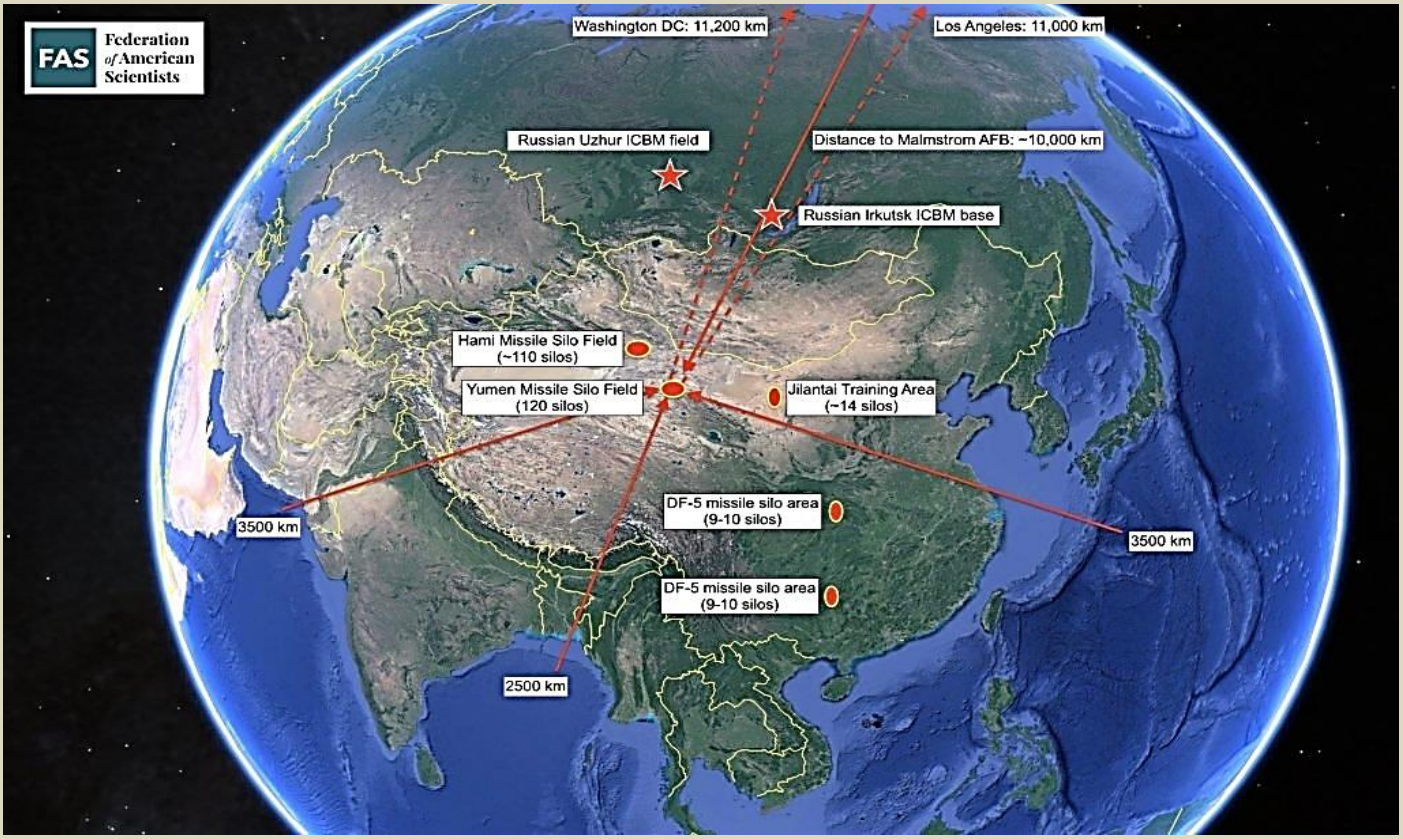
Ensuring survivability of nuclear retaliatory capability: China is concerned that its current ICBM silos are too vulnerable to US (or Russian) attack. By increasing the number of silos, more ICBMs could potentially survive a preemptive strike and be able to launch their missiles in retaliation. China's development of its current road-mobile solid-fuel ICBM force was, according to the US Central Intelligence Agency, fueled by the US Navy's deployment of Trident II D5 missiles in the Pacific. This action-reaction dynamic is most likely a factor in China's current modernization.

Increasing the readiness of the ICBM force: Transitioning from liquid-fuel missiles to solid-fuel missiles in silos will increase the reaction-time of the ICBM force.

Protecting ICBMs against non-nuclear attack: All existing DF-5 silos are within range of US conventional cruise missiles. In contrast, the Yumen and Hami missile silo fields are located deeper inside China than any other Chinese ICBM base (see map below) and out of reach of US conventional missiles.

Overcoming potential effects of US missile defenses: Concerns that missile defenses might undermine China's retaliatory capability have always been prominent. China has already decided to equip its DF-5B ICBM with multiple warheads (MIRV); each missile can carry up to five. The new DF-41 ICBM is also capable of MIRV and the future JL-3 SLBM will also be capable of carrying multiple warheads. By increasing the number of silos-based solid-fuel missiles and the number of warheads they carry, China would seek to ensure that they can continue to penetrate missile defense systems.

Transitioning to solid-fuel silo missiles: China's old liquid-fuel DF-5 ICBMs take too long to fuel before they can launch, making them more vulnerable to attack. Handling liquid fuel is also cumbersome and dangerous. By transitioning to solid-fuel missile silos, survivability, operational procedures, and safety of the ICBM force would be improved.



The Hami and Yumen missile silo fields are located deeper inside China than any other ICBM base and beyond the reach of conventional cruise missiles.

Transitioning to a peacetime missile alert posture: China's missiles are thought to be deployed without nuclear warheads installed under normal circumstances. US and Russian ICBMs are deployed fully ready and capable of launching on short notice. Because military competition with the United States is increasing, China can no longer be certain it would

have time to arm the missiles that will need to be on alert to improve the credibility of China deterrent. The Pentagon in 2020 asserted that the silos at Jilantai "provide further evidence China is moving to a LOW posture."
Balancing the ICBM force: Eighty percent of China's roughly 110 ICBMs are mobile and increasing in numbers. The US military projects that number will reach 150 with about 200 warheads by 2025. Adding more than 200 silos would better balance the Chinese ICBM force between mobile and fixed launchers.
Increasing China's nuclear strike capability: China's "minimum deterrence" posture has historically kept nuclear launchers at a relatively low level. But the Chinese leadership might have decided that it needs more missiles with more warheads to hold more adversarial facilities at risk. Adding nearly 250 new silos appears to move China out of the "minimum deterrence" category.
National prestige: China is getting richer and more powerful. Big powers have more missiles, so China needs to have more missiles too, in order to underpin its status as a great power.

What to do about it?
China's construction of nearly 250 new silos has serious implications for international relations and China's role in the world. The Chinese government has for decades insisted it has a minimum deterrent and that it is not part of any nuclear arms race. Although it remains unclear how many silos will actually be filled with missiles, the massive silo construction and China's other nuclear modernization programs are on a scale that appears to contradict these polices: the build-up is anything but "minimum" and appears to be part of a race for more nuclear arms to better compete with China's adversaries. The silo construction will likely further deepen military tension, fuel fear of China's intensions, embolden arguments that arms control and constraints are naïve, and that US and Russian nuclear arsenals cannot be reduced further but instead must be adjusted to take into account the Chinese nuclear build-up.
The disclosure of the second Chinese silo missile field comes only days before US and Russian negotiators meet to discuss strategic stability and potential arms control measures. Responding to the Chinese build-up with more nuclear weapons would be unlikely to produce positive results and could cause China build up even more. Moreover, even when the new silos become operational, the Chinese nuclear arsenal will still to be significantly smaller than those of Russia and the United States.
The clearest path to reining in China's nuclear arsenal is through arms control, but this is challenging. The United States has been trying to engage China on nuclear issues since the late-1990s, but so far with minimal success. Rather than discuss specific limitations on weapon systems, these efforts have been limited to increasing transparency about force structure plans and strategy, and well as discussing nuclear doctrine and intentions.
The Trump administration correctly sought to broaden nuclear arms control to include China, but fumbled the effort by turning it into a public-relations pressure stunt and insisting that China should be part of a New START treaty extension. Beijing not surprisingly rejected the effort, and Chinese officials have plainly stated that "it is unrealistic to expect China to join [the United States and Russia] in a negotiation aimed at nuclear arms reduction," particularly while China's arsenal remains a fraction of the size.
Bringing China and other nuclear-armed states into a sustained arms control dialogue will require a good-faith effort that will require the United States to clearly articulate what it is willing to trade in return for limits on Chinese forces. In this regard, it is worth noting that the absence of limits on US missile defenses is of particular and longstanding concern to both China and Russia. When the Bush administration decided to withdraw from the Anti-Ballistic Missile Treaty in 2002, officials from both countries explicitly stated that the treaty's demise would be highly destabilizing, and implied that they would take steps to offset this perceived US advantage. Nearly 20 years later, the knock-on effects of this decision are clear. Putting US missile defenses on the negotiating table could help clear the path towards enacting a new arms control agreement that ultimately keeps both Chinese and Russian nuclear arsenals in check.
But the Chinese nuclear modernization is driven by more than just missile defenses. This includes the nuclear modernization programs of the United States, India, and Russia, the significant enhancements of the conventional forces of those countries and their allies, as well as China's own ambitions about world power status.
Later this year (or early next year) the parties to the nuclear Non-Proliferation Treaty (NPT) will meet to review the progress of the treaty. Although the treaty does not explicitly prohibit a country from modernizing or even increasing its nuclear arsenal, reduction and eventually elimination of nuclear weapons are key pillars of the treaty's goal as reaffirmed by numerous previous NPT conferences. It is difficult to see how adding nearly 250 nuclear missile silos is consistent with China's obligation to "pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament…"

Matt Korda *is a Research Associate for the Nuclear Information Project at the Federation of American Scientists, where he co-authors the Nuclear Notebook with Hans Kristensen. Matt is also an Associate Researcher with the Nuclear Disarmament, Arms Control and Non-proliferation Programme at the Stockholm International Peace Research Institute (SIPRI). Previously, he worked for the Arms Control, Disarmament, and WMD Non-*

Proliferation Centre at NATO HQ in Brussels. Matt is also the co-director of Foreign Policy Generation—a group of young people working to develop a progressive foreign policy for the next generation. He received his MA in International Peace & 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. He also completed an internship with the Verification, Training and Information Centre (VERTIC) in London, where he focused on nuclear security and safeguards.

***Hans M. Kristensen** is director of the Nuclear Information Project at the Federation of American Scientists where he provides the public with analysis and background information about the status of nuclear forces and the role of nuclear weapons. He specializes in using the Freedom of Information Act (FOIA) in his research and is a frequent consultant to and is widely referenced in the news media on the role and status of nuclear weapons. Kristensen is co-author of the Nuclear Notebook column in the Bulletin of the Atomic Scientists and the World Nuclear Forces overview in the SIPRI Yearbook. The Nuclear Notebook is, according to the publisher, "widely regarded as the most accurate source of information on nuclear weapons and weapons facilities available to the public."*

Why did the atomic bomb dropped on Hiroshima leave shadows of people etched on sidewalks?

By Stacy Kish

Source: https://www.livescience.com/nuclear-bomb-wwii-shadows.html

A human shadow on the steps of a bank in Hiroshima, following the explosion of the nuclear bomb in August 1945. (Image credit: Universal History Archive/Universal Images Group via Getty Images)

Black shadows of humans and objects, like bicycles, were found scattered across the sidewalks and buildings of Hiroshima and Nagasaki, two of the largest cities in Japan, in the wake of the atomic blast detonated over each city on Aug. 6 and 9, 1945, respectively.

It's hard to fathom that these shadows likely encapsulated each person's last moments. But how did these shadows come to be?

According to Dr. Michael Hartshorne, emeritus trustee of the National Museum of Nuclear Science and History in Albuquerque, New Mexico, and professor emeritus of radiology at the University of New Mexico School of Medicine, when each bomb exploded, the intense light and heat spread out from the point of implosion. Objects and people in its path shielded objects behind them by absorbing the light and energy. The surrounding light bleached the concrete or stone around the "shadow."

In other words, those eerie shadows are actually how the sidewalk or building looked, more or less, before the nuclear blast. It's just that the rest of the surfaces were bleached, making the regularly colored area look like a dark shadow.

Powered by fission

The intense energy released during an atomic explosion is the result of nuclear fission. According to the Atomic Heritage Foundation, a nonprofit based in Washington, D.C., fission occurs when a neutron strikes the nucleus of a heavy atom, like the isotopes uranium 235 or plutonium 239. (An isotope is an element with varying numbers of neutrons in its nucleus.) During the collision, the element's nucleus is broken apart, releasing a large amount of energy. The initial collision sets off a chain reaction that continues until all of the parent material is exhausted.

"The chain reaction occurs in a pattern of exponential growth that last[s] a millisecond or so," said Alex Wellerstein, an assistant professor of science and technology studies at the Stevens Institute of Technology in New Jersey. "This reaction splits about a trillion, trillion atoms in that period of time before the reaction stop[s]."

The atomic weapons used in the 1945 attacks were fueled by uranium 235 and plutonium 239 and released a massive amount of heat and very shortwave, gamma radiation.

Energy flows as photon waves of varying lengths, including in long waves, like radio waves, and in shortwaves, like X-rays and gamma-rays. Between long waves and shortwaves lie visible wavelengths that contain energy that our eyes perceive as colors. However, unlike energy with longer waves, gamma radiation is destructive to the human body because it can pass through clothing and skin, causing ionizations, or the loss of electrons, that damage tissue and DNA, according to Columbia University.

The gamma radiation released by the atomic bombs also traveled as thermal energy that could reach 10,000 degrees Fahrenheit (5,538 degrees Celsius), Real Clear Science reported. When the energy hit an object, like a bicycle or a person, the energy was absorbed, shielding objects in the path and creating a bleaching effect outside the shadow.

In fact, there were likely many shadows initially, but "most of the shadows would have been destroyed by subsequent blast waves and heat," Hartshorne told Live Science.

A person's shadow on bank steps in Hiroshima, Japan, which was created during the 1945 nuclear blast. (Image credit: Universal History Archive/Universal Images Group via Getty Images)

Fat Man and Little Boy

On Aug. 6, 1945, an atomic bomb nicknamed Little Boy detonated 1,900 feet (580 meters) above Hiroshima, Japan's seventh-largest city. According to the World Nuclear Association, the explosion was equivalent to 16,000 tons (14,500 metric tons) of TNT exploding, which sent a pulse of thermal energy rippling across the city. The pulse flattened 5 square miles (13 square kilometers) of the city. Almost one-quarter of the population of Hiroshima died immediately. Another quarter died of the effects of radiation poisoning and cancer in the months that followed.

Three days after that blast, the United States detonated a second atomic bomb, nicknamed Fat Man, over Nagasaki. The plutonium 239 bomb released a 21,000-ton (19,000 metric tons) explosion that produced similar patterns of destruction and death across the city.

Emperor Hirohito announced Japan's surrender on Aug. 15 and signed the formal declaration on Sept. 2, 1945, ending the hostilities in the Pacific theater and bringing World War II to a close.

The United States targeted both Japanese cities during the war for their military significance. As time has passed, the long-term consequences of the radiation released by each bomb has raised significant questions about their use. Many of the shadows etched into the stone were lost to weathering and erosion by wind and water. Several nuclear shadows have been removed and preserved in the Hiroshima Peace Memorial Museum for future generations to ponder these events.

"I think it is very important to keep in mind the consequences of the use of nuclear weapons," Wellerstein told Live Science. "It is very easy to regard these weapons as tools of statecraft and not weapons of mass destruction. The nuclear shadows serve as a potent reminder of the human cost of [atomic weapon] use."

*As a scientist, **Stacy Kish** has focused her research on Earth science, specifically oceanography and climate change. As a science writer, she explores all aspects of science from mites living books to noctilucent clouds, stretching across the mesopause.*

The U.S. Says It Can Answer Cyberattacks with Nuclear Weapons. That's Lunacy!

Source: http://www.homelandsecuritynewswire.com/dr20210802-nukes-vs-cyberattacks-coexisting-with-dictators-missing-the-point-about-cuba

Aug 02 – Recent months saw ever-more-brazen cyberattacks by Russian ransom gangs on American companies: Kaseya (which serves about 1,500 companies); Colonial Pipeline (which supplies nearly half the diesel, gasoline and other fuels used on the East Coast); JBS (the world's largest beef and pork supplier), and many more.

Scott D. Sagan and Allen S. Weiner write in the *Washington Post* that

These incidents were bad enough. But imagine a much worse cyberattack, one that not only disabled pipelines but turned off the power at hundreds of U.S. hospitals, wreaked havoc on air-traffic-control systems and shut down the electrical grid in major cities in the dead of winter. The grisly cost might be counted not just in lost dollars but in the deaths of many thousands of people.

Under current U.S. nuclear doctrine, developed during the Trump administration, the president would be given the military option to launch nuclear weapons at Russia, China or North Korea if that country was determined to be behind such an attack.

This is because in 2018, the Trump administration expanded the role of nuclear weapons by declaring, for the first time, that the United States would consider nuclear retaliation in the case of "significant non-nuclear strategic attacks," including "attacks on the U.S., allied, or partner civilian population or infrastructure." The same principle could also be used to justify a nuclear response to a devastating biological weapons strike.

Sagan and Weiner write:

But our analysis suggests that using nuclear weapons in response to biological or cyberattacks would be illegal under international law in virtually all circumstances. Threatening an illegal nuclear response weakens deterrence because the threat lacks inherent credibility. Perversely, this policy could also wind up committing a president to a nuclear attack if deterrence fails. While the American public would indeed be likely to want vengeance after a destructive enemy assault, the law of armed conflict requires that some military options be taken off the table. Nuclear retaliation for "significant non-nuclear strategic attacks" is one of them.

Iran "10 Weeks Away" from Weapon-Grade Uranium

Source: http://www.homelandsecuritynewswire.com/dr20210804-iran-10-weeks-away-from-weapongrade-uranium

Aug 04 – Last Friday, in the early hours of the morning, Iranian "suicide" drones exploded on the deck of the *Mercer Street* oil tanker in the Gulf as it was making its way to the UAE. Two men were killed – the Romanian captain of the ship and a British security officer. Earlier Wednesday, Israel's Defense Minister Benny Gantz and Foreign Minister Yair Lapid held a meeting in Jerusalem with the ambassadors to Israel of the five permanent members of the UN Security Council, in which they shared with the ambassadors intelligence information showing Iran's responsibility for the attack – and even named the two high-level commanders in Iran's Revolutionary Guard who ordered the attack.

Gantz and Lapind used the occasion to talk about more than last Friday's Iranian attack on the oil tanker. They highlighted the growing pace, reach, and breadth of Iran's military activity across the region, and especially Iran's reliance on ever-more-sophisticated, home-made drones.

Iran has a fleet of hundreds of different unmanned aerial vehicles, most based reversed-engineered Western technology.

The second topic discussed by Gantz and Lapid was Iran's steady advances toward becoming a nuclear weapon threshold state. Iran's march toward the bomb was retarded by the 2015 nuclear deal, but since the Trump administration has withdrawn from the deal in 2018, Iran has felt free to violate the deal's restrictions.

Gantz told the ambassadors that Iran is now only ten weeks away – if it decided to move forward – from enriching sufficient quantities of uranium to weapon-grade level, so that it would have available the fissile material needed for a nuclear weapon.
Gantz's reference to how close Iran is to be in possession of weapon-grade material echo the analysis by a respectable Israel think tank, Tel Aviv University's Institute for National Security Studies (INSS) (see "Iran's Strategic Challenge to Israel," *HSNW*, 4 August 2021)

Counting the dead at Hiroshima and Nagasaki

Source: https://thebulletin.org/2020/08/counting-the-dead-at-hiroshima-and-nagasaki/

Aug 04 – How many people died as a result of the atomic bombings of Hiroshima and Nagasaki? There is one thing that everyone who has tackled this question has agreed upon: The answer is probably fundamentally unknowable. The indiscriminate damage inflicted upon the cities, coupled with the existing disruptions of the wartime Japanese home front, means that any precise reckoning is never going to be achieved.
But beginning in 1945, people have tried to estimate the number of the dead and injured. The casualties from the first atomic

bombings are not of mere historical interest. They are part of how we understand the effects of nuclear weapons today — for Hiroshima and Nagasaki, thankfully, remain the only instances of these weapons being used in warfare, and thus provide an invaluable "data set" upon which to base other understandings and simulations. The estimated casualties also play a nuanced role in the various narratives and arguments about the end of World War II.

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

A First: 3D Printed Nuclear Reactor Components Now Installed at a Nuclear Plant

Source: http://www.homelandsecuritynewswire.com/dr20210810-a-first-3d-printed-nuclear-reactor-components-now-installed-at-a-nuclear-plant

Aug 10 – Four first-of-a-kind 3D-printed fuel assembly brackets, produced at the Department of Energy's Manufacturing Demonstration Facility at Oak Ridge National Laboratory, have been installed and are now under routine operating conditions at the Tennessee Valley Authority's Browns Ferry Nuclear Plant Unit 2 in Athens, Alabama.
The components were developed in collaboration with TVA, Framatome and the DOE Office of Nuclear Energy–funded Transformational Challenge Reactor, or TCR, program based at ORNL.
"Deploying 3D-printed components in a reactor application is a great milestone," said ORNL's Ben Betzler, TCR program director. "It shows that it is possible to deliver qualified components in a highly regulated environment. This program bridges basic and applied science and technology to deliver tangible solutions that show how advanced manufacturing can transform reactor technology and components."
"ORNL offers everything under one roof: state-of-the-art printing capabilities, world-class expertise in machining, next-generation digital manufacturing technologies, plus comprehensive characterization and testing equipment," said Ryan Dehoff, ORNL section head for Secure and Digital Manufacturing.

The channel fasteners' straightforward, though non-symmetric, geometry was a good match for a first-ever additive manufacturing application for use in a nuclear reactor.

The current focus of the TCR program is to further mature and demonstrate industry-ready technology informed by advanced manufacturing, artificial intelligence, integrated sensing and deployment of a digital platform for informed certification of components.

ORNL's broad nuclear research and development activities are directed toward providing science and technology breakthroughs to extend the viability and operations of the nation's nuclear power plant fleet, while also accelerating the deployment of new, advanced nuclear power technologies.

"Collaborating with TVA and ORNL allows us to deploy innovative technologies and explore emerging 3D printing markets that will benefit the nuclear energy industry," said John Strumpell, manager of North America Fuel R&D at Framatome. "This project provides the foundation for designing and manufacturing a variety of 3D-printed parts that will contribute to creating a clean energy future."

"TVA is actively engaged in developing new nuclear technology for tomorrow," said Dan Stout, TVA's director of Nuclear Technology Innovation. "Partnering with ORNL and Framatome in this innovative manufacturing approach could pave the path for use across the existing nuclear fleet and also in advanced reactors and small modular reactors."

Operations at Browns Ferry resumed April 22, 2021, after a planned outage to replace a variety of components for continued safe, reliable operation and delivery of carbon-free electricity. The brackets will remain in the reactor for six years with regular inspections during that period.

Treaty On The Prohibition Of Nuclear Weapons – Analysis

By Rajiv Nayan

Source: https://www.eurasiareview.com/12082021-treaty-on-the-prohibition-of-nuclear-weapons-analysis/

Aug 12 – The world once again bowed its head in shame and paid tribute to the victims on the Hiroshima and Nagasaki days on 6 August and 9 August, respectively. The comity of nations wrestled with the guilty conscience on the 76th anniversary of both days. Quite ritually, the future of nuclear weapons or nuclear disarmament came up for discussions during many of the prayer meets.

A section of the international community strongly believes that the Treaty on the Prohibition of Nuclear Weapons (TPNW), popularly known as the Ban Treaty, could help in realising the idea of nuclear disarmament, and has therefore urged the international community, especially the nuclear weapon states to sign the treaty. In fact, the Mayor of Hiroshima appealed to the Japanese government to sign the treaty a few days before the Hiroshima Day. Japan is one of the important countries, which has not signed the treaty as yet. The treaty, at present, has 86 signatories.

Is nuclear disarmament going to become a reality soon? The idea of nuclear disarmament has somewhat gathered momentum after the Ban Treaty came into force, i.e., became operational after 90 days of ratification by the 50th member on 22 January 2021. The treaty now is generating curiosity as well as hope.

The oft-repeated question is: Is this a treaty for nuclear disarmament? Is it similar to The Biological and Toxin Weapons Convention (BTWC) or the Chemical Weapons Convention (CWC)? The BTWC and the CWC are the disarmament treaties for the other two categories of Weapons of Mass Destruction (WMD). A large number of nuclear disarmament enthusiasts belonging to civil society along with some non-nuclear weapon countries want the world to believe that TPNW, or the Ban Treaty, is nuclear equivalent to the BTWC or the CWC.

In fact, like the other two WMD treaties, the Ban Treaty, too, has comprehensive prohibition measures. The treaty bans development, testing, production, manufacturing, acquisition, transfer, use, threat to use, and so on. However, the most interesting provision of the treaty is the ban on "stationing, installation or deployment of any nuclear weapons or other nuclear explosive devices" in the territory or at any place under the jurisdiction or control of a member country.[1]

The treaty has indeed regenerated hope and optimism for nuclear disarmament in the international community. Although President Barack Obama did not deliver the promised nuclear disarmament for which he had received the Nobel Peace Prize in advance, yet his promise at least did not weaken the nuclear taboo or norm against the use of nuclear weapons existing since the first and last use in 1945. The Ban Treaty is credited to have assembled support for the nuclear disarmament narrative in the Donald Trump era. Nuclear disarmament did not enthuse President Trump much. Even other dominant nuclear weapon powers did not go beyond some inconsequential resolutions in the United Nations (UN) for nuclear disarmament. The Ban Treaty consolidated the momentum of humanitarian initiatives. The treaty, in its preamble, has maintained the essence of the humanitarian consequences of nuclear weapons. In fact, the treaty was adopted and opened for signature in 2017 in an adverse situation, for nuclear disarmament.

However, the treaty has not succeeded in adding any additional universal stigma to nuclear weapons. In fact, it lacks the support base needed for replacing the Cold War vintage "Mutual Assured Destruction" with "Mutual Assured Abstinence". The nuclear weapon countries' faith in the deterrence logic remains intact. Nuclear deterrence, even though the most sanitised narrative, requires a continuance of nuclear weapons.

None of the nuclear weapon countries participated in the negotiation process for the treaty. All had different arguments, logic and rationale for abstaining from negotiations for the treaty. Some of the reasons could be valid but in general, the reliance on the salience of nuclear weapons has put a spanner in the participation for the treaty. Moreover, carving a new treaty by sidestepping the crisis-ridden Treaty on the Non-Proliferation of Nuclear Weapons (NPT), which has a larger base, including all old nuclear weapon countries, has not gone down well with many countries and writers. A major section believes that the non-nuclear member countries should have forced member countries possessing nuclear weapons to implement Article 6 of the NPT.

Interestingly, not only nuclear weapon countries but also as discussed, the nuclear umbrella holding countries like Japan have stayed away from negotiations. Of the North Atlantic Treaty Organization (NATO) members, only the Netherlands participated in negotiations but cast the only negative vote against the treaty. All the NATO countries, including the Netherlands, are still desisting from the treaty.

The treaty exhibited an intriguing response pattern of some peace activist nations. Sweden participated in negotiations but has not signed the treaty as yet. Norway, which has been at the forefront of funding various peace, humanitarian and disarmament initiatives, too, skirted negotiations and of course, the signing of the treaty. A former nuclear umbrella holding country, New Zealand, has signed, ratified and submitted the declaration that it does not possess or station any nuclear weapon on its territory.

Over the years, the institutions for disarmament have evolved. The Special Sessions of the UN General Assembly devoted to Disarmament have been of immense help. The United Nations Disarmament Commission and the Conference on Disarmament (CD) have played an important role in shaping the disarmament initiatives. Admittedly, these institutions are turning non-functional. For instance, the CD has not succeeded in delivering a treaty in years because of the principle of consensus. However, escaping the negotiating body is not a solution. The challenge lies in building a consensus over the provisions for a disarmament treaty and galvanising public opinion in its favour.

Quite significantly, even the provisions of the Ban Treaty are blocking the path of many countries joining it. The treaty merely mentions the need for bearing the cost for verification but any disarmament treaty needs an elaborate verification and inspection machinery and infrastructure to build confidence among the members and the global community. The verification deficit indicates the ad hoc nature of the treaty.

At the time of negotiations, many accused that some dominant forces pushed a readymade text and that the entire process of negotiations was merely a façade. The treaty does not have a roadmap for nuclear weapons disarmament/dismantlement. The next meeting may set a deadline but the absence of nuclear weapon countries will make it futile.

Several countries have complained that through the Ban Treaty the longstanding principle of *sovereign consent prevalent in international law is damaged. Proponents of the Ban Treaty are advised to read the Vienna Convention on the Law of Treaties in letter and spirit.*

India, too, has stayed away from the treaty. It has neither participated in negotiations nor signed the treaty. India wants a treaty to be negotiated in the CD for universal, non-discriminatory and verifiable nuclear disarmament. The Indian government observes that the Ban Treaty "does not constitute or contribute to the development of customary international law; nor does it set any new standards or norms."[2]

In the absence of other nuclear weapon countries, India joining the treaty may amount to opting for unilateral nuclear disarmament. This cannot be recommended to a country, which is surrounded by two hostile nuclear neighbours. However, the Ban Treaty needs to be seen as a transitional initiative of a creative new disarmament politics. The oft-repeated idea—a feasible, comprehensive, verifiable and enforceable nuclear disarmament regime—could

become a reality only by a genuine commitment of nuclear weapon countries to a Nuclear Weapons Convention negotiated in the CD.

Rajiv Nayan *is Senior Research Associate at the Manohar Parrikar Institute for Defence Studies and Analyses*[1]*, New Delhi.*

Radioactive snakes may monitor Fukushima fallout

By Susan D'Agostino

Source: https://thebulletin.org/2021/08/radioactive-snakes-may-monitor-fukushima-fallout/

A Japanese rat snake is fit with a GPS transmitter that will allow researchers to track its movements over the next several weeks. Photo credit: Hannah Gerke. Used with permission.

Aug 17 – When a massive earthquake followed by a tsunami hit Japan a decade ago, the Fukushima Daiichi Nuclear Power Plant experienced a catastrophic meltdown. Humans fled a wide area around the plant that today is known as the Fukushima Exclusion Zone, while animals and plants remained. Now, scientists have enlisted the help of snakes in the zone to make sense of the disaster's impact on the environment. Their findings, reported in an *Ichthyology and Herpetology* paper, indicate that Fukushima's native rat snakes, like canaries in a coal mine, may act as living monitors of radiation levels in the region.

"Because snakes don't move that much, and they spend their time in one particular local area, the level of radiation and contaminants in the environment is reflected by the level of contaminants in the snake itself," Hannah Gerke, a lead author on the study, said.

[1] The Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA), is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues. The Manohar Parrikar Institute for Defence Studies and Analyses (MP-IDSA) was formerly named The Institute for Defence Studies and Analyses (IDSA).

Animals, plants, or other life forms whose health provides insight into environmental health are known as bioindicators. For example, frogs, with their permeable skin and limited abilities to detoxify, are bioindicators of environmental pollution. And lichens, which have no roots and rely on nutrients from the atmosphere, are bioindicators of atmospheric pollution. Gerke's recent study suggests that rat snakes may be useful bioindicators of radioactive contamination in nuclear disaster zones. But that does not necessarily mean that Fukushima's environment or its snakes are languishing.

"Everybody expects Fukushima to be a barren wasteland full of mutated animals. In real life, it is quite beautiful," Gerke said. "I was there in summer when everything was lush and green. There is wildlife everywhere—just a surprising lack of people."

The scientists' findings reinforced their 2020 study that found a high correlation between levels of radiocesium—a radioactive isotope of cesium—in the snakes and levels of radiation in their environment.

Why snakes and not, for example, birds?

Not every animal in Fukushima's exclusion zone is suited to the "work" of a bioindicator. That's because the radiocesium that spewed from the nuclear disaster did not blanket the region evenly. For example, birds that travel far are exposed to contaminants all over the zone, which leaves them unable to provide insight into degrees of contamination in the zone's smaller "neighborhoods." But rat snakes have relatively small home ranges; they travel an average of 65 meters (approximately 213 feet) each day, according to the study. And they are susceptible to accumulating radionuclides—unstable atoms with excess nuclear energy—from disasters such as the one that took place in Fukushima. A rat snake that makes its home in a small but heavily contaminated area will tell a different story than a rat snake lives in a less contaminated locale.

In the decade since the nuclear disaster, most of the contaminants have settled in the soil. This means that animals such as birds that spend much of their time in trees have limited insight to offer about contaminants on the ground. But snakes, whose long bodies slither in and burrow under the soil, can help determine degrees of contamination.

Also, snakes live long, which means that the data they gather provides information about environmental contaminants over time.

How did scientists enlist the help of the snakes?

The rugged Abukuma Highlands are situated approximately 15 miles northwest of the Fukushima Daiichi Nuclear Power Plant. This verdant terrain of hills and valleys is peppered with abandoned villages and farms—and, for a few recent months, scientists in search of snakes.

"Driving around these small curvy mountain roads, we watched for snakes crossing the road," Gerke said, noting that snakes are active when the weather warms up. "Whenever we found one, we jumped out, caught it, and took it back to the lab at Fukushima University."

As long as a snake was of sufficient size, Gerke and her team wrapped a piece of tape around its body. Next, they superglued a tiny GPS tracking device and a tiny dosimeter—a radiation-measuring tool—to the tape, which ensured that they could remove the devices upon the study's completion. Then, they returned the snake to its natural habitat. The team outfitted nine snakes this way, after which they collected the data remotely.

The scientists identified more than 1,700 locations in the region that the snakes frequented. Rat snakes in Fukushima, it turns out, avoid evergreen broadleaf forests but spend time close to streams, roads, and grassland. They also frequent trees and buildings.

What did the snakes reveal?

Some of the snakes' radiation exposure in the Fukushima Exclusion Zone hails from contaminated prey they eat, but most—80 percent—comes from contact with contaminated soil, trees, and plants.

"Understanding how contaminants move throughout an ecosystem and how they move in different animals throughout the food web gives us a better picture of the impacts [of the nuclear disaster] to the ecosystem," Gerke said.

An individual snake's exposure is related not only to the small region in which it spends time but to its behavior. For example, snakes that spent time in abandoned buildings had lower doses relative to those that did not, suggesting that buildings may act as contamination shields. Also, snakes that spent more time in trees had lower doses relative to snakes that spent more time on the ground. Gerke hypothesizes that species that spend their time primarily on the ground are potentially more vulnerable to **negative health effects of radiation, should negative health effects for snakes exist.**

"At a population level, we don't think that they're impacted that much [by radiation]. But there could be stuff going on at a cellular level that we don't know about," Gerke said. She noted that scientists understand levels of radiation that harm animals like mammals, birds, and frogs, but not snakes.

The current study was the first to describe home range size, movements, and habitat selection of Japanese rat snakes. The results suggest that these animals could be effective bioindicators of local environmental contamination in nuclear disaster zones. But many questions remain. For example, will scientists be able to develop models clarifying the link

between habitat use, radiation exposure, and radiation accumulation? If so, they might provide insight into the health effects of chronic radiation exposure in animals or humans.

Why take time to understand snakes, anyway?

"I'm scared of snakes," Gerke often hears upon revealing that she is a herpetologist. Others offer unsolicited testimony suggesting that humans' negative attitudes about snakes hold potential to harm the animals: "I found a snake in my backyard, and I killed it." Gerke grew up in Florida with a pet rat snake; she confides that she cannot relate to such sentiments.

"Teaching people to hate snakes is a disaster for ecology," Melissa Amarello, cofounder of Advocates for Snake Preservation, wrote in an article. According to psychologists, fear of snakes is learned, not innate. Of the 3,000 species of snakes on the planet, only about 200—seven percent—are able to significantly harm or kill a human. Meanwhile, snakes prey on disease-carrying rodents. And they play an integral role in nearly every ecosystem's food chain.

In addition to human fear of and hatred for snakes that may harm them, these animals face additional challenges that threaten their populations worldwide, including legal and illegal collecting, habitat loss, disease, and climate change.

Appreciation for snakes should not rely on their service to humans. But by demonstrating that snakes may be effective bioindicators, Gerke and her team have offered a new on-ramp for snake appreciation. That is, not only are snakes an important component of biodiversity, but they broadcast important information about the natural environments in which they live. They might even be enlisted to help in a future nuclear disaster. Humans might consider snakes allies.

Still, Gerke is quick to add, "There's a lot more research that needs to be done."

Susan D'Agostino *is an associate editor at the* Bulletin of the Atomic Scientists. *Her writing has been published in* The Atlantic, Quanta Magazine, Scientific American, The Washington Post, BBC Science Focus, Nature, Financial Times, Undark Magazine, Discover, Slate, Times Higher Education, *and* The Chronicle of Higher Education, *among others. Susan is the author and illustrator of* How To Free Your Inner Mathematician: Notes on Mathematics and Life *(Oxford University Press, 2020). She served as editor-in-chief of* A Celebration of the EDGE Program's Impact on the Mathematics Community and Beyond *(Springer, 2019), a book of essays and articles written by women mathematicians. She is a member of the editorial board of the Mathematical Association of America's* Math Horizons *magazine. Susan earned a PhD in mathematics at Dartmouth College and is currently pursuing an MA in science writing at Johns Hopkins University. She has received science writing fellowships from the National Association of Science Writers, the Council for the Advancement of Science Writing, and the Heidelberg Laureate Forum Foundation.*

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

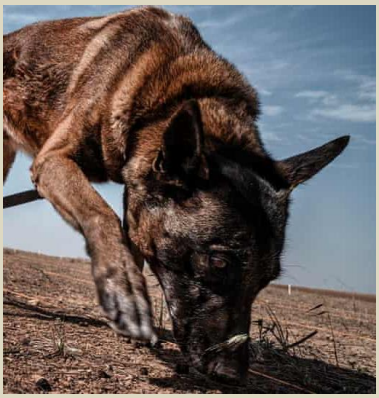
HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

EXPLOSIVE NEWS

Canine 'super-detectors': the dogs working to free Iraq from Isis mines

Source: https://www.theguardian.com/global-development/2021/jul/26/how-super-detector-dogs-are-helping-free-iraq-from-the-terror-of-isis-mines



July 27 – On the wide, flat plain of the Sinjar district of northern Iraq, Naif Khalaf Qassim lets his dog, an eight-year-old Belgian shepherd, range across the dry earth on a 30-metre leash until Branco stops and sits, tail wagging, looking towards his handler with enthusiasm.

Branco has detected something underground and, when the mine-clearing team is brought in to investigate, they find an improvised explosive device (IED), known locally as a VS500.

It is about 30cm (1ft) wide, with a plastic casing and a central pressure pad. The VS500 is not the name Islamic State give the device; no one knows that. All that is certain is that it is one of thousands produced when the terror group held sway over this part of Iraq and commandeered plastics factories in their Mosul base, forcing the workers to make souped-up versions of the Italian-made VS50 landmine.

A VS50 could fit on the palm of your hand, and contains about 100g of explosives. The deminers call this type of mine the VS500 because it is 10 times the size and packed with up to 15kg (33lb) of explosives. The pressure pad is sensitive enough for a child to activate, even through 30cm of packed earth. The explosion can take out an armoured vehicle.

Branco is trained to sniff ahead in a controlled manner and stop if he gets a scent – so he doesn't tread on the mine. Belgian and German shepherds are used because they are most adept at distinguishing scents.

"I knew Branco would find the IED," says Naif proudly. "I believe in him and his abilities; I know him and what he can do. He is more of a friend to me than a dog."

Branco, with his handler Naif Khalaf Qassim, can do rapid searches either side of a known mined corridor

Four years ago, Iraqi forces managed to take the last stronghold that Isis had left in the country, the city and surroundings of Tal Afar. The Iraqi flag was raised on the historic Ottoman citadel at the heart of the city, and the militia was pushed into Syria.
The war might have appeared over by late August 2017, but retreating Isis forces seeded the towns, villages and countryside in that area of Sinjar with IEDs, and the job of clearing them is still far from done.
But it is moving at a much faster pace, thanks to the introduction of the small sniffer dog team, including Branco, and his handler, Naif, 35.

Mine-detection dogs are not new – the British-based Mines Advisory Group (MAG) has been working across northern Iraq for three decades. In the year from June 2020 to June 2021 the Iraqi dog team has found and destroyed 3,540 landmines and explosive remnants of war, including 670 improvised mines and 148 other improvised devices.
Now MAG has embarked on a specific programme to better detect the explosives used by Isis and other non-state groups.

Isis made workers at plastics factories in Mosul produce the so-called VS500, based on an Italian landmine

Dogs are usually trained to sniff out explosives, mainly TNT, but the IED dogs take this a step further. Trained in Bosnia-Herzegovina, their noses are attuned to rubber, metal and batteries as well.
This is key where explosives are often improvised from domestic items such as pots and kettles, with detonators and batteries. Training dogs to focus on a wider range of scents allows for more opportunities to detect anomalies below the surface.
The new four-strong dog team (with two more on their way from Bosnia-Herzegovina) is currently working on 8sq km of land near Tal Afar that was used as a barrier minefield by retreating Isis fighters in 2017. While people armed with mine detectors painstakingly scour a known mined corridor, the dogs range across the areas either side, deemed low or medium risk, to seek out any randomly planted devices.

Vian Khaider Khalaf, with X-Lang, wants to clear landmines so families can return and farm the land

The programme for the "super-detector" dogs was curtailed until now by Covid and by difficulties negotiating with the administration in Sinjar – divided between the Iraqi federal government and the Kurdistan regional government.
The dogs start work at 5am, so that they can finish before the sun is too high – last week temperatures there hit 49C (120F). The handlers are from the Yazidi community.
Vian Khaider Khalaf, 26, was a student before starting work with the dogs in 2017. She works to support her family in Sinuni, but like everyone on the team, her driving motivation is to clear the mines so that families can return to their farms.

Vian Khaider Khalaf says some of her family, as Yazidis, are still in camps for displaced people

"We always had dogs at home, as my family are farmers and shepherds," says Khalaf. "I fled with my family in 2014 when *Daesh* [Isis] came. I still have family in an IDP [internally displaced people] camp in Kurdistan. My family are afraid for me, of course. But they are proud of me and see me working hard and bravely, and that makes me want to take on more challenges."

Khalaf has worked with her dog, X-Lang, since she started with MAG. He was originally a mine-detector dog, but was selected for the IED upgrade training. She says: "The relationship between me and my dog is not really that of a human and an animal. He is my dear friend. If I could take him home with me at the weekend, or live on the base with him, I would."

After a morning's work the dogs can go into a custom-made pool that allows them to exercise in the heat

The relationship between me and my dog is not really that of a human and an animal. He is my dear friend
Vian Khaider Khalaf, handler

After their shifts out in the fields, handlers and dogs spend the rest of the day together, often around the pool on the base.

The team supervisor is Salam Rasho, a former noncommissioned officer with the Kurdistan military, the peshmerga. He is also a Yazidi and has seen the devastation of his community. "Our aim is to return the people to their land, to get people farming the land again," he says.

It's impossible to estimate how much unexploded ordnance there is in Iraq – one of the most mined countries in the world, according to some estimates. There is little information about where mines were laid over the past 40 years, from the Iran-Iraq war in the 1980s, to Saddam Hussein's assaults on his own people, the Gulf War, and finally Isis. It is thought that in federal Iraq alone there are some 3,000 sq km of mined land yet to be cleared, with 8.5 million people living in close proximity.

The real benefit of the dogs, says Salam, is that they can cover a huge area much quicker than humans – about 1,500 sq metres a day. The success of the Iraq deployment means that MAG is stepping up its IED dog training and even going to the next level – finessing the programme so that dogs can also be used to help clear booby-trapped homes.

Clearing Iraq of unexploded mines is a task that will take many more years, but at least now the land is being freed from the lingering grip of Isis at a faster pace than before thanks to Branco, X-Lang and the other dogs of war.

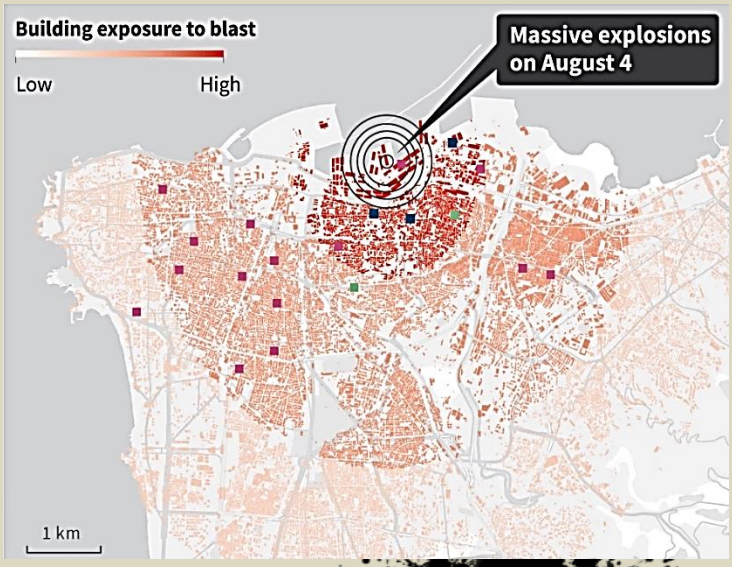
A Year since the Port Blast in Numbers

Source: http://www.naharnet.com/stories/en/282918-a-year-since-the-port-blast-in-numbers

Aug 02 – Lebanon on Wednesday marks a year since a fire at Beirut's port led to the country's worst peacetime disaster and precipitated its decline.

The August 4, 2020 blast and its aftermath in numbers:

- 214: people killed
- 6,500: people injured
- 300,000: people left homeless immediately after the explosion
- 70,000: people who lost their jobs due to the blast
- 73,000: damaged apartments
- 9,200: damaged buildings
- 163: damaged schools and educational centers
- 106: damaged health care facilities, including six hospitals and 20 clinics
- 2,750: tons of ammonium nitrate initially stored at the port
- 6: years it was stored in the warehouse that blew up



- 3.3 to 4.5: estimated magnitude of equivalent earthquake
- 200: kilometers to Cyprus, where a shock wave was felt
- 5: days the government said it would take for initial findings
- 0: people sentenced over the blast
- 6: days after blast the government resigned
- 359: days Lebanon has been without a government since

Imaging Tool under Development Reveals Concealed Detonators — and Their Charge

Source: http://www.homelandsecuritynewswire.com/dr20210803-imaging-tool-under-development-reveals-concealed-detonators-and-their-charge

Aug 03- Behold the neutron, the middle child of subatomic particles. At times overshadowed by its electrically charged siblings the proton and the electron, neutrons quietly play important roles in national security. They start nuclear reactions for weapons and power plants. They bombard materials for nuclear safety tests. And now they have a new skill: telling whether a concealed, electric detonator is charged. Sandiaquantum-sensing expert Yuan-Yu Jau is helping neutrons develop their talent. He's leading an effort to build a new kind of neutron-based imaging system. When finished, it will enable people to safely examine sealed metal boxes when opening them could be dangerous, whether that's because inside is an explosive weapon or a malfunctioning, high-voltage fire set at a missile range. "There are no other technologies that can directly image an electric field with physical barriers," Jau said. "One advantage of this imaging technology is that it can absolutely determine the magnitudes and directions of the electric fields."
Jau has already shown neutrons are up to the task at a large, specialized facility — the National Institute of Standards and Technology Center for Neutron Research in Gaithersburg, Maryland. He is currently exploring how to redesign the system into a smaller, fieldable prototype for security applications.
Compact neutron generators are commercially available for laboratory, medical and industrial uses, but by and large, these spit out neutrons with so much energy that the imaging system cannot manipulate and analyze them. Jau is working toward building a custom generator that tosses neutrons with much lower energies. The National Nuclear Security Administration is funding his efforts.

Neutron Spin Exposes Electric Fields
A metal box, or Faraday cage, blocks electromagnetic waves attempting to enter or exit. This conceals electrically charged devices inside and makes contents difficult to probe without opening the box. Charged particles like protons and electrons have trouble penetrating the barrier, which gives neutral neutrons the opportunity to shine.
Neutrons pass through metal with relative ease, and although they don't have an electric charge, they do spin. That spin changes ever so slightly when the particle passes through an electric field. Jau takes advantage of this phenomenon by polarizing neutrons, so they all have the same spin, and firing them through a metal box into a detector on the other side.
Some of the neutrons will never make it to the detector because they bump into the concealed object. The neutrons that make it create an X-ray-like silhouette on the detector. Of these particles, any that also pass through an electric field will have a different spin when they hit the detector than when they started. This creates a second image that shows where electric fields are. From that picture, operators can decipher the voltage of the object and whether it's charged, even if it is turned off or in sleep mode.
According to Jau, neutrons also could be used in similar ways for other applications. They could be used to study electrical properties of new materials, analyze storage capacity in advanced batteries or diagnose electrical components of complex, assembled machines without removing them. "In practice, different applications require different electric-field sensitivity and imaging resolution," Jau said. "It doesn't mean that our proof-of-concept demonstration is ready for all applications. Several of them can already be done using the demonstrated experimental setup, but some others require further improvements in performance or in fieldable technologies." In other words, the mighty neutron might have more surprise talents to show off in the future.

7 Weapons Banned In Modern Warfare

Source: https://www.warhistoryonline.com/war-articles/weapons-banned-in-modern-warfare.html

Aug 05 – The idea of banning certain weapons of war might seem ironic. After all, isn't the purpose of weapons created for war to wreak havoc against other nations? However, some weapons that have surfaced throughout the history of warfare have seemingly caused so much unnecessary pain and suffering that they have been banned from use in any conflict.

Some specific types of weapons are banned entirely, while other weapons are subject to various limitations. Here we take a look at some of the most dangerous banned weapons of war.

1. Blinding Laser Weapons

Laser Weapon System on USS Ponce (Photo Credit: United States Navy)

Blinding laser weapons are defined under international law as a weapon specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision (that is, to the naked eye).
Blinding laser weapons were banned in 1995, under Protocol IV of the Convention on Certain Conventional Weapons. Although blinding laser weapons that have been specifically designed to blind a person have been banned, "blinding as an incidental or collateral effect of the legitimate military employment of laser systems, including laser systems used against optical equipment" is not covered under the Protocol on Blinding Laser Weapons. In other words, if blindness occurs from a laser whose main intended purpose is not to blind, then that is okay.
Although this sounds like a weapon straight out of a science fiction movie, mention of them infrequently appears in the media. So do blinding lasers even really exist? Well, the answer is of course they exist, or they wouldn't have been banned in the first place.
America alone has many different types of blinding lasers, including dazzlers used in Iraq, although the weapon is used in different ways rather than just to blind its opponent. Similarly, the American media has argued that China has developed many different types of blinding laser weapons.

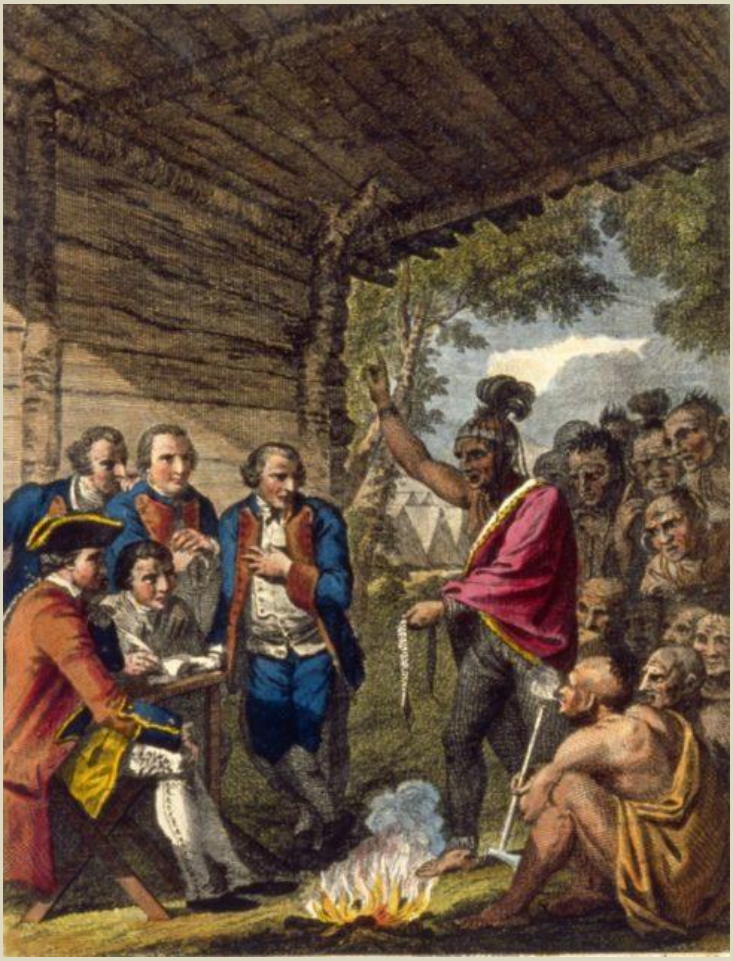
2. Chemical weapons

American soldiers wearing different styles of gas masks used by Allied and German forces during the First World War. (Photo Credit: Hulton Archive / Getty Images)

The modern use of chemical weapons began with the First World War when both sides developed and used poisonous gases on the battlefields. These chemical weapons used well-known commercial chemicals put into standard munitions, such as grenades and artillery shells. Perhaps the most famous chemical weapons used in the First World War that have since been banned are mustard gas, chlorine gas, and phosgene gas.
Mustard gas was the most common gas used throughout the First World War. Mustard gas caused chemical burns on contact and large, oozing blisters. When the blisters popped, the wounds typically became infected. Initial exposure was typically symptomless, so it was too late to take preventative measures by the time skin irritation had begun.
Chlorine and phosgene gas were also used throughout the First World War. Unlike mustard gas, which causes terrible skin wounds, chlorine and phosgene gases cause death by asphyxiation.

The Germans first used chlorine gas on April 22, 1915 during the Second Battle of Ypres. Phosgene gas, however, was much more lethal during the First World War as it was colorless, meaning soldiers would not be aware until days later that they had inhaled the gas. Days after the attack, the victims' lungs would fill with fluid, and they would slowly suffocate. Phosgene gas was responsible for 85% of chemical-weapon fatalities during the First World War.
There was a large public outcry against the chemical weapons used in the First World War. As a result, the Geneva Protocol signed in 1925 banned the use of chemical weapons in war but did not outlaw their development or stockpiling.
Other types of chemical weapons have been banned since the 1925 Geneva Protocol, including nerve agents that break down the neurotransmitters that allow organs to function. Victims who inhale these nerve agents slowly lose control of their bodily functions, and death eventually comes from respiratory failure.
Similarly, nettle agents have also been banned. Nettle agents irritate the skin but do not cause blisters. Different chemical weapons, including tear gas and pepper spray, were banned for use in war at the 1993 Convention on the Prohibition of Chemical Weapons.

3. Biological weapons



Painting of the Ottawa Chief Pontiac confronting Colonel Henry Bouquet who authorized his officers to spread smallpox amongst Native Americans by deliberately infecting blankets. (Photo Credit: MPI/ Getty Images)

Biological weapons are some of the oldest weapons used in warfare for mass destruction. Examples of biological warfare can be seen throughout history. For example, during the European colonization of North America, smallpox was used intentionally to wipe out the Native Americans who lived there by gifting blankets infested with the disease to different tribes. Smallpox was a European disease that Native Americans did not have any immunity to yet. Similarly, in 1343 during the Siege of Caffa, the Mongols tossed rotting corpses over the city walls to spread disease and infection throughout the city. The weaponization of diseases is obviously horrible and very dangerous. Biological weapons were effectively banned in 1972 with the Biological Weapons Convention. The provisions of this convention prohibit the development, production, and stockpiling of biological weapons.

4. Poisoned Bullets

Portrait of painter and inventor Leonardo da Vinci, who invented a type of poisoned bullet which was later banned. (Photo Credit: DEA/ D. DAGLI ORTI/ Getty Images)

One of the earliest weapons banned from warfare were poisoned bullets. In 1675, the Strasbourg Agreement, signed between France and the Holy Roman Empire, was created in response to the increased use of poisoned bullets.
Although toxins as a weapon can be traced back to ancient history, the poisoned bullets prohibited in the 1675 Strasbourg Agreement were actually developed by Leonardo da Vinci, who developed a bullet that had powdered arsenic and powdered sulfur packed into shells.
The 1675 Strasbourg Agreement stated that neither the French nor Holy Roman Empire would use poisoned bullets in conflict, making it the first agreement in modern history to ban a weapon of war.

5. Incendiary weapons

Fireballs as a result from the dropping of Napalm on suspected Viet Cong targets in South Vietnam, circa 1966. (Photo Credit: PhotoQuest/ Getty Images)

Incendiary weapons are defined as devices specifically designed to cause fires. Incendiary weapons such as napalm are devastating weapons that have been used in some of the deadliest conflicts and battles in human history. Napalm was dropped on 66 Japanese cities during the Second World War by American pilots. Similarly, from 1963 to 1973, 388,000 tons of napalm were dropped on Vietnam, terrorizing Vietnamese citizens who were innocent bystanders in this conflict. Certain incendiary weapons were banned under Protocol III at the 1980 Convention on Certain Conventional Weapons. Weapons whose primary design is to set fire to objects or to cause burn injuries to persons through the actions of flame, heat or a combination of the two were banned outright.
There are limitations to the usage of flamethrowers, shells, rockets, bombs, and napalm. For example, napalm as a substance itself is not banned as a weapon of war, but using it on anything other than a concentrated area where an enemy is located is forbidden.

6. Landmines

An American army engineer planting a landmine, circa 1945. (Photo Credit: PhotoQuest/ Getty Images)

Landmines are one of the most dangerous weapons of war ever developed — not just because they target civilians, but because there is such a variety of different landmines that have been developed. The 1997 Convention on the Prohibition of Anti-Personnel Mines (also known as the Ottawa Treaty) banned anti-personnel mines, a form of mines designed for use against humans.
The Ottawa treaty did not ban anti-tank mines, booby traps, and remote mines. In 1996, an amendment was made to Protocol II to the Convention on Certain Conventional Weapons to regulate but not outright ban booby traps and other exploding devices. However, this Protocol does ban the use of non-detectable anti-personnel mines and the use of non-self-destructing and non-self-deactivating mines outside of fenced and monitored areas.
Non-detectable anti-personnel mines are essentially plastic mines, which are no less dangerous than metal landmines, but they are much harder to detect during war and in times

of peace because metal detectors cannot locate them. Furthermore, the plastic pieces used in non-detectable mines cannot be X-rayed by doctors, so the injuries they cause are much harder to treat.
Non-self-destructing landmines are landmines that pose a risk to civilians as they have the potential to detonate at any time. All landmines must now be equipped with a timer to render themselves harmless so they do not pose a threat if abandoned or forgotten.

7. Cluster munitions

Two cluster bombs being dropped over Kiel, Germany circa 1944. One cluster bomb has already broke and scattered the smaller munitions while the other one had not yet broken. (Photo Credit: Bettmann/ Getty Images)

One of the most recently banned weapons of war is cluster munitions, or cluster bombs, which were banned at the 2008 Convention on Cluster Munitions. A cluster bomb is a weapon that releases a number of projectiles upon impact to injure or damage people, vehicles, or structures. These weapons are extremely dangerous as there is no way to distinguish civilians from combatants. Furthermore, cluster bombs leave behind large numbers of unexploded munitions.
The 2008 Convention on Cluster Munitions banned any use of cluster bombs, as well as the development, production, or stockpiling of these weapons.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

CYBER NEWS

C2BRNE DIARY

Were Tokyo Olympic Games Target to Cyber Attack?

Source: https://i-hls.com/archives/109803

July 26 – The Olympic Games have always been targeted by cyber threat actors looking to capitalize on the event. The Japanese government has been bracing itself for a greater intensity of cyber attacks during the Tokyo Olympic Games than those launched against the Rio and London games. In fact, it has been unveiled by a local government official that the user names and passwords of the Olympic Games ticket holders and event volunteers were reportedly leaked online.
The official told Kyodo news agency on condition of anonymity that the stolen credentials could be used compromising personal data such as names, addresses, and bank account numbers. Claiming that the scale of the data leak was "not large", the official said measures were taken to prevent further spread of the compromised data.
The Japanese government and the Tokyo 2020 organizing committee, have conducted cybersecurity exercises, such as Cyber Colosseum, to simulate potential attacks, both in cities and rural areas. Earlier this year, it also trained 220 white hat hackers from Japanese ICT firms such as NTT and NEC in a security training program.
Mihoko Matsubara, the chief cybersecurity strategist at NTT, noted in a February 2021 report on Japan's cybersecurity strategy for Tokyo 2020, that the coronavirus pandemic has complicated ways to secure the event both physically and virtually.
With over 90% of Tokyo 2020 organizing committee members working from home to prevent Covid-19 infections, Matsubara said it was important to secure not only Tokyo 2020-related infrastructure such as electricity, transportation, and venues, but also remote work environments, as reported by computerweekly.com.

Terrorist Organizations Have New Non-Lethal Weapon

Source: https://i-hls.com/archives/109764

July 25 – Cryptocurrency can be difficult to track, making it a popular tool for money laundering and other illicit activity. As cryptocurrency technology advances and becomes more user-friendly, terrorist activity in this sphere is likely to grow.
Cryptocurrency is digital money that can be used to buy goods and services but uses an online ledger with strong cryptography to secure online transactions.
The US Department of Homeland Security is worried about an increase in cryptocurrency use by terrorist organizations as the technology becomes easier to handle. Groups are in a "nascent stage" with digital money but are increasingly using it for fundraising, said Stephanie Dobitsch, deputy undersecretary in the Department of Homeland Security's Office of Intelligence and Analysis during a hearing before the House Homeland Security Intelligence & Counterterrorism Subcommittee.
Cryptocurrency is becoming mainstream among transnational criminal organizations, Dobitsch said, and is used in ransomware attacks by nation-states and cybercriminals.
The U.S. announced last August that it had seized more than 300 cryptocurrency accounts from terrorist groups, including al-Qaida. Those groups solicit donations via cryptocurrency, Dobitsch said.
A growing familiarity with cryptocurrency may open the door to cyberattacks by terrorist organizations, Dobitsch said, adding that the groups have displayed a "rapid ability to adapt" and may turn to ransomware to fund their operations.
Questioned whether the DHS and the Secret Service needed expanded legal authorities to track cryptocurrency and combat related cybercrime effectively, the Secret Service said they need more investigative authorities, more law enforcement officers, and more computer scientists to "keep pace with the adversary", according to bgov.com.

New Book Helps Readers Spot Online Health Scams

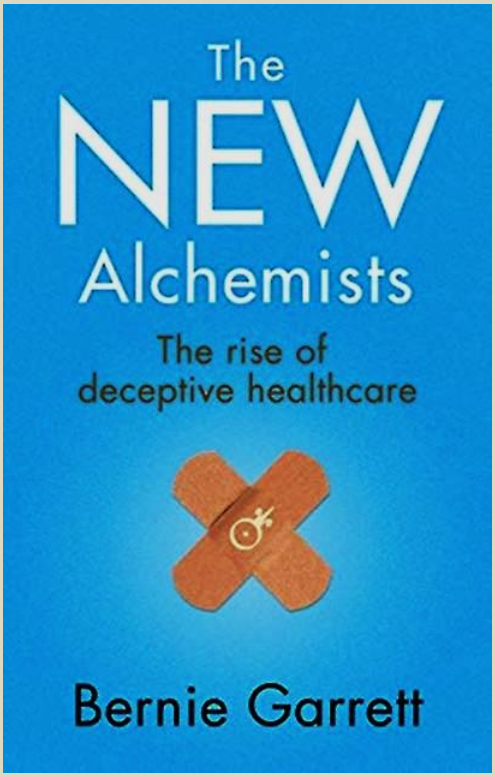
Source: http://www.homelandsecuritynewswire.com/dr20210729-new-book-helps-readers-spot-online-health-scams

July 29 – Internet health scams have increased in recent years, often spread through social media and causing untold harm, according to a new book by UBC nursing professor, Dr. Bernie Garrett.
The New Alchemists focuses on some of the many deceptive healthcare and marketing techniques used to mislead people—and offers readers tips to avoid falling prey to scammers.
Dr. Garrett has more than 35 years of experience in nursing and research on health care practices. In this Q&A with Lou Corpuz-Bosshart of UBC News, he explains why online health scams are so pervasive, shares recent examples, and gives advice to minimize their impacts.

Lou Corpuz-Bosshart: Why is your book called The New Alchemists?

Bernie Garrett: The alchemists are best known for trying to turn metal into gold, but they also sought to develop an immortality potion. These ancient philosophers acquired a reputation for being charlatans and crooks, and so the title fits very well with what we're seeing today where people are marketing various fake remedies.

Corpuz-Bosshart: Why is it important to understand and detect health scams?



Garrett: Deliberately selling a product using false marketing or spreading false information can have serious health consequences. Probably the worst examples are the fake cancer clinics that sell remedies or treatments for cancer patients who are desperately searching for solutions.

We've also seen hugely deceptive practices in the pharmaceutical industry, such as lawsuits over the mis-marketing of drugs such as OxyContin or Abilify.

Stranger examples include the 18-year-old fake doctor in Florida who operated for a number of years, as well as bizarre fake health machines, and alternative practitioners who market useless therapies using false claims.

Corpuz-Bosshart: Why are people seemingly deceived so easily?

Garrett: Scam marketers are well-versed in modern advertising techniques and the psychology of persuasion. They know all the triggers that can help sell a product. Examples include making it appear that a treatment is scarce, with language like "supplies are running out" or "buy it quickly now before it's gone." They often link their product to positive images, such as photos of mothers, or claim that a product is "healthy" or "natural".

There are certainly conditions that the medical field does not have good treatments for and so people seek alternatives. Unfortunately, this can also make them easier prey for deceptive practitioners.

Corpuz-Bosshart: Have these deceptive practices proliferated during COVID-19?

Garrett: They definitely have proliferated, and this has been aided by social media. You've only got to look at the success of the anti-vaccination campaign, where we see people being falsely advised that they will become magnetic or infertile or claiming vaccines have not been tested. Unfortunately, people can post misinformation on social media with no real consequences.

Corpuz-Bosshart: How can people protect themselves from internet health scams?

Garrett: As we outline in the book and in previous research, look for trigger words, such as if the marketer suggests that something is only available for a short time or from this one site. Watch for claims that mention "science hasn't caught up with this" or "amazing results." Be very wary of claims that are based on personal testimonies or celebrity endorsement.

Check the source of information. Use established, reliable sources such as Health Canada, the World Health Organization or even the FDA in the United States. These type of sources are certainly more trustworthy than a blog post from relatives or friends or people you've never heard of on social media. [What about sources in between?]

It's also important for all of us to lobby for better health regulation and advertising standards of practice.

We do need to take an interest in our health and in what we are being told. Deception is more widespread than people think, but you can take some simple steps to avoid getting caught up in it.

Overall, if something sounds too good to be true, it probably is.

Using Empathy to Teach Students about Cybersecurity and AI Ethics

Source: http://www.homelandsecuritynewswire.com/dr20210802-using-empathy-to-teach-students-about-cybersecurity-and-ai-ethics

Aug 02 – While empathy is important in almost every aspect of daily life, it is not always a priority in the development of technology, especially technology using artificial intelligence (AI). University of Illinois School of Information Sciences (iSchool) researchers are working to address this gap by using empathy to teach high school students about cybersecurity and AI ethics issues. Led by Associate Professor Yang Wang, the project, "Teaching High School Students about Cybersecurity and Artificial Intelligence Ethics via Empathy-Driven Hands-On Projects," has received a two-year, $297,575 National Science Foundation (NSF) Early-Concept Grant for Exploratory Research (EAGER). Assistant Professor Yun Huang; Pilyoung Kim, associate

professor of psychology at the University of Denver; and Tom Yeh, associate professor of computer science at the University of Colorado Boulder, will serve as co-principal investigators.
"We have seen many AI technologies that are fraught with ethical issues, for instance, having implicit biases toward certain populations or treating them unfairly," said Wang. "If we want tomorrow's AI technologies to be ethical, we need to plant the seed today and educate the future AI designers now."
According to Wang, developers are under a lot of pressure to ship products quickly, so ethics and empathy tend to get sidelined or ignored. In addition, "developers probably didn't get empathy-driven education when they were in school."
"Our project makes an initial step towards changing that," he said.
For their project, the researchers will develop hands-on labs that cover a variety of scenarios, such as online gaming, social media, mobile apps, and smart toys. The labs, which will be made publicly available for schools to use, will include real-life examples of young children who are interacting with unethical AI or exposed to cybersecurity risks. Using a cutting-edge non-invasive neuro-imaging technique, functional near-infrared spectroscopy (fNIRS), the researchers will be able to assess the impact of these labs on the activation of brain regions associated with empathy in high school students.
"We hope the hands-on labs we develop in this project are effective and will be adopted widely in teaching high school students about AI and cybersecurity ethics issues," said Wang. "And that students will have more empathy for others, especially those who are vulnerable and can be disproportionately affected by these emerging technologies."

Empathy is the capacity to understand or feel what another person is experiencing from within their frame of reference, that is, the capacity to place oneself in another's position. Definitions of empathy encompass a broad range of emotional states. Types of empathy include cognitive empathy, emotional (or affective) empathy, somatic, and spiritual empathy.
The English word *empathy* is derived from the **Ancient Greek** ἐμπάθεια (*empatheia*, meaning "physical affection or passion"). This, in turn, comes from ἐν (*en*, "in, at") and πάθος (*pathos*, "passion" or "suffering"). In modern Greek: εμπάθεια may mean, depending on context, prejudice, malevolence, malice, or hatred.

Trends in Terrorist and Violent Extremist Use of the Internet, Q1-Q2 2021

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/trends-in-terrorist-and-violent-extremist-use-of-the-internet-q1-q2-2021/

Aug 02 – Islamist terrorist organisations including al-Qaeda, Islamic State (IS),and their supporter networks are increasingly exploiting open-source software to create "cloud platform" websites to store their content. These are password-protected websites that enable terrorist actors to share content via URLs. Many of these contain an extensive and regularly updated archive of terrorist material.
This trend is likely due in part to a broad improvement in moderation of terrorist content by mainstream tech platforms. Cloud platforms currently provide terrorist actors with a comparatively stable, centralised location in which to store their material. This is because the process of taking down cloud platforms is extremely challenging. As a result, content stored on cloud platforms canstay active without significant threat of being removed. Mostcloud platforms monitored by Tech Against Terrorism exploit open-source software developed by Germany-based company NextCloud.
The exploitation of the decentralised web –or Dweb –by terrorist and violent extremist (TVE) actors in recent months has both expanded and diversified. Messaging apps and social media platforms built on Dweb technology are serving critical roles in the online TVE ecosystem, ensuring the ongoing availability of terrorist content online. Decentralised web hosting software and file storage systems like Skynet and the InterPlanetary File System (IPFS), are also increasingly being exploited for the hosting of terrorist content. The administrators of a prominent pro-IS propaganda archive website, for example, have been using a Dweb browser plugin since at least late 2020 to circumvent frequent takedowns over the past several months. The plugin enables users to locate a stable landing page on which the latest link for the website can be found.
This shift is likely the result of a combination of improved moderation by centralised platforms alongside a flawed perception among TVE actors that Dweb services cannot be moderated. We anticipate that TVE actors are likely to further expand their exploitation of Dweb services in the coming months, particularly if centralised platforms continue to make improvements in moderating terrorist content.

▶▶ Read the report at Tech Against Terrorism

An Escalating Threat: How Smart Buildings Can Fall Victim to a Cyber Attack

By Amy Mintz

Source: https://www.hstoday.us/subject-matter-areas/infrastructure-security/an-escalating-threat-how-smart-buildings-can-fall-victim-to-a-cyber-attack/

Aug 10 – It is well known that violent physical attacks against tall buildings are on the rise,[1] but an even more concerning threat will take the form of cyberattacks, with the potential to be catastrophically as destructive. In response, security departments securing their tall buildings will now require more than protecting the physical area and surrounding perimeter from physical access by threat actors who might attack a building. They now have to exponentially expand controlling the access to their increasingly smart buildings with their soaring amounts of IoT (Internet of Things) devices and converged OT (Operational Technology) and IT (Information Technology). With the number of entry points multiplying exponentially, the attack surface is now wide open to malicious cyber threat actors not just on location, but from anywhere around the world. Currently, most new buildings with 100,000 square feet or more are smart buildings with energy efficiencies and Building Automation Systems (BAS) that offer autonomous functionality to control lighting, climate and elevators, and also energy management, electric power distribution, fire detection, video surveillance and badge access. However, these attractive benefits come replete with security concerns. Many building protocols lack adequate cybersecurity features. For example, one of the most widely used data layer protocols for HVAC control, BACnet, is deployed in an unencrypted format. And while more secure versions are emerging, they are not commonly used.

Each one of these autonomous subsystems depends upon hundreds to thousands of sensors and computers and connects to local servers and also to the Internet. Preventing cyberattacks does still entail concerns regarding the physical layout of big buildings, as devices may be in unprotected areas where people can easily access them. One compromised IoT device is all it takes for a cyberattack, and the sheer quantities of devices means this could go undetected for long periods of time. But obviously, physical access is not necessary for a cyberattack to infiltrate and compromise a BAS. In fact, these systems are oftentimes housed in satellite facilities, with minimal to no direct IT support.

A Kaspersky report published in 2019 revealed that 37.8 percent of 40,000 smart buildings had been impacted by a cyberattack, most of which tried to compromise computers controlling the BAS, with 26 percent of threats coming from the web, 10 percent from removable media, 10 percent from phishing links, and 1.5 percent from shared folders on corporate networks.[2] In most cases it was regular malware in the forms of ransomware, worms and spyware, not malicious software specifically intended for BAS, but rather to infect any corporate network.

OT and IT cybersecurity efforts are often siloed, with gaps between OT and IT defenses exploited by adversaries who gain access to OT systems with weak defenses as an entry point into corporate IT networks. The Target retail chain data breach in 2013 was an infamous cyberattack on an HVAC system, used to gain access to the corporate financial systems to steal payment card data from over 40 million people.

The growing use of cyber-physical systems in smart buildings brings with it the capacity to wreak havoc not just in the form of costly breaches compromising data confidentiality, but even more worryingly in the form of physical consequences, such as a cyberattack on a smart building that compromises the availability of a BAS. For example, news circulated in 2017 of a cyberattack on the Romantik Seehotel Jägerwirt , a prominent hotel in Austria, by cyber criminals who compromised the electronic key system, leaving hotel guests unable to enter their hotel rooms, and disrupting other business operations.[3] One can easily imagine physical safety concerns that could arise from a cyberattack on critical BAS functions (such as water, electricity, air ventilation, elevators, as well as fire alarm and extinguishing systems), not to mention the damaging fallout of a disruption of mission-critical operations in hospitals or prisons.

In addition to the aforementioned examples of cyberattacks compromising the confidentiality and availability of a BAS, cyberattacks compromising integrity are not to be ignored. For example, temperature manipulation via a BAS hack could result in physical damage to items such as data servers or perishable goods. Cyberattacks on industrial control systems (ICS) in critical infrastructure sectors are notorious for their physical consequences, such as the BlackEnergy malware that brought down the Ukrainian power grid in 2015, and the Stuxnet worm that resulted in damages to Iran's nuclear program in 2010, acknowledged as the world's first large-scale cyber warfare attack.

As noted in *Forbes*, BAS may become the next target of cyberattacks. Security credentials for smart buildings can be sold for profit on the dark web by cybercriminals, not to mention substantial Bitcoin payments to be reaped from ransomware demands. The threat actors behind these attacks are more than just cybercriminal organizations motivated by financial gain.

Potential threat actors may include hacktivists who oppose corporate policies and products. Adversary nation states and state-sponsored criminal groups are well-funded and highly sophisticated with capabilities to disrupt building operations, as well as cause physical destruction and loss of life.

Whether motivated politically, financially or otherwise, smart buildings are now on the radar of threat actors. Disruptions to a BAS can cause significant damages to a building's commercial tenants in the form of business downtime, financial loss, and public safety threats, such as shutting down a building's electricity grid.

Addressing these critical issues will require collaboration amongst city planners, engineers and cybersecurity professionals, as well as cybersecurity frameworks and risk-analysis tools for the building industry to effectively meet the present and future challenges of securing tall smart buildings.

Securing tall buildings is, therefore, no longer about just securing the physical space of a building from potentially violent attacks. Moreover, cybersecurity is no longer about just preventing loss of data or confidentiality breaches to business entities but to major buildings that house a multitude of potentially affected tenants, including retail establishments.

Cybersecurity concerns for interconnected BAS devices within smart buildings extend into the realm of physical damages, and potential threats to tall smart buildings now include a complete building takeover from hackers who could gain remote access from other countries. While financial loss and reputational damage are serious concerns, a catastrophic event resulting in loss of life can now occur, not just by the physical presence of a terrorist or an active shooter engaging in workplace violence, a deliberate crash by a car bomb or a plane crash, but by the stroke of a computer's keyboard far, far away.

[1] See Joshua Sinai, https://www.asisonline.org/security-management-magazine/articles/2021/03/mitigating-rising-risks-for-high-rises/.
[2] See Cassandra Faro, https://usa.kaspersky.com/about/press-releases/2019_smart-buildings-threat-landscape.
[3] See Padraig Belton, https://www.bbc.com/news/business-42352326.

Amy Mintz *is a PhD Candidate in Critical Infrastructure at Capitol Technology University. Her doctoral research is focused on ways to mitigate smart city cyber challenges and contribute to the cyber forensics domain by applying tools such as visual link analysis and other techniques to emerging smart city challenges to better secure critical infrastructure. Her academic background includes an M.S. in Digital Forensics and Graduate Studies in Cybersecurity Policy, and Curriculum and Instruction. She recently co-founded the AAPI Institute, a think tank for research concerning topics central to the Asian American Pacific Islander (AAPI) community and Cybersecurity.*

Why Three Random Words Make the Best Passwords

Source: https://www.hstoday.us/subject-matter-areas/cybersecurity/why-three-random-words-make-the-best-passwords/

Aug 09 – Cybersecurity experts have revealed the logic behind their advice to use three random words when creating passwords.

In a new blog post, experts at the National Cyber Security Centre (NCSC) – which is a part of GCHQ – said a key reason for using three random words is they create a password which is easy to remember and strong enough to keep online accounts secure from cyber criminals.

The blog post noted that using three random words to coin a password is more effective than traditional advice to create complex passwords, which can be difficult to remember and yet guessable for criminals.

Other reasons for choosing the three random words approach were:

- Length. Passwords made from multiple words will generally be longer than passwords made from a single word and therefore meet minimum length requirements.
- Impact. 'Three random words' contains all the essential information in the title, and can be quickly explained, even to those who don't consider themselves computer experts.

- Novelty. A password containing multiple words encourages a range of passwords that have not previously been considered.
- Usability. It's easier for users to enter a three random word password than one which contains a complex range of characters.

NCSC Technical Director Dr Ian Levy, said: "Traditional password advice telling us to remember multiple complex passwords is simply daft. There are several good reasons why we decided on the three random words approach – not least because they create passwords which are both strong and easier to remember. By following this advice, people will be much less vulnerable to cyber criminals, and I'd encourage people to think about the passwords they use on their important accounts, and consider a password manager."

Rocio Concha, Which? Director of Policy and Advocacy, said: "Ensuring you use strong yet memorable passwords online and with smart products is more important than ever – our research has repeatedly highlighted poor security practices in a range of connected devices, from routers and wireless cameras to apps. There's a reason why new legislation announced by the government to improve standards for smart devices includes a ban on generic default passwords – these can make it easy for hackers to take control of devices or even your home network. Strong passwords can stop cyber criminals in their tracks, and we'd urge everyone to ensure they adopt good practice to safeguard their data and privacy."

Creating passwords using three random words is one of the six key steps recommended by the U.K.'s Cyber Aware campaign to protect accounts and devices from most cyber crime.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

HOTZONE SOLUTIONS GROUP

C2BRNE DIARY

DRONE NEWS

Management of Drone Swarm Traffic – European Initiative

Source: https://i-hls.com/archives/109696

July 21 – Drones can be useful in different applications, such as delivering and transporting goods, monitoring in different environments, or accessing places that are difficult to reach in emergencies, for example. However, safely managing drone traffic in cities and other areas with high levels of congestion will be a major challenge.

The **European LABYRINTH project** was designed to create and validate new swarm drone applications to enhance safety, security, and efficiency in the civil system transport, through the research and development of drone swarming 4D (3 spatial dimensions + ti me) path-planning algorithms – for implementation in Ground Control Stations. New European U-space services (drone swarm deconfliction and flight planning) supporting drone swarms auto-guidance will also be researched.

It is aimed at integrating a certain degree of automation so that an operator can control a small fleet of up to 10 drones from a single ground station. In addition to planning and controlling routes, two other areas of technology are being subject to work: communication using 5G networks (so that drones are connected at all times) and the computer security behind the entire system.

The project is part of U-Space, a new European drone air traffic management system led by the SESAR (Single European Sky ATM Research) initiative. This new framework is designed to integrate low-level drone operations, below 120 meters (400 feet), safely and efficiently into European airspace.

The applications within the project framework concern different environments in Spain. For example, work is being undertaken with the Directorate-General for Traffic (DGT, in its Spanish acronym) to use drones to improve road transport, analyzing aspects such as speed control, measuring the distance between vehicles, identifying license plates, and following up on and providing support in the event of accidents. Another initiative with the National Institute of Aerospace Technology (INTA, in its Spanish acronym) is intending to use drones at airports to control unauthorized access, inspect tracks, or use them as a deterrent against birds, according to eurekalert.org.

Greece – Archytas (UAV)

Archytas (435/410–360/350 BC) was an Ancient Greek philosopher, mathematician, astronomer, statesman, and strategist. He was a scientist of the Pythagorean school and famous for being the reputed founder of mathematical mechanics, as well as a good friend of Plato. Somewhere around the year 300 B.C., Archytas mystified and amused the citizens of Tarentum by flying a model pigeon. Escaping steam propelled the bird, which was suspended on wires. The pigeon used the same action-reaction principle as the rocket, which was not stated as a scientific law until the 17th century.

Can Drone Warfare in the Middle East Be Controlled?

By Cathrin Schaer and Kersten Knipp

Source: http://www.homelandsecuritynewswire.com/dr20210728-can-drone-warfare-in-the-middle-east-be-controlled

July 28 – Three weeks ago, the US launched airstrikes against militant groups loyal to Iran near the Iraqi-Syrian border. According to a statement issued by United States defense officials, the strikes were in retaliation for the groups' drone attacks on American troops in Iraq. The US military said that drones, also known as Unmanned Aerial Vehicles (or UAVs), have been used against their personnel at least five times since April. In the most recent attacks, an armed drone was detonated at a dining area used by Americans inside Baghdad's airport. Another damaged an American hangar in northern Iraq.

The drone attacks are part of a disturbing trend in the region: The escalating use of UAVs, both for surveillance purposes and to attack opponents, by countries in the region — but also by nonstate actors there, like militia groups in Iraq, Yemen and Syria, among others.

Political Pressure by Drone

Research by the Milan-based Institute for International Political Studies (ISPI) suggests that Middle Eastern nations (excluding Israel) spent at least $1.5 billion (€1.27 billion) on military drones over the last five years. Of all nations in this area, Israel is probably the most advanced drone-maker. But the country tends not to pass on its technology to those it considers potential enemies. Turkey, Iran, the United Arab Emirates and China are other major suppliers of drones in the region. Iran has one of the longest-running drone programs, ISPI researcher Frederico Borsari explains. Hampered by international sanctions and lacking a modern air force, Iran has long understood that drones, supplied to allies elsewhere, could add to their air power and give them "plausible deniability," Borsari said.

Drones are likely being used by Iraqi militias against the US, or by the anti-government Houthis in Yemen against Saudi Arabia, yet experts agree it's highly likely the technical know-how comes from neighboring Iran. At the same time, Iran can deny it had anything to do with it. "From Tehran's point of view, this is an advantage," Borsari told DW. "The drones in their hands can be used to exert political pressure."

Superior Air Power

The proliferation of drones in the Middle East is "dangerous because it alters military hierarchies in the region," explained Fabian Hinz, an independent Middle East analyst based in Berlin, who focuses on drones and ballistic missiles. "Previously, you predict the outcome of any conflict. As in, this country has so many planes and this much training, so you could estimate how strong they were. Drones and ballistic missiles shake all that up."

One key to resolving the Middle East's growing drone issue could be better regulation. In a December 2020 editorial in *The Bulletin of Atomic Scientists*, Agnes Callamard, a former United Nations special rapporteur on executions, warned that the world has entered a "second drone age … marked by the uncontrolled proliferation of armed drones, the most advanced of which are stealthier, speedier, smaller, and more capable of targeted killings than a previous generation."

At last count in March 2020, there were more than 102 countries with military drones, along with an additional estimated 63 nonstate actors.

Robust Standards Needed

Callamard argued that nation-states must work together to establish a new regime that would include "robust standards for the design, export and use of drones" and the transfer of related military technology.

But would such a regulatory regime work in the Middle East, given how widespread drones are there already? And, would this be any better than what the US military did over the weekend — that is, simply striking back at drone users?

"When it comes down to military strategy, it would seem most effective to strike at points where these systems are being manufactured, or by taking out those who are highly trained to make them," agreed James Rogers, a professor of political studies and special advisor to

the UK government on drones, who is based in Denmark. "However, when there is still a very clear link between the nation-state as a supplier — for instance, to the militias in Iraq or the Houthis in Yemen — then there are other diplomatic means that I think should go alongside this. It is also imperative that any strikes are in line with international law and uphold, not degrade, a nation's sovereignty."

Custom Designs by Iran

While in the Middle East, Rogers was able to inspect some of Houthi drones closely. They are a mixture of Iranian-inspired drone design, with wiring from China, the latest digital cameras from leading international manufacturers and drone engines coming from a variety of European companies, Rogers told DW. A number of parts are likely made by the Houthi militants themselves, probably copied from original parts from elsewhere.

Evidence points to Iran providing proxies in other countries with custom designs, Hinz said, referring to a report from UN experts that listed components in just one Houthi drone flown against Saudi Arabian targets. Some parts were made locally, he noted — but there were also components from the United Kingdom, Poland, Sweden, Italy, Japan, Ireland, South Korea and the US.

This is why both Hinz and Rogers agree that while exports of the latest military drone technology could be controlled, it would be almost impossible to stop commercially made drone parts from reaching nonstate actors with potentially criminal intentions in the Middle East.

Violating Sovereignty

"You could control these [commercially made] parts more strictly, but it would likely only have a limited impact," Hinz explained. "It would make the whole drones arms race more expensive and more difficult, and it would slow things down a little. But those who want the parts will be able to find a middleman to sell to them, or they could substitute parts they can make themselves."

Rogers, who with Agnes Callamard co-authored the 2020 editorial calling for a better drone regulatory regime, believes that one way of doing this might be to focus on how drones are used, rather than the supply of parts.

"There is a very important way in which drones have started to violate international law," Rogers argued. "Drones have led to more violations of the sovereignty of other nation-states. When you conduct war by remote control, it gives the sense that it is less risky, less costly. For example, you are able to send a remote control vehicle over a border without the risk of your pilot being shot down or captured. You can also surveil vast regions without crossing a border. So we are starting to see worrying norms of use."

Implications for Future AI-Based Weapons

This is why he is advocating for more robust standards for drone use, and suggests something like a good-faith agreement where countries agree on how drones can be used, including on issues like crossing borders, following international law, establishing best practices and the passing on of drone technology to third parties. This could be included in agreements on use between drone-selling states and their consumer nations.

"That benefits all those involved because obviously no nation state wants their sovereignty violated," he told DW. "And if that agreement is violated, then you do not continue to sell drones to those state actors."

Despite the drone-watchers' overwhelming pessimism about coming up with completely effective controls, James argues that thinking about all this is vital for the future of conflict and human rights.

"Because if you can control the most high-tech systems and how they are used," he concluded, "then you are setting a framework in place for how you could potentially control the artificial-intelligence autonomous [military] systems that are emerging, for which drones are just the entry point."

Cathrin Schaer is a DW journalist.
Kersten Knipp is a journalist and author.

Pentagon: Iran attacked tanker ship with explosive-laden drone

Source: https://www.upi.com/Top_News/US/2021/08/06/oman-iran-uss-ronald-reagan-Oman-tanker-drone-attack/1121628275342/

Aug 06 – Iran was behind a deadly drone attack on an oil tanker last month off the coast of Oman, a U.S Defense Department team has concluded.

The U.S. Central Command announced the finding in a statement on Friday following an investigation by an expert team from the USS Ronald Reagan dispatched to examine evidence and interview crew members of the Mercer Street tanker who survived the July 30 attack.

After two unsuccessful attacks the evening before, the Liberia-flagged tanker was struck with a drone loaded with military-grade explosives that left a 6-foot hole in the pilothouse and killed two crew members, the team found.

Investigators found small remnants of one drone that the Mercer Street crew had recovered from the water. They also found several pieces of the third drone, including part of a wing and other components that were nearly identical to those recovered from previous attacks from Iran.

The Mercer Street's location was within range of previous documented "one-way" drone attacks from the Iranian coast. Explosive experts from the United Kingdom and Israel agreed with the team's findings.

An accompanying report said Iran is increasingly using drones for one-way or "kamikaze" attacks in the region.

"They are actively used by Iran and their proxies against coalition forces in the region, to include targets in Saudi Arabia and Iraq," the report said.
Foreign ministers from the G7 group of countries condemned Iran following the release of the findings.
"Iran's behavior, alongside its support to proxy forces and non-state armed actors, threatens international peace and security," they said in a joint statement issued Friday. "We call on Iran to stop all activities inconsistent with relevant U.N. Security Council resolutions and call on all parties to play a constructive role in fostering regional stability and peace."

Drones and Violent Nonstate Actors in Africa

By Karen Allen
Source: https://africacenter.org/spotlight/drones-and-violent-nonstate-actors-in-africa/

Aug 06 – The risk of militarization of drone technology in Africa represents a new asymmetric tool that violent nonstate groups may deploy to extend the reach of their coercion, reshaping the African battlefield.

A drone flying above Madagascar. (Photo: WFP/Adam Marlatt)

In late 2016, the Islamic State (ISIS) reached an important milestone during the battle to secure the city of Mosul in Northern Iraq. In what is thought to be the first ever recorded use by violent nonstate actors in theatre, ISIS deployed a weaponized drone or Unmanned Aerial System (UAS). The device, with a range of about a mile and a half, had been built and loaded with explosives and detonated in a densely populated urban battlefield. The impact was both physical and psychological. Civilians found themselves trapped deeper in the city while Kurdish Peshmerga and Shi'ite militias joining Iraqi government troops, struggled to regain control.
Since that time, the use of UAS by violent nonstate actors has been observed in other conflict settings including Syria, Yemen, and Ukraine.

Expanding Applications of Drones in Africa
Within Africa, the potential for insurgent groups to emulate such tactics as those observed in Iraq, has received little attention. There has been some focus on Libya with proxy supporters of both the Libyan Arab Armed Forces coalition of militias led by Khalifa Haftar in the east of the country and the Government of National Accord supplying drones for surveillance and long-range strategic strikes. However, it is the recent escalation in hostilities in the Cabo Delgado Province of northern Mozambique that has raised the specter of violent nonstate actors in Africa deploying this technology.
Mozambique's Interior Minister Amade Miquidade reported that UAS have been deployed by militant Islamist groups in Cabo Delgado Province where a SADC stabilization force has recently been authorized. Mozambique's armed forces have been battling these militant groups who operate under the name of Ahlu Sunnah Wa Jama'a or Ansar al Sunna since 2017.
"Informal acquisition and enhancement of commercially available or so-called "hobbyist" drones are also a trend Africa may witness more."

The tensions are rooted in long-established local grievances and form part of the ongoing battle to control an area that is home to Africa's largest liquefied natural gas pipeline project. During the attacks in late March and early April 2021 that targeted, among other areas, the strategically important town of Palma, Miquidade claimed that the militants used drones to assist in precision targeting.
This aligns with other unverified reports by private security companies operating in the region that small drones have been deployed by armed nonstate actors for surveillance purposes. Jasmine Opperman, a former South African intelligence analyst, observed that "If we look at the ease with which [the insurgents] are getting weapons and mounting attacks on the military, I will never underplay the possibility that they start making use of more technologically advanced capabilities, and with that I include drones." She added that "If you can bring in cellphones by the hundreds through illegal smuggling routes, what is preventing them from bringing in drones?"
The Mozambican experience mirrors other reports emerging from Africa. In Somalia, private security contractors have described how in the past year the violent extremist group al Shabaab has deployed UAS for surveillance purposes. Although eyewitness accounts are hard to verify, Colonel (ret.) David Peddle, a former military service member in South Africa and the UK with ongoing contact in Somalia, confirmed that armed nonstate actors have been using UAS for surveillance purposes and believes it will only be "a matter of time" before the deployment of "swarms" or clusters of offensive drones in Africa, given their accessibility and relatively low cost.
Libya has also emerged as a technological testing ground for similar aerial assets, supplied by external forces such that UAS are now a mainstay of the Libyan conflict. But informal acquisition and enhancement of commercially available or so-called "hobbyist" drones are also a trend Africa may witness more and more. Across the Bab al Mandab Strait, Yemen has also reported the use of similar aerial systems by Houthi rebels, where they have been deployed as strike platforms to mount attacks against energy installations.
The global commercial drone market is forecast to reach $43 billion by 2024 with South Africa, Nigeria, and Kenya expected to be the biggest players in Africa. In addition to business uses, drones are increasingly being used for humanitarian purposes. Drones also hold much scope for expansion into other areas such as maritime security and border policing operations.
Yet the unintended consequences of commercial or hobbyist drone proliferation and its impact on African security is an area that has attracted little research. The announcement that an EU training mission will train the Mozambican army to use drones to track militants' movements is testament to a growing drone ecosystem in Africa, with both military and customized commercial UAS sitting alongside hobbyist or shop-bought drones.
The use of UAS represents a new iteration of digital technology. The rapid rollout of mobile- and smartphone technology has seen militants in remote settings such as the deserts of Mali detonate IEDs using mobile phones where in the past they would have relied on trip wires. Smartphone applications used to pilot drones present both an opportunity and a threat. Although drone technology is largely used for positive purposes, the possibility for individuals to build drones with smartphones and open-source software will accelerate, and the results may be destabilizing. In short, drones are likely to be an integral part of future warfare in Africa.

Changing the Nature of Conflict in Africa

To date, most of the research on the use of UAS by violent nonstate actors has been conducted outside of Africa. However, analysts believe the experience in the Middle East where drones have been weaponized "unlocks a genie of sorts, as [ISIS] demonstrated what was possible with a little bit of sinister engineering." They can also be quickly brought to scale. When Iraqi forces took major parts of Mosul back from ISIS in November 2016, they found an ISIS workshop dedicated to weaponizing drones. Such was the ability to scale up that, in the spring of 2017, there were between 60 and 100 aerial ISIS drone strikes each month across Iraq and Syria.
The experience of the Middle East does not necessarily mean that drones may be weaponized in the same way in Africa. The experience in Libya, for example, suggests that the tactical utility of drones may be limited as a weapon. However, drones are potentially of enormous value for wider intelligence gathering, collection of footage and propaganda materials, and for precision targeting.
A study of UAS in the Sahel and East Africa concludes that the ease with which shop-bought or hobbyist drones can be acquired across Africa suggests that indigenous innovation may appear to be more likely than direct technology transfer. Given the growing ecosystem of drone use in Africa, there is a logic to this conclusion.
As a tool which is hard to detect and harder still to shoot down, UAS may offer some utility to violent nonstate actors for surveillance and targeting purposes both on land and at sea. Indeed, during the recent attacks in northern Mozambique, eyewitness accounts described how aerial vehicles were used during the Palma attack. Nevertheless, to date there has not been a drone strike on a major piece of infrastructure such as a hotel or airport in Africa. Arguably, the psychological advantage of threatening to deploy a commercially available hobbyist drone as an instrument of intrusion or a weapon may give violent nonstate actors a degree of leverage over their adversaries as well as expanding their spheres of control.

Priorities Looking Forward

Expanding drone use in Africa for commercial and humanitarian purposes should lead policymakers to consider the unintended consequences. Mapping the use of drone activity across Africa by violent nonstate actors could be an important tool to ensure that aid programs that rely on humanitarian corridors like those established by UNICEF in Malawi, or emergency response capabilities such as the World Food Program in Mozambique, are not compromised and the benefits of drones undermined.

"Conventional militaries no longer have a monopoly on appropriating technological innovation that will shape the battlefield."

Such a mapping exercise would also benefit large-scale private or private-public partnerships such as oil and gas refineries, ports and harbors, airports, and military bases, to help them develop technical countermeasures such as defense shields or jamming technologies.

While policymakers in Africa may be unable to easily control the proliferation of commercial drones, there is scope for exploring early warning systems to flag the large consignments of drones procured and delivered to areas of known conflict. Research from Syria and Iraq demonstrates the supply chain of drone acquisition by ISIS. In response, a registration scheme similar to that used for mobile phones may be considered for smaller shop-bought drones that are not mandated to apply for a license.

There may also be scope for considering export control regimes such as the Wassenaar Arrangement, which governs the export of dual-use technologies, and possibly even the Missile Technology Control Regime (MTCR), which was designed to regulate nuclear-capable missiles able to strike from a significant distance. Given the potential for drones to be used as a weapons delivery system, this may have some utility. However, the shortcomings of both agreements are that they are nonbinding and their classifications are considered by some scholars to be rather outdated.

A Denel UAV Seeker 400 drone in South Africa. (Photo: Bob Adams)

At the international level, the Global Counterterrorism Forum led by Germany and the United States have developed the Berlin Memorandum under the Initiative to Counter Unmanned Aerial System Threats. It urges states to observe a number of UN Security Council Resolutions, including Resolution 1540, which prohibits states from "providing any form of support to non-state actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery." The Resolution also requires states to put in place "effective measures to establish domestic controls to prevent the proliferation of nuclear, chemical, or biological weapons and their means of delivery" with means of delivery including UAS (i.e., drones).

The Berlin Memorandum recommends that these "effective measures" include governments conducting risk assessments to identify vulnerabilities and pre-empt technological developments that may be utilized by terrorist actors, public information campaigns to advocate responsible UAS use, and crisis response mechanisms including sanctions following UAS incidents. Additionally, governments are urged to consider developing tactical countermeasures and technical solutions, while not impeding beneficial and legitimate UAS uses.

Given their growing exposure to the spread of this technology African policymakers should play an active role in shaping future drone policy. This emerging threat demonstrates how conventional militaries no longer have a monopoly on appropriating technological innovation that will shape the battlefield.

Karen Allen is a former BBC Foreign Correspondent and currently a Visiting Fellow in the War Studies Department at King's College London and a consultant at the Institute for Security Studies in Pretoria, South Africa.

The Militant Drone Playbook

By Austin C. Doctor and James Igoe Walsh
Source: https://warontherocks.com/2021/08/the-militant-drone-playbook/

Aug 12 – Since January, militants in Iraq and Syria have attempted or executed nearly a dozen weaponized drone attacks against American targets. Most of these involved midsize fixed-wing craft crashing into their targets and detonating, while some involved smaller quadcopter-style drones dropping lightweight munitions, often a 40 mm grenade. None of these attacks have resulted in fatalities or critical damage, but they did prompt the Biden administration to order retaliatory airstrikes against the militant groups behind them.

For years, defense and security leaders have called attention to militants' increasingly adept use of drones. Earlier this year, U.S. Central Command Gen. Kenneth McKenzie referred to the proliferation of small drones as the "most concerning tactical development" in Iraq since the emergence of improvised explosive devices. But while it is clear that militant drone operations pose a threat, there has been less consensus on the nature and scope of that threat.

Our research leads us to conclude that, while drones give militant groups a new and effective means of tactical disruption, insurgents have been unable or unwilling to use drones for strategic bombing. In coming years weaponized militant drone operations will likely increase, but there is reason to believe that the logic shaping the use of these systems will remain the same. In other words, militants are unlikely to use drone technology to target their opponents' military centers of gravity or to engage in widespread attacks on civilian targets. As a result, policymakers, soldiers, and security officials should prepare for militant drone operations to expand in degree but not in form. This means developing better counter-drone technologies while still relying on traditional elements of counter-militant strategy.

Pages from the Playbook

The first recorded successful armed drone attack by militants occurred in 2006, when Hizballah struck an Israeli warship with a fixed-wing drone rigged with explosives. Since then, weaponized drone activity has increased significantly — 99 percent of observed attacks have occurred after 2015 — and been dominated by a handful of militant actors in the Middle East. Recent research records 440 drone attacks conducted by militants through 2020. Over 98 percent of recorded attacks have occurred in the Middle East, with two groups, the Islamic State and Houthi rebels in Yemen, responsible for over 80 percent of these.

Our research identifies two prominent patterns in militants' tactical application of weaponized drones. Together, these indicate that militant groups find drones especially useful for disrupting opponent command and logistics and delaying the movement of military personnel and materiel.

First, militants often use drones for theater air attacks. In some cases, drones are used to support ground operations, providing militants with a combined arms capability. The best-known example of this is the Islamic State's modifying commercial drones — or engineering its own — to deploy small munitions in Iraq and Syria. The Islamic State routinely and effectively used its makeshift drone arsenal to disrupt enemy fighting positions and troop movements in a number of campaigns, including the Battle of Mosul. In other cases, militants with access to fixed-wing drones have used these as the leading component in a one-two

punch of indirect fire — flying below radar to damage enemy air defense systems or military positions in order to open the field for more destructive strikes from missile or rocket systems.
Second, it is common for militants to use armed drones to damage logistic hubs, arms depots, critical infrastructure, and command headquarters behind front lines. Strikes against civilian airports, air bases, factories, and other forms of critical infrastructure disrupt the movement and command of opposing forces. The Houthis, one of the only militant groups possessing military-grade drones, have used this tactic to great effect. From April 2018 to October 2019, the Houthis executed 115 drone attacks. Of these, 62 were conducted against civilian airports or critical infrastructure. Only 27 were conducted against military bases or enemy troops. (The remaining attacks were reported as intercepted or as striking unknown targets.)
A number of militant groups also use unarmed drones strictly for intelligence, surveillance, and reconnaissance operations. While it rarely grabs the headlines, drone-based intelligence, surveillance, and reconnaissance offers significant value to militants for relatively little cost or risk. For example, the Islamic State's affiliate in West Africa has reportedly used drones to surveil the locations and movement of counter-insurgent forces in northeast Nigeria. Similarly, the Taliban have used drones extensively for years to monitor U.S. and Afghan troop movements.
However, militant groups have rarely used drones for more strategic aims, such as targeting opponents' civilian populations or undermining their capacity to govern or raise military forces. Even the Houthi forces, who have an unmatched capacity to use long-range drones to strike major cities such as Riyadh, do so only sparingly. And the Islamic State, which regularly commissioned suicide and terrorist attacks in cities that remained under government control, only occasionally used drones to target civilians.
Why is this the case? Sustained strikes that do widespread structural damage would be logistically difficult for militant groups, while terrorist attacks, though logistically feasible, have political drawbacks.
Targeting the enemy's center of military and political gravity is a challenge for militant groups. Doing so effectively would mean sustaining strikes over time and against multiple targets. This would require fixed-wing systems with greater flight range and payload capacity. It would also necessitate the establishment and defense of drone bases, which would be vulnerable to attack since they could be easily located and targeted. This would require a substantial investment of militant troops, and might prove infeasible unless militants could also invest in air defense systems. A drone fleet would require a reliable logistical supply chain, which would be susceptible to disruption. This highlights how even the most capable militant organizations remain fundamentally different from their state opponents, who have the links to the outside world, reliable sources of income, and territorial depth to sustain strategic strikes.
More surprising, perhaps, is that, with a handful of exceptions, militants have not used drones for terror attacks either. This is true even for groups that have shown a willingness to systematically target noncombatants, such as the Taliban or Boko Haram. Drones would seem particularly well-suited to such a task, since smaller drones could attack many targets and their novelty as a terrorist weapon would amplify their psychological effects. Militants' calculations about using drones for terrorism appear more political than logistical. Militants engage in terrorism to convince their opponent and civilians that they are ruthless and highly resolved. Terrorist attacks via drone, which lower the risks to perpetrators of being caught or killed, do not signal strong resolve, and instead suggest that the militants are unwilling to put much skin in the game.

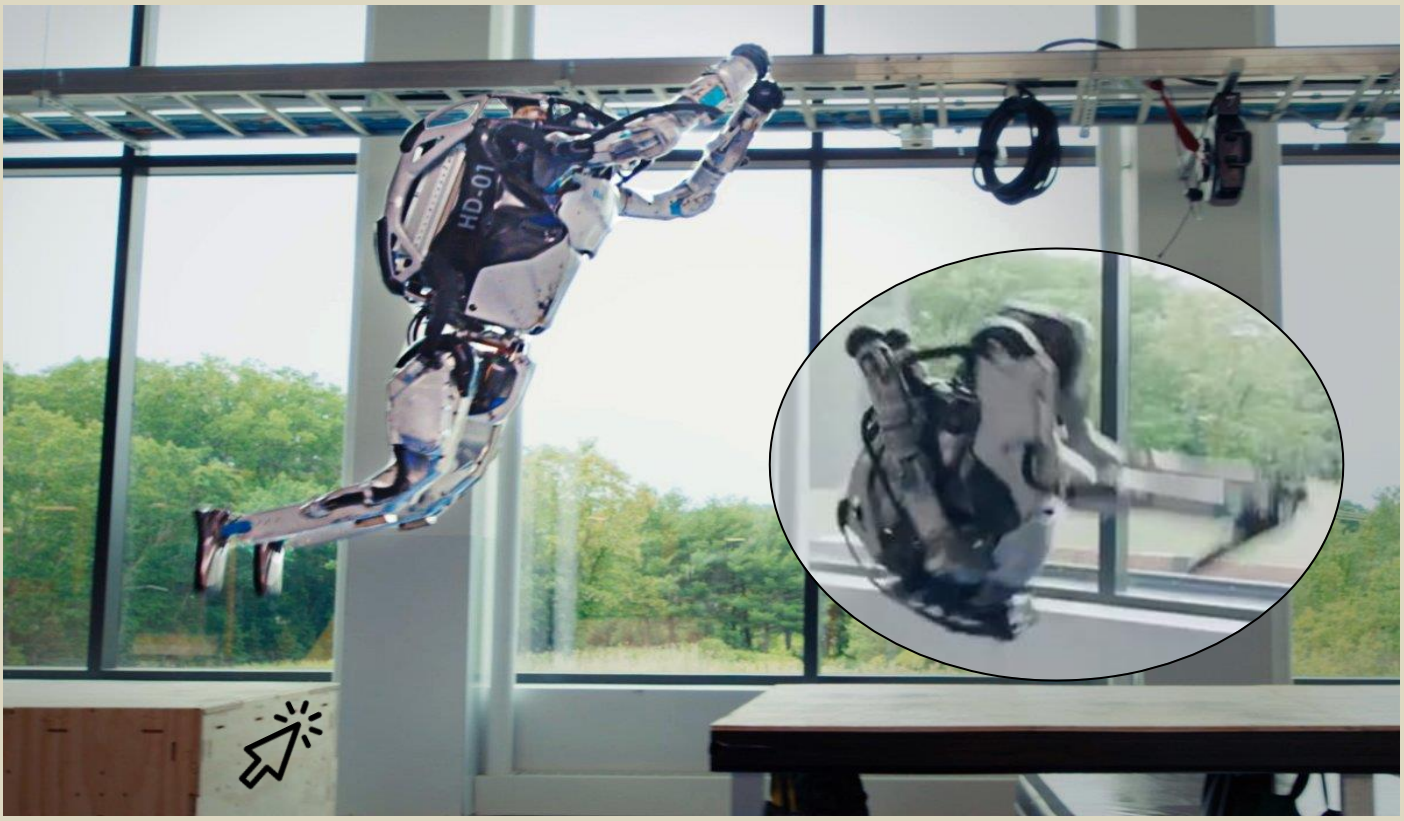
Looking Ahead

Thinking about the future of militant drone use requires understanding both the strengths and limitations of drone technology as well as militants' political goals and military capabilities. As drone systems become more common in civilian and military environments, militants' ability to acquire or develop drones will increase. Indeed, more armed groups will likely adopt these systems in coming years. While militant drone use has been highly concentrated in the Middle East, militant groups in other regions of the world (e.g., East and West Africa and Central Asia) will likely soon incorporate weaponized drones into their tactical operations. This is especially likely for groups with operational connections to transnational movements such as the Islamic State and al-Qaeda. Other factors may create greater opportunity for their use as well. The anticipated increase of urban warfare is particularly worrisome, as urban terrain is especially well suited to small drone use.
While we expect the use of armed drones by militant groups to increase and expand, the pattern of militant drone use is unlikely to change soon. Even with larger drones, targeting an adversary's center of gravity will still require militants to control and defend territory and access global supply chains, areas where state opponents tend to have large advantages. And militants may find that alternative airborne weapons systems — rockets and missiles, for instance — remain better suited to the task of producing destructive effects against strategic targets. Therefore, we believe that militants will continue to view drones as a useful adjunct to their existing military repertoires, using them to assist in targeting forces on the battlefield, to harass command and logistic hubs, and to disrupt the supply and movement of adversaries' soldiers and materiel.
What can state actors do to counter this threat? On the one hand, our analysis offers good news — in the near future, most militants are unlikely to be capable or willing to develop fleets of drones to pursue strategic objectives. The bad news, at least for state militaries, is primarily on or near the battlefield. It has proved difficult to develop military systems that can

reliably intercept smaller drones. The development of counter-drone technology is and should remain a priority. But even improved counter-drone technology will only help mitigate the threat, and militants will be quick to adapt. This means that, even in an era of drone warfare, traditional elements of counter-militant strategy will remain essential: rooting out the deeper militant drone threat means disrupting supply chains, targeting sources of revenue, finding and engaging combat and support units, and cutting militant forces off from any territorial safe havens.

__Austin C. Doctor__ is an assistant professor of political science at the University of Nebraska at Omaha and a member of the executive committee of the National Counterterrorism Innovation, Technology, and Education (NCITE) Center, a U.S. Department of Homeland Security Center of Excellence. He earned a Ph.D. in political science from the University of Georgia. He writes on militant organizations, terrorism, armed conflict, and political instability.
__James Igoe Walsh__ is professor of political science at the University of North Carolina at Charlotte. He holds a Ph.D. in international relations from American University. His research interests include technology and conflict, human rights violations, and forced displacement and return. His book, Combat Drones and Support for the Use of Force, *is available from the University of Michigan Press. His work has been supported by the Army Corps of Engineers, the Department of Homeland Security, and the Minerva Research Initiative and Army Research Office.*

Acrobatic robots



Reevaluating U.S. Military Use of Drone Technology

By Loully Saney
Source: https://9381c384-0c59-41d7-bbdf-62bbf54449a6.filesusr.com/ugd/14d834_966819f877264a0287bc30f549310837.pdf

In the 21st century, drone technology has become commonplace in warfare. In fact, drones are increasingly preferred by both state and non-state actors over other modes of warfare. But widespread use of drones in war engenders considerable controversy. Civilian casualties and collateral damage have grown alongside drone deployment with little accountability or transparency. As the Biden-Harris Administration works to rebuild America's place on the world stage and as a member of the global community, the Administration should boost accountability for civilian deaths by rethinking when and how drones are used. Specifically, the Administration should (1) sign an executive order to boost

transparency and oversight of drone technology used by the military, (2) work with Congress to review use of drones in U.S. military operations, and (3) lead efforts to launch an international drone accountability regime.

Loully Saney *is Chief of Staff for the Day One Project. Prior to joining the Day One Project, she worked as Deputy Press Secretary for U.S. Senator Tim Kaine. As a congressional staffer, she participated in fellowships with the Wilson Center and Hoover Institution at Stanford University focused on foreign and economic policy. While still in college during President Barack Obama's Administration, Loully interned at the White House National Economic Council, the Office of Science and Technology Policy, and the U.S. Department of State's Office of Iranian Affairs. In 2015, Loully received a Certificate of Appreciation for contributions toward U.S. government efforts to reach a comprehensive nuclear deal with Iran. Loully is a graduate of Princeton University where she studied Politics and received a certificate in Near Eastern Studies and a certificate in History and the Practice of Diplomacy.*

Is Ethiopia Flying Iranian-Made Armed Drones?
Source: https://www.bellingcat.com/news/rest-of-world/2021/08/17/is-ethiopia-flying-iranian-made-armed-drones/

Aug 17 – Since the outbreak of the conflict in Ethiopia's Tigray Region, there have been reports on the possible use of drones by the ENDF, or the Ethiopian National Defence Force. Opponents of the government claimed that the Ethiopian military operated armed drones from an airbase in neighbouring Eritrea, a claim which Bellingcat addressed in a previous article in 2020.
For some time, the only firm open source evidence of drone use by the Ethiopian government has been of small unarmed Chinese commercial drones operated by the country's police, which were subsequently used by the military.

One of the images included in the Facebook post provides a glimpse inside the GCS. It shows a video feed from a camera, often seen as part of Intelligence, Surveillance and Reconnaissance (ISR) pods on drones. In short, this is the view which a drone operator at a military base would see on their computer screen.

As the conflict dragged on, Ethiopian military figures broadly acknowledged some use of drones. "Our air force is equipped with modern drones. We have our own technicians and controllers who run and fly them. We don't need others to help us out with this in our fight against the extremists. We're pretty self-reliant", remarked Major General Yilma Merdasa of the Ethiopian Air Force in an interview to local media last November.

But Maj. Gen. Merdasa's interview didn't answer one particularly important question — who built Ethiopia's fleet of drones?
That's even more important to ask in light of reports which surfaced last week by open source researchers alleging that Ethiopia now operates Iranian-manufactured armed drones. Bellingcat obtained new satellite imagery from Planet SkySat and MAXAR, as well as evidence from social media, to further analyse these claims.

Two lower images from Tasnim News Agency via ArmyRecognition.com. They are published here solely for comparative purposes.

On August 3, photos began to appear on social media showing the Ethiopian Prime Minister Abiy Ahmed at an airport accompanied by Ethiopian military officers. In images posted on Facebook and Twitter we see the Prime Minister with Temesgen Tiruneh, head of the National Intelligence and Security Service (in a blue jacket) walking away from the tarmac.
Although it has not been possible to establish precisely who took this set of images, they first appeared that same morning on several Facebook pages strongly supportive of the government, including Ethio Times and Kiyya Hararghe. The images were also later published on the Facebook page of Voice of America's Oromo service, a major language in Ethiopia.
Ethiopian social media users stated the location as Semara (ሰመራ), the capital city of the country's Afar Region. This province borders the Tigray Region, where heavy fighting with anti-government forces continues.
Bellingcat and open source researchers such as flight tracker expert @Gerjon_ were able to independently geolocate these photos to Semara Airport (11.791731, 40.991712).

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


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

Greece: The successor of Canadair?

Seagle – hydrofoils; two tanks; anti-corrosion materials; 360^0 cockpit

Do not kill tanks when they become old!

Firefighting Leopard 1A5 "Made in Greece"

Sensor Detects When Firefighters' Protective Clothing No Longer Safe

Source: http://www.homelandsecuritynewswire.com/dr20210810-sensor-detects-when-firefighters-protective-clothing-no-longer-safe

Aug 10 – Firefighters risk their lives battling blazes, and aging protective gear can put them at even greater risk.
A University of Alberta researcher is working with industry to reduce that risk with a sensor that can detect the gradual breakdown in garments from exposure to heat, moisture and ultraviolet (UV) light.
"These fibers age silently and lose their performance, so this sensor technology is a breakthrough in terms of safety for workers exposed to heat and flame," said clothing and textiles scientist Patricia Dolez, the project's lead researcher and an assistant professor in the U of A Faculty of Agricultural, Life & Environmental Sciences (ALES).
Damage to the garments may not be visible to the naked eye before performance is reduced considerably, said Dolez, a researcher in the Department of Human Ecology.
"Firefighters have no good way to know how safe their clothing really is—you can't tell just by looking at it."
Once fully developed, the sensor patch would provide a way to assess the garment without destructive testing—for example, having to cut out samples to test the fabric's condition through conventional methods such as strength testing.
Developed in partnership with Edmonton-based company Davey Textile Solutions and other industry partners, the sensor patch uses graphene, a flaky substance composed of carbon atoms, to form conductive tracks on the patch's surface. When exposure to heat, moisture or UV light exceeds a certain level, the graphene track is disrupted and loses its electrical conductivity.
Firefighters would use a simple voltmeter to check the safety levels of their clothing on the sensor patch—a result that comes within seconds.
The sensor has been provisionally patented and is still under development. It comes at an optimal time, Dolez said, as the National Fire Protection Association (NFPA) prepares to upgrade its recommendations on garment maintenance because of an underlying threat of diseases such as cancer, which can be caused by fire-associated harmful substances leaching into the fabric.
"The current recommendation is to wash firefighting garments twice a year, but the problem is all the existing data that determines when the clothing needs to be replaced is based on that once- or twice-a-year washing," she said.
New NFPA recommendations are expected to bump up the laundering frequency to after each exposure to a firefighting incident, which means the monitoring technology also needs to be amped up. "The sensor is important to be able to gauge what the garment is going through with each washing."
Davey Textile Solutions, one of five industry partners working with Dolez, manufactured the fire-resistant fabrics that will be used as part of the sensor patch. The company is producing reflective trims for protective garments.
The sensor could also be used in the oil and gas, electrical, construction and mining industries, said Lelia Lawson, research and development specialist for Davey Textile Solutions.
"This is an example of how we try to be ahead of the curve to provide new proactive items to the marketplace," said Lawson, noting that one of the biggest questions for clients in heavy industry is knowing when to retire personal protective equipment (PPE).
"The sensor takes the ambiguity out of that question."
The sensor research, which began in 2018, also includes the expertise of Jane Batcheller from the U of A Department of Human Ecology and Hyun-Joong Chung, associate professor in the Department of Chemical and Materials Engineering.
The work has produced two scientific papers by graduate students studying clothing and textiles science in ALES and chemical and materials engineering in the Faculty of Engineering. The papers explored the application of graphene on high-performance fabrics and how its conductivity is affected by different aging conditions simulating service use.
Through the Human Ecology Practicum Program, a student worked with Davey Textiles Solutions to develop a business case for market applications for the sensor. The student "was able to provide a lot of good information which supported the need for this product in the industry," Lawson said.
The expertise offered by the company is invaluable, said Dolez.
"Their collaboration ensures that what we develop will be relevant for industry. As researchers we can develop something that is a great idea, but if no one is able to produce it, it's not useful," she said.
"By having industries like Davey Textile Solutions at the table, we're making sure what we develop will end up being used."
The sensor technology is the latest in a series of projects the Department of Human Ecology has had with the company through the U of A's Protective Clothing and Equipment Research Facility, including developing clothing to protect workers against steam burns.
That work resulted in the Canadian General Standards Board updating a standard used by employers when selecting appropriate PPE for their workers.
Currently, Dolez and Davey Textile Solutions are collaborating to develop methods to recycle cotton-based material from used industrial coveralls—otherwise destined for the landfill—into fibers that can be used to make new textiles.

"We're aiming to manufacture new fabrics for PPE and for other consumer goods," Lawson said. "There are more clients who want to purchase sustainable products."
Working with various U of A researchers from human ecology and the Department of Mechanical Engineering, Davey Textiles Solutions benefits greatly from their applied research, Lawson said.
"We can commercialize products from their work, and it's rewarding to have research that evolves into something that can be realized in the marketplace."
The company has hosted practicum students over the years who bring fresh perspectives to developing clothing and textiles, Lawson said, adding that the company has hired six graduates from the human ecology program, including her.
"It speaks volumes to the caliber of students from the program. They are very well-rounded because they study humans in their near environment, how they interact. Along with the theoretical knowledge of textiles, they also help with understanding how these textiles can impact lives. And that helps create better products."

Citizen's thoughts on Greek wildfires

By the Editor-in-Chief of *C²BRNE Diary*

The record hot July was followed by many wildfires that burned to ashes forests and parts of the urban web attached to hot zones. I will commend only on the wildfire (03-09 August) that indirectly threatens the village I reside in (~40 km from Athens downtown. I am not a firefighter but I do have personal experience on fires from my time in the military and the mega-fire that stormed our premises in June 2010. In addition, if we want problems identified to become lessons learned we must act fast and effectively because the next wildfire is in the corner waiting. And next time we might not be as lucky as this time!

You plan based on what you have in the field and not on what you would like to have

Based on the number of available active firefighters and fire engines you calculate how many additional seasonal firefighters you need and for how long. In addition, you explore the available pool of volunteers and the tasks and responsibilities that can be assigned to them. Then you estimate the aerial means available (civilian; military) and negotiate with third parties the possibility to rent airplanes and helicopters until the end of fire season. Keep in mind that you are not the only one interested to rent – especially the big "water bombardiers" like the Beriev-200 or the Ilyushin

Il-76. Keep in mind that it is not necessary to ask NATO for Chinooks; instead, you can ask for water buckets to be fitted in your military helicopter fleet. Finally, you must be aware of the equipment and ground forces (rescEU) are available via the Emergency Response Coordination Center (ERCC) to make the appropriate official request on time[2].

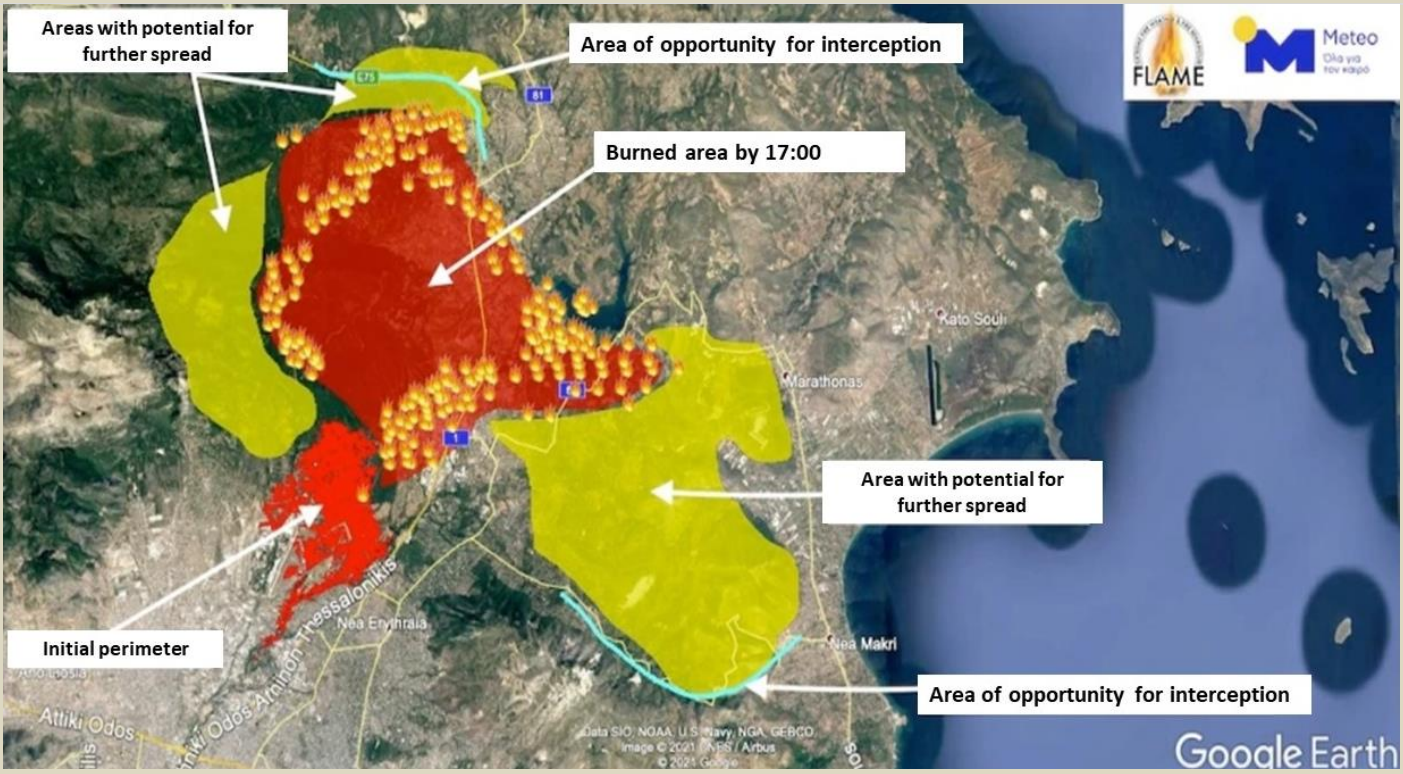
Prevention is better than treatment and costs less

We usually blame the central government for the overall unpreparedness of the state to prevent fires. This might be true, but certain lower levels of governance are equally responsible when comes to prevention. Municipalities and prefectures are responsible for the small or bigger urban forests and this means they have to clean them, remove biomass under the trees, cut the branches touching the ground, etc. At the same time, they have to take care of the harvesting of the cut branches of the houses with a garden. If they do not do that, all this plant waste will be added to naturally occurring biomass. In addition, local authorities must ensure that residents follow the existing legislation defining the deforestation of plots and the area surrounding them. Each community should maintain and update local maps showing the exact location of houses, schools, churches/monasteries, animal shelters, and pens, gas stations, nursing homes, summer camps, supermarkets, pharmacies, etc. Provision should be taken to establish and maintain more than one escape route. Finally, in areas neighboring an urban forest a very wide fire zone with fire hydrants should be created. How wide? Our recent experience showed that even a 40m national asphalt road was not enough to slow down or halt the wildfire (crown fires). A 100m fire zone might not look very nice but the survival of a village or a suburb is more preferable to a burned to ashes village or suburb. Observation posts and surveillance drones 24/7 would help spot any fire before it gets threatening. None of the above was applicable in the Attika wildfires of August 2021 (but also in previous wildfires that evolved in the last decade).

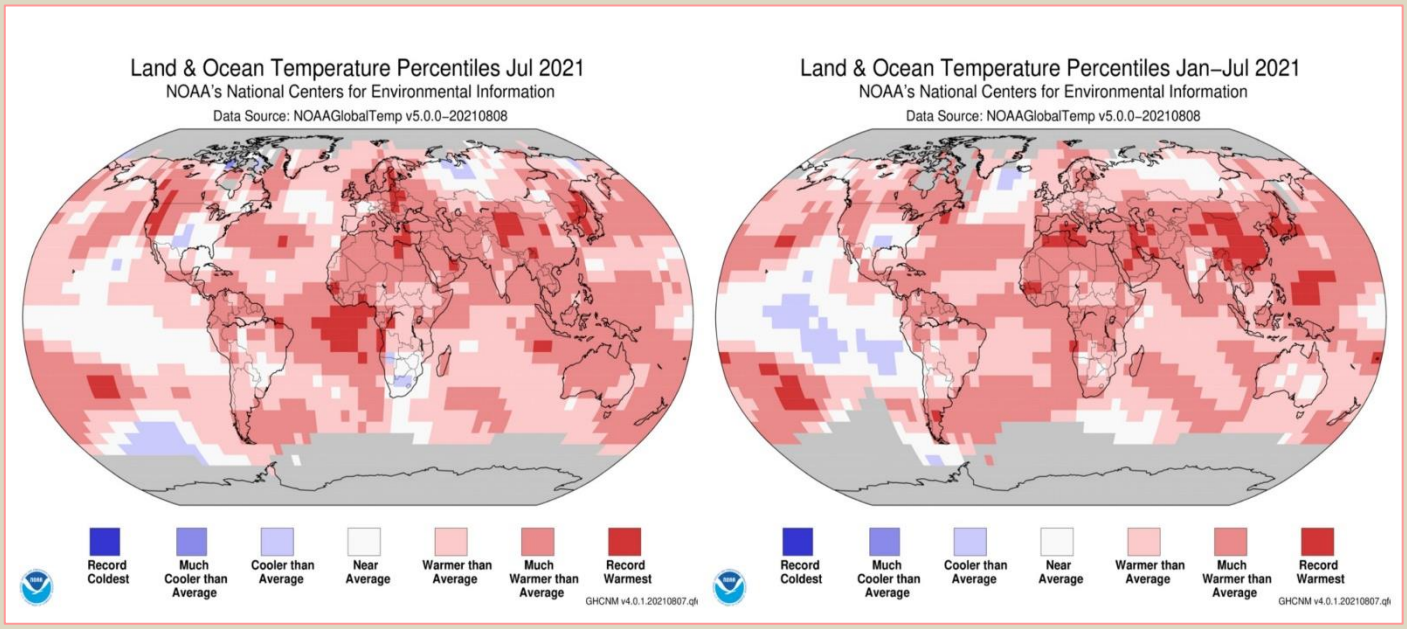
Take advantage of modern technology both for training and in the field

In CBRN operations we use special software plotting the movement of the contaminated plume and the concentrations of the hazardous materials dispersed. Similar software is available for wildfires as well. But there is no point to have them if not use them. And this was the case with the IRIS 2.0 software that the National Observatory of Athens created via the DISARM EU-funded project (Greece, Cyprus, Bulgaria). This software if fed with relevant data (temperature, humidity, fuel moisture, wind velocity, and direction, etc.) can provide the desired estimate about how the wildfire will progress (100m grid spacing; rate of spread) to know where to deploy available fire defenses. Same for software FLAME by the same organization and EU Copernicus. Both were not used in time.

[2] https://ec.europa.eu/commission/presscorner/detail/en/MEMO_15_5411



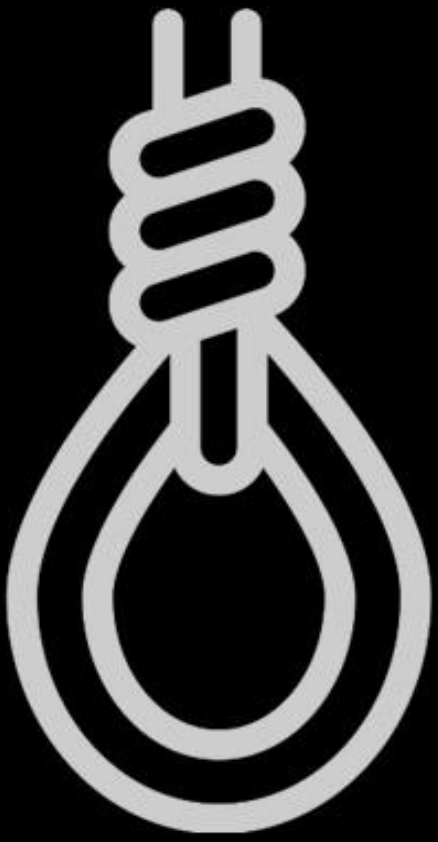
A national and international fleet of firefighting airplanes and helicopters were deployed with excellent performance. But old methods using "*fire to stop the fire*" were not used for a variety of reasons ranging from lack of experience to existing legislation.



July 2021 was Earth's hottest month on record

Evacuation

The Greek government chooses the easy solution of early evacuation via the "112" number to avoid loss of lives. It might sound logical but if buildings are left alone and without the above-mentioned preventive measures it is a sure bet that calamity will follow. For those without a personal experience of how is life in a burned area I can assure you that it is awful both physically and emotionally. Nights are more black than usual (you have to see it to believe it!). Many people lost their permanent (and not vocational) houses and suddenly became homeless. Not to mention the looting cases observed in many areas affected by the fire or been isolated. This sick phenomenon is something that needs to be addressed seriously.



NO MERCY

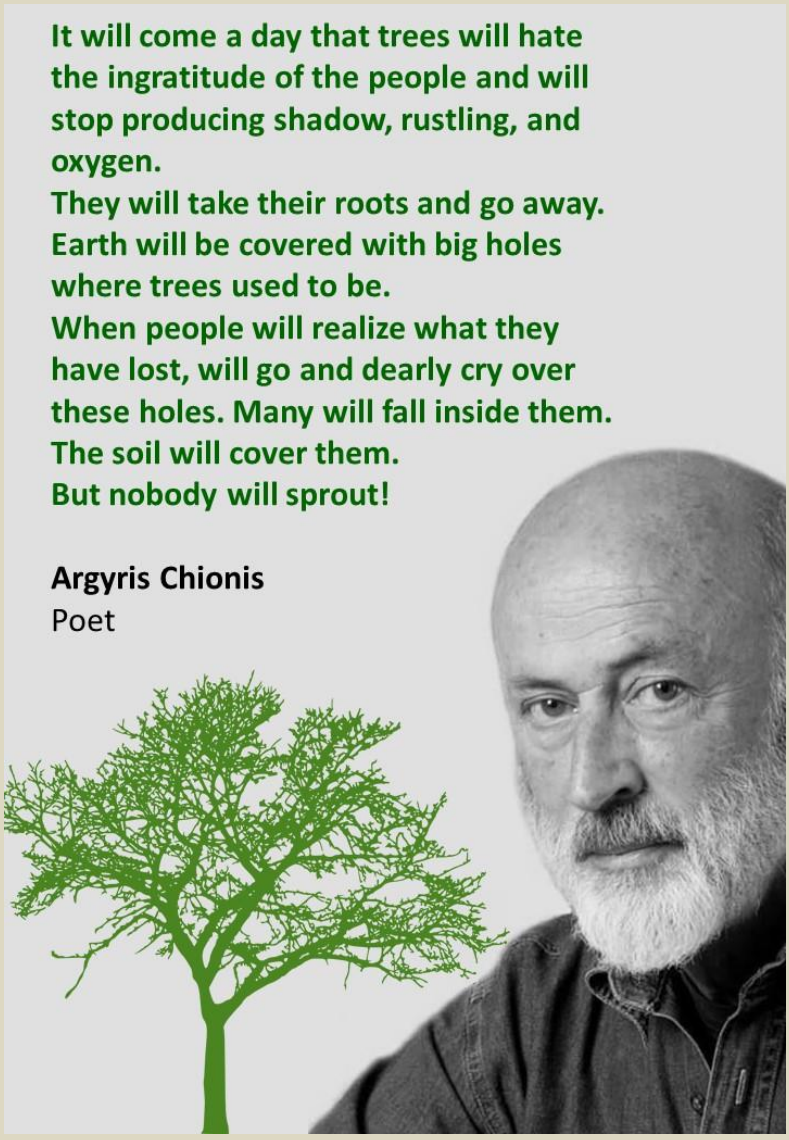
TO ARSONISTS

Logistics

In a war, logistical support equals front-line fighters. The same applies to firefighters operating in wildfires. Exposure to very high temperatures and contaminated environment affects the body's physiology and fatigue emerges faster than usual. Firefighters need food, water, rest, first aid medications (light burns; eye drops) and this should be done in an organized matter and not relied on volunteers and NGOs. This is a task that belongs to the Fire Service but usually is forgotten even without a serious reason.

Equipment

Part of the logistical field support is the equipment and personal protective gear (especially boots and gloves) used during fire fighting. Not always of premium quality, urges responders to buy certain parts of their equipment with their own money. The comparisons made with international crews supporting Greek firemen (i.e., Romanian crew) were disappointing but this can become the springboard for major changes and improvement.



Conclusion

Despite the announced changes in the way Civil Protection operates in the case of wildfires, it is obvious that there are many things to be done in many sectors. Unfortunately, although firemen know how to handle water, they (and those of civil protection) have very poor performance in planning at tactic and strategic levels (of course, every rule has its exceptions but these "exceptions" are usually left aside or ignored). A wildfire is a form of war. Therefore, military people (land forces plus airmen for aerial coordination) are a better choice to supervise the incident and support the efforts of the heroic front-line firefighters. They might do not like it but there is a common goal here that is to save lives, properties, and nature. All the major gaps identified above can be fixed in the months to follow towards Summer 2022. "*No plan of operations extends with certainty beyond the first encounter with the enemy's main strength*" (German field marshal Moltke the Elder) or "*no plan survives contact with the enemy [fire]*" but it is helpful to have a plan that will have a good chance to win the fight and the war!

- Detection
- Monitoring
- Sampling & Analysis
- Protection
- Decontamination
- Destruction & Waste Management
- Scene Management Training
- Instructional Equipment
- Live Agent Testing & Validation

HOTZONE SOLUTIONS GROUP

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

hotzonesolutions.org/