Dedicated to Global First Responders

CBRNE NEWSLETTER TERRORISM

CBRNE-Terrorism Newsletter

February 2018

www.cbrne-terrorism-newsletter.com


CBRNE-Terrorism
Newsletter
W
O
M
D
Dirty R News

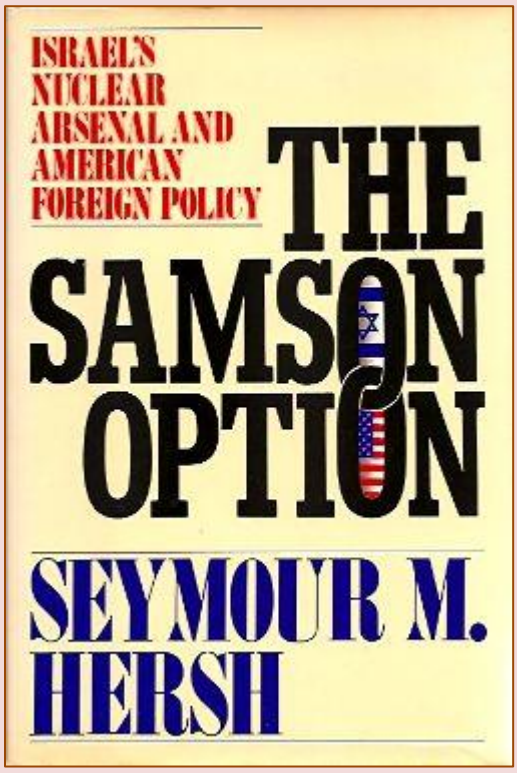
When Israel Invited a South African Nazi on a State Visit

By Asa Winstanley

Source: https://www.mintpressnews.com/when-israel-invited-a-south-african-nazi-on-a-state-visit/236578/

Jan 22 – One of the most under-reported aspects of security policy in the Middle East is Israel's nuclear weapons program.

The apartheid state is estimated by the U.S. government to have somewhere in the region of 200 nuclear warheads. The secret program to develop these weapons of mass destruction started in the late 1950s and eventually bore fruit – under the tutelage of French companies – when, in 1968, Israel went fully nuclear.



As I previously mentioned in this column, the best book on the subject is Seymour Hersh's *The Samson Option*.

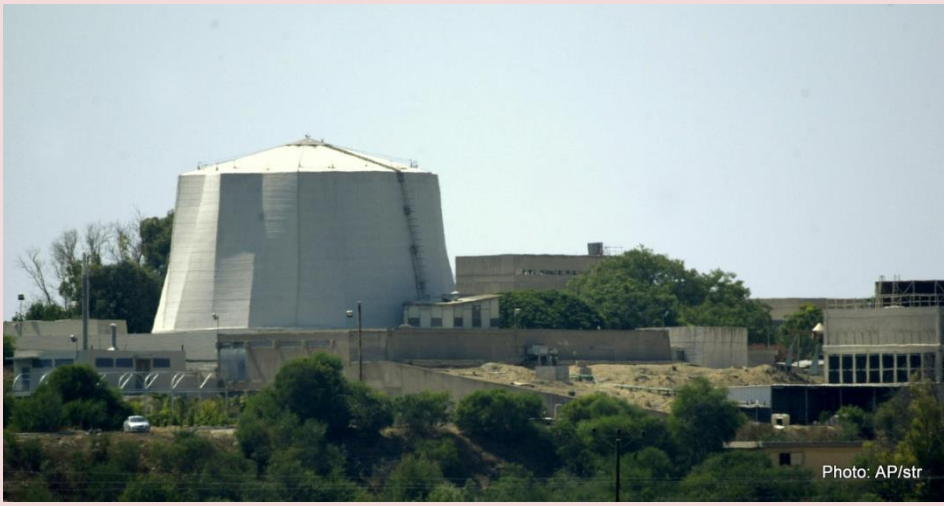
The book is titled after the Israeli nuclear doctrine. The idea is based on the biblical tale of the Israelite judge Samson, who was betrayed and blinded by his lover Delilah. She had stabbed out his eyes after cutting off his magical strength-giving hair while he slept. Helpless, Samson was handed over to his worst enemies the Philistines, who paraded him in their temple.

But rather than submit to them, Samson used the last of his strength to destroy the temple, bringing it down on top of both him and his enemies while he prayed to God, "Let me die with the Philistines."

The idea is that Israeli leaders would rather, as a last resort, set off a nuclear bomb on the small country of historic Palestine rather than submit to their enemies – the Palestinians and other Arabs.

That Israeli military planners titled their nuclear doctrine "The Samson Option," was clearly intended to invoke this psychopathic image among its enemies – but also among politicians in its superpower patron, the U.S. religious Protestant-Americans, well versed in Old Testament Bible stories like Samson, would instantly understand the reference.

And as Hersh recounts, U.S. Presidents from Eisenhower to Kennedy, Johnson and Carter had an ambiguous relationship with Israel's nuclear weapons. Eisenhower – perhaps ironically as a Republican – was the most hostile. But Kennedy and Johnson, while in theory dedicated to "nuclear non-proliferation" in the rest of the world, ultimately decided on a systematic policy of refusing to know about Israel's development of the bomb. In effect, they deliberately shut their eyes to what was going on at the nuclear reactor in the Dimona Desert.



Israel's Sorek nuclear reactor center near the central Israeli town of Yavne.

As Hersh shows, time and again, high U.S. officials learned more and more about what Israel was doing through various intelligence reports. But, time and again, their attempts to bring the facts to their superiors were rebuffed. They quickly learned to let it go.

Modern day proponents of Israeli propaganda in the West – and particularly in the U.K. – attempt to portray their doctrine of Zionism as something progressive and enlightened, rather than the gross form of racist discrimination against the native population that it really is.

Part of this particular tactic – championed by Israeli front organizations in the Labour Party such as the Labour Friends of Israel and the Jewish Labour Movement – is to emphasize the Israeli Labour Party and how it is different to the "right-wing government of Benjamin Netanyahu."

But the reality is that the Israeli Labour Party is just as racist and violent towards the Palestinians and their Arab neighbors as the Zionist right – if not more so considering its actual historical record.

While Israel's "Sampson option" nuclear threat was enthusiastically endorsed by Menachem Begin after his right-wing government came to power in 1977, it was, in fact, the "Zionist left" governments which spearheaded, led, developed and championed Israel's nuclear weapons, bringing the arsenal into existence.

Furthermore, it was Israel's supposed "man of peace," the war criminal Shimon Peres who ushered Israel's "Samson option" into reality.

A mostly forgotten aspect of history is how Israel's "left-wing" Zionist regime in the 1970s collaborated with the vicious South African apartheid regime to discuss nuclear weapons testing in the South African desert.

Seymour Hersh recounts how the Labour "defense" minister Moshe Dayan made a secret trip to Pretoria in 1974 to discuss a possible Israeli nuclear test in the country. Nuclear testing in historic Palestine – a small country – was a lot harder to hide.

(From left) Israeli defense minister Shimon Peres, South African prime minister B. J. Vorster, and Israeli prime minister Yitzhak Rabin, Jerusalem, April 1976. CREDIT: RAHAMIM ISRAELI

Later, in 1976, Yitzak Rabin was Labour prime minister. He was a notorious Zionist officer personally involved in the 1948 massacre and expulsion of Palestinian civilians from Lydda – which resulted in the notorious Lydda death march. During the first intifada, he ordered his troops to "break the bones" of young Palestinian protesters and stone-throwers.

Rabin and his "defense" minister Shimon Peres – both still sometimes bizarrely hailed by politicians in the West as "men of peace" – enthusiastically embraced collaboration with the racist white minority South African regime. The meetings led to the full restoration of diplomatic relations between the two apartheid regimes.

Peres made at least one secret visit to Pretoria to secure military and nuclear understandings between the two regimes. This culminated in a 1976 state visit to Israel of the South African regime's leader B J Vorster – at a time when South Africa was otherwise being internationally shunned.

Israel had no qualms about breaking this global cold shoulder because, as a former Israeli official explained to Hersh:
there is a certain sympathy for the situation of [white] South Africa among Israelis. They are also European settlers standing against a hostile world."
The Vorster trip was internationally condemned. But what is often forgotten now is that Vorster had literally been a South African Nazi.
During World War II, the South African regime was allied with the British government in its war against Nazi Germany (albeit tepidly). But several groups, both Parliamentary and paramilitary, were to varying degrees far more sympathetic to the racist Nazi regime. Many Afrikaaners shared their ideas of white supremacy.
B. J. Vorster – eventually to become the South African Prime Minister that Peres and Rabin gushed over – belonged to one of the most extreme of the pro-Nazi groups – the *Ossewabrandwag*.
As a general in the group's armed wing, Vorster was interned without trial during the war because his group engaged in sabotage intended to help welcome a Nazi regime into South Africa.
According to Brian Lapping's *Apartheid: A History*, the group's armed wing was called the *Stormjaers* – or Storm-troopers: "They adopted the Swastika badge, gave the Hitler salute, threatened death to the Jews and provoked fights with army volunteers."
As it always in history though, Israel and its leaders – even its supposedly "left-wing" leaders – had no qualms about encouraging racism and anti-Semitism, so long as it is perceived to aid their project of colonization in historic Palestine.

***Asa Winstanley** is an investigative journalist living in London who writes about Palestine and the Middle East. He has been visiting Palestine since 2004 and is originally from South Wales. He writes for the award-winning Palestinian news site The Electronic Intifada where he is an associate editor and also a weekly column for the Middle East Monitor.*

Press Release: IT IS NOW 2 MINUTES TO MIDNIGHT

Source: https://thebulletin.org/press-release-it-now-2-minutes-midnight

WASHINGTON, D.C. – January 25, 2018 **–** Citing growing nuclear risks and unchecked climate dangers, the iconic Doomsday Clock is now 30 seconds closer to midnight**, the closest to the symbolic point of annihilation that the Clock has been since 1953 at the height of the Cold War.** The decision announced today to move the Doomsday Clock to two minutes before midnight was made by the *Bulletin of the Atomic Scientists*' Science and Security Board in consultation with the Board of Sponsors, which includes 15 Nobel Laureates.

The full text of the Doomsday Clock statement is available at http://www.thebulletin.org and includes key recommendations about how to #RewindtheDoomsdayClock.
Video from the Doomsday Clock announcement at the National Press Club in Washington, D.C., is available at http://clock.thebulletin.org/ and on the *Bulletin of the Atomic Scientists'* Facebook page at https://www.facebook.com/BulletinOfTheAtomicScientists/.
The statement explaining the resetting of the time of the Doomsday Clock notes: "In 2017, world leaders failed to respond effectively to the looming threats of nuclear war and climate change, making the world security situation more dangerous than it was a year ago—and as dangerous as it has been since World War II. The greatest risks last year arose in the nuclear realm. North Korea's nuclear weapons program appeared to make remarkable progress in

2017, increasing risks for itself, other countries in the region, and the United States. Hyperbolic rhetoric and provocative actions on both sides have increased the possibility of nuclear war by accident or miscalculation …. On the climate change front, the danger may seem less immediate, but avoiding catastrophic temperature increases in the long run requires urgent attention now …. The nations of the world will have to significantly decrease their greenhouse gas emissions to keep climate risks manageable, and so far, the global response has fallen far short of meeting this challenge."

Fueling concerns about the potential of a nuclear holocaust are a range of U.S.-Russian military entanglements, South China Sea tensions, escalating rhetoric between Pakistan and India, and uncertainty about continued U.S. support for the Iran nuclear deal. Contributing to the risks of nuclear and non-nuclear clashes around the globe are the rise of nation-state information technology and internet-based campaigns attacking infrastructure and free elections, according to the statement.

Also highlighted as an overarching global concern: The decline of U.S. leadership and a related demise of diplomacy under the Trump Administration. "… [T]here has also been a breakdown in the international order that has been dangerously exacerbated by recent U.S. actions. In 2017, the United States backed away from its longstanding leadership role in the world, reducing its commitment to seek common ground and undermining the overall effort toward solving pressing global governance challenges. Neither allies nor adversaries have been able to reliably predict U.S. actions or understand when U.S. pronouncements are real, and when they are mere rhetoric. International diplomacy has been reduced to name-calling, giving it a surrealistic sense of unreality that makes the world security situation ever more threatening."

In January 2017, the Doomsday Clock's minute hand edged forward by 30 seconds, to two and half minutes before midnight. For the first time, the Doomsday Clock was influenced by statements from an incoming U.S. President, Donald Trump, regarding the proliferation and the prospect of actually using nuclear weapons, as well as statements made in opposition to U.S. commitments regarding climate change.

Rachel Bronson, president and CEO, Bulletin of the Atomic Scientists, said: "Because of the extraordinary danger of the current moment, the Science and Security Board today moves the minute hand of the Doomsday Clock 30 seconds closer to catastrophe. It is now two minutes to midnight—the closest the Clock has ever been to Doomsday, and as close as it was in 1953, at the height of the Cold War."

Lawrence Krauss, director of the Origins Project at Arizona State University, Foundation Professor at School of Earth and Space Exploration and Physics Department, Arizona State University, and chair, Bulletin of the Atomic Scientists' Board of Sponsors, said: "The current, extremely dangerous state of world affairs need not be permanent. The means for managing dangerous technology and reducing global-scale risk exist; indeed, many of them are well-known and within society's reach, if leaders pay reasonable attention to preserving the long-term prospects of humanity, and if citizens demand that they do so. This is a dangerous time, but the danger is of our own making. Humankind has invented the implements of apocalypse; so can it invent the methods of controlling and eventually eliminating them. This year, leaders and citizens of the world can move the Doomsday Clock and the world away from the metaphorical midnight of global catastrophe by taking common-sense action."

Robert Rosner, William E. Wrather Distinguished Service Professor in the Department of Astronomy and Astrophysics and Physics at the University of Chicago, and chair, Bulletin of the Atomic Scientists' Science and Security Board, said: "We hope this resetting of the Clock will be interpreted exactly as it is meant—as an urgent warning of global danger. The time for world leaders to address looming nuclear danger and the continuing march of climate change is long past. The time for the citizens of the world to demand such action is now: #RewindtheDoomsdayClock."

Sharon Squassoni, research professor of practice at the Institute for International Science and Technology Policy, Elliott School of International Affairs, The George Washington University, and Bulletin of the Atomic Scientists' Science and Security Board, said: "In the past year, U.S. allies have needed reassurance about American intentions more than ever. Instead, they have been forced to negotiate a thicket of conflicting policy statements from a U.S. administration weakened in its cadre of foreign policy professionals, suffering from turnover in senior leadership, led by an undisciplined and disruptive president, and unable to develop, coordinate, and clearly communicate a coherent nuclear policy. This inconsistency constitutes a major challenge for deterrence, alliance management, and global stability. It has made the existing nuclear risks greater than necessary and added to their complexity."

Sivan Kartha, senior scientist at the Stockholm Environmental Institute and co-leader of SEI's Gender and Social Equity Program, and Bulletin of the Atomic Scientists' Science and Security Board, said: "2017 just clocked in as the hottest year on record that wasn't boosted by an El Nino. And that matches what we've witnessed on the ground: the Caribbean suffered a season of historic damage from exceedingly powerful hurricanes, extreme heat waves struck across the globe, the Arctic ice cap hit its lowest winter peak on record, and the U.S. suffered devastating wildfires. And while this was happening, the Trump administration dutifully carried through on the campaign promise of derailing U.S. climate policy, putting avowed climate denialists in top cabinet positions, and announcing plans to withdraw from the Paris climate Agreement. Thankfully, this didn't cause global cooperation to unravel, and other countries have reaffirmed their commitment to take action against climate change."
#RewindtheDoomsdayClock is a major message of the 2018 statement, with the following **action steps among those recommended:**

- U.S. President Donald Trump should refrain from provocative rhetoric regarding North Korea, recognizing the impossibility of predicting North Korean reactions. The U.S. and North Korean governments should open multiple channels of communication.
- The world community should pursue, as a short-term goal, the cessation of North Korea's nuclear weapon and ballistic missile tests. North Korea is the only country to violate the norm against nuclear testing in 20 years.
- The Trump administration should abide by the terms of the Joint Comprehensive Plan of Action for Iran's nuclear program unless credible evidence emerges that Iran is not complying with the agreement or Iran agrees to an alternative approach that meets U.S. national security needs.
- The United States and Russia should discuss and adopt measures to prevent peacetime military incidents along the borders of NATO.
- U.S. and Russian leaders should return to the negotiating table to resolve differences over the INF treaty, to seek further reductions in nuclear arms, to discuss a lowering of the alert status of the nuclear arsenals of both countries, to limit nuclear modernization programs that threaten to create a new nuclear arms race, and to ensure that new tactical or low-yield nuclear weapons are not built, and existing tactical weapons are never used on the battlefield.
- U.S. citizens should demand, in all legal ways, climate action from their government. Climate change is a real and serious threat to humanity.
- Governments around the world should redouble their efforts to reduce greenhouse gas emissions so they go well beyond the initial, inadequate pledges under the Paris Agreement.
- The international community should establish new protocols to discourage and penalize the misuse of information technology to undermine public trust in political institutions, in the media, in science, and in the existence of objective reality itself.

How North Korea Built a Nuclear Arsenal on the Ashes of the Soviet Union

By Simon Shuster
Source: http://time.com/5128398/the-missile-factory/

Feb 01 – Viktor Moisa, a retired rocket scientist, welcomed the North Koreans to his institute in eastern Ukraine just as he would with any other guests. He took them upstairs to the showroom of Soviet satellites and rocket engines, the pride of the institute's collection. Then they went out to the yard, where an array of parts for ballistic missiles were on display. This was in the early 2000s, well before North Korea would test its first nuclear bomb in 2006. So the visitors' interest in missile technology did not arouse Moisa's suspicion. "They came as tourists," he told TIME on a breezy afternoon last fall. "At least that's how they presented themselves."
We were standing in the same yard he had shown to the North Koreans, a paved lot in the city of Dnipro where old missile components are still on show, many of them made at a nearby rocket factory known as Yuzhmash. Guidance systems, fuel pumps and the massive cones designed to hold nuclear warheads at the tip of a rocket all stood in the autumn sun like leftovers from a military rummage sale. Moisa, a cheerful 79-year-old with a puff of silver hair, says he understands in retrospect that his guests from North Korea were probably

spies. “It’s just a guess,” he told me with a smile. “But they were probably dreaming of being a real missile power.”

That dream has since been achieved. Over the past eight months, North Korea has test-launched three rockets capable of striking the U.S. mainland. According to missile experts in the U.S. and Europe, the key components of these rockets are based on Soviet designs, much like those displayed in Moisa’s museum. The latest North Korean breakthrough, the Hwasong-15 missile, was tested in November; experts believe it could be powerful enough to lob a nuclear warhead all the way to New York City.

This feat of engineering, which only a few nations have ever achieved, exposed a long history of failures on the part of the U.S. and its allies. It showed that the strict sanctions they imposed on North Korea failed to isolate its military. It showed that North Korea, a country so poor that its cities go dark at night to save power, was still able to acquire some of the world’s most sensitive technology and hire experts who know how to use it. It showed that, despite decades of nonproliferation efforts, a rogue nation had obtained a weapon capable of starting World War III.

A 1952 nuclear detonation at the Nevada Proving Grounds, which Trump has ordered to prepare for resuming tests.
Photograph by Bettmann Archive/Getty Images

Now, as the world adjusts to the reality of a nuclear North Korea, its young dictator Kim Jong Un has begun to sell this technology abroad. One of his most eager customers is the regime in Syria, which is also under strict international sanctions, according to a classified report that the U.N. Security Council is due to discuss at the end of February. A draft of the report, which was seen by TIME in January, suggests that Russia–Syria’s steadfast supporter–may be turning a blind eye to this trade while stonewalling U.N. efforts to investigate it.

As a permanent member of the Security Council, Russia has always denied such accusations. President Vladimir Putin insisted in December that he has tried to help the West in curtailing the spread of weapons of mass destruction. But in the same breath, he blamed the U.S. for leaving Kim no choice but to go nuclear. “For North Korea, this was the only way of self-preservation,” Putin said. “WMDs and missiles.”

Pyongyang’s weapons program had help from a variety of sources. The regime’s ability to enrich uranium, a key step in building a nuclear warhead, is believed to have come from Pakistan. But launching those warheads across continents would be impossible without Russian or Ukrainian technology, experts have concluded; and that, they say, is what allowed North Korea to become a truly global threat.

Starting in the early 1990s, the North Korean military methodically sought to assemble its weapons program from the ruins of the Soviet missile industry. The regime’s first team of foreign missile experts was recruited inside Russia, and recruitment efforts have continued in the decades since.

Such scientists, including experts in chemical, nuclear and biological arms, are not hard to find in Russia and Ukraine. By U.S. estimates, tens of thousands of them were left jobless after the Soviet Union fell apart. “And there were huge temptations for scientists to take some of their knowledge and potentially sell it elsewhere,” says former U.S. Ambassador to Ukraine Carlos Pascual, who headed the Russia desk at the White House in the late 1990s. “Given what was at stake, and what the cost of that knowledge leaking out might be, I think few had a clear understanding of how important this was.”

The warning signs look painfully clear in hindsight. As early as 1991, and as recently as 2011, North Koreans were caught trying to acquire Soviet-era missile technology, which has not always been kept under lock and key. In 2002, six tons of components for a Soviet ballistic missile turned up in a Ukrainian scrapyard. In another case in Russia last summer, two sets of surface-to-air missiles were found in a garbage dump in eastern Siberia.

Among the experts studying North Korea’s newest rockets, the first to raise the alarm over their Soviet origins was Michael Elleman, a former U.N. weapons inspector and consultant to the Pentagon. He had seen many of these weapons up close over the years. After the fall

of the Soviet Union, he took part in U.S. programs to dismantle some of the largest missiles in the Russian stockpile, and he understood how easy it would be for this technology to leak. "As a proliferation risk," he told me, "this has never really gone away."

That seemed clear from North Korea's latest missile launches. At his think tank in London, the International Institute for Strategic Studies, Elleman compared footage of those launches shown on North Korean television in July with photos of Soviet missile engines dating to the 1960s. One of them appeared to match the RD-250, an outdated but highly reliable machine.

Roughly 200 of these engines still exist, according to Yuzhmash, the missile factory in Dnipro that made them. Nearly all are stored in Russia, but Elleman concluded that if one had been stolen, it would more likely have been from a smaller stockpile in Ukraine. He pointed in particular to Yuzhmash itself, which was known to have been a target of North Korean spies not posing as tourists. Two of them were arrested in Ukraine in 2011 while trying to purchase copies of the factory's designs; both are now serving eight years in prison for espionage.

In some ways, the plant was an obvious target. Founded during World War II to help the Red Army defeat the Nazis, it went on to develop many of the Soviet Union's most powerful ballistic missiles. When TIME visited Yuzhmash last October, we were greeted by the sight of a missile code-named "Satan," which was once capable of orbiting the earth and, at Moscow's command, dropping a hail of nuclear warheads on its target. "This was our pride," says Vladimir Platonov, the factory's in-house historian. "We kept the Americans up at night."

Engineers assemble a rocket at the Yuzhmash factory in eastern Ukraine / Maxim Dondyuk for TIME

But the end of the Cold War made such weapons seem unnecessary. Under pressure from the U.S. and Russia, Ukraine agreed in 1994 to give up the arsenal of nuclear warheads it inherited from the Soviet Union. It also pledged to disarm the ballistic missiles meant to carry those warheads. For the cause of global disarmament, this was a breakthrough. For Yuzhmash, it was a disaster. Thousands of its engineers lost their jobs as the state's demand for missiles dried up. Today the factory makes tractors and trolley buses to make ends meet. What rockets it still builds are intended to launch satellites into orbit. Traditionally, its most reliable customer for these rockets has been Russia. But the conflict that broke out between the two countries in 2014 severed many of the economic ties between Russia and Ukraine, especially in sensitive fields like rocket technology. Yuzhmash fell on even harder times, slashing wages, rationing electricity and laying off the bulk of its staff. "It was a question of survival for us," says Oleg Lebedev, the factory's chief of production.

It's not hard to see how these troubles made the factory more vulnerable to theft, Elleman said. "A small team of disgruntled employees or underpaid guards … could be enticed to steal a few dozen engines," like the RD-250, he wrote in a report that was published in August. These machines, he added, "can be flown or, more likely, transported by train through Russia to North Korea."

The report put Ukraine's government on the defensive, and it scrambled to find all the ballistic-missile engines stored inside the country. In little over a week, it tracked down about a dozen RD-250s, nearly all of them stored at Yuzhmash, and announced that the investigation was closed.

But what the commission did not examine was the risk of the weapons scientists finding their way to North Korea. According to Lebedev, who took part in the investigation on behalf of Yuzhmash, the size of the factory's workforce shrank sixfold between 2014 and 2017. "We're talking about thousands of workers," he says. "Everyone from the welders on the factory floor to the top engineers in our design bureau. We lost them all."

The impact was obvious when Lebedev showed TIME around the missile factory. Its main production hall was almost deserted. About a dozen workers busied themselves inside a few space rockets, each one about the size of a jumbo jet. There was not a computer in sight. All measurements were done by hand, and elderly women in heavy coats noted them down in paper ledgers.

Yuri Simvolokov, a union organizer who has helped Yuzhmash workers stage strikes over unpaid wages, says many of them have gone abroad to find work over the years–not just to North Korea, but also to Iran and Pakistan. "They pay big money over there," he says of these countries, over dinner with a few of his fellow teamsters. "And if they want to build a rocket, they bring our specialists over. It's nothing new."

In fact, the exodus began decades ago. In April 1991, as the Soviet Union was dissolving, a specialist in solid-state physics named Anatoly Rubtsov was approached by a group of North Koreans at an academic conference in Beijing. He had worked for years at a top-secret facility in southern Russia, producing intermediate-range missiles for the Soviet arsenal. But his loyalties seem to have flagged as his nation fell apart, and he became one of North Korea's first known recruits from the former Soviet Union.

The North Korean offer, compared with Rubtsov's prospects back home, must have seemed like a saving grace. As he later explained in interviews with Russian and Western reporters, he was invited to set up a research institute in North Korea and staff it with Russian engineers. Their aim would be to establish the regime's missile program, according to Rubtsov's own published accounts. But it didn't stay secret for long. On Oct. 15, 1992, about 60 of his recruits were detained at a Moscow airport, and news of their plans caused an international scandal. Under pressure from the U.S. and South Korea, the Kremlin agreed to prevent Russian scientists from working on the North Korean missile program.

Pyongyang took this as a sign of betrayal. The regime's relations with the Soviets had always been comradely. The founder of the dynasty that still rules North Korea, Kim Il Sung, was installed in power by the Soviet military in 1945 on the direct orders of Joseph Stalin, and the Soviets provided Kim with the tanks and artillery he used in 1950 to invade South Korea.

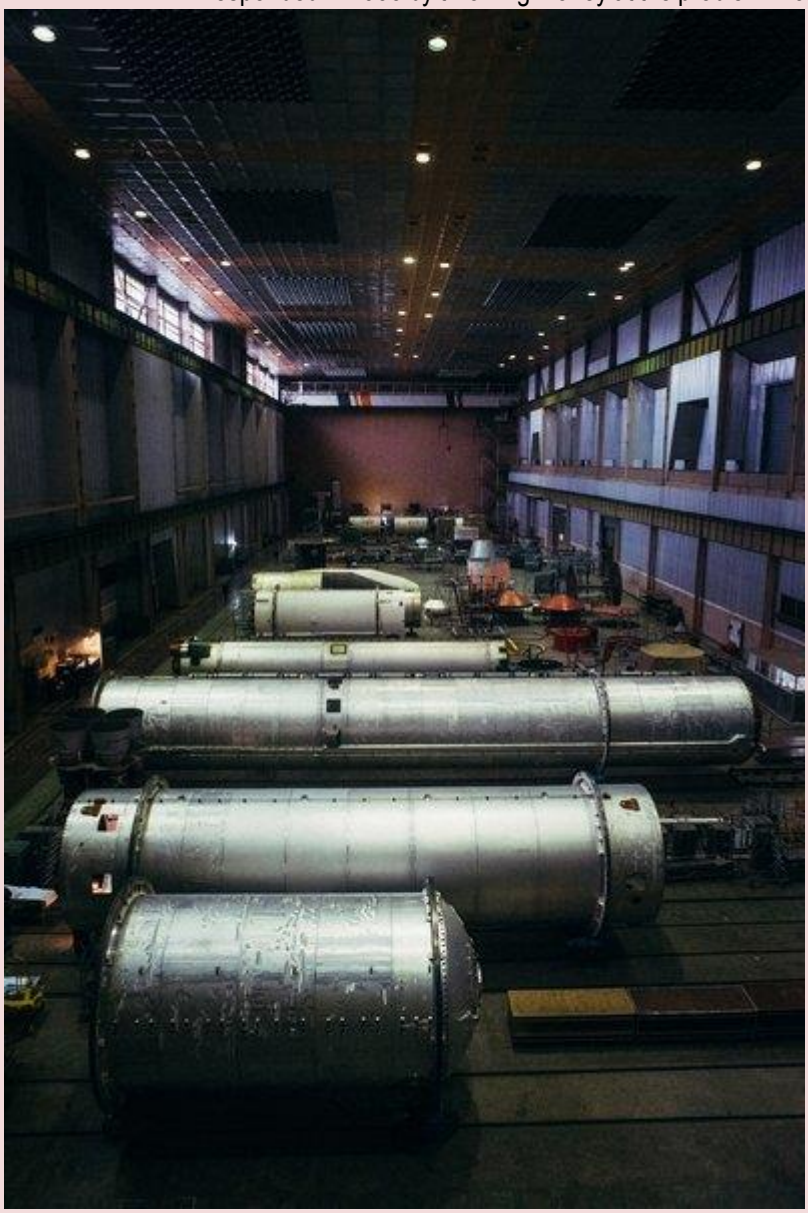
In 1961, Moscow signed a treaty of mutual defense and cooperation with Pyongyang. The agreement obliged the Soviet Union to defend the Kim regime if it ever came under attack. But President Boris Yeltsin and his band of reformers had no intention of honoring that agreement after they took power in Russia in 1991. "We had a different understanding of that responsibility," says Georgy Kunadze, who as Russia's Deputy Foreign Minister for Asia was dispatched to Pyongyang to explain how Russian thinking had changed.

He understood upon arrival that the North Koreans felt abandoned by Moscow. Their subsequent push to build a nuclear weapon was, to a large extent, driven by a resulting sense of insecurity, Kunadze says. During his meetings in Pyongyang, he asked that North Korea stop inviting Russian scientists to build their arsenal for them. "They gave some mild assurances, and that was that," he says.

These assurances meant little in practice, as did Russia's attempts to stop its scientists from going to work where they pleased. In a recent interview, the prominent missile designer Yuri Solomonov admitted that Russian scientists did wind up working on the North Korean weapons program in the 1990s. "They took the bait," he told the state-run newspaper Rossiyskaya Gazeta in December.

Kunadze, who went on to serve as Russia's ambassador in South Korea, says there was little the government could do to stop them. "Russia at the time … was a total mess," he says. "Nobody had any money. The borders were open." And the Russian scientists who traveled to North Korea were not in violation of any Russian laws. "So all we could do was reason with them," says Kunadze. "In the end, it was their choice."

The most immediate impact of the Rubtsov scandal was the alarm it caused in Western capitals, which were forced to realize the potential danger of an unchecked Soviet brain drain. The U.S. and Europe responded in 1993 by throwing money at the problem. Acting in sync with partners in Europe and Canada, the U.S. set up two organizations that year, one based in Moscow and the other in Kiev, with the aim of giving tax-free grants to scientists in Russia, Ukraine and other formerly communist nations.



Rocket parts await assembly at Workshop 97 of the Yuzhmash plant /Maxim Dondyuk for TIME

"Our goal was never to fund science," says Curtis Bjelajac, the director of this operation in Kiev, which is called the Science and Technology Center in Ukraine. "The whole thought process behind the STCU was, It's a handout." By his estimate, between 15,000 and 20,000 experts in weapons of mass destruction were left jobless in Ukraine alone after the fall of the Soviet Union. The number in Russia was likely far higher. Most of them were middle-aged or elderly. So the aim was to keep them busy until they either transitioned to work in the private sector or grew too old to go abroad.

Initially, it worked. At its peak around 2003, the programs in Moscow and Kiev were jointly giving out some $100 million per year in the former Soviet Union. This lifeline did not simply make the difference between a steady income and abject poverty for researchers across the region. It also nurtured their dignity by allowing them to continue working in their fields, says Dimitry Bazyka, one of Ukraine's leading experts in nuclear technology. "It gave us a reason to value ourselves," he says.

His nuclear institute still functions today with Western support, but it is a shoestring affair. Its campus abuts an outdoor bazaar in eastern Kiev full of kebab shops and peddlers of bric-a-brac. The entrance to the compound was so hard to find amid the maze of alleyways and vendors that I ended up climbing over a fence to get inside. No one stopped me.

Scientific institutes in Russia have generally fared better, but their record of security is mixed at best. In the winter of 2011, two bloggers found a way to sneak into one of Moscow's most secretive missile factories, Energomash, and spent several nights photographing its technology. They did not encounter a single security guard. Although highly embarrassing for Russia's missile industry, the incident did not make many headlines in the West, where terrorism and the wars in the Middle East had eclipsed other security concerns in the early 2000s. Public interest in the safety of Soviet-era weapons technology dwindled, as did support for obscure programs like the STCU. "Our donors concluded that the threat from weapons scientists had been contained," says Bjelajac. But Serhiy Komisarenko, one of Ukraine's leading experts in biological weapons, said the money was never enough to cease the flow of personnel. "The temptation to go abroad was always intense," he said. "And it still is."

Whether any of Ukraine's impoverished scientists have gone to work in North Korea is difficult to prove. In eastern Ukraine, one rocket scientist agreed through an intermediary to discuss his work in Pyongyang with TIME, but then changed his mind at the last minute and

refused to meet me. It's hard to blame him. With the renewed concern over technology leaking out, Ukraine's security services have stepped up monitoring of former weapons scientists. Those caught selling their expertise abroad could face charges of treason.

The U.N. panel of experts on North Korea has not found anyone either. In preparing its latest report to the Security Council, the panel sent inquiries to Russian officials, asking for the names and passport numbers of any weapons scientists who might have passed through Russia on their way to Pyongyang. They received no response, according to the draft of their report. In some sense, the silence was typical of Russia's two-faced position on the issue. Throughout his 18 years in power, Putin has supported or acquiesced to U.N. sanctions that have sought to isolate the Kim regime. But he has also offered Pyongyang ways to escape that isolation.

Less than two months after Putin took power in 2000, Russia signed a treaty of friendship and co-operation with North Korea, reviving many of the diplomatic ties that bound Moscow to Pyongyang during the Cold War. A few months later, Putin became the first Russian or Soviet leader ever to pay an official visit to North Korea. "That totally revitalized our relationship," says the former Russian diplomat Konstantin Pulikovsky, who helped steer Moscow's relations with Pyongyang. "The main thing was the personal rapport between the two leaders."

The factory's old missile workshops now produce rockets that launch satellites into orbit / Maxim Dondyuk for TIME

The second tyrant of the ruling dynasty, Kim Jong Il, had an even deeper connection to Russia than did his father. He was born in the Soviet Union, in a dirt-road village called Vyatskoe, where he lived for the first few years of his life under the name Yuri Irsenovich Kim. During that first meeting with Putin, he made no secret of his nuclear ambitions. "He told me back then that they have an atom bomb," Putin recalled during a televised interview last October. "And more than that, he said they could use some pretty basic artillery to launch it all the way to Seoul."

That first impression has not discouraged Putin from building bridges to the Kim regime. Even amid the spate of new missile tests over the past year–and the new U.N. sanctions imposed on North Korea in response–Moscow has continued to assist Pyongyang in crucial ways. A major Russian telecommunications firm provided North Korea with a new link to the Internet in October, relieving it of its dependence on China's fiber-optic cables. Around the same time, North Korean ships were spotted picking up loads of fuel in Russia and, despite a tightening international oil embargo, bringing it back to their homeland.

For Putin, there would seem to be little obvious upside in nurturing this friendship. His country shares a border with North Korea, whose refugees would likely pour over the so-called Bridge of Friendship into Russia if a war ever broke out. A nuclear explosion in the area would also put Russian citizens in serious danger, especially in the nearby city of Vladivostok.
But Putin's thinking goes beyond such immediate considerations, says Kunadze, the former Russian diplomat. Only in the broader context of Russia's rivalry with the West does it start to make sense. "In that context, North Korea is the enemy's enemy," Kunadze says. "It keeps the U.S. distracted. And that's valuable in itself."
Whether it is valuable enough for Putin to arm North Korea directly–or turn a blind eye to smugglers who are seeking to do the same–remains an open question. The most likely players in this trade have so far tended to blame each other: Ukraine insists that Russia is the source of North Korean arms, and Russia points the finger at Ukraine.
As we stood among the old missile parts on display outside his institute in Dnipro, I asked Moisa, the former rocket scientist, whether the blame could be so neatly apportioned. He pointed at an RD-250 engine next to us. It had been in that spot for more than two decades, he said, exposed to the elements, yet it had no obvious corrosion or other damage. "That was the quality of what we made back then," he said proudly. "I can tell you, it took a lot of work, a lot of people and a very long time." In order to clone this technology, he added, the North Koreans would need many years to master the materials and the science involved.
And if the North Koreans had a team of Soviet-trained professionals helping out? Moisa smiled again and looked at the engine. "We could do it in a year and a half."

New radiation detectors developed at Sandia used for New START inspections

Source: http://www.homelandsecuritynewswire.com/dr20180205-new-radiation-detectors-developed-at-sandia-used-for-new-start-inspections

Feb 05 – Sandia National Laboratories designed, tested, and delivered new radiation detection equipment for monitoring under the New START Treaty. Defense Threat Reduction Agency inspectors recently used this equipment for the first time in Russia for a New START inspection.
New START, or the New Strategic Arms Reduction Treaty, is a treaty between the United States and Russia that, among other limits, reduces the deployed nuclear warheads on both sides to 1,550 by 5 February. These limits will be maintained for as long as the treaty remains in force. The treaty includes regular on-site inspections of warheads and delivery systems. These inspections require measurements of objects declared non-nuclear to confirm that they are non-nuclear. Specific neutron-detecting equipment is defined in the treaty for this confirmation.
Sandia Lab says that the first generation of this equipment was designed by Sandia in the late 1980s. It was originally developed for the Intermediate-Range Nuclear Forces Treaty to discriminate between intermediate-range missiles that were prohibited by the treaty and strategic-range missiles that were not prohibited. The first-generation equipment was later approved for START and New START inspections, where the purpose was different but the measurements were the same.
The latest version of the radiation detection equipment is lighter, more rugged and designed to be more sustainable into the future than the original generation of equipment. Just imagine trying to maintain a 30-year-old Walkman in a smartphone world.

"A viable long-term solution" for treaty verification
"It was getting to the point where the team was calling up retired vendors to see if they still had spare parts to repair the old equipment. That wasn't a viable long-term solution," said Dianna Blair, senior manager for Sandia's nuclear security and nonproliferation group.
For equipment designed to last as long as the original equipment, it is important that it be rugged, robust and produce reliable results
The equipment was subjected to numerous tests to ensure its robustness and reliability. Mary Clare Stoddard, manager for arms control technology development at Sandia, said,

"Over the course of all the testing we did about 1,000 tests to stress the hardware. The carrying cases got a little thrashed but the hardware was fine."

After the team of Sandia engineers and physicists designed equipment that would meet the needs of the

treaty with modern parts, they invited some U.S. inspectors to evaluate the prototypes. One of their tests involved rolling a calibrated detector down a steep hill, while in its carrying case, and then verifying that the equipment still gave accurate results. It did.

"The ability of this equipment to make reliable, accurate measurements after being kicked down a hill is pretty amazing," said Stoddard.

In addition to being able to take some hard use, the equipment doesn't need to be calibrated as frequently and is lighter weight. The original set of equipment, containing two detectors and everything needed to set them up and operate them, weighed about 200 pounds and fit in four cases. The new equipment weighs 120 pounds and fits in three cases with wheels. Wheels aren't helpful all the time, but on smooth surfaces they can be quite a boon.

"The Sandia team's balance of technical excellence with pragmatic field-oriented engineering was key to coming up with the right product," said Carolyn Pura, a former Sandia employee who now works at the National Nuclear Security Administration supporting New START.

Russians inspect and approve radiation detectors

Before the new equipment was approved for on-site inspections, Pura and others were involved in lengthy discussions with Russia, our treaty partner. The Russians inspected the new equipment for 30 days as part of the treaty-defined process for approval.

The team fabricated and tested enough equipment to support New START inspections — fewer than 24 sets — made of a mixture of custom and commercially available parts. Though the equipment is essential for treaty inspections, it wouldn't be profitable for a private company to specially design and produce so few systems, Stoddard added.

Sandia notes that in addition to Sandia's long history supporting nonproliferation and treaty verification efforts, the NNSA Office of Nuclear Verification, which funded the work, came to Sandia because of its nuclear weapons expertise. Stoddard said, "This is our mission. We understand how design affects the measurements so we can advise on how to use the equipment in the field."

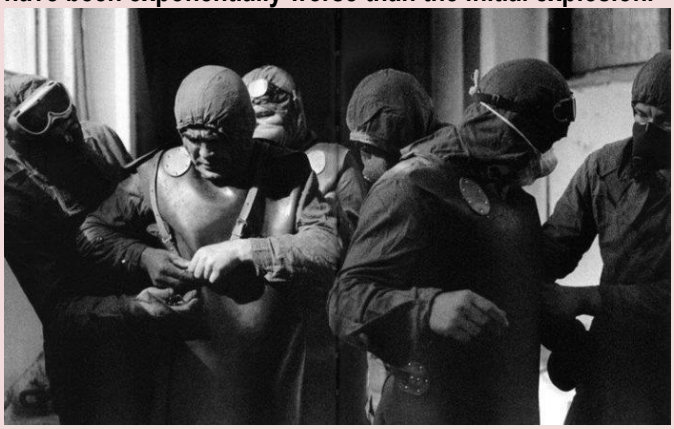
You probably don't know their names, but 30 years ago, they saved Europe.

Source: http://www.upworthy.com/you-probably-dont-know-their-names-but-30-years-ago-they-saved-europe

On April 26, 1986, the world experienced the worst ever nuclear disaster.
It occurred at the Chernobyl Nuclear Power Plant, located in Ukraine. Immediately after the meltdown, dozens died. 30 years later, the number of lives lost to the plant's radiation lies somewhere in the tens of thousands.
If not for the work of three brave men, we may have lost *millions* of lives instead.
10 days after the Chernobyl meltdown, engineers learned of a new threat: nuclear steam explosions.
The plant's water-cooling system had failed, and a pool had formed directly under the highly radioactive reactor. With no cooling, it was just going to be a matter of time before a lava-like substance melted through the remaining barriers, dropping the reactor's core into the pool. If this would have happened, it might have set off steam explosions, firing radiation high and wide into the sky, spreading across parts of Europe, Asia, and Africa.

"Our experts studied the possibility and concluded that the explosion would have had a force of three to five megatons," said Soviet physicist Vassili Nesterenko. "Minsk, which is 320 kilometers from Chernobyl, would have been razed and Europe rendered uninhabitable."

Three brave men volunteered to dive under the plant and release a critical pressure valve.
Just one available man knew the location of the release valve. His name was **Alexei Ananenko**, and he was one of the plant's engineers. He along with fellow engineer **Valeri Bezpalov** and shift supervisor **Boris Baranov** were asked to take on what amounted to a suicide mission.
The men were told they could refuse the assignment, but Ananenko later said, "How could I do that when I was the only person on the shift who knew where the valves were located?"
The men released the valve in time and, in doing so, saved the world from a disaster that would have been exponentially worse than the initial explosion.



Over the following days, more than 5 million gallons of water were released from below the plant. **A report later confirmed that without the work of Ananeko, Bezpalov, and Baranov, a nuclear explosion would have taken place,** turning hundreds of square miles into an inhabitable radioactive wasteland.
By the time the men surfaced from under the reactor, all three were showing signs of severe radiation poisoning. Tragically, none of them survived for more than a few weeks.
Like other victims of the Chernobyl disaster, the three men were buried in lead coffins.

What makes their actions unique in comparison to those of the disaster's first responders is that these men were warned outright of the danger radiation posed — firefighters weren't given any background on radiation poisoning before running to put out the flames. **They're all heroes, but these three men knew they'd die; they did it anyway, saving the lives of hundreds of thousands.**
Their story has been mostly lost to time, with references only popping up in books about catastrophe, danger, and disaster. But the names of these three men shouldn't be forgotten.
Alexei Ananenko, Valeri Bezpalov, and Boris Baranov didn't prevent the Chernobyl disaster; they prevented something much, much worse.
Their story really makes you think about the label "hero." For some, like the three Chernobyl divers, heroics come quietly as the result of a quashed threat. For others, like the first responders at Chernobyl or Fukushima, during 9/11, or in response to other terrorist attacks, heroics are the result of running toward danger so that others may run away from it.

The truth is that heroes are all around us. Teachers, health care workers, and just everyday people are and have the capacity to be heroes in their own right. No capes needed, just a little faith in the human spirit.

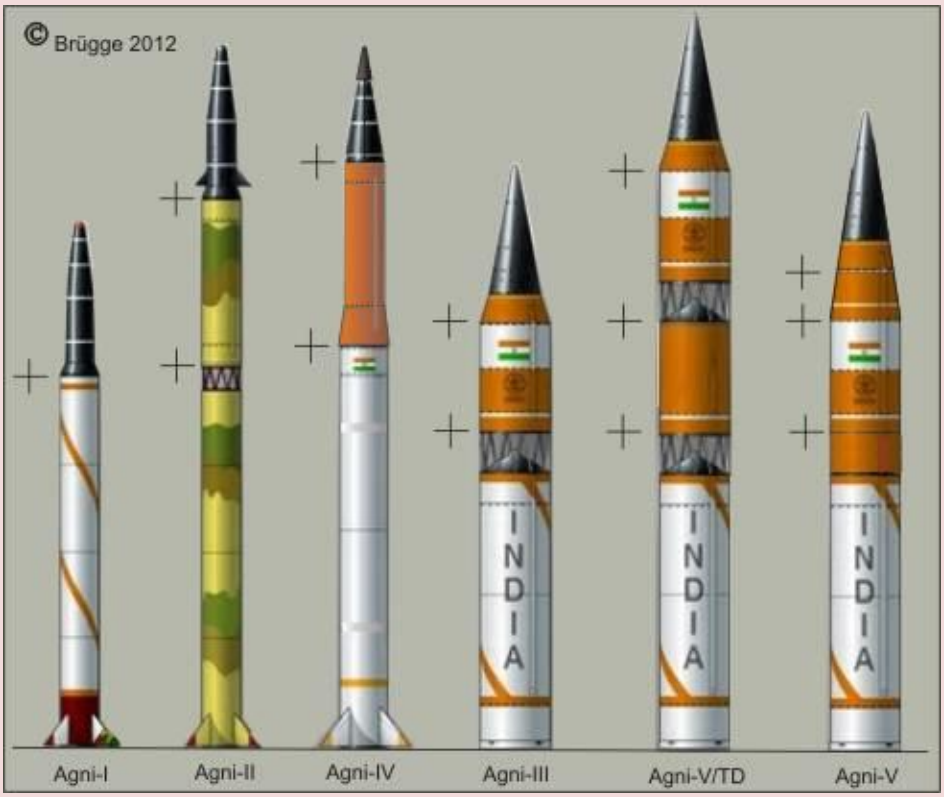
'Pinpoint Accuracy': India Tests Short-Range Nuclear Ballistic Missile

Source: https://www.globalsecurity.org/wmd/library/news/india/2018/india-180207-sputnik02.htm

Feb 07 – India's Strategic Forces Command (SFC) test-fired the Agni-I short-range ballistic missile at their Integrated Test Range in the Bay of Bengal on Tuesday. The **nuclear-capable missile** was fired at 8:30 a.m. local time, and SFC reported that the test was a "complete success."

"The trajectory of the trial was tracked by a battery of sophisticated radars, telemetry observation stations, electro-optic instruments and naval ships right from its launch till the missile hit the target area with pinpoint accuracy," SFC sources told The Diplomat.

The Agni-I was first developed by India's Defense Research and Development Organization (DRDO) in 1989 but didn't enter service until 2004. It is a single-state missile, meaning none of its components detach after launch, and uses solid fuel technology, meaning it can be pre-fueled before being fired, and is thus ready to be used in anger at a moment's notice.



The Agni-I is also equipped with an inertial navigation system, meaning it uses internal systems such as accelerometers and gyroscopes to track its own location, rather than requiring an external guidance system. It has an operational range of up to 560 miles and can carry a warhead as heavy as 5,500 pounds.

Named for the Vedic god of fire, Agni-I is the father of the Agni family of nuclear and nuclear-capable missiles. The newest member of the missile family, the Agni-VI ICBM, is still in development by DRDO. SFC fields approximately 75 Agni-I launchers, and last tested the missile in November 2016.

The aggressive expansion of the Agni program has coincided with worsening relations with New Delhi's primary geopolitical rivals: China and Pakistan. All three nations have experienced strong economic and military growth in recent years, along with increased tensions and border friction.

China and India are the only nations to maintain the "No First-Use" policy, where they pledge not to use nuclear weapons under any circumstances, except as a response to another state using them first. The remaining members of the "nuclear club" opt for the "Mutually Assured Destruction" policy, where they can use nuclear weapons to defend themselves or their allies from invasion.

With the Agni-V three-stage solid fueled ICBM, last tested in January 2018, India also seeks a reliable second-strike capability: the ability to assuredly respond to a nuclear attack with one of their own.

They intend to accomplish this by developing a multiple independently targetable reentry vehicle (MIRV) for the Agni-V, meaning the missile will carry multiple warheads that can strike at multiple targets with a single launch. MIRV-equipped missiles are effectively immune to anti-ballistic missile systems, but India has yet to demonstrate a combat-capable one.
The Agni-IV intermediate-range ballistic missile was also tested in January 2017, and the test was similarly successful. The Agni-VI, once it concludes development, will expand India's nuclear range to cover Australia, Africa and Western Europe.

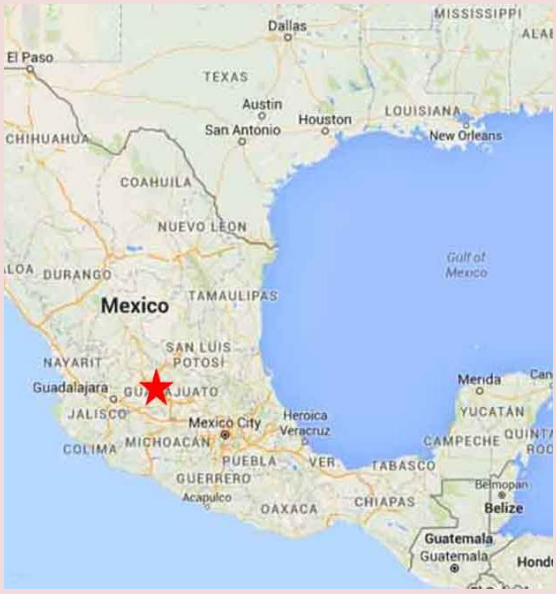
Massive alert in Mexico after radioactive device stolen

Source: https://www.rt.com/news/418408-radioactive-device-stolen-mexico/

Feb 10 – Mexico's interior ministry has issued an alert across seven states following the theft of a radioactive device.

The item in question is a **nuclear densometer** which is used in geotechnical engineering to measure density. It contains radioactive material and there are fears such material could be used to make a *"dirty bomb."*

The theft of the device took place in the city of León in the state of Guanajuata on Thursday morning. It was stolen from a vehicle belonging to an engineering firm. The National Coordination of Civil Protection warned that the material in the device is highly dangerous if removed from its container.
As well as Guanajuata, the ministry issued warnings in Querétaro, Jalisco, Michoacán, San Luis Potosí, Aguascalientes, and Zacatecas. The National coordinator of Civil Protection, Luis Felipe Puente, tweeted a picture showing what the device looks like.



Thieves have successfully got their hands on radioactive material several times in Mexico in recent years.
In April last year, a nine-state alert was issued following the theft of industrial radiography equipment which was filled with Iridium-192, a radioactive element that can cause burns, acute radiation sickness, and death. Similar heists also took place in April 2015 and July 2014.

What is it?

A nuclear densometer is a field instrument used in geotechnical engineering to determine the density of a compacted material. Also known as a *soil density gauge*, the device uses the interaction of **gamma radiation** with matter to measure density, either through direct transmission or the "backscatter" method. The device determines the density of material by counting the number of photons emitted by a radioactive source (**cesium-137**) that are read by the detector tubes in the gauge base. A 60-second time interval is typically used for the counting period. A nuclear densometer is used on a compacted base to establish its percentage of compaction. Before field tests are performed, the technician performs a calibration on the gauge which records the 'standard count' of the machine. Standard counts are the amount of radiation released by the two nuclear sources inside the machine, with no loss or leakage. This allows the machine to compare the amount of radiation released to the amount of radiation received. With the use of a 3/4" diameter rod a hole is created in the compacted base by hammering the rod into the base to produce a hole that the densometer's probe can be

inserted into. The densometer is placed on top of the hole, and then the probe is inserted into the hole by unlocking the handle at the top of the probe. One source produces radiation that interacts with the atoms in the soil, and is then compared to the standard count, to calculate the density. The other source interacts with hydrogen atoms to calculate the percentage of water in the soil. In direct transmission mode, the source extends through the base of the gauge into a predrilled hole, positioning the source at the desired depth. The testing procedure is analogous to burying a known quantity of radioactive material at a specific depth, and then using a Geiger counter at the ground surface to measure how effectively the soil's density blocks the penetration of gamma radiation through the soil. As the soil's density increases, less radiation can pass through it, owing to dispersion from collisions with electrons in the soil being tested. Since the soil's moisture level is partly responsible for its in-place density, the gauge **also contains a neutron moisture gauge** consisting of an **americium/beryllium** high-energy neutron source and a thermal neutron detector. The high-energy neutrons are slowed when they collide with hydrogen atoms, and the detector then counts the "slowed" neutrons. This count is proportional to the soil's water content, since the hydrogen in this water (H_2O) is responsible for almost all the hydrogen found in most soils. The gauge calculates the moisture content, subtracts it from the soil's in-place (wet) density, and reports the soil's dry density.

Radiation: A Primer for Emergency Responders

By Robert Shelton

Source: http://www.fireengineering.com/articles/print/volume-169/issue-11/features/radiation-a-primer-for-emergency-responders.html

An old-school fire lieutenant who worked in a heavily industrialized part of the city was asked what he would do if a hazmat run occurred at one of the factories in his first-due area. He said he would wait for the hazmat team to arrive. I asked what he would do if a viable victim needed help. He said he would still wait for the hazmat team instead of effecting a rescue. That answer violates everything we stand for as firefighters, and I can only assume that his answer was based on a lack of knowledge of the basics of hazardous materials response.

Whenever I have asked firefighters whether they would rather deal with a hazardous chemical or a radiation incident, the vast majority always answered, “A hazardous chemical.” Why? Generally, the chemicals are more dangerous than the radiation sources we may encounter on the street and are more abundant and pose a greater chance of injury or death. Therefore, the reason firefighters answer this way has to be that they lack knowledge on this topic. Every firefighter knows that a lack of knowledge can be fatal; hence, we need to learn as much as possible to be safe when dealing with the transportation or malicious use of a radiation source.

Weapons of mass destruction (WMD) are our reality, and fire departments all over the country must train for them just as we do for fire, emergency medical services (EMS), hazardous materials, technical rescue, and other responses. Recently, I saw this statement on Facebook: “You can’t train too much for a job that can kill you.” So it is with hazardous materials whether they are chemicals, WMD, or radioactive sources. The difference is that we are more likely to be hurt or killed by the chemical than the radiation.

Following is some information that can help you to be street smart when dealing with radioactive responses in the transportation setting. Although the safety principles and practices apply to all incidents, things do change, and our way of going to work must adapt to that specific type of incident when radiation is used as a WMD.

Note: I am not an expert on radiation; however, I have studied the subject and worked with people in the radiation field who have given me the benefit of their experience to better recognize what we are up against. I was confused about radiation and how to respond to these calls, but I have learned the principles necessary for a safe response, and I want to help make radiation responses less of a mystery so we all can go to work with the knowledge to carry out our mandate to protect the public.

Background Radiation

Everyone is exposed to some amount of background radiation; according to the Nuclear Regulatory Commission (NRC), on average an American receives a background radiation dose of about 0.62 rem (Roentgen Equivalent Man/Mammal) each year. A rem is

based on the tissue damage caused by the ionizing radiation a mammal may have been exposed to or may have absorbed. Half of this dose comes from natural background radiation from radon in the air; smaller amounts come from cosmic rays and the earth itself, including some of the foods we eat.
According to the National Council of Radiation Protection and Measurement (NCRP), the largest percentage of exposure comes from naturally occurring sources like radon and thoron. Radon is a natural product of the environment and the principal natural background radiation exposure source in the United States. Thoron is an isotope of radon and the remaining product of decayed thorium. Keep in mind that an isotope is an atom with the same number of protons but differing numbers of neutrons; therefore, isotopes are different forms of a single element.

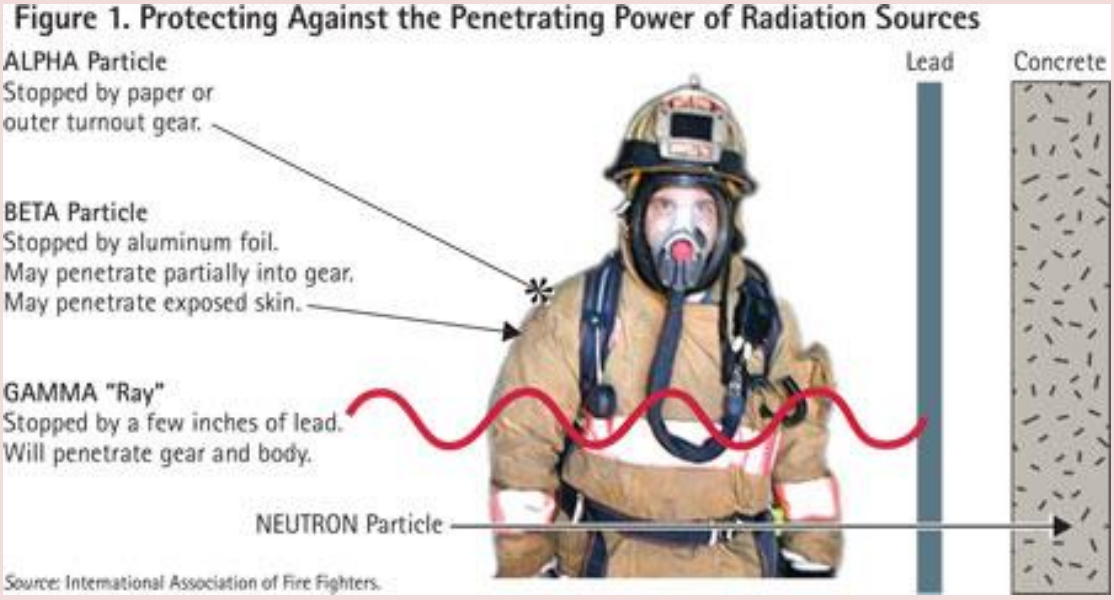
The Basics

What is radiation? On an atomic level, negatively charged electrons are orbiting the nucleus and positively charged protons and neutrally charged neutrons are close to the nucleus. That's basic chemistry and physics. If there are too many or too few neutrons in the nucleus compared to the number of protons in the nucleus, the atom is unstable and gives off energy (radiation) in an attempt to become stable—in other words, radiation is the energy given off by a radioactive material.
When you hear the terms "nonionizing" vs. "ionizing" radiation, think of energy. Nonionizing radiation does not carry enough energy to move electrons from molecules. Examples of nonionizing radiation include ultraviolet, visible light, radio frequencies, microwaves, and infrared, things we are exposed to daily. On the other hand, ionizing radiation has more energy to move those same electrons, and that is where things can become problematic for responders and the public.

Types of Radiation

There are four basic types of ionizing radiation with which we should be familiar. All are different in the energy they possess, how they affect us, and how we can protect ourselves from them.

- *Alpha (α).* It is considered a "particle" because of its mass and weight; it expends energy quickly and thereby can travel only a very short distance, a few inches or so. Also, because of its lack of energy, its penetrating power is negligible. Intact skin; paper; and, obviously, personal protective equipment (PPE) can protect responders from it *externally.* However, when Alpha is inhaled or ingested, it can have a detrimental effect on the body's cells and organs. The primary means of protection is self-contained breathing apparatus as a part of your full PPE. At a working fire, we would never dream of making entry without our breathing air; likewise, when dealing with radiation, we should use *all* of our PPE with SCBA.
- *Beta (β).* It has smaller, lighter particles that possess more energy and can travel several feet. Thick cardboard; plastic; aluminum; and, again, full PPE with SCBA will shield against its penetrating ability. Although Beta can penetrate skin only a fraction of an inch, it can travel several feet in air with higher levels of Beta radiation. It can damage skin and eyes, but it will cause less harm to cells or organs internally because it releases energy over a larger area.
- *Gamma (γ).* This is the type of ionizing radiation with which people are most familiar because it gives superheroes, like the Incredible Hulk, their powers. Unlike Alpha and Beta, Gamma is a ray, electromagnetic radiation in waves of energy with no mass and no electrical charge. It can travel long distances and necessitates more than PPE and SCBA as protection. Lead, steel, and concrete are common mediums of protection against this powerful source of radiation that can significantly damage living cells and tissue.
- *Neutron.* This is the only type that can make other objects radioactive. It can penetrate other materials and can travel great distances in air. Very thick hydrogen-containing materials (such as concrete and water) are necessary to block neutrons. Fortunately for first responders, neutron radiation primarily occurs inside a nuclear reactor. Figure 1 illustrates the penetrating power of radiation sources and the types of protection against them.



Contamination vs. Exposure

How do we become contaminated by radiation? If your organization provides EMS, your emergency medical technicians and medics understand that there is a difference between contamination and exposure. Simply put, contamination is radiation where you do not want it. When a source of radiation gets on or in a person, that person becomes contaminated. If you are in the vicinity of a source and don't get any on you, you are at risk of exposure with the risk ending when you are no longer in the area of the material. You can be exposed and not be contaminated; but if you are contaminated, you will continue to be exposed until the material is removed by means of decontamination.

Contamination may be external or internal, and it is difficult, if not impossible, to remove internal contamination. Internal contamination will affect tissue, cells, and organs and can cause changes in DNA. Decontamination can remove external contamination, depending on the physical state of the radioactive material whether a solid or a liquid.

Responders may encounter Alpha, Beta, and Gamma forms of radiation in transportation incidents. Neutrons should not pose a threat to us in a transportation setting because they are used and generated primarily inside a nuclear reactor, as mentioned previously. This article will focus on those hazards we are most likely to encounter in the course of our work.

Protection and Protective Actions

Protecting first responders is our number-one priority. To this end, two principles work in concert with each other—the radiation model and the acronym ALARA. The radiation model and its concepts apply to *any* event we respond to that could endanger us. The principles of protection are time, distance, and shielding.

Time

The less time spent in the confines of a radioactive material, the less exposure—and, thus, the less chance of contamination by the materials. If personnel can be rotated regularly, the exposure of each individual would be less as opposed to one or two people receiving a large, possibly detrimental dose. At fires, we rotate crews regularly, especially in the warmer or colder climates, to minimize exposure to the elements and complications from that exposure; the same principle applies.

Distance

Of course, the farther away we are, the safer we will be. On a fully involved structure fire with no chance of survivability for victims, going defensive with elevated master streams, deck guns, and so on maximizes distance, thereby increasing the safety factor and protecting us from the heat generated by the fire. Also related to distance is the inverse square law, which states that if you double your distance from the radiation source, you cut the dose by one

quarter. Therefore, if you are dealing with a rad source of 100 millirem/per hour (mR/hr) at one foot, it would be 25 mR/hr at two feet, 6.25 mR/hr at four feet, and so on.

Shielding

Whatever material is available that can block or absorb the effects of the radiation, be it concrete, lead, dirt, the fire apparatus, or PPE, make sure it is between you and the source. In EMS, your gloves, masks, garments, and the like act as shielding from airborne and bloodborne pathogens; again, the principle has already been established for us.

ALARA

ALARA is an acronym that stands for "as low as reasonably achievable," making every reasonable effort to maintain exposures as far below the dose limits as practical, taking into consideration circumstances such as life safety of responders and victims. Time, distance, and shielding in conjunction with ALARA should be used to protect ourselves on all of our runs; radiation runs are no different. We need to use these principles for radiation because in the United States, approximately three million packages of radioactive materials are shipped each year either by highway, rail, air, or water, according to the Nuclear Regulatory Commission (NRC).

Since radioactive materials are shipped in such large quantities and by all modes of transportation, we need to know how they are labeled and packaged for our protection and that of the public. We most likely will encounter rad sources through transportation; and along with the protection principles, there should be some sort of administrative controls that come on the form of shipping information such as placards, labels, and markings.

Placards and Labels for Radioactive Materials

We are all familiar with the trefoil (radiation propeller) and class 7 Department of Transportation (DOT) placards. The placards designate three classes of radiation materials: I, II, and III. **These classes are based on how much external contact radiation is on the package; the greater the number, the higher the surface contact radiation level.**

1. White-I is 0.5 mR/hr or less.
2. Yellow-II is greater than 0.5 mR/hr up to 50 mR/hr.
3. Yellow-III is greater than 50 mR/hr up to a maximum of 200 mR/hr.

The International Atomic Energy Agency (IAEA) and the International Organization for Standardization (ISO) designed a symbol to provide a clearer warning for people not familiar with the traditional symbol. In addition to a black trefoil with waves of radiation streaming from it, the ISO/IAEA radiation warning symbol features a black skull-and-crossbones and a symbol of a man running toward an arrow, away from the radiation (photo 1). This symbol is meant to provide a final warning and is placed only on devices that house radiation sources such as food irradiation and cancer therapy equipment to clearly communicate that dismantling the device presents the risk of death or serious injury. A video from 1987 on an incident that occurred in Goiania, Brazil, relating directly to this signage and how some of the devastating effects may have been avoided is circulating on the Internet; YouTube has a three-minute synopsis of what happened at www.youtube.com/watch?v=dv-87QKy37M.

The International Atomic Energy Agency and the International Organization for Standardization radiation symbol

Other labeling protections for radiation packaging are acronyms such as LSA and SCO. Low specific activity (LSA) materials have limited amounts of radioactivity in relation to the quantity of material being shipped. Radioactive waste and contaminated earth are two examples of LSA. Surface-contaminated objects (SCO) have radioactive material on a surface, but the material is not necessarily radioactive; the product by definition is contaminated (see how things are all related in the world of radiation?). Items like contaminated clothing fall under SCO. This does not cover all of the radioactive packaging labels, but it gives us a starting point for

determining what we may be exposed to. Radiation incidents do occur, but they are almost nonexistent in transportation because of the type of packaging used to ship and transport rad sources.

Radioactive Packaging

Radioactive shipping packages are based on the quantity, the level of radioactivity, and whether the item is a solid or a liquid. In the United States, radioactive packages are one of four types:

- *Excepted Packaging.* An example of excepted packaging would be any radioactive material in limited quantities that has very little hazard risk if released. An example would be smoke detectors that come in a standard cardboard box when shipped or sold. Excepted means that the material doesn't have to have any specific labeling and shipping papers but requires the four-digit UN number as found in the *Emergency Response Guidebook.* Excepted packages also have no requirement for special testing of the packaging material to assess for failure potential.
- *Industrial Packaging.* LSA/SCO shipments of radioactive waste are under specific DOT rules for packaging with the requirements outlined in the *Code of Federal Regulations* (*CFR*) (49 *CFR* 173. 410-412). This type of packaging doesn't allow any measurable or identifiable release into the environment during transport and handling.
- *Type A Packaging.* When it comes to Type A packaging, the concentrations of rad materials are significantly higher. Type A packaging materials are constructed of steel, fiberboard, and wood, but they also have an inner containment of materials composed of metal, plastic, or other materials and then are packed in rubber, polyethylene, or vermiculite. There are testing requirements outlined in the CFR to ensure integrity and shielding of these materials. For first responders, the most common occurrence may be from a car accident where a vehicle is carrying radiopharmaceuticals between medical facilities or labs.
- *Type B Packaging.* This is designed to carry the highest levels of radioactivity in transport, such as spent nuclear fuel and highly radioactive materials like cobalt and high-level radioactive waste. Type B packaging undergoes extremely stringent testing based on the worst-case scenario with the release of materials that would endanger life. A shipping container may weigh several tons but contain smaller quantities of material. The container or cask *must* be that robust because of the radioactive material within. Responders should be able to quickly recognize the shipping containers should they respond to an incident involving radiation sources.

Response to the Incident

You arrive on the scene and have identified the labels/placards used in shipping. You determined from the shipping container approximately how radioactive or dangerous the material is. Just as in any hazardous materials incident, you consult the *ERG* and establish hot, warm, and cold zones as part of incident control and protective actions. A good policy is to use an initial isolation distance of 75 feet in *all* directions and stay upwind and uphill from the event, per the *ERG*. If you have the four-digit UN number or the name of the material, consult the Yellow or Blue sections of the book, respectively. But, of particular importance are the Orange guide pages for protective actions; guide numbers 161-165 are for radioactive materials, and guide number 166 is specific to Radioactive Corrosive materials.

It is important to remember that radiation may not be the only hazard associated with a particular material. There are radioactive materials that are corrosive or water-sensitive as well as being a radioactive source. Radiation is measured in a special way; specific terminology and instrumentation are used. We will touch on only what we need to know to protect us *initially* on the street to stay safe until more qualified personnel arrive on scene. If your organization has a radiation standard operating procedure (SOP), you may have emergency exposure guidelines at your disposal and should adhere to your jurisdiction's policy. If a radiation SOP is not in place, this may be a good time to have a discussion about what can be done to further protect you from the threats posed by the use of radiation at a transportation accident or if used as a WMD.

Depending on the agency, the maximum emergency dose limits for lifesaving by first responders can vary from 25 rem [Environmental Protection Agency (EPA)] up to 100 rem (IAEA). For the sake of perspective, the annual average dose of radiation Americans are exposed to is 0.62 rem, which equals 620 millirem. One important number is 25 rem, which is the acceptable dose for lifesaving for *volunteers* who fully understand the health

implications or 10 rem for the protection of large populations. The results are possibly some short-term effects such as detectable blood changes at 5 rem or a definite blood change at 25 rem, but again with no serious injury. The EPA guideline for *maximum* dose to emergency workers volunteering for lifesaving work is 75 rem with the possibility of Acute Radiation Sickness (ARS) within a few hours. Hallmarks of ARS at this dose are nausea, vomiting, diarrhea, fatigue, and reduction in resistance to infection.

Common Monitoring Devices

You don't need to be a radiation or a hazardous materials specialist to use some of the monitoring devices available. Many departments have monitoring devices on their rigs, in their EMS bags, or in the form of personal devices they wear on the work uniform. A personal radiation detector (PRD) is a small pocket-sized device that sounds an alert in the presence of radiation. In general, it alerts you to the presence of a radioactive material, giving you a point of reference for protective clothing and establishing control zones. However, they do not identify the source, the dose rate, or how much of an exposure was given over a certain period of time.

Dosimeters are small pager-like devices that measure personal radiation doses. The dosimeter tells you the total amount of rad (radiation absorbed dose) you received. There are different types of dosimeters; each has pros and cons. Your agency should investigate which type would best fit your needs or if you need one at all. Numerous brands of monitoring devices are on the market.

Electronic Resources

We live in the age of smartphones and tablets that have numerous applications to assist us during a radiological event. A few (there are many more) I have come across and used are WISER (Wireless Information System for Emergency Responders) by the U.S. National Laboratory of Medicine; REMM (Radiation Emergency Management) by the U.S. Department of Health and Human Services; and RAD Responder, a collaboration of the Federal Emergency Management Agency, Department of Energy/National Nuclear Security Administration, and the EPA. All are useful when responding to hazardous materials incidents involving radioactive materials.

Educational Opportunities

There are also classes you can attend for free; room, board, and travel are completely paid by the federal government. The classes are offered by the following organizations: Counterterrorism Operations Support Center for Radiological/Nuclear Training in Las Vegas, Nevada; Security and Emergency Response Training Center in Pueblo, Colorado; and Centers for Domestic Preparedness in Anniston, Alabama. Each has excellent classes in radiation and WMD with top-notch instructors and real-world hands-on practical scenarios using live radiation sources. I attended all of them more than once. Even though I had to use my personal time from my job, it was well worth it.

Wrapping Up the Mystery

A mystery sometimes cannot be solved regardless of the resources at your disposal. Radiation is not a mystery at all, and we have the tools and resources to make it completely understandable. Learning about radiation takes a willingness to learn the basics, put forth some effort, and maybe do some studying to grasp what you need to know to be safe.

Hopefully, this article will spur some discussion in departments where training on or an understanding of radiation response is lacking. Hazardous materials, including radiological materials, are all around us and are shipped on a daily basis. Chemicals pose the greater threat of the two, but make no mistake about it: Mishandling a rad will kill you. But, if we know what we need to know, we can make a safe response.

Robert Shelton is a 25-year veteran of the fire service serving in various capacities including firefighter, hazmat specialist, rescue technician, and paramedic for a career fire department in southwest Ohio. He is the president of and lead instructor for Life-Line Solutions Safety Training and Consulting and a former FDIC classroom instructor on education methodology and hazmat response.

EDITOR'S COMMENT: The yellow highlighted text is dedicated to a colleague (fireman) from Spain insttisting that in case of a dirty bomb "we go in, no matter what". It is the same attitude that killed may of New Yorks's finest firefighter during the 9/11 incident.

IAEA to Cooperate with Japan on Nuclear Security at 2020 Olympic Games in Tokyo

Source: https://www.iaea.org/newscenter/pressreleases/iaea-to-cooperate-with-japan-on-nuclear-security-at-2020-olympic-games-in-tokyo

Feb 07 – The International Atomic Energy Agency (IAEA) and the Government of Japan signed an agreement today aimed at enhancing nuclear security measures for the summer Olympic Games and Paralympic Games in Tokyo in 2020. The agreement follows previous IAEA support to major public events, including the 2016 Olympic Games in Rio de Janeiro and the 2012 European soccer championship in Poland and Ukraine.

IAEA Director General Yukiya Amano and Japanese Foreign Minister Taro Kono presided over the signing ceremony at the Agency's headquarters in Vienna. Practical Arrangements outlining the planned cooperation were signed by IAEA Deputy Director General Juan Carlos Lentijo, head of the Department of Nuclear Safety and Security, and H.E. Mitsuru Kitano, Japan's Ambassador to the International Organizations in Vienna.

"The IAEA has extensive experience in supporting Member States on nuclear security for major public events," Amano said at the ceremony. "The Agency welcomes the cooperation to support the Olympic and Paralympic Games in Tokyo, and is already cooperating with Japan by sharing the experiences of Member States which previously hosted the Olympics."

The details of the cooperation will be decided in due course, but the possible areas of cooperation include the IAEA offering Japanese authorities training courses, workshops, technical visits and exercises related to nuclear security, hosting preparatory technical meetings and lending supplementary radiation detection equipment. The IAEA and Japan may also exchange information related to nuclear security events as appropriate and through the cooperation, the IAEA will also benefit from Japan's good practices on nuclear security.

"The IAEA has vast knowledge and experience in supporting preventive measures against nuclear terrorism in international sport events," Kono said. "I warmly welcome the signing of the Practical Arrangements with the IAEA on cooperation in this area for the Tokyo 2020 Olympic and Paralympic Games."

In August last year, Japan hosted a regional workshop on nuclear security measures, attended by countries preparing to stage major public events. During the workshop, experiences related to nuclear security were shared, including on the implementation of measures undertaken at previous Olympic Games.

Last month, Japan participated in an IAEA Technical Visit to the Super Bowl of the U.S. National Football League in the city of Minneapolis, which enabled participants to review contemporary nuclear security measures implemented for this annual sporting event.

The IAEA serves as the global platform for strengthening nuclear security and assists Member States to prevent, detect and respond to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material or radioactive substances.

The Agency supports Member States in planning and preparing for nuclear security as part of overall event security. Last November, the IAEA and the Government of Panama signed Practical Arrangements to strengthen nuclear security measures for World Youth Day 2019, a week-long event for young Catholics that Pope Francis is expected to attend. The IAEA was also involved in efforts to ensure nuclear security at other major public events, including the Olympic Games in Beijing in 2008 and the World Cup soccer tournaments in Germany (2006), South Africa (2010) and Brazil (2014).

Why North Korea and Iran get accused of nuclear collusion

By Jim Walsh

Source: https://thebulletin.org/why-north-korea-and-iran-get-accused-nuclear-collusion11504

Feb 17 – Iran and North Korea are often rhetorically linked, most famously in President George W. Bush's 2002 speech in which he labeled them part of an "axis of evil." In practice, however, they have been largely treated as separate challenges for American foreign policy. There are good reasons for this. The Islamic Republic of Iran and the Democratic People's Republic of Korea are in different regions, have different economies and political systems, and affect different sets of US allies.

Still, there are analysts and commentators who worry that the axis of evil is not simply a list of bad actors, but instead a *team*, whose members cooperate and assist each other. In public discourse, suspicions and accusations of Iran-North Korea cooperation are raised and then recede, only to return again when one or both countries are in the headlines. Recent allegations have run the gamut from speculation about new political ties between the two countries to claims that they are building a nuclear weapon together.

What are we to make of these allegations? Are Iran and North Korea in cahoots? As it turns out, while there are good reasons for suspecting cooperation between the two, the actual record is rather modest, limited to an earlier period of missile trade. There is no evidence of collaboration on nuclear weapons, despite numerous claims in the media. The prospect of future cooperation appears even more unlikely.

The logic of cooperation

At first glance, it would seem that Iran-North Korea military or even nuclear cooperation makes "sense." Both nations face the United States as an adversary, and both have been subject to US and international sanctions. If my enemy's enemy is my friend, then Iran and North Korea should be best friends forever. In addition, both Pyongyang and Tehran have demonstrated a willingness to cooperate in secret with foreign partners. Both countries received illicit assistance from the network founded by Pakistani nuclear physicist A. Q. Khan, and North Korea sold a nuclear reactor to Iran's neighbor and ally Syria. Finally, both Iran and North Korea view missiles as a vital defense need (though for different reasons), and both have had clandestine nuclear weapons efforts.

While this logic seems to suggest that Iran and North Korea are meant for each other, the record of the last three decades points to a different conclusion.

Soon after the Iranian revolution ushered in the country's current system of government in 1979, Tehran and Pyongyang did cooperate on missiles. During the Iran-Iraq War in the 1980s, Saddam Hussein rained missiles down on Iranian cities. North Korea provided Iran with ballistic missiles so that it could respond in kind. That cooperation continued into the 1990s but began to taper off by the end of the decade. As missile-defense expert Michael Elleman observed in 38 North,

> *...interviews with Russian and Ukrainian specialists aiding the Iranian missile program during the late-1990s suggest that cooperation between Pyongyang and Tehran was isolated and not comprehensive. Iran's compartmentalisation of the missile programs would have impeded deep technical collaboration with North Korea, if not preventing it altogether.*

The US intelligence community offered a somewhat different assessment, suggesting that missile cooperation continued into the 2000s. In 2006, Iranian officials acknowledged that they had received assistance from North Korea in the past, but said they had now established an indigenous program. By 2013, US Defense Department reports referred to Iran-North Korea missile collaboration in the past tense, and in early 2016, Director of National Intelligence James Clapper testified that "Of late... there has not been a great deal of interchange."

On the nuclear front, there appears to have been no cooperation. Period. As the Congressional Research Service concluded in 2016, "no public evidence exists that Iran and North Korea have engaged in nuclear-related trade or cooperation with each other." Indeed, neither the US intelligence community, nor the International Atomic Energy Agency, nor the UN Panel of Experts set up to support

sanctions against North Korea has ever made such a claim. Likewise, virtually no journal article in the scholarly literature has suggested nuclear collaboration between Pyongyang and Tehran.

Unreliable sources

So where do these allegations come from? Unsubstantiated media reports. In preparation for Congressional testimony on Iran-North Korea collaboration, I reviewed some 76 media reports covering a span of 11 years, from 2005 to 2015. About a third of those were from media that most observers would associate with a particular ideological point of view, like the *Free Beacon*, the *Tower*, and *Anti-War.com*. Forty-two of these reports—more than half—were published in 2014 and 2015, as opponents of the Iran nuclear deal attempted to kill the agreement. In no case did these media reports provide any actual evidence for the allegations. It is worth noting in this context that the Directorate of National Intelligence concluded Iran had halted its nuclear weapons program in 2003, so claims of nuclear cooperation after that date would be especially questionable.

Why wasn't there more of an Iran-North Korea partnership? One cannot know for sure why these two international outcasts did not cooperate more on missiles or at all in the nuclear domain. Someday, Iranian or North Korean officials might explain their reasoning, but in the meantime one can only speculate.

First, these are very different countries, in different geo-strategic positions, with very different national security objectives. As has become clear, North Korea's main goal for its missile program is to develop an intercontinental ballistic missile (ICBM) capable of delivering a nuclear warhead to the United States. With that capability, the North would hope to deter a US attack and possibly drive a wedge between the United States and South Korea.

By contrast, Iran's objectives were (and are) more limited and local, as Greg Thielmann recently pointed out on Lobe Log. It wanted to acquire a nuclear weapons capability, but as the US Director of National Intelligence repeatedly testified, had not made the political decision to build nuclear weapons. Iran also worried more about regional adversaries—Iraq, Israel, Saudi Arabia—and what it saw as a need to deter countries in the region with superior air power or missile capabilities. Put another way, it did not want to again find itself defenseless as it did during the Iran-Iraq War. Accordingly, Tehran has focused on shorter range, conventional ballistic missiles.

Second, the two countries occupy different positions in international politics. North Korea appears to relish its role as international bête noir, flaunting its nuclear aspirations and engaging in over-the-top rhetoric (only recently matched by another world leader). Iran, on the other hand, consistently denied that it was pursuing nuclear weapons. The denials were false, but they demonstrate the very different ways these two countries approached the same issue. This initial difference deepened in the wake of the Iran nuclear talks, a diplomatic process—beginning in 2013 and culminating with the Joint Comprehensive Plan of Action, or JCPOA, in 2015—meant to demonstrate that Iran was not pursuing nuclear weapons and to return the Islamic Republic to the community of nations. It would be odd for Iran to have signed up for all the restrictions and surveillance measures in the nuclear agreement if it intended to cheat with the North Koreans.

Finally there is an issue of risk, particularly for Iran. Iran and North Korea are the most-watched countries in the world. What were the odds that these two countries in different parts of the world could secretly collude without being caught? Could Iran tolerate the risk that a North Korean defector might spill the beans, or that the Pyongyang regime itself might collapse of its own weight, thus exposing an illicit relationship? In today's international context, a Tehran-Pyongyang secret alliance would carry high risks with little benefit.

Motivated to mislead

Despite the ongoing absence of any evidence pointing to nuclear cooperation between Iran and North Korea, the claims continue. Why?

Perhaps one clue can be found in the sources and timing of the allegations. One might expect that accusations of Iran-North Korea collusion would show up in Asia, in particular from South Korean and Japanese sources. But that is not the case. Virtually all the claims originate in the United States and the Middle East. When the occasional claim does emanate from Asia, it invariably turns out to be an accusation by a US or Middle Eastern source that is being reprinted in the Asian press.

The timing of accusations is also notable, as they correlate quite strongly with the timing of domestic political fights in the United States

over Iran policy. We see these allegations almost exclusively when the Iran nuclear deal is in the news and being attacked by its opponents.

In short, it would appear that these claims are more about politics than facts. If that assessment is correct, then we should expect outlandish and baseless accusations to continue, especially at moments when the Iran nuclear deal is most vulnerable, for example at the three-month intervals when the US president is required by law to certify to Congress that Iran is in compliance with the JCPOA. The next certification deadline is in April.

Of course someday, under different conditions, Iran and North Korea might collaborate on a nuclear weapons program. Prudence would therefore dictate that American policymakers keep watch for signs of such cooperation. Ironically, the most likely scenario for such collaboration would be if the JCPOA opponents get their wish, destroy the nuclear agreement, and pursue a policy of regime change against Iran. Then their dire warnings may finally be more than politically motivated mudslinging. They could then take "credit" for leading us down a path that produced the very outcome they had warned against.

Jim Walsh *is a senior research associate at the Massachusetts Institute of Technology's Security Studies Program. His research and writing focus on international security, in particular topics involving nuclear weapons, the Middle East, and East Asia. He is the international security contributor to the NPR program "Here and Now," and his comments and analysis have appeared in the* New York Times, *the* New York Review of Books, *the* Washington Post, *the* Wall Street Journal, *ABC, CBS, NBC, Fox, and numerous other national and international media outlets. He received his PhD from the Massachusetts Institute of Technology and has taught both there and at Harvard University.*

Khamenei military adviser: West uses lizards to spy on Iran's nuclear program

Saying that their skins absorb "atomic waves", a top military adviser to Iranian Supreme Leader Ayatollah Ali Khamenei charged that Western countries use "lizards, chameleons" to spy on Iran's nuclear program. Hassan Firuzabadi, a former chief-of-staff for Iran's army, said that the spy lizards were released in various places in Iran to find out where inside the Islamic republic of Iran we have uranium mines and where we are engaged in atomic activities.

Quicker response to airborne radiological threats

Source: http://www.homelandsecuritynewswire.com/dr20180222-quicker-response-to-airborne-radiological-threats

Feb 22 – Researchers from North Carolina State University have developed a new technique that uses existing technologies to **detect potential airborne radiological materials in hours instead of days**.

"We wanted a rapid way of detecting radiological aerosols that are usually associated with the production of dirty bombs or other radiological weapons," says Joseph Cope, a Ph.D. student and fellow with the Consortium for Nonproliferation Enabling Capabilities (CNEC) at NC State and lead author of a paper on the work.

NCSU notes that at present, emergency responders who are characterizing potential radiological risk need to take an air sample and ship it to a radiochemistry lab after preliminary screening analysis. The process means it can take days or weeks to get quality results that authorities can use to make informed decisions.

"We've found a way that repurposes existing tools, and can give first responders quality information in as little as two hours," Cope says.

"The more time you have, the more precise the data becomes – but our approach allows the authorities to make decisions about evacuating the area, etc., based on defensible information," says Robert Hayes, an associate professor of nuclear engineering at NC State and co-author of the paper.

The new approach involves using a radiation detector to take multiple periodic measurements of an air sample for at least two hours. The measurements are then run through a computer model that uses the data to estimate the potential worst case scenario regarding "transuranic" activity in the area.

Transuranic elements have an atomic number at least as high as uranium. In general, these are elements that can be used to create radiological weapons.

"Providing the authorities with a conservative estimation method of transuranic activity allows them to make informed decisions, based on robust data and analysis, as soon as possible," Cope says.

"This approach provides additional rapid characterization capability for emergency responders to radiological events, enabling further optimization of limited resources," Hayes says.

The paper is published in *Health Physics Journal*.

— Read more in S. Joseph Cope and Robert B. Hayes, "Preliminary Work Toward a Transuranic Activity Estimation Method for Rapid Discrimination of Anthropogenic from Transuranic Activity in Alpha Air Samples," Health Physics Journal (December 2017)

First woman in history takes helm of US nuclear weapons arsenal

Source: http://www.washingtonexaminer.com/first-woman-in-history-takes-helm-of-us-nuclear-weapons-arsenal/article/2649778

Feb 22 – Energy Secretary Rick Perry on Thursday swore in the first woman in history as head of the nation's nuclear weapons arsenal.

Lisa E. Gordon-Hagerty was sworn in as administrator of the National Nuclear Security Administration, which under President Trump's fiscal 2019 budget proposal would comprise nearly half of the Energy Department's funding.

"I am especially proud of the fact that she is the first woman in history to lead the NNSA and look forward to working together to address the administration's goal of modernizing our nuclear security enterprise," Perry said.

Gordon-Hagerty has background in national security and combating weapons of mass destruction. She served as president of Tier Tech International Inc., which the Energy Department described as a small business owned by disabled veterans that provides "professional expertise to combating weapons of mass destruction terrorism worldwide."

Tier Tech was founded in 2003, the same year as the U.S. invasion of Iraq. The firm provides consulting services to clients seeking to stop or respond to chemical, biological, radiological, nuclear terrorism global on land or at sea, according to the firm's website.
Gordon-Hagerty was also president and CEO of the consulting firm LEG Inc., which focuses on national security issues. She also served prior administrations in senior posts that included membership on the National Security Council, and began her career as a health physicist at the Energy Department's Lawrence Livermore National Laboratory.
The lab houses the Weapons and Complex Integration Directorate, which is in charge of ensuring the nation's remaining nuclear weapon "deterrent remains safe, secure, and reliable," according to the lab's website.

The quest to build radiation-resistant humans

By Keith A. Spencer
Source: https://www.salon.com/2018/02/25/the-quest-to-build-radiation-resistant-humans/

Feb 26 – It turns out that our atmosphere is really important. (Surprise!) No, not just because we have to breathe. The thin layer of (mostly) oxygen and nitrogen that girds Earth also serves as a buffer zone for highly charged particles — gamma rays, X-rays, cosmic rays and their ilk — which constantly bombard our world. That's because the cosmos is an energetic place; somewhere out there, there are physical processes occurring that are far more energetic than those happening on Earth. Yet as said photons and particles scream through the upper atmosphere, they almost always evaporate into more harmless things. Think of our atmosphere as the sand pit that the long-jumper lands in, slowing and buffering their fall.
It's a good thing, too, that we have this atmospheric buffer zone. Organisms don't do that well when exposed to the unprotected glow of space. NASA institutes a "career limit" for radiation exposure for its astronauts — specifically, that limit is 800 to 1,200 millisieverts a unit of ionizing radiation dosage. For context, the average American is exposed to around 6 millisieverts of radiation a year, from natural exposure to things like radon gas and granite countertops, and unnatural exposure to things like medical X-rays.
Since life as we know it evolved on a planet well-shielded from the radiation of space, organisms aren't very adept at surviving without this shield. Any kind of novel natural resistance, including to radiation, can and does take eons to evolve. There are peculiar exceptions, however. Case in point: A Science News article from 2014 described how most organisms in the Chernobyl Exclusion Zone suffered deleterious effects from the high radiation levels, but there were a few exceptions in some bird populations. An academic article in the journal Functional Ecology noted that some birds had developed radiation resistances such that their bodies reacted in the opposite manner than expected. "Studies of birds and other taxa including humans show that chronic exposure to radiation depletes antioxidants and increases oxidative damage," the authors wrote, describing the typical effects of radiation on organisms. Conversely, researchers "found a pattern radically different from previous studies in wild [bird] populations" near Chernobyl. With this subset, researchers noted that as background radiation increased, "oxidative stress and DNA damage decreased." "Thus, when several species are considered, the overall pattern indicates that birds are not negatively affected by chronic exposure to radiation and may even obtain beneficial hormetic effects following an adaptive response," they wrote.
The idea that animals could not only adapt to radiation but potentially even gain a beneficial reaction to it is a clue in the biological puzzle as to how humans might adapt to high-radiation environments — such as poorly shielded spacecraft or a foreign planet or moon with a thin atmosphere or no atmosphere. Radiation protection is an unsolved problem in space travel. Hence, a new paper published in the journal Oncotarget ("onco" as in oncology, the study of cancer), titled "Vive la radiorésistance!: converging research in radiobiology and biogerontology to enhance human radioresistance for deep space exploration and colonization," presents itself as a roadmap of

sorts toward protecting humans from the off-world radiation levels.

"While many efforts have been made to pave the way toward human space colonization, little consideration has been given to the methods of protecting spacefarers against harsh cosmic and local radioactive environments," write the co-authors, who include researchers in biophysics, biomedicine, computer science and radiobiology. "Herein, we lay the foundations of a roadmap toward enhancing human radioresistance for the purposes of deep space colonization and exploration."

There is no single path toward "enhancing human radioresistance," as the writers put it. Their roadmap consists of a multi-pronged approach that includes "radioprotective mechanisms," gene therapy, "the substitution of organic molecules with fortified isoforms," and "methods of slowing metabolic activity while preserving cognitive function." The latter two methods are perhaps the most sci-fi: one way of slowing metabolic activity might be to go into "stasis," a trope common to many science fiction books and films like "Alien."

The Oncotarget article is as interesting scientifically as it is politically. Science is an inherently collaborative enterprise, as is a civilization-wide intensive effort such as space colonization — an effort that is not, strictly speaking, purely scientific, but more of an engineering and political doctrine. For this pessimistic political moment, the Oncotarget paper is rare expression of political optimism: the notion that humans might prepare to endeavor, communally, towards the goal of preparing our bodies for the rigors of space travel.

Keith A. Spencer *is a cover editor for Salon. A former astrophysics researcher and high school science teacher, his writing has appeared in* Dissent, Jacobin, *and* McSweeney's Internet Tendency. *He is the former editor-in-chief of* The Bold Italic. *His book, "A People's History of Silicon Valley," is coming out in 2018 from Eyewear Press.*


CBRNE-Terrorism Newsletter
W
O
M
D
Explosive
News

New high temperature calibration gas generator to reach 200 degrees C for use with low volatile chemicals and explosives

Source: www.owlstoneinc.com

Owlstone is excited to announce the planned launch later this year of our "**high temperature gas calibration generator---the VOVG-HT**." The VOVG-HT will be the first calibration gas generator to reach 200 degrees C, making it an ideal solution for the generating NIST traceable, repeatable and accurate concentrations of **low volatile chemicals and explosives**. (Note: Current calibration generators in the market typically reach up to 100 to 150 degrees C.) – *more info in the March 2018 issue.*

Mine explosion on civilian vehicle central Mali kills 26

Source: https://www.reuters.com/article/us-mali-security/mine-explosion-on-civilian-vehicle-central-mali-kills-26-idUSKBN1FE251

Jan 25 – **A landmine explosion blew up a civilian passenger vehicle in central Mali on Thursday, killing 26 people and wounding several others, state TV reported.**

The vehicle had crossed the volatile border with neighboring Burkina Faso, where militants loyal to Islamic State are known to operate, when it ran over the mine, Malian army spokesman Colonel Diarran Kone said.

State TV said many of the dead and wounded in the explosion, which took place by the village of Boni, not far from central Mali's medieval Islamic city of Mopti, once a popular tourist spot, were Burkina Faso nationals.

In the past three years, Islamist groups that had long been destabilizing the thinly populated desert north of Mali have swept south into its wetter, more populated central regions, exploiting local conflicts to spread jihad.

That has shifted the battlefield closer to the more prosperous south and capital Bamako, raising concerns for the security of a presidential election expected between July and November.

In a separate incident, the Malian military said its forces came under attack in the town of Youwarou, also near Mopti, but that they had repelled it.

"They neutralized seven terrorists and recovered equipment abandoned by the assailants," it said in a statement.

Mali and its western neighbor Senegal plan to deploy 1,000 troops soon in an operation to pacify central Mali and contain jihadists who had previously been confined to its Saharan expanses in the north.

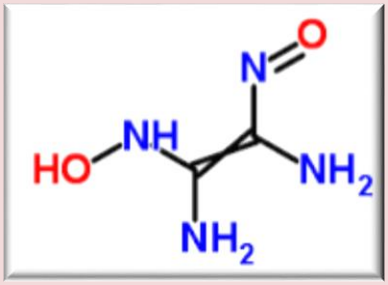
But analysts doubt they will be able to do so purely through military means. The Islamists exploit the grievances of Fulani cattle herders and their disputes with local farmers over access to grazing lands.

Periodic crackdowns on suspected jihadists have therefore tended to target the Fulani, driving some of them into the militants' arms.

Making production of high explosives cheaper, safer

Source: http://www.homelandsecuritynewswire.com/dr20180125-making-production-of-high-explosives-cheaper-safer

Jan 25 – Scientists from the U.S. Army Research Laboratory (ARL) and the Lawrence Livermore National Laboratoryfound a solution to a significant challenge in making high-energy explosives. They safely improved the overall chemical yield derived from **diaminoglyoxime**, known as DAG, and significantly increased the amount of material made per reaction.



ARL says that scientists traditionally synthesize DAG by reacting a mixture of hydroxylamine hydrochloride and sodium hydroxide with an aqueous solution of the dialdehyde glyoxal at 95°C. DAG proceeds in a low chemical yield of 40 percent by this synthesis method, with the remaining 60 percent of the possible product being lost.

"A low-yielding reaction is problematic because this means that less material is made, thus increasing overall production costs. The traditional method of making DAG is not safe because the reaction releases a significant amount of heat. This can lead to an unintentional combustion event or an unintended explosion. Due in part to these cost and safety issues, explosives derived from DAG have seen limited potential application," said Dr. Jesse J. Sabatini, an ARL chemist.

"**By simply adding an aqueous solution of glyoxal to an aqueous solution of hydroxylamine heated to 95 o C, followed by stirring for 3 days, DAG is produced in a much improved 80 percent yield.** Since the new method to make DAG does not release a significant amount of heat, the potential explosion and combustion hazards are minimized. Therefore, the new DAG synthesis is much cheaper and safer to produce, thus paving the way for this material to be made in larger scale quantities," Sabatini said.

— Read more in Eric C. Johnson et al., "A Convenient and Safer Synthesis of Diaminoglyoxime," Organic Process Research & Development *21, no. 12 (29 November 2017): 2073-75.*

Ambulance bomb kills 95, wounds 158 in Kabul attack

Source https://m.economictimes.com/news/international/world-news/explosion-rocks-kabul-leaving-multiple-casualties/amp_articleshow/62671709.cms?__twitter_impression=true

Jan 27 – The casualty toll from Saturday's ambulance bomb attack in the Afghan capital Kabul reached at least 95 dead and 158 wounded, a health ministry official said.

The explosion -- one of the biggest since a truck bomb ripped through the Afghan capital's diplomatic quarter on May 31 last year -- triggered chaotic scenes as terrified people fled the area where several high-profile organisations, including the European Union, have offices.

An AFP reporter saw "lots of dead and wounded" civilians in the nearby Jamuriate hospital where overwhelmed medical staff struggled to treat bloodied men, women and children lying in corridors.

The force of the blast shook windows of buildings at least two kilometres away and shattered windows within hundreds of metres of the site. Some low-rise structures in the vicinity of the explosion also collapsed.

"The suicide bomber used an ambulance to pass through the checkpoints. He passed through the first checkpoint saying he was taking a patient to Jamuriate hospital and at the second checkpoint he was recognised and blew his explosive-laden car," interior ministry deputy spokesman Nasrat Rahimi told AFP. The Taliban claimed responsibility for the attack on social media -- their second deadly assault in Kabul in the space of a week. The Italian NGO Emergency said seven dead and 70 injured had been taken to its hospital, with its coordinator Dejan Panic tweeting that it had been a "massacre".

Outside civilians walked through debris-covered streets carrying wounded people on their backs as others loaded several bodies at a time into ambulances and private cars to take them to medical facilities around the city.

Aminullah, whose stationery shop is a just metres from the site of the blast, said the force of the explosion shook the foundations of his building. "The building shook. All our windows broke. The people are in shock in our market," he told AFP. Photos shared on social media purportedly of the blast showed a huge plume of smoke rising into the sky. A man told Tolo News he was passing the area when the explosion happened. "I heard a big bang and I fainted," he said, outside the Emergency hospital. "There were dozens of people who were killed and wounded. There were pools of blood."

The explosion happened in a busy part of the city where the High Peace Council, which is charged with negotiating with the Taliban, has offices. "It targeted our checkpoint. It was really huge -- all our windows are broken," Hassina Safi, a member of High Peace Council, told AFP. "So far we don't have any reports if any of our members are wounded or killed."

Members of the European Union's delegation in Kabul were in their "safe room" and there were no casualties, an official told AFP. The explosion comes exactly a week after Taliban militants stormed a luxury hotel in Kabul, killing at least 22 people, the majority foreigners. A security alert issued to foreigners this morning had warned that the Islamic State group, which has terrorised the city in recent months, was planning "to conduct aggressive attacks" on supermarkets, shops and hotels frequented by foreigners.

Taliban Must Choose Between Islam and Terrorism: Ghani

Source: https://www.tolonews.com/afghanistan/taliban-must-choose-between-islam-and-terrorism-ghani

Jan 29 – Addressing a joint press conference with his Indonesian counterpart, the president said the Taliban must separate itself from barbarism. In his first public appearance since the Intercontinental Hotel attack just over a week ago, President Ashraf Ghani came out in support of the country's security forces who are fighting insurgency on the battlefields and in the cities.

Ghani said at a joint press conference with visiting Indonesian President Joko Widodo that the Taliban was carrying out attacks in Afghanistan on the orders of their masters.

But in a show of support for security forces he said: "I salute the bravery of our security forces, especially the police who are our first line of defense against these cowardly suicide bombers. Reforms in our intelligence services and Ministry of Interior are our top priority now."

"Taliban must choose between Islam and terrorism, between humanity and barbarism," Ghani said a day after Afghans observed a day of national mourning following Saturday's deadly ambulance bombing that killed at least 103 people.

Ghani said if the Taliban really believes in Islam and humanity, then the group must separate itself from barbarism and puppets of religious manipulators and intelligence agencies.

"Those who consider themselves Muslims and Afghans must now separate themselves, in words and

actions, from those barbaric puppets of religious manipulators and intelligence agencies," he said, adding that today Afghans are at a crossroads in the country's history and must take decisive and clear steps to bring lasting stability to the country.

"We can no longer wait for peace to come to us, we must win it through collective national resolve," he said.

Ghani also thanked Afghanistan's international partners who supported the country during difficult times and urged other nations to act against what he described as state sponsorship of terrorism.

"We appreciate the sympathies extended by our international partner nations. Thank you for standing with us. It is also an infliction point for our partners. Afghans expect our partners to condemn and take all possible action against state-sponsor of terrorism," Ghani said.

He went on to say that Islam is for all Muslims. Those who distinguish between Muslims, in their Fatwas, by arbitrary lines for their political gains and legitimize the massacre of Muslims are war criminals and must be sanctioned.

The president also briefly touched on the political developments in the country and asked Afghan political elites to come together and unite to defeat terrorism.

"Afghan political elite must rise above petty politics and unite to serve our people and defend our nation and country against state-sponsored, regional, and international terrorism.

In conclusion, Ghani said he will speak to the nation and present more details about the next steps once his Indonesian counterpart departs.

Ghani made the remarks at a joint press conference with Indonesian President Joko Widodo, who arrived in Kabul at about mid-day on Monday – just two hours after a deadly attack on a military academy in the capital was brought under control.

Widodo in turn said his government will establish an Islamic center in Afghanistan and continue to stand by the country. He also says Indonesia is ready to help Afghanistan with various projects.

Over the past few days, Taliban and Daesh militants have carried out a wide range of attacks across the country, including three assaults in Kabul that left almost two hundred people dead and hundreds more wounded.

Where do Yemeni missiles come from?

Source: http://www.presstv.com/Detail/2018/01/28/550512/Yemen-missile-Houthi-Ansarullah-Iran-North-Korea-Scud-Borkan

Yemeni soldiers stand next to a domestically developed Qaher-2 missile. (File photo)

Jan 30 – Saudi Arabia's brutal military aggression against Yemen has taken quite a few drastic turns ever since its beginning in March 2015. The deadly war has seen Saudis use illegal weapons such as cluster bombs over populated areas without any raised eyebrows in the West. The war has also seen the Riyadh regime's allies such as the US and the UK ramp up their arms deals with the monarchy despite international outcry.

All of this, however, has been overshadowed by one question the answer to which has so far defied observers: **How did Yemen's Ansarullah fighters lay their hands on ballistic missiles? How did the militiamen acquire the know-how to maintain, launch and even upgrade their arsenal?**

Ever since the Yemeni forces unveiled their game-changing capability, Saudi Arabia and its allies, including the United States, have been furiously pointing their fingers at Iran, accusing it of providing the Houthis with advanced missiles and the technical knowledge required to operate them.

Nikki Haley, the US ambassador to the United Nations, has even held a televised demonstration of purported debris of a Yemeni missile that escaped all US-provided Patriot missile defenses and landed close to King Khalid International Airport near Saudi Arabia's capital, Riyadh, last November.

Saudis knew well that the tit-for-tat attack meant only one thing: Yemenis were indeed able to fire a ballistic missile from over 600 miles (more than 965 km) and successfully land it on a target deep inside the kingdom.

But was the answer that simple? Has Iran been able to sneak missile parts into Yemen even though the impoverished country's important ports and airports are under a strict blockade by Saudi military forces to the point that aid shipments and even medical crew sent to the country seldom get the chance to actually enter the country and help soothe the humanitarian crisis that is in full swing there?

A typical Scud missile, a Soviet-era missile with a limited range that Yemeni forces have based their domestically developed Borkan-2 missiles on, is more than 11 meters (~37ft) long and weighs between 4 and 6.5 tons depending on its type.

Smuggling a large and heavy piece of weaponry of this scale into Yemen is quite a feat, specially when taking into account that Yemeni forces are certainly in possession of tens and maybe even hundreds of this family of missiles.

It is a mission that to complete it would be rather flattering and would speak to the lacking skills of a Saudi-led coalition, which has been ferociously bombing Yemeni civilians and

paying mercenaries for more than three years to reinstate their staunch ally, Yemen's former president, Abd Rabbuh Mansur Hadi.

There are, however, other sides to this story that the West is leaving out in order to create a stronger case against Iran.

Going back in history, we can trace a rather close relationship between Yemen and North Korea.

It is only logical to assume that Yemen's ballistic missile arsenal dates back to before the current military confrontation between the two sides.

In the early 1990s, the Saudi-backed North Yemen, which was at the time led by ex-president Ali Abdullah Saleh, was at the middle of a war with South Yemen. Saleh became the unified Yemen's first president and publicly supported Houthis down the road, when they took over from a fugitive Hadi.

The support, however, soon frayed and Saleh was eventually killed by popular forces for creating "chaos" in Yemen through cooperating with "militias of aggression."

Pyongyang has been always interested in striking ties with South Yemen for its communist past, where it was ruled by the Marxist party, the National Liberation Front, and its successor, Yemeni Socialist Party.

North Korea reportedly even backed an ill-fated secession bid by South Yemen in 1994.

In 2015, a South Korean intelligence official claimed that Pyongyang had provided Yemeni forces with no less than 20 Scud missiles.

The allegation was later on confirmed by a former North Korean security official, who told the South Korean news outlet Yonhap that Pyongyang had even sent engineers to help Saleh's government with the technical part.

The ties took the spotlight in 2002, when Spain announced that it had intercepted a ship carrying Scud missiles from North Korea to Yemen.

Yemen immediately announced at the time that it would end all military ties with Pyongyang and said it had only accepted the missiles to fulfill pre-existing contracts.

Yemen has so far unveiled two variants of its new Borkan family of missiles that are thought to be upgraded Scuds.

ISIS bomb-making videos continue to be available on Google platforms

Source: http://www.homelandsecuritynewswire.com/dr20180131-isis-bombmaking-videos-continue-to-be-available-on-google-platforms

Jan 31 – One of ISIS's most notorious bomb-making videos is frequently and continually uploaded to Google web platforms, and there is little indication that the company is taking the appropriate steps to prevent these reuploads. "You Must Fight Them O Muwahhid" is one of ISIS's most infamous videos, urging attacks in the West, displaying knife attack tactics on a live human target, and notably, providing instructions for building an explosive device with easily obtainable materials.

The Counterextremism Project (CEP) notes that ISIS released the video more than one year ago, and it has been removed from Google platforms several times,

but has reappeared again. "The video was reuploaded most recently in January of 2018, indicating Google's ongoing failure to address the problem of extremist content on their services in a consistent and transparent manner," CEP says.

The video shows how to manufacture TATP, a powerful but unstable explosive that can be made using basic household components—making it a favorite of different extremist groups. TATP explosives have been detected in multiple terror plots: the September 2017 Parsons Green attempted bombing; the Barcelona terror cell in August 2017; the Manchester Arena attack in May 2017; the Brussels airport and metro station attacks in March 2016; the November 2015 Paris attacks; the 7/7 al-Qaeda attacks in London; and even Richard Reid's airborne shoe bombing attempt in December 2001.

Specifically, these how-to TATP bomb-making guides and videos have been linked to deadly incidents. Easily available explosive video tutorials were cited by *The Times* as aiding the Manchester bomber, Salman Abedi. More recently, Munir Mohammed, found guilty in January of preparing a terror attack in the United Kingdom, had viewed "You Must Fight Them O Muwahhid" and was acquiring the components necessary

Despite the demonstrable risks to public safety, the video continues to be available online. Since November 2016, the video has been uploaded to Google-owned platforms and removed at least eleven times. "You Must Fight Them O Muwahhid" was most recently accessible on Google Drive on 9 January 2018, on YouTube on 30 December, and on Google Photos on 27 December, where it remained for almost 24 hours after it was uploaded.

CEP notes that even though Google has made numerous public commitments to tackle extremist content—including promises to using a hashing system to prevent the spread of known extremist content and increasing staff to remove this material—the video continues to be available. The continued reappearance of known ISIS bomb-making material, however, raises questions about Google's commitment to actually implementing these pledges.

Moreover, on 9 January, the European Commission met with approximately twenty tech and social media companies in Brussels, and—in a sign of displeasure with tech companies' progress—demanded that the firms remove extremist content within two hours of upload. "If videos like 'You Must Fight Them O Muwahhid' are constantly reuploaded and can remain accessible and downloadable for a full day, it's unclear how companies can meet this two-hour limit without making significant improvements to policies and capacity for implementation," CEP says. "Furthermore, it's unclear how fines will affect a multibillion dollar company that spent over $13 million on lobbying in the United States in 2017. The Commission's decision would be the first-time rules for the timed removal of extremist content have been introduced in a major market, which could lead to greater global advancements in takedown mechanisms," CEP says.

CEP concludes: "Google has come a long way since ignoring terrorist material on their sites, but more must be done to ensure the transparent and consistent enforcement of their terms

of service. Google has still not publicly detailed how they plan on combating dangerous extremist content on Google Drive or Google Photos especially, but they owe the public a response."

Yemen: Naval mines planted by the Houthis destroyed in Midi coasts

Source: https://english.alarabiya.net/en/News/gulf/2018/02/06/Yemen-Naval-mines-planted-by-the-Houthis-destroyed-in-Midi-coasts.html

Feb 06 – Yemeni naval forces, in cooperation with the engineering teams of the Arab coalition forces destroyed on Monday naval mines planted by the Houthi militias in the international waters near Midi coasts of the Hajjah governorate in northwestern Yemen.

A military source confirmed that the naval mines were washed away by the **waves near the coast of Midi, west of Hajjah province.**

The source said the Houthi militia's mine implanting forms a threat to the international community with the aim of pressing for a halt to the progress of the national army and the Arab coalition.

Last week, the naval formation forces thwarted the attempt to plant and marine mines by Houthi mine experts, eliminated them and destroyed their boats on Midi coasts.

Houthi leaders threatened more than once to cut off international shipping in the Red Sea and carried out several attempts using booby-trapped boats as well as naval mines.

Advanced missiles wreck Syrian rebels' underground hospital

Source: https://www.debka.com/

An estimated five advanced missiles dropped from the air Thursday night wrecked a rebel hospital built under 20m of rock in the Hama province.

The hospital, one of the best protected in the country, served a population of 50,000. No deaths were reported since the staff and patients were evacuated to a safe room when they heard enemy jets overhead. But the hospital was put out of commission.

Meet the heroes behind the 50-hour wartime bomb disposal operations in Hong Kong

Source: http://www.scmp.com/news/hong-kong/law-crime/article/2131617/meet-heroes-behind-50-hour-wartime-bomb-disposal-operations

Feb 01 – After two bomb disposal operations that lasted 50 hours in total over the past five days, the Hong Kong police unit responsible for disarming explosives can finally take a breather.

Fifteen officers from the Explosive Ordnance Disposal Bureau (EOD) worked through the night to defuse a 450kg (1,000lbs) wartime bomb uncovered on Wednesday at a building site in a busy commercial district of the city.

Wearing protective gear including suits weighing 30kg (70lbs) and 11kg helmets, the EOD officers worked in the cold and wet. They described the nearly 24-hour operation as "dirty, difficult and dangerous."

"We couldn't sleep. In such situations, the longer [the operation] takes, the more unstable [the bomb] is. That's why we had to work as quickly and as safely as possible," a haggard officer told the *Post* after the operation on Thursday.

To defuse the bombs, officers drilled holes in the metal casing, removed the explosives and burned them using a special igniter that capped the temperature at below 280 degrees Celsius (536 degrees Fahrenheit), according to senior EOD officer Tony Chow Shek-kin.

Risks involved in such operations left officers facing "the cold fact that you will either have complete success or total failure," Adam Roberts, a veteran bomb disposal officer, wrote in a letter to the *Post* last February to thank the public for their support during an operation to defuse a 220kg bomb at a Pok Fu Lam construction site the previous month.

Roberts took part in the two latest operations, spending his birthday on Saturday disarming the first device.

Hong Kong has not suffered a catastrophe from unearthed wartime bombs, but there have been numerous accidents overseas. In some incidents, a bomb disposal officer made an error due to fatigue and stress, and some were just "simply cases of back luck", Roberts wrote.

"We do not rely on luck, we rely on experience, training and the quality of our brother officers; luck is something we seldom discuss."

Established in 1972, the EOD unit had by 2014 grown to 41 members, including six full-time officers, five assistants and 30 reservists trained to defuse home-made bombs. Four were women, all reservists.

Their tasks extend beyond bomb disposal to post-blast investigation, underwater operations and the handling of chemical, biological, radiological and nuclear incidents.

The unit carries out over 100 operations each year on average. EOD officers also deal with "plenty of grenades and mortar rounds" annually, a police spokeswoman said. These tend to appear in former battlefield areas that are now country parks.

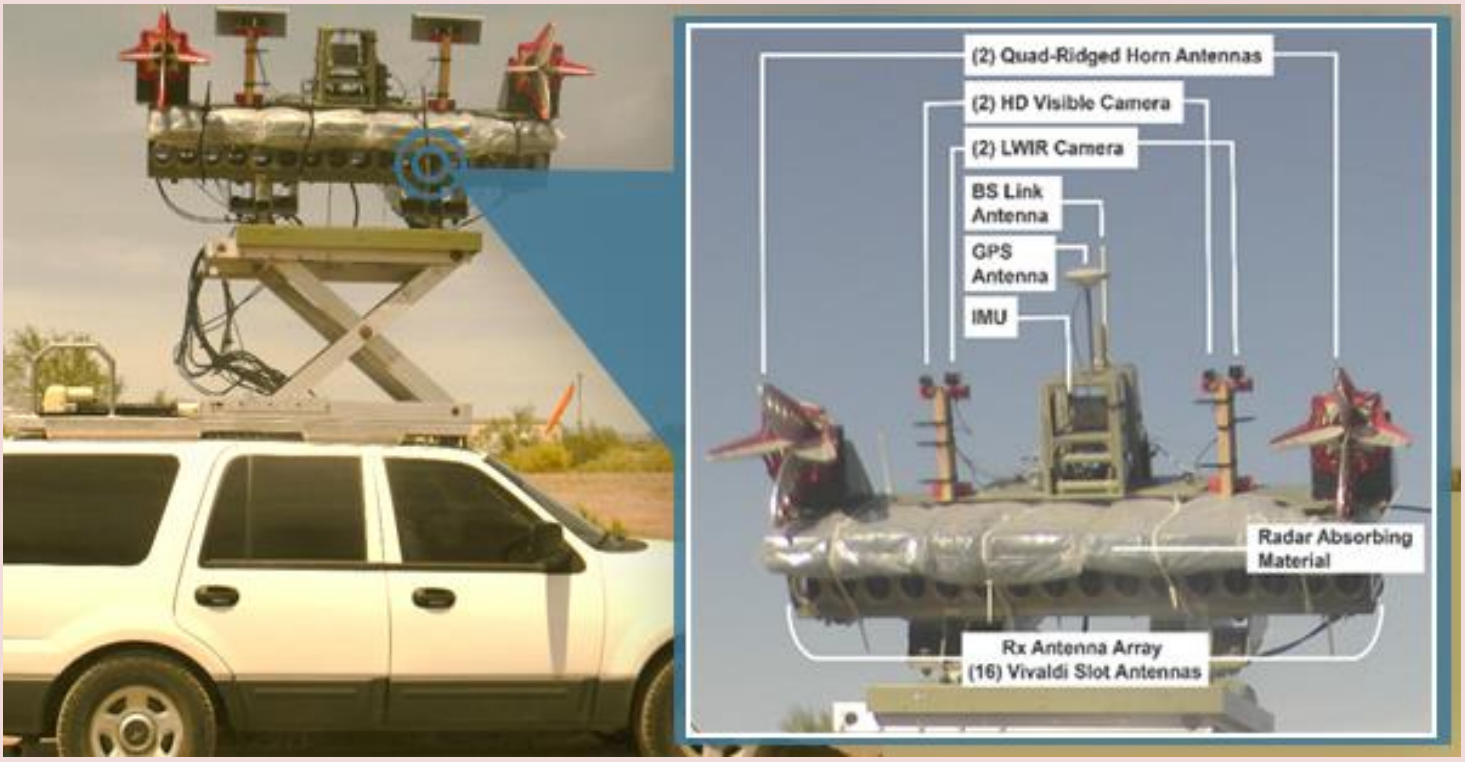
To qualify as EOD officers, they had to undergo four years of training, even learning how to build a bomb. They could spend weeks and months in Britain or the United States, where the skills they learn include evidence collection and handling court cases.
The unit operates on a "minimum risk" or "one man risk" principle, which means that the least number of people should bear the largest risk.
A team usually consisted of only two people – a bomb disposal officer and an assistant, referred to simply as No 1 and No 2, Roberts said. No 1 does the hands-on disposal and No 2 ensures that the No 1 has the equipment to do the job; each relies heavily on the other.
At a time when the force's image has taken a hammering over incidents related to the 2014 Occupy protests, the EOD unit offers a chance to rebuild citizens' confidence in the police.
Many internet users expressed gratitude to the EOD officers on the police's Facebook page, where two live videos drew over 130 encouraging comments.
One user, Francis Cheung, wrote: "A most difficult job extremely professionally done!"
In February 2014, the EOD unit defused a 900kg bomb in Happy Valley, the largest wartime bomb dug up in Hong Kong. The device, an AN-M66 bomb, was the biggest of its kind dropped on Hong Kong by US bombers. When it was found, more than 2,000 people were evacuated from nearby buildings.

Spotting IEDs from a safe distance

Source: http://www.homelandsecuritynewswire.com/dr20180212-spotting-ieds-from-a-safe-distance

Feb 12 – Soldiers in combat have to constantly scan their surroundings for improvised explosive devices (IEDs), a signature weapon of modern warfare. These homemade bombs are often hidden—nestled in bushes, buried underground, or sometimes stuffed inside other objects.
Now, a research group at the University of Delaware is developing technology to detect explosive devices from a distance. Chandra Kambhamettu, professor of computer and information sciences and director of the Video/Image Modeling and Synthesis (VIMS) Lab, has received a five-year, $1 million grant from the U.S. Army Research Office for this project.
Landmines, improvised explosive devices (IEDs), and other homemade bombs struck 6,461 people worldwide in 2015, killing at least 1,672, according to a report by the International Campaign to Ban Land Mines and Cluster Munition Coalition.
Survivors are often left with devastating injuries. In a study published in BMJ Open, 70 percent of people hit by IEDS in Afghanistan required multiple amputations.
To keep soldiers away from these deadly weapons, researchers are developing technology that can spot explosive hazards precisely and from a safe distance. UDEL says that

Kambhamettu and Philip Saponaro, a post-doctoral fellow, are creating an augmented reality system that will use traditional cameras, thermal infrared sensing and ground penetrating radar to find and classify potentially dangerous objects from up to 30 meters away.
The technologies complement each other. Regular cameras collect visible light, while infrared cameras detect heat and are unaffected by light, making them ideal for nighttime use, foggy conditions, and dust storms. The system's radar uses radio waves to probe the surrounding environment.



On the left, an equipped vehicle was recently field tested in Arizona. The photo on the right shows the mounting locations of the antennas, camera, GPS, and other technology that makes this UD-developed system function.

"With infrared, you can see and understand more than you would with just visible light," Kambhamettu said. "Then, with radar, you can see objects that differ from their surroundings, buried up to 3-5 inches."
Even if one sensor modality fails to detect an IED, another may reveal it.
"Some objects that are completely invisible to traditional cameras are easily spotted by the thermal cameras," Saponaro said.
The multi-camera systems could be deployed on autonomous vehicles, drones, or robots sent to scout the surroundings before troops move in.
The technology being developed in Kambhamettu's lab is tested on vehicles at a military training facility. Kambhamettu and his team will gather data from the cameras, apply deep learning to the data, and develop algorithms to make target detection more effective. They will also visualize scenarios in a virtual reality environment.
The goal: "Take the data, feed it into a computer algorithm and be able to tell whether a target is present or not," said Saponaro.
This research may also have applications that extend far beyond the military.
"What we're doing here is useful for day-to-day life, too," said Kambhamettu.
For example, a device that spots hidden objects could help elderly or blind people walk more safely by alerting them to hurdles in their path.
Kathy McCoy, the Chair of the Department of Computer and Information Sciences, said, "The cutting-edge work being done in this lab has tremendous potential for significant positive impact. This particular project that involves teaming up with the Army Research Lab and using a creative battery of vision techniques to find IEDs will enable detection that goes far beyond what is currently possible. The consequences to the safety of our soldiers is enormous."

Explosives & Handheld Trace Detection

By Ryan Holland and Mark Fisher

Source: https://www.domesticpreparedness.com/commentary/explosives-handheld-trace-detection/

Feb 21 – The threat of homemade explosives (HMEs) is not new. From the Oklahoma City bombing in 1995, to the "shoe bomber," London underground bombings, "underwear bomber," and attacks in Paris and Brussels in the 2000s, the threat is ever changing. Not only do post-incident crime scenes present danger to responders until secondary devices have been ruled out, but also makeshift laboratories where the bombs are made. Handheld explosives trace detection (ETD) equipment can help responders quickly determine on-scene threats, like Triacetone Triperoxide (TATP) and react appropriately and expediently. TATP has been used in bombing and suicide attacks, including the 2016 Brussels and 2017 Manchester Arena bombings. It was also used in the explosion that preceded the 2017 terrorist attacks in Barcelona. Terrorists frequently use this chemical because it is relatively easy to make using household supplies. As such, TATP is often produced in makeshift laboratories found inside apartments, homes, or other residential structures.

Evidence of TATP manufacture may include glassware such as beakers or flasks, mixers, filtration systems, and distillation equipment. TATP is often kept cold to increase its stability, so ice baths or refrigerators may indicate production. Its instability makes it very dangerous to responders investigating makeshift laboratories. Even trace level quantities can be dangerous if detonated.

TATP Chemical Relevance

Given the instability and volatility of TATP, it is important for responders to know what to look for and how to approach explosion sites or suspected makeshift laboratories where the chemical has been found or handled. TATP appears as a white crystalline powder with a bleach-like odor. Shock, static, sparks, heat, and friction can cause detonations.

Large volumes of easily obtained chemicals such as acetone, sulfuric acid, or peroxide-based bleaching formulations can be indicators of TATP production (Figure 1):

- Acetone is found in nail polish remover or paint thinner.
- Sulfuric acid is present in car batteries and acidic drain cleaners.
- Cosmetic or wood bleaching solutions can be a source of concentrated hydrogen peroxide.

These ingredients are not just dangerous on their own, but gaseous byproducts produced by them can be toxic and explosive.

Fig. 1. TATP can be made from commonly available household ingredients (*Source:* FLIR, 2018).

Using Explosive Trace Detection

In a suspected bomb-making environment, both surfaces and containers may be investigated using particle or vapor sampling procedures. Responders should always be

aware of the possibility of booby traps or secondary devices, and the dangers of entering homemade laboratories.

Numerous technologies can be used for detection, including colorimetric kits (using wet chemistry and color change indicators), Raman spectroscopy (confirmatory tool), ion mobility spectrometry (IMS), and chemiluminescence. The data provided in this article demonstrates TATP detection using a chemiluminescence-based ETD.

Detection of trace explosive signatures results from either directly collecting trace quantities of explosive particles, or by sampling vapor that emanates from an explosive source. Particulates can be solid explosive residue or non-explosive particulates contaminated with explosives, with surface contamination occurring in two primary scenarios:

- When explosives are handled or moved, small particulates of explosives can become suspended in the air and settle onto surfaces.
- Surface contamination can also occur through direct contact with explosive-contaminated or contact with another explosive-contaminated surface. Primary transfer occurs when bulk explosive materials (a quantity that can easily be seen) come into direct contact with a surface, such as a person's hand when handling explosives. Secondary transfer occurs when a surface that was contaminated by primary transfer comes into contact with a second surface. An example of secondary transfer would be a transfer of explosive materials to an identification card, door handle, cellphone, etc.

Vapor – TATP vaporizes very quickly, resulting in a vapor signature that can be readily detected with a handheld ETD. The vapor enters the sensor via direct vapor sampling (Figure 2). The direct vapor method is effective for screening bottled liquids and concealed, high-volatility explosives.

Fig. 2. Vapor-based sample collection and analysis (*Source:* FLIR, 2018).

Vapor becomes more dilute as it travels further from the source and mixes with the surrounding air, resulting in lower concentrations of explosives. Vapors can accumulate to higher concentrations in confined spaces, such as a box, bag, or car trunk. When vapor from confined spaces can be directly sampled, the likelihood of detection increases.

Advantages to vapor sampling are that it does not require contact with an object to collect a sample and the sample can be cleaner, which may improve sensor performance. Vapor is the suggested method of detection in cases where it is not possible to make contact with the object that needs to be sampled, or when explosives are suspected of being friction sensitive.

Environmental factors, such as temperature and wind, affect vapor sampling more than swab sampling. Higher temperatures produce more vapor to be sampled. Concentrated "plumes" of vapor will only be present down current or downwind of the target, due to non-uniform mixing of the explosive molecules in the air.

Particulate – Trace particulate residues can be collected from contaminated surfaces using a particulate swipe that is then inserted into the ETD (Figure 3). If a bulk quantity of white powder is suspected as being TATP, it should not be directly sampled. Responders should call the bomb squad and evacuate all personnel to a safe distance.

Fig. 3. Particulate-based sample collection and analysis (*Source:* FLIR, 2018).

Particulate screening allows for detection of secondary transfer on personnel and vehicles. Screening is rarely impacted by environmental conditions. Because particulate screening requires contact with the sampled objects, it is not recommended in situations that pose an imminent threat to the screener.

Fluorescence and chemiluminescence based ETDs are capable of detecting trace levels of TATP and hydrogen peroxide, materials that are often used in the manufacture of Homemade Explosive Devices. It can be detected in both particle and vapor modes. Detection of TATP is indicated by audible and onscreen alerts (Figure 4). These ETDs use an open sample flow path, which enables a faster clear-down than other methods, so subsequent screenings can be performed quicker.

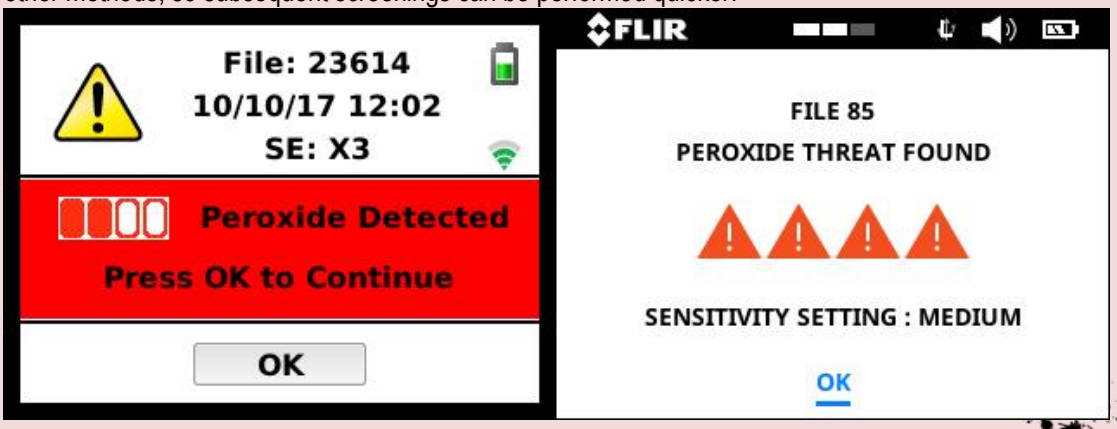


Fig. 4. Peroxide alarm screens on TrueTrace®-based sensor (*Source:* FLIR, 2018).

Summary
TATP is a common threat used by terrorists, because it can be made from easily available household supplies and produced in makeshift laboratories. This unstable chemical is dangerous to first responders in bulk (visible) quantities. Responders should be aware of the unique signs to look for when TATP manufacturing is suspected and understand that trace (invisible) quantities of TATP can be detected by ETDs using particle (swipe) or vapor sampling methods.
Ryan Holland (pictured above), product manager for explosives and narcotics detection at FLIR Systems, has over 15 years of experience in the development of the Fido X Series sensor (U.S. patent #6,558,626) for detection of ultra-trace levels of explosive vapor and particulates. He has served as a research scientist on a variety of projects related to trace detection of explosives, including landmine detection, improvised explosive device (IED) detection, detection of explosives in marine environments, ageing and chemical transformation of trace explosives residues in the environment, the characterization of explosive chemical signatures associated with IEDs and persons involved in the fabrication of explosive devices, development of forensics tools for use by warfighters in battlefield environments, detection of explosives using canines, and sensor algorithm development.
Dr. Mark Fisher, scientist at FLIR Systems, holds a Ph.D. in physical chemistry from Oklahoma State University. He has been instrumental in the development of the Fido X Series sensor (U.S. patent #6,558,626) for the detection of ultra-trace levels of explosive vapor and particulates. He has served as technical lead on a variety of projects related to trace detection of explosives, including landmine detection, improvised explosive device (IED) detection, detection of explosives in marine environments, ageing and chemical transformation of trace explosives residues in the environment, the characterization of explosive chemical signatures associated with IEDs and persons involved in the fabrication of explosive devices, development of forensics tools for use by warfighters in battlefield environments, detection of explosives using canines, and sensor algorithm development. He has an extensive background in the development of methods and hardware for sampling of trace chemical signatures in gas and condensed phases, including development of noncontact methods for sampling trace particles from surfaces.

IDF reveals it thwarted attempted Islamic State bombing of Australian flight

Source: https://www.timesofisrael.com/idf-reveals-it-thwarted-attempted-islamic-state-bombing-of-australian-flight/

Feb 21 – The Israeli army on Wednesday revealed that the Military Intelligence Unit 8200 foiled an Islamic State attempt to bomb a flight from Australia last August.
"The unit provided exclusive intelligence that led to the prevention of an air attack by the Islamic State in 2017 in Australia," a senior IDF officer said.
Get The Times of Israel's Daily Edition by email and never miss our top stories Free Sign Up

"The foiling of the attack saved dozens of innocent lives and proved Unit 8200's position as a major player in the intelligence fight against the Islamic State," the officer said, on condition of anonymity.
Wednesday's revelation was an unusual move for the Israeli army, which generally keeps mum on the operations of the secretive Unit 8200, which is similar to the American National Security Agency, collecting information from electronic communication, also referred to as signals intelligence.

Soldiers from the 8200 Unit in training (photo credit: Moshe Shai/Flash90)

Later in the day Prime Minister Benjamin Netanyahu thanked the unit for foiling the attack.
"Thank you to the Israeli intelligence services. We revealed today that the security agencies prevented the shooting down of an Australian airliner. This is just one of the dozens of terrorist attacks that we have stopped around the world. [The intelligence services] deserve all the support we can give, not only for protecting the citizens of Israel, but for protecting people all over the world," he said in a speech to American Jewish leaders.
Indeed, this prowess in intelligence gathering and counter-terrorism is a central selling point for Israel in its efforts to create and maintain relationships with foreign countries.

The foiled attack

In August, Australian security forces arrested two men suspected of trying to place an improvised explosive device on an Etihad Airways flight out of Sydney in a plot directed by Islamic State.

People crowd a terminal at Sydney's domestic airport as passengers are subjected to increased security, in Sydney, Australia, Monday, July 31, 2017 (Dean Lewins/AAP Image via AP)

The components of the device they planned to use, including what Phelan described as a "military-grade One of the men, a 49-year-old from Sydney, brought the device to Sydney airport on July 15 in a piece of luggage that he had asked his brother to take with him on the flight — without telling

the brother that the bag contained explosives, Australian Federal Police Deputy Commissioner Michael Phelan said at the time. But the bag never got past the check-in counter. Instead, Phelan said, the 49-year-old man left the airport with the bag, and his brother continued onto the flight without it.

"This is one of the most sophisticated plots that has ever been attempted on Australian soil," Phelan told reporters at the time. "If it hadn't been for the great work of our intelligence agencies and law enforcement over a very quick period of time, then we could well have a catastrophic event in this country."

explosive," were sent by a senior Islamic State member to the men in Sydney via air cargo from Turkey. An Islamic State commander then instructed the two men how to assemble the device, which police later recovered, Phelan said.

According to Australian authorities, when that attack failed, the suspects then planned to release highly toxic hydrogen sulfide gas in order to poison people. But they were arrested before their plot could advance significantly.

No specific targets had been chosen for the planned hydrogen sulfide attack, though an Islamic State member overseas had given the men suggestions about where such devices could be placed, such as crowded areas or on public transportation, Phelan said.

Police had no idea either of the plans were in the works until they received the tip from Israel on July 26. They arrested the men on July 29.

The big Unit 8200

On Wednesday, the IDF also revealed it thwarted a recent Iranian cyber attack against Israeli public and private systems, though it did not provide additional details on what was targeted and when.

"This foiling was possible thanks to the close tracking of the Iranian network's activities," the officer said.

The intelligence unit also credited itself with helping reduce the number of terror attacks in the West Bank by so-called lone wolves — people who act independently, without direction from a terrorist group — through special algorithms that identify potential assailants.

"We work closely with all the divisions and regional commands. The unit's products are critically and operationally relevant, directly assisting the activities of forces in the field," the officer said.

Unit 8200 is one of the largest units in the IDF.

According to the prime minister, the unit is the "second largest" national security agency in the world, after only that of the United States.

"The United States is 42 times larger than the State of Israel. Its NSA is not 42 times the size of Israel's NSA, it's not even 10 times the size," Netanyahu boasted to business leaders in Munich on Friday.

Explosive device thrown at U.S. embassy building in Montenegro

Source: https://www.reuters.com/article/us-montenegro-usa-attacks/explosive-device-thrown-at-u-s-embassy-building-in-montenegro-idUSKCN1G609X

Feb 22 – An unknown person threw an explosive device, probably a hand grenade, at the United States embassy building in Podgorica, the capital of Montenegro, before blowing himself up, the government said on Thursday.

Messaging in English on its official Twitter account, the government said that half an hour after midnight (1130 GMT), "An unknown person committed suicide with an explosive device."

It added, "Immediately before, that person threw an explosive device from the intersection near the Sport Center into the U.S. embassy compound."

It said, "Most probably, the device was a hand grenade," adding that police investigation and identification were underway.

Police guard the entrance to the United States embassy building in Podgorica, Montenegro, February 22, 2018. REUTERS/Stevo Vasiljevic

A Reuters photographer in Podgorica said a police vehicle blocked the street where the embassy is located, adding that no damage was visible.

The embassy warned U.S. citizens to stay away until further notice.

"The U.S. embassy in Podgorica advises U.S. citizens there is an active security situation at the U.S. embassy in Podgorica," it said on its website. "Avoid the embassy until further notice."

Earlier, media in Montenegro had said the attack occurred minutes before midnight.

Montenegro, the smallest of all former Yugoslav republics, was the 29th country to join NATO last May.


CBRNE-Terrorism
Newsletter
W
O
M
D
Cyber News

How secure is your data when it's stored in the cloud?

By Haibin Zhang

Source: http://www.homelandsecuritynewswire.com/dr20180125-how-secure-is-your-data-when-it-s-stored-in-the-cloud

Jan 25 – As cloud storage becomes more common, data security is an increasing concern. Companies and schools have been increasing their use of services like Google Drive for some time, and lots of individual users also store files on Dropbox, Box, Amazon Drive, Microsoft OneDrive and the like. They're no doubt concerned about keeping their information private – and millions more users might store data online if they were more certain of its security.

Data stored in the cloud is nearly always stored in an encrypted form that would need to be cracked before an intruder could read the information. But as a scholar of cloud computing and cloud security, I've seen that where the keys to that encryption are held varies among cloud storage services. In addition, there are relatively simple ways users can boost their own data's security beyond what's built into systems they use.

Who holds the keys?

Commercial cloud storage systems encode each user's data with a specific encryption key. Without it, the files look like gibberish – rather than meaningful data.

But who has the key? It can be stored either by the service itself, or by individual users. Most services keep the key themselves, letting their systems see and process user data, such as indexing data for future searches. These services also access the key when a user logs in with a password, unlocking the data so the person can use it. This is much more convenient than having users keep the keys themselves.

But it is also less secure: Just like regular keys, if someone else has them, they might be stolen or misused without the data owner knowing. And some services might have flaws in their security practices that leave users' data vulnerable.

Letting users keep control

A few less popular cloud services, including Mega and SpiderOak, require users to upload and download files through service-specific client applications that include encryption functions. That extra step lets users keep the encryption keys themselves. For that additional security, users forgo some functions, such as being able to search among their cloud-stored files.

These services aren't perfect – there's still a possibility that their own apps might be compromised or hacked, allowing an intruder to read your files either before they're encrypted for uploading or after being downloaded and decrypted. An encrypted cloud service provider could even embed functions in its specific app that could leave data vulnerable. And, of course, if a user loses the password, the data is irretrievable.

One new mobile app says it can keep phone photos encrypted from the moment they're taken, through transmission and storage in the cloud. Other new services may arise offering similar protection for other types of data, though users should still be on guard against the potential for information to be hijacked in the few moments after the picture is taken, before it's encrypted and stored.

Protecting yourself

To maximize cloud storage security, it's best to combine the features of these various approaches. Before uploading data to the cloud, first encrypt it using your own encryption software. Then upload the encoded file to the cloud. To get access to the file again, log in to the service, download it and decrypt it yourself.

This, of course, prevents users from taking advantage of many cloud services, like live editing of shared documents and searching cloud-stored files. And the company providing the cloud services could still modify the data, by altering the encrypted file before you download it.

The best way to protect against that is to use authenticated encryption. This method stores not only an encrypted file, but additional metadata that lets a user detect whether the file has been modified since it was created.

Ultimately, for people who don't want to learn how to program their own tools, there are two basic choices: Find a cloud storage service with trustworthy upload and download software that is open-source and has been validated by independent security researchers. Or use trusted open-source encryption software to encrypt your data before uploading it to the cloud; these are available for all operating systems and are generally free or very low-cost.

Haibin Zhang *is Assistant Professor of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.*

Cyber incidents doubled in 2017

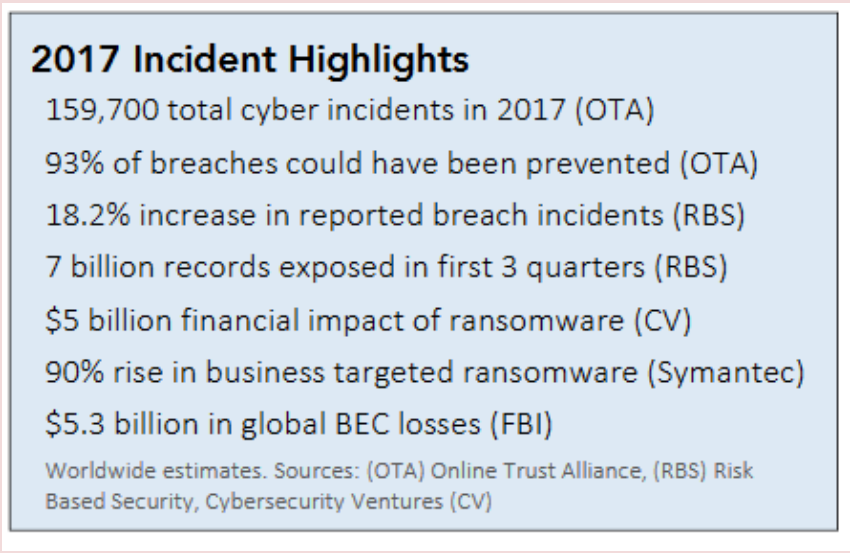
Source: http://www.homelandsecuritynewswire.com/dr20180129-cyber-incidents-doubled-in-2017

Jan 29 – The Online Trust Alliance (OTA), an Internet Society initiative with the mission to enhance online trust, has just released its Cyber Incident & Breach Trends Report. OTA's annual analysis found that cyber incidents targeting businesses nearly doubled from 82,000 in 2016 to 159,700 in 2017. Since the majority of cyber incidents are never reported, OTA believes the actual number in 2017 could easily exceed 350,000.

In the report, OTA analyzes data breaches, ransomware targeting businesses, business email compromise (BEC), distributed denial of service attacks (DDoS), and takeover of critical infrastructure and physical systems over the course of a year. It highlights the Internet Society's concerns around how large-scale data breaches, uncertainties about how data is being used, cybercrime and other online threats are impacting Internet users' trust in the Internet.

"Surprising no one, 2017 marked another 'worst year ever' in data breaches and cyber incidents around the world," said Jeff Wilbur, director of the OTA initiative at the Internet Society. "This year's big increase in cyberattacks can be attributed to the skyrocketing instances of ransomware and the bold new methods of criminals using this attack."

O TA says that it found that in 2017 there were 134,000 ransomware attacks on businesses, nearly doubling that of 2016. In mid-2017 another type of ransomware attack emerged—the ransom denial-of-service attack (RDoS). In this attack, criminals send an email to domain owners threatening a DDoS attack that will make a website inoperable unless a ransom (usually via Bitcoin) is paid. OTA recommends proactive planning for crisis management, forensics specialists and law enforcement, and suggests that organizations be prepared by setting up a Bitcoin wallet in the event ransom payment is deemed necessary for a given incident.



Breaches easily avoidable

As in past years, OTA found most breaches could have been easily prevented. It calculated that in 2017, 93 percent of all breaches could have been avoided had simple steps been taken such as regularly updating software, blocking fake email messages using email authentication and training people to recognize phishing attacks. Of the reported breaches in 2017, OTA found 52 percent were the result of actual hacks, 15 percent were due to lack of proper security software, 11 percent were due to physical skimming of credit cards, 11 percent were due to a lack of internal controls preventing employees' negligent or malicious actions and eight percent were due to phishing attacks.

"Regular patching has always been a best practice and neglecting it is a known cause of many breaches, but this received special attention in 2017 in light of the Equifax breach," said Wilbur. "In 2018 we expect patches to play an even more integral role due to the recently discovered Spectre and Meltdown vulnerabilities where nearly every computer chip manufactured in the last 20 years was found to contain fundamental security flaws."

Methodology

OTA notes that it came to its conclusions in the report by tracking and analyzing threat intelligence data from multiple sources. These sources included but are not limited to Cybersecurity Ventures, the FBI, Malwarebytes, the Ponemon Institute, Proofpoint, Risk Based Security, Symantec and Verizon.

This report, released in recognition of Data Privacy & Protection Day on 28 January, is a precursor to OTA's tenth annual Cyber Incident & Breach Response Guide, to be released in the coming months. The guide provides organizations with tools to enhance data protection, adopt responsible privacy practices and help to detect, mitigate and effectively respond to a cyber incident.

Better cybersecurity for Medical Imaging Devices (MIDs)

Source: http://www.homelandsecuritynewswire.com/dr20180130-better-cybersecurity-for-medical-imaging-devices-mids

Jan 30 – Ben Gurion University's (BGU) Malware Lab researchers are warning medical imaging device (MID) manufacturers and healthcare providers to become more diligent in protecting medical imaging equipment from cyber threats.

In their new paper, BGU researchers demonstrate the relative ease of exploiting unpatched medical devices, such as computed tomography (CT) and magnetic resonance imaging (MRI) machines, many of which do not receive ongoing security updates.

Consequently, an attacker can easily compromise the computer that controls the CT device causing the CT to emit high rates of radiation, which can harm the patient and cause severe damage. Attackers can also block access to MIDs or disable them altogether as part of a ransom attack, which has already occurred worldwide.

This study is a new frontier in cyber security research. It is part of a large-scale research project called Cyber-Med, initiated by Dr. Nir Nissim, head of the Malware Lab at BGU's Cyber Security Research Center (CSRC). Cyber-Med aims to develop security mechanisms for the entirety of medical devices' ecosystems, including implanted pace-makers, robotic surgeon systems (e.g. da Vinci), medical information systems and protocols, ICU medical devices, and MIDs.

AABGU notes that in recent years, MIDs have become more connected to hospital networks, which make them vulnerable to sophisticated cyberattacks that can target a device's infrastructure and components, as well as fatally jeopardize a patient's health and the hospital systems operations.

The research was released ahead of the Cybertech Conference which runs through Wednesday, 31 January, at the Tel Aviv Fairgrounds. BGU is the conference's academic partner. Cybertech is one of the largest cyber events worldwide, drawing thousands of guests and delegations from eighty countries.

Malware Lab experts predict attacks on MIDs will increase. They foresee attackers developing more sophisticated skills directed at these types of devices, the mechanics and software of which are often installed on outdated Microsoft PCs.

"CTs and MRI systems are not well-designed to thwart attacks," says lead author Dr. Nir Nissim, who simulates MID cyberattacks together with his MSc student Tom Mahler. Tom is part of the Malware Lab's team which includes 17 outstanding research students, and conducted the research under the supervision of Dr. Nir Nissim, Prof. Yuval Elovici, director of Cyber@BGU and Prof. Yuval Shahar, director of BGU's Medical Informatics Research Center.

"The MID development process, from concept to market, takes three to seven years. Cyber threats can change significantly over that period, which leaves medical imaging devices highly vulnerable," says Mahler.

The study, conducted in collaboration with Clalit Health Services, Israel's largest health maintenance organization, included a comprehensive risk analysis survey based on the "Confidentiality, Integrity and Availability" risk model, which addresses information security within an organization.

Researchers targeted a range of vulnerabilities and potential attacks aimed at MIDs, medical and imaging information systems and medical protocols and standards. While they discovered vulnerabilities in many of the systems, they found that CT devices face the greatest risk of cyberattack due to their pivotal role in acute care imaging. **Simulated cyberattacks revealed four dangerous outcomes:**

1. Disruption of scan configuration files − By manipulating these files, an attacker can install malware that controls the entire CT operation and puts a patient at great risk.
2. Mechanical MID motor disruption – Medical imaging devices have several components with mechanical motors, including the bed, scanner and rotation motors, which receive instructions from a control unit, such as the host computer (PC). If malware infects the host computer, an attack on the motors can damage the device and injure a patient.
3. Image results disruption − Because a CT sends scanned results connected to a patient's medical record via a host computer, an attack on that computer could disrupt the results, requiring a second exam. A more sophisticated attack may alter results or mix up a transmission and connect images to the wrong patient.
4. Ransomware − This malware encrypts a victim's files and demands a ransom to decrypt them. The WannaCry attack, which affected more than 200,000 devices in more than 150 nations in May 2017, directly infected tens of thousands of U.K. and U.S. hospital devices, including MRIs.

"In cases where even a small delay can be fatal, or where a dangerous tumor is removed or erroneously added to an image, a cyberattack can be fatal," says Mahler. "However, strict regulations make it difficult to conduct basic updates on medical PCs, and merely installing anti-virus protection is insufficient for preventing cyberattacks."
BGU Malware Lab researchers are working on new techniques to secure CT devices based on machine learning methods. The machine-learning algorithm analyzes the profile of the patient being scanned, as well as many additional operational parameters of the CT itself, and produces an anomaly detection model based on a clean CT machine. Once the machine is infected, the detection model can identify the change in its behavior and its operational parameters and alert the administrator accordingly.
In future research, Dr. Nissim and his team will conduct nearly two dozen attacks to further uncover vulnerabilities and propose solutions to address them. They are interested in collaborating with imaging manufacturers or hospital systems for in situ evaluation.
"As the Israeli academic leader in cyber security research, we partnered with Israel Defense to help create the Cybertech conferences four years ago," says BGU President Prof. Rivka Carmi. "Cybertech is the preeminent forum in Israel to showcase our success in cyber research, innovation and commercialization and we will continue to play a leadership role in that arena."

— Read more in Nir Nissim et al., "Know Your Enemy: Characteristics of Cyber-Attacks on Medical Imaging Devices," arXiv:1801.05583 [cs.CR] (17 January 2018).

Critical infrastructure firms face crackdown over poor cybersecurity

By Eerke Boiten
Source: http://theconversation.com/critical-infrastructure-firms-face-crackdown-over-poor-cybersecurity-90869

Jan 31 – An EU-wide cybersecurity law is due to come into force in May to ensure that organizations providing critical national infrastructure services have robust systems in place to withstand cyberattacks. The legislation will insist on a set of cybersecurity standards that adequately address events such as last year's WannaCry ransomware attack, which crippled some ill-prepared NHS services across England.
But, after a consultation process in the U.K. ended last autumn, the government had been silent until now on its implementation plans for the forthcoming law.
The NIS Directive (Security of Network and Information Systems) was adopted by the European parliament in July 2016. Member states, which for now includes the U.K., were given "21 months to transpose the directive into their national laws and six months more to identify operators of essential services."
The Department for Digital, Culture, Media and Sport (DCMS) finally slipped out its plans on a Sunday, but – given its spin on fines – it doesn't seem as though the government was attempting to bury the story.

Interesting spin
The DCMS warned – in rather alarmist language – that "organizations risk fines of up to £17m if they do not have effective cybersecurity measures" in place. There are echoes of the EU's General Data Protection Regulation (GDPR), by matching its €20m (£17m) maximum penalty level – though the option to charge 4% of turnover for NIS as well was dropped after consultation.
However, exorbitant penalties have been used as a scare tactic by GDPR snake oil salesmen, despite clear statements from the Information Commissioner's Office (ICO) indicating a cautious regime. Did the DCMS mean to invite overblown headlines about the NIS directive, too?
Another peculiarity is that the government announcement doesn't once mention the EU. Instead, the NIS directive is presented as an important part of the U.K. Cyber Security Strategy, even though it is an EU initiative. A pattern is emerging here: the removal of mobile roaming fees, a ban on hidden credit card charges and environmental initiatives have all been claimed as U.K. policies by Theresa May's government without any adequate attribution to the EU. Digital minister Margot James said: "We are setting out new and robust cybersecurity measures to help ensure the U.K. is the safest place in the world to live and be online. We want our essential

services and infrastructure to be primed and ready to tackle cyber-attacks and be resilient against major disruption to services."

Who needs to be aware of the NIS directive?

The government consultation response clarifies which operators of essential services and digital service providers the directive will apply to, once transposed into U.K. law. It uses a narrow definition of "essential", excluding sectors such as government and food. Small firms are mostly excused from compliance; nuclear power generation has been left out, presumably to cover it exclusively under national security; and electricity generators are excluded from compliance if they don't have smart metering in place. Digital service providers expected to comply with the NIS directive include cloud services (such as those providing data storage or email), online marketplaces and search engines.

The law requires one or more "competent authorities", which the UK plans to organize by sector. It means communications regulator Ofcom will oversee digital infrastructure businesses and data watchdog the ICO will regulate digital service providers. They will receive reports on incidents, give directions to operators and set appropriate fines.

It's worth noting that the ICO, in its multiple roles, could fine a service provider twice for different aspects of the same incident – once due to non-compliance with NIS and once due to non-compliance with GDPR. But incidents need to be considered significant in order to be on the radar for this directive. It will be judged on the number of affected users, the duration and geographical spread of any disruption and the severity of the impact.

Clearly, once this legislation is in place, the next WannaCry-style incident will be closely scrutinized by regulators to see how well-prepared organizations are to deal with such a major event.

National and international coordination

The coordination of many NIS activities falls to the U.K.'s National Cyber Security Centre (NCSC), part of the government's surveillance agency, GCHQ. It will provide the centralized computer security incident response team (CSIRT), and act as the "single point of contact" to collaborate with international peers as a major cyberattack unfolds. The NCSC will play a central role in reporting and analyzing incidents, but remains out of the loop on enforcing the law and fines.

Sharing cyber incident information within an industry sector or internationally is important for larger scale analysis and better overall resilience. However, there are risks due to the inclusion of cyber vulnerability implications, business critical information and personal data in such sensitive reports. Two EU research projects (NeCS and C3ISP) aim to address these risks through the use of privacy preserving methods and security policies. The C3ISP project says its "mission is to define a collaborative and confidential information sharing, analysis and protection framework as a service for cybersecurity management."

More security standards?

The idea of having prescriptive rules per sector was considered and rejected during the U.K.'s consultation process on the NIS directive. It's in line with how the GDPR imposes cybersecurity requirements for personal data: it consistently refers to "appropriate technical and organizational measures" to achieve security, without pinning it down to specifics. Such an approach should help with obtaining organizational involvement that goes beyond a compliance culture.

A set of 14 guiding principles were drawn up, with the NCSC providing detailed advice including helpful links to existing cybersecurity standards. However, the cyber assessment framework, originally promised for release in January this year, won't be published by the NCSC until late April – a matter of days before the NIS comes into force.

Nonetheless, the NIS directive presents a good drive to improve standards for cybersecurity in essential services, and it is supported by sensible advice from the NCSC with more to come. It would be a shame if the positive aspects of this ended up obscured by hype and panic over fines.

Eerke Boiten *is Professor of Cybersecurity, School of Computer Science and Informatics, De Montfort University.*

Faraday rooms, air gaps can be compromised, and leak highly sensitive data

Source: http://www.homelandsecuritynewswire.com/dr20180208-faraday-rooms-air-gaps-can-be-compromised-and-leak-highly-sensitive-data

Feb 08 – **Faraday rooms or "cages" designed to prevent electromagnetic signals from escaping can nevertheless be compromised and leak highly sensitive data**, according to new studies by Ben-Gurion University of the Negev's Cyber@BGU.

Research led by Dr. Mordechai Guri, the head of research and development of Cyber@BGU showed for the first time that a Faraday room and an air-gapped computer that is disconnected from the internet will not deter sophisticated cyber attackers.

Air-gapped computers used for an organization's most highly sensitive data might also be secluded in a hermetically-sealed Faraday room or enclosure, which prevents electromagnetic signals from leaking out and being picked up remotely by eavesdropping adversaries.

In two newly released reports, the team demonstrated how attackers can bypass Faraday enclosures and air gaps to leak data from the most highly secured computers. The Odini method, named after the escape artist Harry Houdini, exploits the magnetic field generated by a computer's central processing unit (CPU) to circumvent even the most securely equipped room. Click here to watch the demonstration.

"While Faraday rooms may successfully block electromagnetic signals that emanate from computers, low frequency magnetic radiation disseminates through the air, penetrating metal shields within the rooms," explains Dr. Guri. "That's why a compass still works inside of a Faraday room. Attackers can use this covert magnetic channel to intercept sensitive data from virtually any desktop PCs, servers, laptops, embedded systems, and other devices."

In another documented cyberattack dubbed Magneto, researchers utilized malware keystrokes and passwords on an air-gapped computer to transfer data to a nearby smartphone via its magnetic sensor. Attackers can intercept this leaked data even when a smartphone is sealed in a Faraday bag or set on "airplane mode" to prevent incoming and outgoing communications.

▶▶ **Click here to watch the demonstration.**

How to biohack your intelligence—with everything from sex to modafinil to MDMA

By Serge Faguet

Source: https://hackernoon.com/biohack-your-intelligence-now-or-become-obsolete-97cdd15e395f

***Serge Faguet** is founder of Mirror AI, Ostrovok, TokBox. Stanford GSB, Cornell, YCombinator, Google alum. Extreme biohacker. Born in Siberia. Live all over the world.*

Games organisers confirm cyber attack, won't reveal source

Source: indianexpress.com/article/sports/sport-others/games-organisers-confirm-cyber-attack-wont-reveal-source-5059387/

Feb 11 – The Games' systems, including the internet and television services, were affected by the hack two days ago

Pyeongchang Winter Olympics organisers confirmed on Sunday that the Games had fallen victim to a cyber attack during Friday's opening ceremony, but they refused to reveal the source.

The Games' systems, including the internet and television services, were affected by the hack two days ago but organisers said it had not compromised any critical part of their operations.

"Maintaining secure operations is our purpose," said International Olympic Committee (IOC) spokesman Mark Adams.

"We are not going to comment on the issue. It is one we are dealing with. We are making sure our systems are secure and they are secure."

Asked if organisers knew who was behind the attack, Adams said: "I certainly don't know. But best international practice says that you don't talk about an attack."

The Winter Games are being staged only 80km (50 miles) from the border with North Korea, which is technically still at war with the South since their 1950-1953 war ended in a truce rather than a peace treaty.

The two teams marched together at an Olympics opening ceremony for the first time since 2006.

South Korea has been using the Pyeongchang Games to break the ice with the reclusive North, which has been trading nuclear threats with the United States recently.

"All issues were resolved and recovered yesterday morning," Pyeongchang organising committee spokesman Sung Baik-you told reporters.

"We know the cause of the problem but that kind of issues occurs frequently during the Games. We decided with the IOC we are not going to reveal the source (of the attack)," he told reporters.

Russia, which has been banned from the Games for doping, said days before the opening ceremony that any allegations linking Russian hackers to attacks on the infrastructure connected to the Pyeongchang Olympic Games were unfounded.

"We know that Western media are planning pseudo-investigations on the theme of 'Russian fingerprints' in hacking attacks on information resources related to the hosting of the Winter Olympic Games in the Republic of Korea," Russia's foreign ministry said.

"Of course, no evidence will be presented to the world."

Cyber security researchers said in January they had found early indications that Russia-based hackers may be planning attacks against anti-doping and Olympic organisations in retaliation for Russia's exclusion from the Pyeongchang Games.

Stakeholders of the Olympics have been wary of the threat from hacking and some sponsors have taken out insurance to protect themselves from a cyber attack.

How Will Artificial Intelligence And Machine Learning Impact Cyber Security?

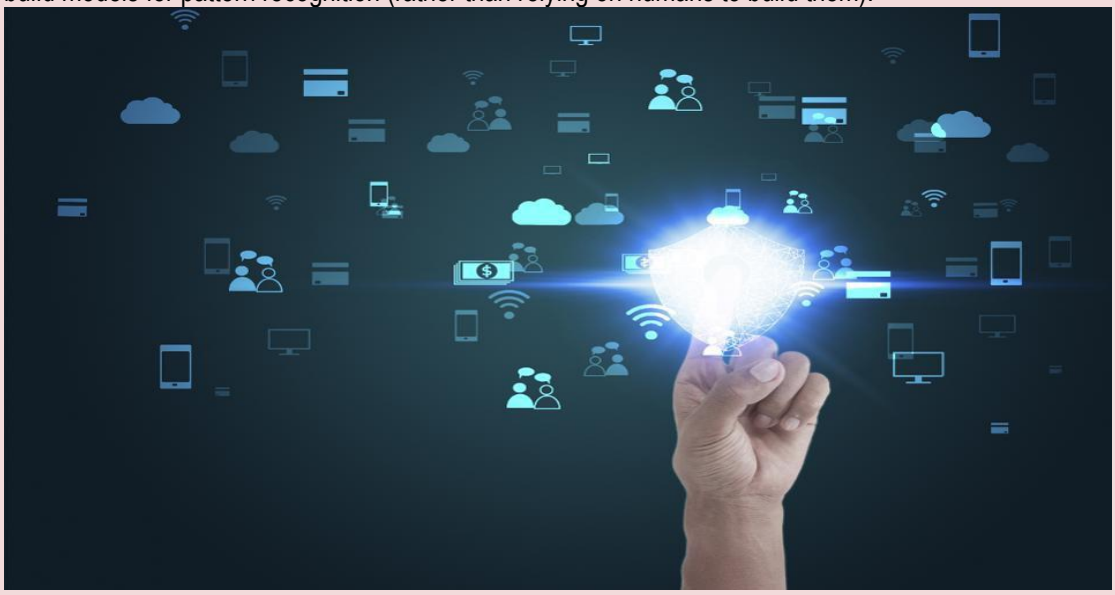
Source: https://www.forbes.com/sites/quora/2018/02/15/how-will-artificial-intelligence-and-machine-learning-impact-cyber-security/#e5aa47561475

Feb 15 - *In what way will AI and ML impact the security domain? originally appeared on Quora: the place to gain and share knowledge, empowering people to learn from others and better understand the world.*

Answer by Kris Lahiri, Co-founder, Chief Security Officer, Egnyte, on Quora:

Machine learning is a branch of artificial intelligence (AI) that refers to technologies that enable computers to learn and adapt through experience. It emulates human cognition – i.e. learning based on experience and patterns, rather than by inference (cause and effect).

Today, deep learning advancements in machine learning allow machines to teach themselves how to build models for pattern recognition (rather than relying on humans to build them).



The last five years have really seen a rise in AI and ML technologies for enterprises. Most of which can be attributed to advancements in computing power and the evolution of paradigms like distributed computing, big data and cloud computing.

Early commercial applications of ML were pioneered by technology titans like Google (in its search engine), Amazon (with its product recommendations) and Facebook (with its news feed). These businesses managed to build a veritable treasure trove of valuable behavioral data from hundreds of millions of users. In order to effectively collect, cleanse, organize and analyze their consumer data, these companies built scalable big data frameworks and applications then open sourced them to the world. By opening access to these big data frameworks, they improved fast, scaled quickly, and allowed businesses to derive more value from their data.

Organizations are already beginning to use AI to bolster cybersecurity and offer more protections against sophisticated hackers. AI helps by automating complex processes for detecting attacks and reacting to breaches. These applications are becoming more and more sophisticated as AI is deployed for security.

Data deception technology products can automatically detect, analyze, and defend against advanced attacks by proactively detecting and tricking attackers. So, when you combine very smart security personnel with adaptive technology that continues to change and become smarter over time, this provides a competitive edge to defenders that have primarily been absent from most cybersecurity technologies to date.

On the other hand, AI can open vulnerabilities as well, particularly when it depends on interfaces within and across organizations that inadvertently create opportunities for access by "bad actors" or disreputable agents. Attackers are beginning to deploy AI too, enabling it to have the ability to make decisions that benefit attackers. Meaning they will gradually develop automated hacks that are able to study and learn about the systems they target, and identify vulnerabilities, on the fly.

Fake news "vaccine": online game may "inoculate" by simulating propaganda tactics

Source: http://www.homelandsecuritynewswire.com/dr20180220-fake-news-vaccine-online-game-may-inoculate-by-simulating-propaganda-tactics

Feb 20 – A new online game puts players in the shoes of an aspiring propagandist to give the public a taste of the techniques and motivations behind the spread of disinformation – potentially "inoculating" them against the influence of so-called fake news in the process.

Researchers at the University of Cambridge have already shown that briefly exposing people to

tactics used by fake news producers can act as a "psychological vaccine" against bogus anti-science campaigns.

While the previous study focused on disinformation about climate science, the new online game is an experiment in providing "general immunity" against the wide range of fake news that has infected public debate.

The game encourages players to stoke anger, mistrust and fear in the public by manipulating digital news and social media within the simulation.

Players build audiences for their fake news sites by publishing polarizing falsehoods, deploying twitter bots, photo-shopping evidence, and inciting conspiracy theories in the wake of public tragedy – all while maintaining a "credibility score" to remain as persuasive as possible.

Cambridge says that a pilot study conducted with teenagers in a Dutch high school used an early paper-and-pen trial of the game, and showed the perceived "reliability" of fake news to be diminished in those that played compared to a control group.

The research and education project, a collaboration between Cambridge researchers and Dutch media collective DROG, is launching an English version of the game online today at www.fakenewsgame.org.

The psychological theory behind the research is called "inoculation":

"A biological vaccine administers a small dose of the disease to build immunity. Similarly, inoculation theory suggests that exposure to a weak or demystified version of an argument makes it easier to refute when confronted with more persuasive claims," says Dr. Sander van der Linden, Director of Cambridge University's Social Decision-Making Lab.

"If you know what it is like to walk in the shoes of someone who is actively trying to deceive you, it should increase your ability to spot and resist the techniques of deceit. We want to help grow 'mental antibodies' that can provide some immunity against the rapid spread of misinformation."

Based in part on existing studies of online propaganda, and taking cues from actual conspiracy theories about organizations such as the United Nations, the game is set to be translated for countries such as Ukraine, where disinformation casts a heavy shadow.

There are also plans to adapt the framework of the game for anti-radicalization purposes, as many of the same manipulation techniques – using false information to provoke intense emotions, for example – are commonly deployed by recruiters for religious extremist groups.

"You don't have to be a master spin doctor to create effective disinformation. Anyone can start a site and artificially amplify it through twitter bots, for example. But recognizing and resisting fake news doesn't require a PhD in media studies either," says Jon Roozenbeek, a researcher from Cambridge's Department of Slavonic Studies and one of the game's designers.

"We aren't trying to drastically change behavior, but instead trigger a simple thought process to help foster critical and informed news consumption."

Roozenbeek points out that some efforts to combat fake news are seen as ideologically charged. "The framework of our game allows players to lean towards the left or right of the political spectrum. It's the experience of misleading through news that counts," he says.

The pilot study in the Netherlands using a paper version of the game involved 95 students with an average age of 16, randomly divided into treatment and control.

This version of the game focused on the refugee crisis, and all participants were randomly presented with fabricated news articles on the topic at the end of the experiment.

The treatment group were assigned roles – alarmist, denier, conspiracy theorist or clickbait monger – and tasked with distorting a government fact sheet on asylum seekers using a set of cards outlining common propaganda tactics consistent with their role.

They found fake news to be significantly less reliable than the control group, who had not produced their own fake article. Researchers describe the results of this small study as limited but promising. The study has been accepted for publication in the *Journal of Risk Research*.

The team are aiming to take their "fake news vaccine" trials to the next level with today's launch of the online game.

With content written mostly by the Cambridge researchers along with Ruurd Oosterwoud, founder of DROG, the game only takes a few

minutes to complete. The hope is that players will then share it to help create a large anonymous dataset of journeys through the game.
The researchers can then use this data to refine techniques for increasing media literacy and fake news resilience in a 'post-truth' world. "We try to let players experience what it is like to create a filter bubble so they are more likely to realize they may be living in one," adds van der Linden.

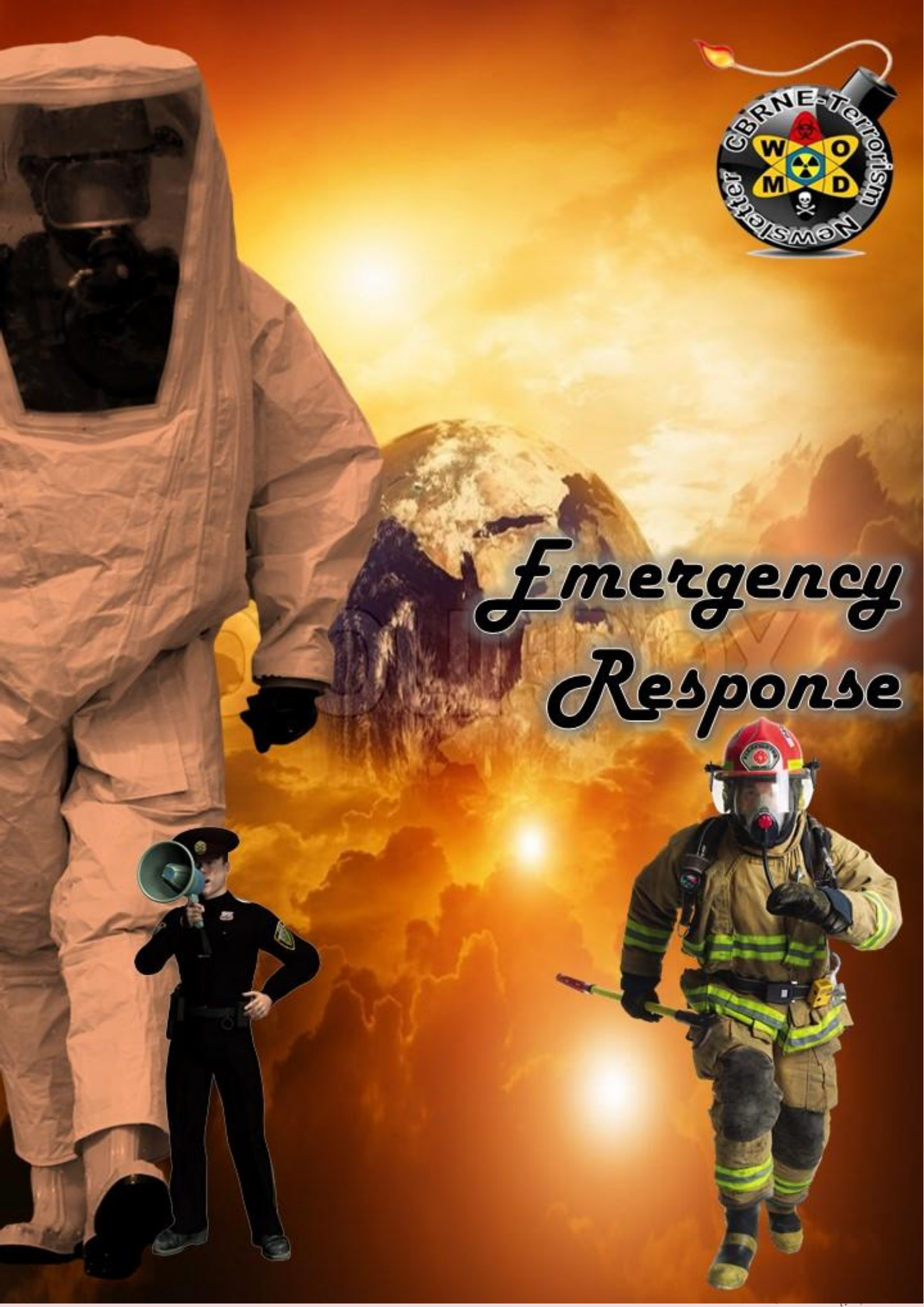
— Read more in Jon Roozenbeek and Sander van der Linden, "The Fake News Game: Actively Inoculating Against the Risk of Misinformation (forthcoming, Journal of Risk Research).

New Anti-Terrorrist Drive on Web

Source: https://i-hls.com/archives/81480

Feb 21 – Complex challenges are faced by the tech world and governments alike when it comes to terrorists on the internet. Terrorists have been finding new ways to post their recruitment and incitement messages on the net in spite of tech firms' efforts to prevent these publications.
Now, blogs, chat rooms and encrypted chat apps can serve as ways for terrorist groups to radicalize and recruit new members, says Kirstjen Nielsen, secretary of the US Department of Homeland Security.
Tech companies have had to learn how to keep ISIS, for example, from running Twitter accounts, or from sharing graphic videos involving beheadings or other forms of executions on YouTube.
Meanwhile, DHS says it has developed a strategy of supporting people within communities where recruitment is taking place who want to spread a counterterrorism message, rather than trying to put out its own "terrorism doesn't pay" style communications, according to cnet.com.
"Users around the world post four hours of content every minute," Nielsen noted. She highlighted the Global Internet Forum to Counter Terrorism, an effort led by Facebook, Google, Microsoft and Twitter that was announced in June, as a key factor in removing terrorist recruitment content from their sites.
In December, the companies announced they were sharing information with each other to identify users posting terrorist content.
UK Home Secretary Amber Rudd also referred to the subject recently, saying technology like machine learning will be instrumental in finding and removing online recruitment content. The UK is partnering with machine learning company ASI Data Science for just this purpose.

▶▶ **See the related article on** UK anti-terrorist efforts on the web


CBRNE-Terrorism Newsletter
W
O
M
D
Emergency Response

2017 Critical Incident Exercise put first responder technologies to the test

Source: http://www.homelandsecuritynewswire.com/2017-critical-incident-exercise-put-first-responder-technologies-test

Jan 26 – In the wee hours of 29 October 2017, more than 200 people participated in a critical incident exercise and technology assessment conducted by DHS' Science and Technology Directorate (S&T) in partnership with the New York Police Department (NYPD), the New York Fire Department (FDNY), and the Metropolitan Transportation Authority (MTA). During this exercise, the agencies tested and evaluated not only tactics, techniques and procedures, but also the efficacy of emergent relevant technologies.

"The recent school shootings in Kentucky and Texas, and October's horrific Las Vegas shooting are painful reminders of the importance to be prepared in the event of such terrible critical incidents. This exercise could not be more relevant to our efforts to protect the safety of the American people," said S&T Undersecretary William Bryan. "S&T has been involved in similar exercises and technology assessments since 2013."

First responders participate in such exercises to improve tactics, address capability gaps, and because of the need and desire to do things better. "We hope to incorporate several new tactics from lessons learned from this exercise such as training on an interagency communication channel," said Lieutenant Arthur Mogil from NYPD. Besides evaluating technologies, "we reinforced the response of our relatively newly formed joint agency unit, the Rescue Task Force, which requires different NYPD units to work together with the FDNY to perform security and life safety operations," said Lt. Mogil.

The exercise took place at the Grand Central Terminal in New York City, with most of the action occurring on parked trains and on track platforms, and other indoor spaces within the Terminal. Emergency medical technicians were dispatched to quickly convert ramps in front of several track platforms into triage stations. Outside, first responders set up an incident command post and an operations center to coordinate the simulated response.

Right before the exercise, each technology was on display for VIPs and observers; representatives explained how the devices and software work in preparedness and response operations for active shooter and other critical incidents.

S&T said that S&T's National Urban Security Technology Laboratory (NUSTL) had overall responsibility for technology selection, assessment, and reporting oversight. The Homeland Security Advanced Research Projects Agency provided technical, program and

administrative support of the exercise. The exercise ended with an after-action discussion with key participants and S&T's Homeland Security Operational Analysis Center (HSOAC).

The U.S. Army Armament Research, Development and Engineering Center installed 20 cameras throughout the path of the exercise and also used mobile cameras carried by videographers to cover all areas of movement. The video live streamed to the VIP Room on a video wall in Grand Central Terminal's Vanderbilt Hall. S&T installed four more cameras in the exercise path for its social media analysis tool. Later, HSOAC and S&T's Behavioral, Economic, and Social Science Engine (BESS-E) analyzed the footage to evaluate technology performance.

"Planning for this exercise began eight months before the exercise and was not a direct response to Las Vegas," said Bryan.

This was the eighth exercise S&T planned and coordinated to support technology demonstrations and evaluations. The other seven were held in New Jersey, New York and Massachusetts in the past four years. The settings included schools, a movie theater, a synagogue, a subway station, a college, and a Major League Baseball stadium, where different scenarios played out – each with a different number of simulated shooters, explosive devices, hostage situations, presence of chemical or biological weapons, and more.

"S&T saw these exercises as a unique opportunity to try out relevant existing and emergent technologies to see what kind of an impact they have on first responders' preparedness and response," said Lawrence Ruth, director at NUSTL's Test and Evaluation Division.

According to Ruth, the technology selection was based on the needs expressed by first responder agencies, and choosing relevant technologies from S&T and those offered by private industry.

"Following the event, S&T will produce an After Action Report that provides a detailed assessment of the impact the technologies have made on the efficacy of the first responders during an active shooter scenario," said Ruth. HSOAC and S&T's BESS-E will develop the report under NUSTL's oversight.

In the exercises to date, technologies were assessed to determine effectiveness for law enforcement and other responders, and how well they fit into first responder operations.

These exercises are representative of incidents such as an active shooter event and help the first responder community evaluate their preparedness and response. "S&T provides expert technical assistance to first responders for the development and execution of training and exercises, and assessment of equipment performance," said Lt. Mogil.

"We know that having the right technology in the hands of a first responder can save critical minutes or seconds, and reduce injuries and save lives. The needs of responders and the public are at the center of every decision we make," said Bryan.

S&T says that these are some of the technologies that were assessed during this most recent exercise:

- **Android Team Awareness Kit (ATAK):** Smartphone mapping app used for sharing video, audio, and other information that enables a common operating picture and improved situational awareness for incident commanders. Plug-in architecture allows needed functionality to be added. (Funded and developed by DOD).
- **MOLE:** Footwear-worn position tracker designed to work in buildings and other GPS-denied environments that is integrated with ATAK and Wireless Data Network. MOLE enables a common operating picture for incident commanders. (Developed by S&T and Robotic Research).
- **Wireless Data Network:** Wireless network to support audio/video that provides a wireless feed of the live video from the exercise to Command and Control Centers, VIP locations, or to any Emergency Operations Center; also provides tactical meshed network and portable radios that enable first responders to wirelessly exchange and update each other's indoor location using ATAK. (Developed by Persistent Systems Inc.)
- **FLING Patient Tracker: Smartphone** based patient tracking system in which patients are identified largely through their photos from initial triage to evacuation to treatment at hospitals, assisting both with medical treatment and locating the whereabouts of patients for their families. (Developed by Emergency Services Group International)
- **TacID Mobile:** Smartphone/laptop app for comparing facial photos with face image libraries; suitable for pre-event security and real-time response – can identify suspects by scanning victims against watch lists. (Developed by Ideal Innovations Inc.)

- **NEON Personnel Tracker:** 3-D personnel tracking and mapping that can operate in GPS-denied environments to enable a common operating picture for incident commanders. (Initially developed by S&T and advanced by TRX Systems)
- **Social Media Analysis Tool (DHS S&T):** Monitors various social media platforms to aid in preparedness for and response to an incident so that incident commanders can monitor social messaging in real time during the exercise.
- In addition, a **Crowd Evacuation Modeling and Simulation Software (DHS S&T),** which helps visualize and understand complexities of evacuating large numbers of people from venues, was exhibited at the event prior to the exercise.

Disasters are destroying places we hold dear. What we do next will make all the difference.

By Stephen Miller

Source: http://www.homelandsecuritynewswire.com/dr20180126-disasters-are-destroying-places-we-hold-dear-what-we-do-next-will-make-all-the-difference

Jan 26 – The news broadcasts of bright orange flames spilling over forested ridgetops at night were as ghastly as they were inescapable. On 2 September 2017, a wildfire ignited in the Columbia River Gorge about 40 miles east of Portland, Oregon. Quickly, flames spread across the canyon's south side and ascended the surrounding cliffs, where dry east winds blew them into an inferno. Within three days the Eagle Creek Fire had enveloped more than 20,000 acres and jumped the river to the north rim.

Only a day before, the gorge had seemed a wonder etched in permanence — an ancient temperate rainforest draped across a 15,000-year-old basalt canyon. For millions living nearby, and many tourists from afar, it was a sacred reprieve of unsurpassed natural beauty. Visitors sought solace amid hidden stands of enormous old growth conifers. They gaped in awe as strands of water ended 600-foot free-falls at the feet of sheer cliffs, and hiked to sweeping views of the wide Columbia River. Its most ardent admirers held fast to these images of the place even as the fire gobbled it up.

While the fire's spread was at its peak, one of those admirers created a Facebook group he originally named "Replant the Columbia River Gorge." Thousands joined immediately, many shovel-ready to seed a new forest. "Me and some buddies are down to replant some trees as soon as the fire is down," wrote one member from nearby Beaverton, Oregon. "If you appeal to local media I think you'll have no shortage of volunteers willing to plant trees and even clear dead timber," offered another.

It didn't take long, however, for someone to disagree. "[N]ature does its own thing pretty well," wrote one group member, arguing that the forest should be allowed to regrow on its own. "Please don't go rogue and plant your own trees," *The Oregonian*pleaded. "It could do more harm than good."

With smoke still choking its skies, the community plunged into a debate over how it should respond to this profound loss: try to reconstruct the past, or accept a new reality?

Inhabitants of a dynamic world have grappled with this question for eons, but today and in a future where climate change is quickly destabilizing our environments, the changes are becoming more frequent and more consequential. More than ever, policy-makers and land managers are needing to make tough choices about humankind's role in managing the natural world.

Disrupting evolution

Change, of course, is natural. Taking the long view, the rock through which the gorge was carved is infantile. The forest that burned atop that rock is younger still, and the lot of it is just a snapshot in time. Those calling for the preservation of the forest in its pre-fire form seek to halt the natural forces that, over some short millennia, created the forest they came to love. Even in the wetter west end of the gorge where blazes are less common, fires are essential, says Columbia River Gorge National Scenic Area fire management officer Darren Kennedy, and this fire was within the lines of the region's fire regime. The last major incident, the Yacolt Burn, charred more than 200,000 acres in 1902; today its scars are part of the view.

If we want forests to be resilient to today's climate we may have to let them burn, says Chad Hanson, a forest ecologist and director of the John Muir Project, which studies and advocates for forest biodiversity. Hanson and a growing body of research assert that fire

suppression has resulted in a fire deficitin the high-elevation West, despite the intensity of recent years' wildfires. For Hanson, it's concerning. Fires, even severe ones, are necessary to the development of the biologically diverse landscapes we cherish.

On the heels of the gorge fire, Representative Greg Walden introduced a bill that would expedite salvage logging and tree replanting. It collided with steadfast resistance from environmental groups and the scientific community.

"If we plant and log these areas, we are disrupting evolution itself," Hanson says. The saplings that sprung up after the Yacolt Burn, for instance, were those best suited to the conditions. The forest, he says, will regrow — though not in our lifetimes and likely in a different form.

Negotiating with a creeping eventuality

In a corner of the U.S. about as far as you can get from the Columbia River Gorge, a community is struggling to hold onto land that is sinking beneath it. As sea level rises, saltwater spills into Everglades National Park, poisoning more than 2,300 square miles of tropical wilderness on the southernmost tip of Florida that harbors critical wading bird habitat, close to 70 threatened or endangered species, and one of the world's largest mangrove forests.

In 2000, Congress authorized the Comprehensive Everglades Restoration Plan(CERP) to protect the fragile ecosystem and ensure a freshwater supply after decades of human development and water diversion had choked the natural marshlands of fresh water. In recent years, however, increased emphasis has been placed on responding to the impacts of climate change and sea level rise, which has caused the freshwater Everglades to shrink in front of advancing saltwater habitat.

To address this, the CERP is removing manmade barricades and redirecting water with pumping stations to allow for the natural flow of freshwater, while establishing retaining ponds for storage and flood mitigation.

"If successful," the National Park Service states on its website, "these efforts will help protect subterranean aquifers from salt water intrusion, delay the impacts of sea level rise along the coast, and buy precious time for wildlife to adapt to the changing environment." Adaptation, like forest building, takes time, and until significant gains are made to reverse global warming, these mitigation efforts are negotiating with a creeping eventuality.

"I had some discomfort with that at first, but I'm getting to the point where I realize how valuable buying time is for these ecosystems," says Stephen Davis, a wetlands ecologist with the Everglades Foundation. Initially, he thought more could be done than merely delaying the effects, but now he says that mentality was naive. Sea-level rise is inevitable. It's not throwing in the towel, he says, "we need to be fighting for the next generation that will derive great benefit from this ecosystem. Even if it's not in its entirety, it will still provide some benefit."

Return and insulate

Similarly, along the rivers that sustain descendants of some of North America's longest inhabitants, warming temperatures are changing landscapes and threatening long-held ways of life.

Existence in the lowlands of the mountainous West has long depended on the seasonal availability of cold-water fish like salmon and trout, but increasing air temperature and diminishing snowpack have resulted in warmer stream water in some areas. Coupled with the impacts of dams, development and ranching, this warming trend is pushing an economic and cultural mainstay of the region's indigenous people to the brink.

In the face of climate models that show a dismal future for some cold-water habitats, Native American tribes are returning landscapes to their pre-developed state and attempting to insulate critical waterways from the effects of climate change.

"Tribes are wanting to restore fish and habitat where other agencies might look at it and decide that that's not the best use of dollars," says Joe Maroney, director of Fishery and Water Resources for the Kalispel Tribe of Indians, whose lands stretch from Washington to Montana. "These are the only resources that we have that are adjacent to the reservation, so we're going to do everything we can to protect them," he says.

The Kalispel and others in the region have invested heavily in studying cold water in streams and the species it supports. They've returned unnaturally straightened rivers to their natural

meanderings. They've repopulated native fish where invasive species have elbowed to dominance. They're building pathways for fish to overcome impassible dams.
Similar to the Everglades, the threats are ever encroaching, and limited resources leave some vulnerable tributaries untended. As temperatures continue to rise and snowfall dwindles, species like the threatened bull trout, sacred to many, face relegation to memory.

Seeding the future
Johanna Varner is a biologist with Colorado Mesa University who has spent more than five years studying pikas in the Columbia River Gorge. For her, the fire's impact was twofold. "As a scientist, you go to a place and make objective observations, but as a human, you can't spend all that time making close observations in a place and not create a personal connection to it as well," she says.
In 2011, Varner's research went up in flames when a fire erupted in Oregon on the flanks of Mt. Hood. "When I first discovered that fire, I didn't know what to do and I just sat down and cried," she says. But over the coming years, she studied how pikas respond to wildfires, and, in the process, witnessed the regrowth of a burned forest.
Varner was in Colorado when the Columbia River Gorge fire began and spent days tracking Twitter obsessively to see how her work would be affected. She still doesn't know; much of the area has remained closed for risk of mudslides in the unstable soil — an issue tragically affecting Southern Californiaat the time of this writing. "It's not that that place has been lost, but that it has been changed," she says. "In my lifetime it will never be the same as it was before the fire. On the other hand, there will be new features that will be equally interesting from a scientific perspective, but also beautiful from a personal perspective."
Varner does not intend to encourage complacency about disasters that arise as a result of human activity. However, she points out that our new reality is likely to be a time of great loss, and how we choose to respond to those losses will make a big difference. In the Columbia River Gorge or elsewhere, whether we re-create what goes missing, build something new or leave it alone entirely, our decisions will seed the future.

***Stephen Miller** is an independent journalist based in Seattle, coverinmg environmental science, climate change, conservation, and energy policy.*

Mental Preparedness for First Responders: Preparing for the Disaster

By Dr. Jarrod Sadulski
Source: https://edmdigest.com/preparedness/mental-preparedness-first-responders/

The Department of Homeland Security encompasses 22 different agencies and departments that are on the daily forefront of domestic security. In addition, many DHS agencies have personnel who play first responder roles and are deployed to natural or manmade disasters in the United States.
These agencies include the Coast Guard, the Federal Emergency Management Agency (FEMA), Customs and Border Protection (CBP), Immigration and Customs Enforcement (ICE), the Countering Weapons of Mass Destruction Office, and the Office of Operations Coordination.
As a member of the Coast Guard, I have been a part of the DHS since its founding in 2002. I experienced a sudden recall to active duty from the Coast Guard Reserve, following the terrorist attacks on 9/11.
I had just transitioned out of active duty two weeks prior to the attacks. I was driving to prepare for a new civilian management career when I received the call that I was to report to Coast Guard Station Miami Beach immediately. So I remained on active duty in Miami Beach and conducted homeland security operations for the next four years.
Transitioning to an unexpected Title 10 recall following the terrorist attacks placed stress on my family and I. We addressed it through exercise, the development of a proper work-life balance, and peer support.
I have witnessed several other incidents when Coast Guard and DHS personnel were temporarily reassigned from their daily work to assist in natural or manmade disasters away

from home. While these responses are important and part of the job, it is also important to examine and mitigate the stress all response personnel face in an emergency.

Emergency personnel who respond to disasters experience a wide range of physical and mental health issues. As a result, it is important to take steps to mitigate the effects of responding to these emergencies.

Step 1: Have a Family Preparedness Plan in Place

Personnel who may be recalled to emergency responder status should have a written plan prepared well in advance. This plan should be coordinated with spouses and family members. It should account for child care, finances (including emergency cash on hand) and changes in work schedules.

The written plan should also take into consideration that communications may be limited during an emergency. Thus the plan should include emergency contact information for family members and their work supervisors. If emergency responders feel confident that their priorities at home are being met, they will be much more effective and focused while in an emergency response role.

Step 2: Complete Deployment Training in Advance

DHS agencies often train emergency personnel on mobilization and de-mobilization. It is important to complete this training, which gives personnel information explaining the different resources and support available to them.

Step 3: Self-Monitor for Problems Following an Event

Emergency responders who are exposed to disasters are at an increased risk of acute stress, including post-traumatic stress disorder (PTSD) and other emotional problems.

DHS personnel and other first responders should learn the signs of emotional problems and PTSD. Symptoms include difficulty moving beyond emotional feelings about an emergency incident, difficulty sleeping and depression.

Studies show that emergency responders are at a substantially higher risk of depression seven months following their participation in a disaster. They are also at a higher risk of acute stress disorder and PTSD 13 months later. Young, single emergency responders are more likely to develop acute stress disorder than older and more experienced responders.

Emergency responders should monitor themselves for signs that they are struggling with their participation in a disaster and seek counseling and guidance through their agency's Employee Assistance Program.

Dr. Jarrod Sadulski *has been with the Coast Guard since 1997. His expertise includes infrastructure security, maritime security, homeland security, contraband*

interdiction and intelligence gathering. He has also received commendations from the Coast Guard. Presently, Jarrod is a supervisor in the Reserve Program and provides leadership to Reserve members who conduct homeland security, search and rescue, and law enforcement missions. He is also a Faculty member, Criminal Justice at American Military University.

Animal Relocation After Disaster – Four Cases in 2017

By Richard (Dick) Green
Source: https://www.domesticpreparedness.com/journals/january-2018/

Between late August and the end of 2017, the American Society for the Prevention of Cruelty to Animals (ASPCA) deployed to six states and the U.S. Virgin Islands in response to four disasters: Hurricanes Harvey, Irma, and Maria, and the wildfires in Northern
California. In all, the ASPCA assisted nearly 37,000 animals affected by these disasters. Although each response required a unique approach, one particular objective was consistent throughout, which likely saved thousands of animal lives – animal relocation.

Richard (Dick) Green, Ed.D., *is the senior director of disaster response for the American Society for the Prevention of Cruelty to Animals (ASPCA). Before the ASPCA, he was the emergency relief manager for disasters at the International Fund for Animal Welfare (IFAW). He has responded to international and national disasters, and his teams have rescued thousands of animals from floods, tornadoes, fires, and hurricanes. Recent international responses include typhoons in Taiwan, Philippines, and Australia, volcano eruptions in Philippines and Iceland, and earthquakes in China, Haiti, and Japan. He has trained hundreds of responders in disaster prevention and response and has developed training curricula and texts for Slackwater Rescue, Water Rescue for Companion Animals, and Rope Rescue for Companion Animals. He is the past chair of the National Animal Rescue and Sheltering Coalition, is on the Board of Directors for the National Alliance of State Animal and Agricultural Emergency Programs, co-chairs the Animal Search and Rescue Best Practice Working Group, and is a member of the Evacuation and Transportation Best Practice Working Group. His doctorate is in education with an emphasis in kinesiology and biomechanics. He was an educator for 27 years, the last 10 at Gonzaga University in the Department of Exercise Science*

Israeli trauma experts teach resilience in Houston

By Abigail Klein Leichman
Source: http://www.homelandsecuritynewswire.com/dr20180201-israeli-trauma-experts-teach-resilience-in-houston

Feb 01 – As Hurricane Harvey ripped through Houston last August, the trauma didn't even spare those whose job is to help others cope. One social worker, barricaded on the second floor of her house, watched in horror as water and mud flooded her first floor. Another was stuck in a closet with her dog for twenty-four hours.
Many mental-health professionals felt helpless or guilty for their inability to respond to people in need as they usually would. And other professionals, such as educators, did not feel adequately prepared to tend psychological wounds among those they work with.
Israel, as always, was quick to send various forms of immediate support to Houston. But the Israel Trauma Coalition knew from experience in Israel and many other countries that a long process of healing was only beginning. The organization reached out to Houston's Jewish Family Services in September.
"They said they'd like to do their 'train the trainer' model in their method of helping people deal with trauma," says JFS Houston Special Projects Coordinator Gittel Francis.

With funding from the UJA Federation of New York, three ITC personnel flew over to meet with representatives of about fifteen social-services agencies in Houston. They explained that their training model involves nine full days spread over a six-month or year-long period. But the time was not yet right. "At that point we were still in the throes of disaster. Schools were just opening up again and people, including at our agency, were just getting back to normal life," says Francis.

ITC Director Talia Levanon, who has organized train-the-trainer sessions in places including France, Germany, Haiti, Sri Lanka, Japan, Philippines, Boston and Mumbai in the wake of natural or manmade disasters, returned in November with colleague Omer Egozi. They worked with JFS to prepare for the first session in January.

Seasoned Israeli resilience counselors Reuven Rogel and Dalia Sivan met with about 65 Houston professionals in three separate categories: educators, administrators and counselors from the city's Jewish schools and UJA Federation; JFS clinicians, case managers and community therapists; and members of a consortium of behavioral health professionals from a variety of nonprofit non-governmental organizations.

"Because in our country there are a lot of crises and traumas, we have learned that if we do an immediate intervention there is a better chance that people won't fall into PTSD," says Sivan.

She directs the northern branches of Amcha, the national Israeli center for psychosocial treatment of Holocaust survivors and their families, as well as other populations in trauma including women with breast cancer.

"From experiencing and trying different approaches to combat the effects of traumatic events, we learned the importance of building resilience in people so they can get back to routine quickly and not get stuck in a helpless state," says Sivan, who has trained trainers on behalf of the ITC in Japan after the tsunami and in Nepal and Sri Lanka after earthquakes.

"The ITC does not provide treatment to the injured because we believe the local people have to do that. We give them the tools to do that sustainably," says Sivan.

How are you feeling?

Francis tells *ISRAEL21c*, "Ruvie and Dalia knew their subject like the back of their hands, and everyone walked out having learned a new way of thinking."

"The first thing they asked us was to describe how we're feeling. People don't generally ask us that, as we're helping clients. Encouraging us to talk about ourselves helped us learn about our own coping skills so we can help clients who may have different coping skills. In social work you start where the client is, so if the social worker comes from a different frame of mind it doesn't help the client."

Sivan said that for traumatized professionals, "Just being able to tell the story allows the person to make sense of it and see the continuity of life beyond that moment of trauma. We make sure they go back and acknowledge their feelings."

This is not the same as therapy, Sivan adds. "This is an immediate intervention that channels the resources of the person and gives them a way to move back to the past with some

changes to get back the sense of coping with the support of the normal system. They learn that they don't have to go to a psychiatrist because they're shaking or vomiting or crying for days on end."
Rogel and Sivan are planning to return to Houston for three-day trainings in April, June and August. They may also lead standalone sessions for healthcare professionals such as pediatricians and hospital nurses.

Abigail Klein Leichman *is a writer and associate editor at ISRAEL21c.*

Humans need to learn to co-exist with wildfires. Here's how we can do it.

By Kendra R Chamberlain
Source: http://www.homelandsecuritynewswire.com/dr20180201-humans-need-to-learn-to-coexist-with-wildfires-here-s-how-we-can-do-it

Feb 01 – In 1992, the city of Wenatchee, Washington, experienced a devastating wildfire that roared through a neighborhood, destroying more than 30 homes and burning over 3,000 acres (121 hectares) in a matter of days. It left the community shaken.
"It's a terrible thing for the community to go through," said Wenatchee economic development director Steven King.
The wildfires began in the shrub steppe and grasslands that surround the city. Recent development had pushed new housing into undeveloped areas, creating what ecologists refer to as a **wildland-urban interface** (WUI). WUI landscapes are common in the western half of the United States, but exist throughout the North and Southeast, too. Homes and other buildings constructed along such interfaces are becoming increasingly prone to fire disaster, thanks to a perfect storm of conditions: a warming climate that produces more fuel for wildfire combined with short-sighted development that ignores the risk inherent in wildfire-prone ecosystems. A growing body of wildfire experts and policy-makers now agree the vulnerability to disaster for these communities is ultimately a development planning issue — not a wildfire prevention issue.

Former U.S. Forest Service research scientist Jack Cohen, who spent his career studying wildland fire and helped develop the U.S. National Fire Danger Rating system, is quick to point out that wildfires in WUI zones are not only completely natural, they're also unavoidable. "They have been an ecological factor for almost all of the ecosystems in North America in their development since the last ice age," he says.
How can we better live with the reality of wildfires? Cohen recommends that preparedness policies expand beyond firefighting and vegetation burning in public lands toward measures that help ensure that homes located in WUI areas can actually survive a fire.
"The bottom line is that we need to get compatible with wildland fire occurrence," he says. "We need to get proactive."
Fire-adapted development requires a fundamental shift in perspective about wildfires and the threat they pose to residents in WUI areas. Preventive strategies include improved urban planning and land management; collaboration among federal, state and local agencies; and campaigns aimed at educating the public about wildfire preparedness.

Designing better neighborhoods

Cohen is an early pioneer in efforts to minimize fire damage to homes. In 2001 he devised an assessment concept called the home ignition zone (HIZ) that helps homeowners determine how vulnerable their home is to wildfire by looking at factors such as building materials, vegetation and debris within a 200-foot (60-meter) area immediately surrounding the house.

Urban planning for WUI areas now centers on creating and maintaining development and building codes that incorporate the HIZ principles. These codes promote practices such as using fire-resistant building materials for siding and rooftops; maintaining "defensible space" by clearing dead leaves from rooftops, gutters and decks; trimming trees and removing vegetation that can fuel fires during the dry season; and governing subdivision design to include multiple routes by which residents can flee and fire-fighting equipment can enter. Collectively, these types of policies are loosely referred to as WUI codes.

The city of Wenatchee adopted a set of WUI codes in 2011 based on guidelines developed by the International Code Council. "We were pretty well ahead of our time for this part of Washington for doing that," King says.

But implementing new codes takes years. In 2015, the city suffered its worst wildfire season to date and lost more than 30 homes. "Unfortunately, those WUI codes didn't exist when those homes were developed. As a result, that disaster was worse than it could have been if those homes had been built today," King says.

Wenatchee neighborhoods destroyed by wildfire in the past are now being rebuilt with the new building codes in place, bringing hope for better outcomes in the future. "The homes are built differently," King says. "The landscape is different, and there's a heightened awareness."

Collaboration is key

WUI regions can be checkerboards of U.S. Forest Service, Bureau of Land Management (BLM) and private lands. The big challenge is getting land use management agencies, fire departments and private landowners to work together to develop and maintain strategies for preventing wildfire damage.

Alison Green, program director of Project Wildfire in Deschutes County, Oregon, says collaboration across all levels of government is a critical piece of wildfire preparedness. Begun in the 1990s, Project Wildfire is a community-led effort that functions as the county's official wildfire mitigation body. It's governed by a 27-person steering committee whose members include elected officials, residents, and representatives of the BLM, U.S. Forest Service, Oregon Department of Forestry, local fire districts, insurance companies and homeowners' associations.

By bringing everyone to the same table, Project Wildfire is able to coordinate efforts such as public education campaigns, prescribed burns, community-wide debris cleanups and home risk assessment events.

"We make sure we are helping our partners' goals move forward, and they are doing the same for us," Green says. "Half my job is buying coffee for people to make sure that we're still good when it comes to collaboration. The network is still a healthy, breathing network that can solve complex problems."

Shifting perspectives on wildfire risk

Another important piece of the wildfire adaption puzzle is getting residents on board with strategies to reduce the threat to their homes. Ultimately, this requires convincing homeowners to take personal responsibility for wildfire preparedness.

Homeowners in WUI zones have much more power over their home's ability to survive wildfire than previously thought. They can dramatically reduce risk of their house catching fire by doing things like creating and maintaining defensible space and keeping HIZ areas clear of debris.

Communities across the U.S. have taken different approaches to public outreach and WUI code enforcement, says Kimiko Barrett, policy analyst at Headwaters Economics, which co-manages Community Planning Assistance for Wildfire (CPAW) in partnership with the community wildfire planning organization Wildfire Planning International. San Diego, California, for example, is notorious for its code enforcement: The fire department inspects homes located in high-risk areas and fines homeowners not in compliance. "They take a very aggressive approach to structure development and building code standards for high risk areas," Barrett says.

But enforcement requires resources, so many communities rely instead on education. Initiatives include holding workshops on how to prepare for wildfire season, appointing wildfire ambassadors in at-risk neighborhoods and offering free debris pick-up events.

Even without enforcement, there's proof that such preventive wildfire adaption approaches are worth the effort. Thanks to remarkable efforts undertaken by elected officials, agency representatives and engaged residents — and all coordinated through Project Wildfire — Deschutes County hasn't lost a single house to wildfire since 2003.

That's exactly the type of result WUI communities like Wenatchee are working to achieve today.

"One of the most challenging parts of this is social change, social awareness. What we desire to see is an awareness within the community of personal responsibility to manage their property," says King. "It's a culture that's being developed."

Kendra R Chamberlain *covers topics related to climate change, environmental policy, and the innovation and technologies that are driving the global transition to low carbon economies.*

Algorithm helps first responders identify vulnerable people during natural disasters

Source: http://www.homelandsecuritynewswire.com/dr20180205-algorithm-helps-first-responders-identify-vulnerable-people-during-natural-disasters

Feb 05 – A new algorithm developed at the University of Waterloo will help first responders and home care providers better help the elderly during natural disasters.

According to the World Health Organization, older adults who live at home face disproportionately high fatality rates during natural disasters as evidenced by Hurricane Katrina where 71 per cent of the deaths resulting from that disaster involved people over 60 years of age.

"Frailty combined with social isolation can mean that older adults still living at home have nowhere to turn during emergencies," said John Hirdes, a researcher in the Faculty of Applied Health Sciences at the University of Waterloo. "With a growing proportion of elderly persons choosing to reside in their own homes, it's a very real concern. Home care services need to have mechanisms in place to manage the needs of their most vulnerable clients during disasters."

Hirdes is also the senior Canadian researcher for interRAI, an international network of researchers committed to improving care and quality of life for vulnerable populations.

Waterloo notes that the algorithm uses data from interRAI's home care assessment to generate an up-to-date list of vulnerable adults using home care services. It takes into account disability, health status, social isolation and the amount of support an individual may receive from informal caregivers.

Eight provinces/territories, including Ontario, already mandate the use of the interRAI assessment for long-stay home care clients. Home care clients are assessed every six months to one year to determine their health status and service needs.

"Older adults living on their own are more difficult to locate and assist than those living in healthcare facilities," said Sandy Van Solm, the Emergency Management Coordinator at the Region of Waterloo who developed the algorithm as part of her PhD at Waterloo. "This algorithm helps us to plan for disasters in advance and allows responders to quickly generate an accurate list of those who may need help during a disaster."

Hirdes and Van Solm are working with the Canadian Institute for Health Information to deploy the algorithm into interRAI home care software used across Canada beginning in 2018.

"It has the potential to save hundreds of lives," said Hirdes. "It's a tool that should be top of mind for any part of the country at risk of natural disasters."

By 2036, seniors aged 65 years and older could represent a quarter of the total Canadian population, and one sixth of the global population.

— Read more in Alexandra I. T. van Solm et al., "Using standard clinical assessments for home care to identify vulnerable populations before, during, and after disasters," Journal of Emergency Management 15, no. 6 (2017).

New Emergency Rule: Challenge for Some, Good for All

By David Reddick and Justin Snair

Source: https://www.domesticpreparedness.com/resilience/new-emergency-rule-challenge-for-some-good-for-all/

Feb 07 – The Centers for Medicare and Medicaid Services (CMS) implemented a comprehensive emergency preparedness rule in 2016 that applies to nearly every healthcare provider in the nation, and outlines steps those providers must take to improve their preparedness and ensure sustainability in the face of a disaster. The rule compels healthcare providers to devote resources – human and fiscal – to emergency planning. This may be seen as burdensome by some but should effectively improve their levels of readiness and improve the quality of healthcare for all. This rule will make providers – from general hospitals to transplant centers and long-term care facilities – safer for patients and visitors.

Although most people outside healthcare have little awareness of the rule or its requirements, there are good reasons everyone should understand, as they and their loved ones will benefit from enforcement of the rule. Describing the effects of Hurricanes Harvey and Maria in a November 2017 *HomeCare Magazine* article, Healthcare Ready Executive Director Nicolette Louissaint wrote, "the devastating and significant impact these events had on health care systems reminds us why it is imperative to have emergency preparedness systems in place to ensure the well-being of patients and providers during a disaster."

Her group, along with others, has spent the past months promoting the emergency rule and encouraging healthcare providers to expand their planning to ensure compliance. Sessions on the rule at a November 2017 National Healthcare Coalition Preparedness Conference in San Diego, California, were popular draws, with more than 60 people attending a half-day workshop co-sponsored by Louissant's Healthcare Ready, FEMA's Center for Domestic Preparedness (CDP), and Bio-Defense Network. A panel discussion later in the conference – featuring representatives of CMS, the California Department of Public Health, and Healthcare Ready – drew a standing-room-only crowd.

Key Elements of the Rule

The FEMA CDP has become a chief source of information on the rule, scheduling dozens of comprehensive and complimentary onsite two-day workshops around the nation for providers and healthcare coalitions. In addition to CDP and CMS, significant support for providers has been made available through the U.S. Department of Health and Human Services (HHS) Assistant Secretary for Preparedness and Response's Technical Resources, Assistance Center, and Information Exchange (TRACIE) service. TRACIE has also produced a series of frequently asked questions and conducted webinars designed to answer questions being raised by providers across the nation.

The rule contains four primary elements, each of which feeds into an organization's overall emergency preparedness program:

- *Risk Assessment and Planning* – Requires providers to assess specific and general risks they face and create plans to respond to those risks.
- *Policies and Procedures* – Must be written, approved, and reviewed on a regular basis, at least annually.
- *Communications Plan* – Must be created and outline how a healthcare provider will communicate both internally and externally, especially when normal means may be unavailable.
- *Training and Testing* – Requires providers to train their staff and conduct periodic testing and exercises to ensure they can do what they must do in the event of a disaster.

These elements sound familiar to business continuity and emergency preparedness professionals, but are not second nature to many healthcare providers, whose backgrounds are focused on healing and medical treatment, not preparedness. This may be why so many providers find themselves in a quandary when faced with complying with the rule. Many providers already do much of what is being required, but full compliance is still necessary, and failure could eventually jeopardize a provider's Medicare and Medicaid funding.

Christus St. Mary's Hospital evacuated their patients to other hospitals, due to the Hurricane Evacuation orders preparing for Hurricane Lili. (Source: Lauren Hobart/FEMA News Photo, 01 October 2002, Port Arthur, LA)

Different Providers, Varying Requirements

CMS has taken significant steps to promote and explain the requirements by conducting numerous webinars and having representatives speak at multiple events. However, many recipients remain unclear about the steps they must take, how they should document those steps, and what full compliance will look like for them.

Part of the lack of clarity is because 17 different provider and supplier types (see Table 1) are covered and, although there must be general compliance, nuances exist among them, for example:

- Outpatient providers are not required to have policies and procedures for the provision of subsistence needs;
- Home health agencies and hospices must inform officials of patients in need of evacuation; and
- Long-term care and psychiatric residential treatment facilities must share information from the emergency plan with residents and family members or their representatives.

Table 1. Providers/Suppliers: Facilities Impacted by the Emergency Preparedness Rule	
1	Hospitals
2	Religious Nonmedical Healthcare Institutions
3	Ambulatory Surgical Centers
4	Hospices
5	Psychiatric Residential Treatment Facilities
6	All-Inclusive Care for the Elderly

7	Transplant Centers
8	Long-Term Care Facilities
9	Intermediate Care Facilities for Individuals with Intellectual Disabilities
10	Home Health Agencies
11	Comprehensive Outpatient Rehabilitations Facilities
12	Critical Access Hospitals
13	Clinics, Rehabilitation Agencies, and Public Health Agencies as Providers of Outpatient Physical Therapy and Speech-Language Pathology Services
14	Community Mental Health Centers
15	Organ Procurement Organizations
16	Rural Health Clinics (RHCs) and Federally Qualified Health Centers
17	End-Stage Renal Disease Facilities

These requirements are not universal for the 17 provider types. Adding to the complexities, advance copies of the all-important Interpretive Guidelines and Survey Procedures were released in the middle of 2017 – just five months before all recipients were expected to be in full compliance.

Healthcare coalitions have become key players in promoting the rule. Many have seen increases in membership from providers seeking help in their planning efforts and involvement, especially in the areas of policies and exercises. In addition, the overall interest in the rule has become clear to national leaders such as Jennifer Pitcher, executive director of the MESH Coalition in Indianapolis, a lead organizer of the National Healthcare Coalition.

"MESH Coalition has continually experienced an increase in national contacts with regard to resources and calls for assistance," Pitcher said in an email, citing what she called an "incredibility encouraging" level of interest apparent last November 2017 at the group's annual preparedness conference. "We are excited for the energy that the rule has brought within our healthcare community and look forward to the successful response as a direct result to those collaborations."

A key requirement of the rule deals with temperature controls and emergency and standby power for hospitals, critical access hospitals (smaller facilities, often located in rural areas), and long-term care facilities. The importance of such controls and backups was made clear in South Florida in 2017, when a dozen people from a Hollywood Hills nursing home died after Hurricane Irma – as the result of what police termed "environmental heat exposure." The facility's emergency generators operated as expected when utility company power was lost, but they were powerful enough to provide only light and other basic power. Since it did not generate enough power to keep the air conditioning system running, residents suffered in the stifling heat for three days following the storm.

Most facilities must include evacuation procedures as part of their emergency program, but some smaller facilities do not have this requirement. As such, the staff at the nursing home monitored the residents for heat exhaustion and attempted to keep them comfortable. However, three days lapsed – and nine residents died – before the decision was made to move the patients to a hospital trauma center directly across the street. The deaths of three more residents also were attributed to the heat after they were moved to the hospital.

Additional Training & Reviews

In the *HomeCare Magazine* article, Louissant cited the past hurricane season as a powerful teacher, which "highlighted the challenges the health care community faces during natural disasters, and underscored why in today's integrated health care system, it is essential to know and trust community partners before disaster strikes." The rule encourages providers to create partnerships through the training and exercise component, which "creates an opportunity for health care coalitions to assist their members in compliance."

As periodic reviews for compliance are undertaken in 2018, it is likely that gaps in emergency planning and execution will be noted, and corrective actions required. It is also likely that some CMS recipients will decry the requirements that they improve their efforts.

Nevertheless, it is clear that preparedness will be enhanced, healthcare will be improved, and lives will be saved.

David Reddick, CBCP, is chief strategy officer and co-founder of Bio-Defense Network, a public health preparedness consultancy based in St. Louis, Missouri, and Mesa, Arizona. He has more than four decades of experience in communications, business continuity, and public health preparedness. He holds a certificate in emergency management and crisis leadership from Saint Louis University, where he is studying for a Master of Public Health degree, with a focus on biosecurity and disaster preparedness.

***David Reddick**, CBCP, is chief strategy officer and co-founder of Bio-Defense Network, a public health preparedness consultancy based in St. Louis, Missouri, and Mesa, Arizona. He has more than four decades of experience in communications, business continuity, and public health preparedness. He holds a certificate in emergency management and crisis leadership from Saint Louis University, where he is studying for a Master of Public Health degree, with a focus on biosecurity and disaster preparedness.*

***Justin Snair,** M.P.A., CBCP, is the founder and principal consultant with SGNL Health Security Solutions and co-founder of Naseku Goods. Formerly, he was a senior program officer with the National Academy of Sciences, Engineering, and Medicine and directed the Forum on Medical and Public Health Preparedness for Disasters and Emergencies and the Standing Committee on Medical and Public Health Research During Large-Scale Emergency Events. In 2012-2015, he served as a senior program analyst for critical infrastructure and environmental security at the National Association of County and City Health Officials. For six years, he was the local preparedness director and environmental health agent with the Acton Public Health Department in Massachusetts. In 2001-2006, he served as a corporal and combat engineer in the U.S. Marine Corps Reserves and is a veteran of the Iraq war. He holds a Master of Public Administration degree from Northeastern University's School of Public Policy and Urban Affairs, a Bachelor of Science degree in Health Science from Worcester State University, and is an executive fellow with Harvard University's National Preparedness Leadership Initiative.*

Lawmakers want to give the federal government the sole responsibility for missile alerts

Source: http://www.homelandsecuritynewswire.com/dr20180208-lawmakers-want-to-give-the-federal-government-the-sole-responsibility-for-missile-alerts

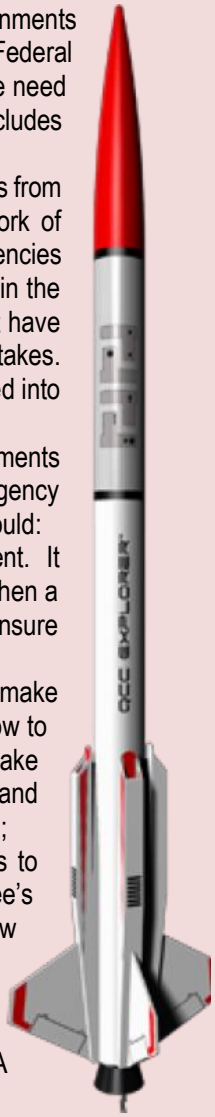
Feb 08 – Following the false emergency alert that went out across Hawai'i on 13 January and caused widespread panic, U.S. Senators Brian Schatz (D-Hawai'i), Kamala Harris (D-California), and Cory Gardner (R-Colorado) introduced the Authenticating Local Emergencies and Real Threats (ALERT) Act, legislation that would improve the emergency alert system and give the federal government the sole responsibility of alerting the public of a missile threat, prohibiting state and local governments from doing so.

"States are laboratories of democracy. They should not be the laboratories of missile alerts," said Senator Schatz, the ranking member on the Commerce Subcommittee on Communications, Technology, Innovation, and the Internet. "The people who know first should be the people who tell the rest of us. This legislation makes clear that the authority to send missile alerts rests with the federal government."

"This is a common-sense step to ensure that accurate national security information is used to assess whether or not an emergency alert about a missile threat should be deployed," said Senator Harris. "It will also ensure that state and local governments continue to play a critical role in emergency response efforts, and provide the federal government with the ability to make missile alerts a more effective public safety tool."

"Our national integrated public alert system is not something we can afford to get wrong," said Senator Gardner. "What happened in Hawaii can never happen again - people terrified by the false alert of a system that must have absolute confidence. We need to make sure

we have safe and reliable protocols in place that quickly alert Americans about serious threats, whether those threats be fast-moving wildfires or actual ballistic missile launches from rogue states like North Korea. Since they have full control over drafting and issuing alerts, state and local governments need to meet certain standards to participate in our national alert system and the Federal government must be heavily involved in any alerts regarding national security crises. We need to continue to do everything in our power to prevent the worst from happening and that includes being prepared for the worst."



State and local governments have been largely responsible for alerting the public of threats from natural disasters and severe weather. But the system they use rests upon a patchwork of technologies and procedures that do not follow consistently across the government agencies that issue these alerts. The false alarm in Hawai'i highlighted some of the weaknesses in the state's emergency alert system, which had a poorly designed user interface and did not have sufficient verification system or computer redundancies to act as a safeguard from mistakes. The incident made clear that there is a need for federal standards in the system and called into question the state's responsibility to issue a missile alert.

The Schatz-Harris-Gardner legislation would strengthen the way states and local governments use the Integrated Public Alert and Warning System (IPAWS), the FEMA platform emergency management professionals across the country use to issue warnings. The ALERT Act would:

- Restrict the authority to alert the public of a missile threat to the Federal government. It would also require FEMA to establish a process to promptly notify state authorities when a missile alert is issued so they can activate their own protective action plans to ensure public safety;
- Require the IPAWS subcommittee of the FEMA National Advisory Council to make recommendations on the best practices that state and local governments should follow to maintain the integrity of IPAWS. At a minimum, the subcommittee would make recommendations regarding the incident management tools used to originate alerts, and the procedures for testing and sending notifications to the public to avoid false alarms;
- Require FEMA to establish minimum requirements for state and local governments to participate in IPAWS within 120 days of receiving the subcommittee's recommendations. States would have reasonable time to implement any new requirements FEMA imposes;
- Require FEMA to establish a process to test the incident management and warning tool that a state or local government adopts to originate and send alerts to the public in the FEMA IPAWS Lab and to certify it meets any technical requirements that FEMA adopts; and
- Require FEMA to review its Emergency Operations, National Watch and Regional Watch Centers to assess their ability to track state and local alerts issued under IPAWS and determine which ones they should be notified about when states send them out.

In addition to Senators Schatz, Harris, and Gardner the ALERT Act is cosponsored by U.S. Senators Dan Sullivan (R-Alaska) and Mazie K. Hirono (D-Hawai'i).

New Drone Integrated in U.S Ambulance Service

Source (+ video): https://i-hls.com/archives/81247

Feb 09 – The Chicago city Ambulance Service started incorporating a new emergency response drone. We have just recently wrote in i-HLS.com about drones being flown by canadian paramedics beyond the pilot's field of vision, and it's clearly showing that drones can be incorporated in many areas of use when it's about first responders.

PropelUAS, a division of Evans Incorporated, announced that it is partnering with Medical Express Ambulance Service (MedEx) in the unveiling of a high-tech "Concept Ambulance" that integrates Unmanned Aircraft Systems (UAS) into its collection of life saving technologies.

According to UASvision.com, the company is providing UAS-related expertise to determine the benefits and the future of UAS integration with traditional apparatuses used in the emergency response vehicles. Together with MedEx, the team is addressing numerous

challenges, such as the ideal drone configuration for this integration, operational considerations for emergency response, and navigation of airspace regulations. The company is collaborating with

Lockheed Martin and MedEx to combine the very best elements of emergency management systems with the potential of tactical UAS. Lockheed's Indago systems are used for a variety of lifesaving military, first responder and civil applications.

The developing company partners with organizations to assist in navigating and integrating UAS technologies into their organizations. As a division of Evans Incorporated, it is uniquely positioned to assist Emergency Responders, such as MedEx, after years of supporting the Federal Aviation Administration with the integration of UAS into the National Airspace System.

It can be shown that many industries, with first responders one of them, can benefit very much from adapting to modern technological advancements.

Lost in the numbers: The hidden traumas of disaster

In the aftermath of disasters – hurricanes, earthquakes, epidemics, armed conflict, and the like – It is difficult to describe the true extent of damage wrought on society. Lost in these numbers is a hidden trauma that is difficult to measure, even when it is diagnosed. Disasters affect the mental health not only of those directly impacted by the disaster, but of those everywhere the disaster causes distress. Mental trauma is widespread, affecting far more people than physical injury. Long after physical wounds heal, mental trauma remains. Failing to address mental trauma neglects the well-being of tens of thousands of Americans, and millions more around the globe, each year.

Hospital Emergency Management: The Anatomy of Growth

By Theodore Tully

Source: https://www.domesticpreparedness.com/healthcare/hospital-emergency-management-the-anatomy-of-growth/

Feb 2008 – For more than a century, the "emergency manager" of a U.S. hospital or any of the nation's other healthcare facilities was seldom if ever identified by that specific job title. The reason was simple: Almost all of the nation's hospitals usually planned – and developed their response capabilities – for a one-time disaster that would result in the unexpected delivery of one patient (or sometimes several) to that hospital – more specifically, to the hospital's Emergency Department. For that reason alone it is not surprising that the person or persons charged with emergency (or disaster) planning for hospitals held more general job titles such as director of emergency medicine, or emergency department nurse manager, or security director, or the director of facilities management.

Some of the nation's more forward-looking hospitals, though, created the role of emergency manager after the 11 September 2001 terrorist attacks. To date, however, most of the nation's healthcare facilities have not yet made any major changes to their emergency-management plans, nor have they assigned the "emergency manager" title to one of their senior healthcare officials – who in most if not all facilities would be responsible for emergency planning as well as emergency management.

On 11 September 2001 itself many if not all hospitals throughout the country, not knowing if and where additional attacks might take place, had those officials responsible for their emergency planning immediately activate some level of the hospital's emergency plan. The typical account of what happened that day would often start with a statement that "My CEO called me and said to meet him in his office immediately." In the weeks immediately after 9/11, hospitals reacted to the terrorist attacks more carefully, more thoughtfully, and in much

greater detail – and also were making a major effort to find the additional funds needed to prepare for the next possible terrorist incident that might eventually affect their institution.

A More Than Tenfold Increase in Three Years

In a survey *(Emergency Preparedness Funding)* of New York City metropolitan area hospitals carried out last year by the Greater New York Hospital Association (GNYHA), the hospitals participating in the survey estimated that they had spent, on average, $126,215 for emergency preparedness in 2000. By 2003 that bottom-line total had increased to $1,355,744 on average, but only a very small percentage of that sum came from federal grant funding – *which means that the average hospital participating in the survey had increased its emergency-preparedness funding more than tenfold in only three years.* Whether the much larger financial resources being allocated for emergency preparedness are now sufficient has yet to be determined, but it is obvious that the city's hospitals are today much more prepared to handle mass-casualty incidents then they had been prior to the 9/11 attacks.

Given the major financial problems facing most of the nation's healthcare facilities today, one can easily understand how difficult it is for hospital administrators to allocate additional resources for a major contingency situation that: (a) is not a "profit center" per se; (b) is minimally paid for through federal grants; and (c) quite possibly may never be needed. Over the past few years most U.S. hospitals, with the possible exception of very large healthcare systems or trauma centers, tapped existing personnel to supervise the emergency planning required for the management of mass-casualty incidents and events. With the list of needs and requirements still increasing annually, though, many – probably most – of these hospital support people have felt overwhelmed by the planning and emergency-management tasks that have been added to their previous workloads.

The Joint Commission (JC – the organization responsible for the accreditation of U.S. hospitals and other healthcare facilities*), recently strengthened and increased the emergency-planning standards required for accreditation and, according to current plans, will publish even more rigorous requirements sometime next year.

The commission's actions, although both necessary and understandable, are forcing the nation's hospitals to ask themselves who, specifically, should be their new emergency managers, what his or her duties will be, and how much administrative and *budgetary* authority they will be given. The answers to those questions will be a reasonably accurate reflection of how seriously a task emergency management is considered to be by a specific hospital or other healthcare organization.

**The commission, founded in 1951 as the Joint Commission on Accreditation of Hospitals (JCAH), changed its name to JCAHO (Joint Commission on Accreditation of Healthcare Organizations) in 1987, but is now usually referred to simply as the Joint Commission. For more information on the Joint Commission see the commission's website: www.jointcommission.com*

***Theodore Tully** has been director of Trauma and Emergency Services at the Westchester Medical Center (WMC) in Westchester County, N.Y., since 1994. Prior to assuming that post he served as a police paramedic/detective and as the Westchester County EMS (emergency medical services) coordinator. He also helped create and administer the WMC Regional Resource Center, which is responsible for coordinating the emergency plans of 32 hospitals in the greater Westchester County area.*


ASYMMETRIC
WARFARE
Asymmetric
Threats
CBRNE-Terrorism
Newsletter
W
O
M
D

Climate change will displace millions in coming decades. Nations should prepare now to help them

By Gulrez Shah Azhar

Source: http://www.homelandsecuritynewswire.com/dr20180123-climate-change-will-displace-millions-in-coming-decades-nations-should-prepare-now-to-help-them

Jan 23 – Wildfires tearing across Southern California have forced thousands of residents to evacuate from their homes. Even more people fled ahead of the hurricanes that slammed into Texas and Florida earlier this year, jamming highways and filling hotels. A viral social media post showed a flight-radar picture of people trying to escape Florida and posed a provocative question: What if the adjoining states were countries and didn't grant escaping migrants refuge?

By the middle of this century, experts estimate that climate change is likely to displace between 150 and 300 million people. If this group formed a country, it would be the fourth-largest in the world, with a population nearly as large as that of the United States.

Yet neither individual countries nor the global community are completely prepared to support a whole new class of "climate migrants." As a physician and public health researcher in India, I learned the value of surveillance and early warning systems for managing infectious disease outbreaks. Based on my current research on health impacts of heat waves in developing countries, I believe much needs to be done at the national, regional and global level to deal with climate migrants.

Millions displaced yearly

Climate migration is already happening. Every year desertification in Mexico's drylands forces 700,000 people to relocate. Cyclones have displaced thousands from Tuvalu in the South Pacific and Puerto Rico in the Caribbean. Experts agree that a prolonged drought may have catalyzed Syria's civil war and resulting migration.

Between 2008 and 2015, an average of 26.4 million people per year were displaced by climate- or weather-related disasters, according to the United Nations. And the science of climate change indicates that these trends are likely to get worse. With each one-degree increase in temperature, the air's moisture-carrying capacity increases by 7 percent, fueling increasingly severe storms. Sea levels may rise by as much as three feet by the year 2100, submerging coastal areas and inhabited islands.

The Pacific islands are extremely vulnerable, as are more than 410 U.S. cities and others around the globe, including Amsterdam, Hamburg, Lisbon, and Mumbai. Rising temperatures could make parts of west Asia inhospitable to human life. On the same day that Hurricane Irma roared over Florida

in September, heavy rains on the other side of the world submerged one-third of Bangladesh and eastern parts of India, killing thousands.
Climate change will affect most everyone on the planet to some degree, but poor people in developing nations will be affected most severely. Extreme weather events and tropical diseases wreak the heaviest damage in these regions. Undernourished people who have few resources and inadequate housing are especially at risk and likely to be displaced.

Recognize and plan for climate migrants now

Today the global community has not universally acknowledged the existence of climate migrants, much less agreed on how to define them. According to international refugee law, climate migrants are not legally considered refugees. Therefore, they have none of the protections officially accorded to refugees, who are technically defined as people fleeing persecution. No global agreements exist to help millions of people who are displaced by natural disasters every year.
Refugees' rights, and nations' legal obligation to defend them, were first defined under the 1951 Refugee Convention, which was expanded in 1967. This work took place well before it was apparent that climate change would become a major force driving migrations and creating refugee crises.
Under the convention, a refugee is defined as someone "unable or unwilling to return to their country of origin owing to a well-founded fear of being persecuted for reasons of race, religion, nationality, membership of a particular social group, or political opinion." The convention legally binds nations to provide access to courts, identity papers and travel documents, and to offer possible naturalization. It also bars discriminating against refugees, penalizing them, expelling them or forcibly returning them to their countries of origin. Refugees are entitled to practice their religions, attain education and access public assistance.
In my view, governments and organizations such as the United Nations should consider modifying international law to provide legal status to environmental refugees and establish protections and rights for them. Reforms could factor in the concept of "climate justice," the notion that climate change is an ethical and social concern. After all, richer countries have contributed the most to cause warming, while poor countries will bear the most disastrous consequences.
Some observers have suggested that countries that bear major responsibility for greenhouse gas emissions should take in more refugees. Alternatively, the world's largest carbon polluters could contribute to a fund that would pay for refugee care and resettlement for those temporarily and permanently displaced.
The Paris climate agreement does not mention climate refugees. However, there have been some consultations and initiatives by various organizations and governments. They include efforts to create a climate change displacement coordination facility and a U.N. Special Rapporteur on Human Rights and Climate Change.
It is tough to define a climate refugee or migrant. This could be one of the biggest challenges in developing policies.
As history has shown, destination countries respond to waves of migration in various ways, ranging from welcoming immigrants to placing them in detention camps or denying them assistance. Some countries may be selective in whom they allow in, favoring only the young and productive while leaving children, the elderly and infirm behind. A guiding global policy could help prevent confusion and outline some minimum standards.

Short-term actions

Negotiating international agreements on these issues could take many years. For now, major G20 powers such as the United States, the European Union, China, Russia, India, Canada, Australia and Brazil should consider intermediate steps. The United States could offer temporary protected status to climate migrants who are already on its soil. Government aid programs and nongovernment organizations should ramp up support to refugee relief organizations and ensure that aid reaches refugees from climate disasters.
In addition, all countries that have not signed the United Nations refugee conventions could consider joining them. This includes many developing countries in South Asia and the Middle East that are highly vulnerable to climate change and that already have large refugee populations. Since most of the affected people in these countries will likely move to neighboring nations, it is crucial that all countries in these regions abide by

a common set of policies for handling and assisting refugees.

The scale of this challenge is unlike anything humanity has ever faced. By midcentury, climate change is likely to uproot far more people than the Second World War, which displaced some 60 million across Europe, or the Partition of India, which affected approximately 15 million. The migration crisis that has gripped Europe since 2015 has involved something over one million refugees and migrants. It is daunting to envision much larger flows of people, but that is why the global community should start doing so now.

Gulrez Shah Azhar *is Ph.D. Candidate, Pardee RAND Graduate School.*

Climate change will displace millions of people. Where will they go?

By Tiffany Challe

Source: http://www.homelandsecuritynewswire.com/dr20180123-climate-change-will-displace-millions-of-people-where-will-they-go

Jan 23 – Barbuda, the sister island of Antigua, is a small, low-lying Caribbean island. Most of its 1,700 residents lived in Codrington, the central location for stores and schools. The town is also the location for the Barbuda Research Complex, where I attended sustainability field school in 2014. What makes this island so unique? The beauty of the natural beaches untouched by tourism developments, the rich vegetation, diverse wildlife, fascinating archaeological sites and the people of Barbuda. During my three-week stay there, it became clear to me that Barbudans were a proud, happy and resilient people. Their community identity is heavily steeped in their food culture, which forges their intricate relationship with the environment. This entry in my field journal captures their spirit: "I admire how Barbudans respect and use all their resources on the island and understand their environment." Their livelihoods and culture center on fishing, hunting and farming. However, climate change has altered the island's food system and therefore their livelihoods. Droughts and rising seas that encroach on freshwater supplies are causing crop yields to decline, and Barbudans must increasingly rely on expensive imported foods.

Hurricane Irma hit Barbuda in September and decimated most of the island – 95 percent of the buildings and infrastructure were destroyed. One person died and countless animals were killed by debris or separated from their owners. For the first time in 300 years, the island was rendered uninhabitable. All the residents were evacuated and temporarily relocated to Antigua, where they still remain today. Barbudans are eager to return to the island, as they have a strong sense of place-based identity. Rebuilding efforts are currently under way, though funds are sorely lacking and a bitter dispute over land rights has ensued. This story illustrates tragedy for the islanders, who are at the front lines of climate change.

And they're not the only ones. This year, hurricane season hit U.S. coastal communities and islands in the Caribbean at an alarming scale, causing massive infrastructure damage and loss of life. Meanwhile, wildfires are wreaking havoc in Southern California. These natural disasters are influenced by a warming climate. As the sea level

rises and average temperatures continue to increase, these disasters will become more frequent and intense. Climate change is expected to displace millions of people in the coming decades, and countries will increasingly have to grapple with this issue.

When disaster strikes, what happens to the communities in harm's way? Where do the displaced people stay? Will they be able to return to their homes in areas that climate change may have rendered unlivable? Experts from Columbia University discussed these challenges and more at a recent event hosted by the Earth Institute.

Climate scientist Radley Horton from the Lamont-Doherty Earth Observatory moderated the panel. The speakers included: Lisa Dale, a lecturer in the undergraduate program in Sustainable Development; Alex de Sherbinin, a geographer at the Center for International Earth Science Information Network; and Michael Gerrard, director of the Sabin Center for Climate Change Law at Columbia Law School. The event was part of the Earth Institute's Climate Adaptation Initiative—a three-year project to enhance Columbia's impact on sustainability problem-solving. One of the themes of this initiative is climate-induced retreat to safer areas.

Where will climate migrants go?

Some experts estimate that climate change could force between 150 and 300 million people to find a new place to live by the middle of this century, though there is considerable uncertainty about the amount. Finding suitable locations to house them will be a significant impediment. As Michael Gerrard explained, "part of the problem is scale. If we're talking about millions of people having to be on the move, it just doesn't work."

In the U.S., there are very few habitable places that aren't already occupied by homes, businesses, or agriculture, or preserved as park lands or forests. Meanwhile, rural areas would provide few opportunities for migrants to find employment and rebuild their lives.

Instead, Gerrard suggested moving people from high-risk areas to cities whose populations are shrinking, such as Detroit, Michigan. He sees cities' potential for vertical development, energy-efficient buildings, and public transportation as a way to sustainably host climate migrants.

The 1951 Refugee Convention defines a protected refugee as someone who leaves his or her home country due to racial, religious, or social persecution, or reasonable fear of such persecution. These refugees have the right to seek asylum and protection from participating members of the United Nations (though these countries are not obligated to take them in). However, people displaced by climate change do not fit this definition. At the international level, there is no legal mechanism in place to protect climate migrants' rights and to ensure assistance from other countries. In terms of cross-border migration, Gerrard said, "there is no international law that compels a

country to take in people from other countries; it's wholly voluntary."

When should climate migration happen?

Once a major disaster strikes with little or no warning, victims can become 'distressed' migrants—people who have lost their homes and are forced to flee with nothing but the shirts on their backs.

A better scenario would be to resettle people outside of at-risk areas before disaster strikes. That way, people would have some degree of choice in where to go and what to bring.

However, Alex de Sherbinin pointed out that the U.S. government has no policy mechanism designed to relocate people before a disaster strikes.

Not only does relocating people cost money, but governments miss out on tax revenues if land is left empty. "This is why there is an impetus to build up and grow in vulnerable coastal zones," said de Sherbinin.

But it's not impossible to be proactive about climate migration. China has 'ecological migration,' a relocation program designed to anticipate future disasters. The government has resettled large communities from rural areas damaged by climate change, industrialization, and other problems. The program is partly an effort to reduce dust storms produced by agriculture. It works out economically because it was no longer financially tenable for the Chinese government to support these communities in rural areas.

Where would the money come from?

Michael Gerrard views carbon pricing as an ideal solution to funding climate relocation. Displacement by sea level rise, hurricanes, and wildfires is, as he put it, "a negative externality of burning fossil fuels, so if you were to build that into the price and pay for some of this through a price on carbon, you would generate a whole lot of money that way." In this scenario, the money paid by carbon emitters could help fund climate relocation while creating a major economic incentive to move away from fossil fuels.

The panelists agreed that countries also need to be forward-looking. In order to avoid the U.S. reactive disaster planning, we must plan ahead for future damage and associated costs from natural disasters when thinking about how to manage the retreat from at-risk areas.

Unfortunately, U.S. disaster response is typically reactive instead of proactive. Lisa Dale explained how, much like flood planning, the federal fire budget is backward-looking. "The U.S. Forest Service's annual budget is based on the last 10 years of fire costs," she said, "so they are always estimating too low." Meanwhile, the cost of suppressing fire has grown substantially, she added.

A more progressive approach would lead to better management of funds to add protective measures against climate-related catastrophes, build resilience, and in extreme cases relocate at-risk communities.

With a lack of finance, policy, and legal frameworks, managed retreat will be a huge challenge in the United States. So it is no wonder that developing nations are not receiving the financial and technical assistance they so desperately need to recover from disasters and to rebuild in a climate-resilient way. Gerrard pointed out that the U.S. is "one of the richest places on the planet and we're struggling to come up with resources to fund it."

Changing climate, changing cultures

For climate relocation to work, governments need to care and commit to international responsibility and burden-sharing. However, in the current global political context of fear of terrorism, an increased refugee influx into Europe, and an overall rise of xenophobia, countries are more likely to opt for stricter policies on cross-border migration. Rex Tillerson announced on 3 December that the U.S. is pulling out of the Global Compact for Migration, arguing (falsely, in Gerrard's view) that it was a threat to U.S. sovereignty.

"There is such an anti-immigrant fervor that it's hard to imagine the U.S. in the short-term taking in large numbers of people," Gerrard said.

According to Alex de Sherbinin, framing migration as a useful adaptation (and life- and cost-saving strategy), rather than a retreat, can encourage governments to take actions to support migration.

On the other hand, there is a human cost to any kind of permanent relocation: The threat of losing one's cultural heritage, particularly in native communities on coastal areas and islands such as Barbuda. Many islanders have a deep attachment to their homeland, which is inextricably linked to their culture and traditions.

Gaston Browne, the prime minister of Antigua and Barbuda, is pushing for tourism development and land

ownership to regenerate Barbuda's economy and reduce the island's reliance on Antigua. The Barbuda Land Act of 2007 formally recognized that citizens communally own Barbuda's land—a practice dating back hundreds of years—and must consent to major developments. In its place, Browne proposes to institute a system in which Barbudans can buy their plots for $1, opening up the possibility of securing bank loans for reconstruction. Many people and representatives in the Barbuda Council are opposed to this new system, as it would threaten their culture and would potentially open up their island to foreign investment and development.

As Alex de Sherbinin noted, "rebuilding homes is one thing, but also rebuilding communities and allowing the tissue of community to reform requires funds to facilitate."

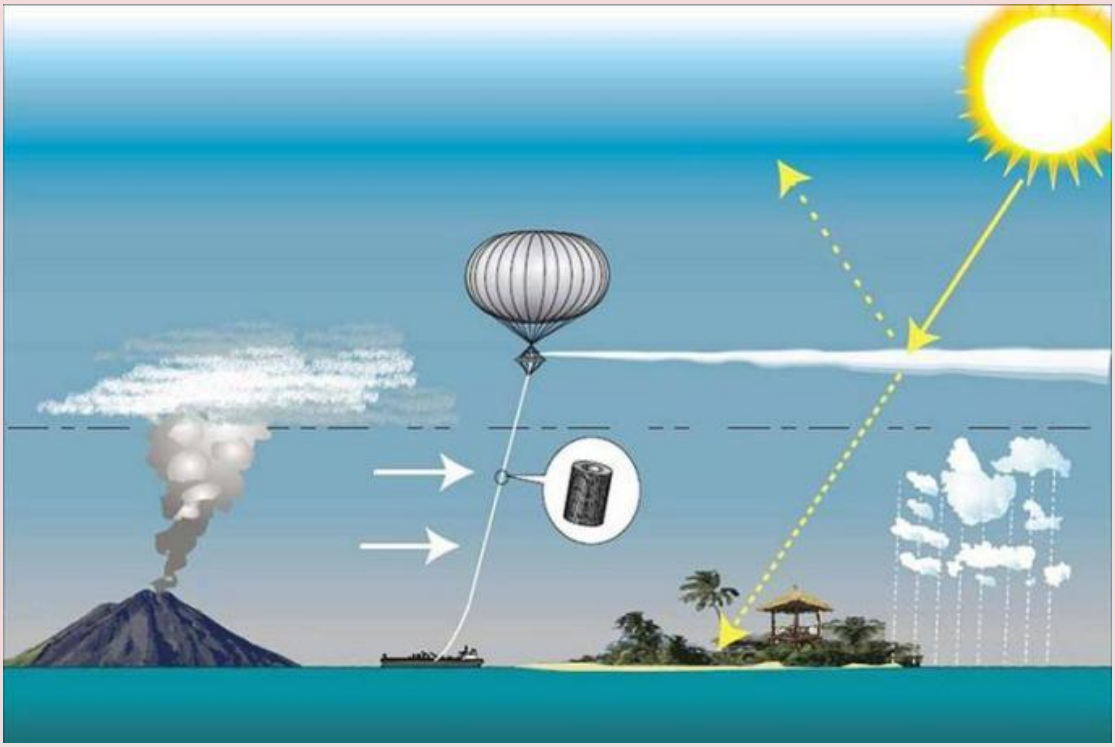
There is a lot of work ahead of us to solve the climate migration issue, and as Michael Gerrard pointed out, "it's really a question of trying to find sufficient humanity."

▶▶ **A video of the event,** *Climate Change Impacts: Relocation to Safer Ground*, can be found here.

***Tiffany Challe** is a communications associate at Columbia's Sabin Center for Climate Change Law.*

Climate engineering, if started, would have severe consequences if stopped abruptly

Source: http://www.homelandsecuritynewswire.com/dr20180124-climate-engineering-if-started-would-have-severe-consequences-if-stopped-abruptly



Jan 24 – **Facing a climate crisis, we may someday spray sulfur dioxide into the upper atmosphere to form a cloud that cools the Earth, but suddenly stopping the spraying would have a severe global impact on animals and plants, according to the first study on the potential biological impacts of geoengineering, or climate intervention.**

The study was published in *Nature Ecology & Evolution*. The paper was co-authored by Rutgers Distinguished Professor Alan Robock, research associate Lili Xia and postdoc Brian Zambri, all from the Department of Environmental Sciences at Rutgers University–New Brunswick. Other co-authors were from the University of Maryland, Yale University and Stony Brook University.

"Rapid warming after stopping geoengineering would be a huge

threat to the natural environment and biodiversity," Robock said. "If geoengineering ever stopped abruptly, it would be devastating, so you would have to be sure that it could be stopped gradually, and it is easy to think of scenarios that would prevent that. Imagine large droughts or floods around the world that could be blamed on geoengineering, and demands that it stop. Can we ever risk that?"

Geoengineering means attempting to control the climate in addition to stopping the burning of fossil fuels, the main cause of global warming, Robock said. While scientists have studied the climate impacts of geoengineering in detail, they know almost nothing about its potential impacts on biodiversity and ecosystems, the study notes.

The geoengineering idea that's attracted the most attention is to create a sulfuric acid cloud in the upper atmosphere as large volcanic eruptions do, Robock said. The cloud, formed after airplanes spray sulfur dioxide, would reflect solar radiation and cool the planet. But airplanes would have to continuously fly into the upper atmosphere to maintain the cloud because it would last only about a year if spraying stopped, Robock said. He added that the airplane spraying technology may be developed within a decade or two.

Rutgers says that in their study, the scientists used a global scenario with moderate cooling through geoengineering, and looked at the impacts on land and in the ocean from suddenly stopping it. They assumed that airplanes would spray 5 million tons of sulfur dioxide a year into the upper atmosphere at the Equator from 2020 to 2070. That's the annual equivalent of about one quarter of the sulfur dioxide ejected during the 1991 eruption of Mount Pinatubo in the Philippines, Robock said.

The spraying would lead to an even distribution of sulfuric acid clouds in the Northern and Southern Hemispheres. And that would lower the global temperature by about 1 degree Celsius (about 1.8 degrees Fahrenheit) – about the level of global warming since the Industrial Revolution began in the mid-1800s. But halting geoengineering would lead to rapid warming – 10 times faster than if geoengineering had not been deployed, Robock said.

The scientists then calculated how fast organisms would have to move to remain in the climate – in terms of both temperature and precipitation — that they are accustomed to and could survive in, he said.

"In many cases, you'd have to go one direction to find the same temperature but a different direction to find the same precipitation," Robock said. "Plants, of course, can't move reasonably at all. Some animals can move and some can't."

He noted that national parks, forests and wildlife refuges serve as sanctuaries for animals, plants and other organisms. But if rapid warming forced them to move, and even if they could move fast enough, they may not be able find places with enough food to survive, he said.

One surprising side effect of rapidly starting geoengineering would be an El Niño warming of the sea surface in the tropical Pacific Ocean, which would cause a devastating drought in the Amazon, he said.

"We really need to look in a lot more detail at the impact on specific organisms and how they might adapt if geoengineering stops suddenly," he said.

— Read more in Christopher H. Trisos et al., "Potentially dangerous consequences for biodiversity of solar geoengineering implementation and termination," Nature Ecology & Evolution (22 January 2018).


CBRNE-Terrorism Newsletter
W
O
M
D
OPEN FOR BUSINESS AS USUAL
Business Interruption
Disaster Event
Business Continuity

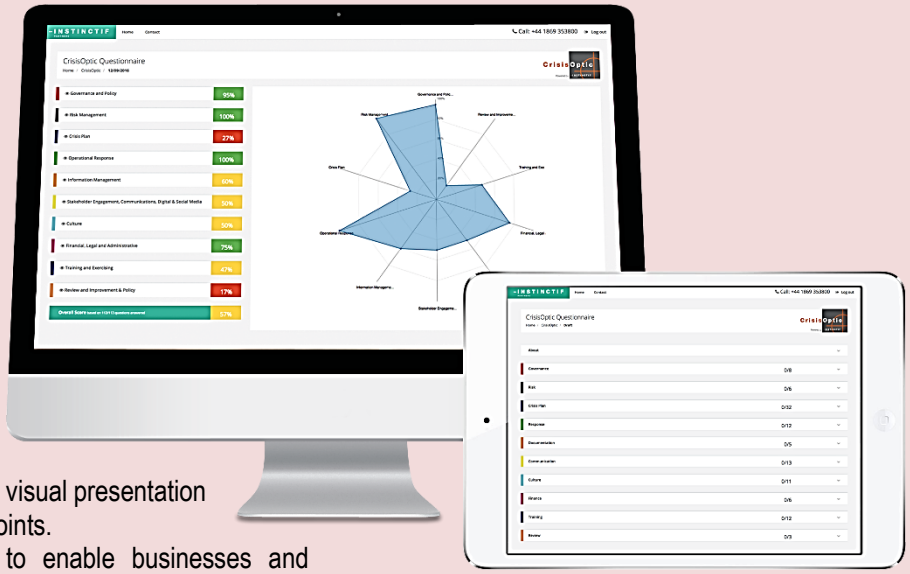
Software identifies common trends and weaknesses in crisis preparedness and business resilience

Source: https://www.crisis-response.com/news/news.php?article=1476

November 2017 – One year on from their successful launch, the CrisisOptic and RecallOptic diagnostic tools have helped more than 50 businesses and organisations quantify their business resilience, says Instinctif Partners.

Free to use, these online tools help businesses and organisations to accurately identify strengths and weaknesses in their approach to business resilience and assist them to focus on the specific areas where they are most exposed.

Victoria Cross, who leads Instinctif Partners' Business Resilience team, said: "A year on from their launch, these tools have been very well received, helping businesses ranging from major food companies to one of the UK's leading health and fitness groups, to take an in-depth look at the business resilience of their organisations.



"Trends from the data we have generated so far show conducting and learning from a thorough post-incident review as the most common area of weakness, with gaps in governance and communication also widespread."

CrisisOptic is an online questionnaire that quickly provides businesses with a snapshot of their preparedness by examining business resilience in ten key areas, from governance and risk management to operational response. Using a carefully weighted assessment system, CrisisOptic generates a bespoke Business Resilience Score and visual presentation based on the examination of 112 data points.

RecallOptic uses the same process to enable businesses and organisations to quantify their product recall readiness against international best practice.

Following completion of the questions, business resilience experts from Instinctif Partners prepare a brief report to accompany the score that can be used to inform policies, procedures and capabilities, to strengthen risk and issues management, and crisis preparedness, and recall readiness.

Victoria Cross concludes: "CrisisOptic has been a game-changer for business resilience, antifragility, and risk and crisis management. Prior to its launch it was impossible to quickly identify strengths and weaknesses across an organisation and comprehensively compare the results against a peer group, but this is exactly what CrisisOptic provides. It's fast, accurate and enables organisations to focus finite resources on the specific areas where they are most exposed."

▶▶ **To calculate your business resilience or recall readiness visit** www.instinctif.com/optic