2 CBRNE DIARY

Dedicated to Global
First Responders

CBRNE-Terrorism Newsletter
W O M D

December 2019

www.cbrne-terrorism-newsletter.com

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DIRTY R-NEWS

The diverse applications of radioisotopes in modern-day industry

By Steven Pike

Source: https://www.argonelectronics.com/blog/applications-radioisotopes-modern-industry

Dec 03 – The ability to predict, recognise and identify the presence of potentially hazardous levels of ionising radiation in even the most "routine" of locations is a crucial skill when responding to HazMat or CBRNe incidents.

While it is not always possible to know exactly which radiological hazards may be involved in any given situation, the environment or location of an incident can often provide vital clues as to the type and quantity of radiological material that is likely to be present.

The variety of settings in which radioisotopes are put to use is surprisingly extensive - with safe quantities of radiological materials being utilised in sectors as diverse as agriculture, mining, food production, manufacturing, construction, oil & gas, molecular biology and nuclear medicine.

In this blog post we provide an overview of the history, nature and modern-day applications of radioisotopes - and the many "everyday" environments in which they may potentially be encountered by those tasked with emergency first response.

An overview of industrial isotopes

Radioisotopes emit one of three predominant types of radiation: alpha particles, beta particles and gamma rays.

Each radioisotope has its own unique properties which makes it a useful tool in solving a specific problem.

Broadly speaking, industrial isotopes fall into two sub-categories: those which are naturally-occurring (of which there are only a few) and those which are artificially-produced.

Examples of naturally-occurring isotopes include:

- **Carbon-14** - used to measure the age of wood, carbon-containing materials and subterranean water)
- **Chlorine-36** - used to measure sources of chloride and the age of water, up to 2 million years
- **Lead-210** - used to date layers of sand and soil up to 80 years

Among the variety of artificially-produced radioisotopes are:

- **Cobalt-60** - widely used in gamma sterilisation and **industrial radiography**
- **Caesium-137** - used as a radiotracer in identifying sources of soil erosion and soil deposition and for low-intensity gamma sterilisation
- **Selenium-75** - used in gamma radiography and non-destructive testing (NDT)
- **Gold-198** - used to study the movement of sewage and liquid waste, sand movement in river beds and ocean floors and to trace the causes of ocean pollution

Early discovery and development of isotopes

For well over a century, scientists have understood that many of the earth's elements occur in different atomic configurations or isotopes - and some of these possessed radioactive qualities.

The existence of naturally decaying atoms, or radioisotopes, was the subject of much contention within the global scientific community until the early 1920s, when Francis Aston's Nobel-prize-winning experiments in mass spectrography and his reinterpretation of atomic theory formulated what was described as "a new atomic paradigm."

Research into the nature and characteristics of radioisotopes reached another crucial milestone in the 1930s with Ernest Lawrence's invention of an improved version of the particle accelerator, known as the cyclotron.

Scientists soon discovered that by bombarding different materials with cyclotron-produced high energy beams it was possible to obtain small quantities of artificial radioisotopes.

Modern applications of industrial isotopes

Sealed radioactive sources are widely used in industrial radiography, gauging applications and for mineral analysis.

Radioactive materials have a key role to play in the inspection of metal parts and the integrity of welds, using industrial gamma radiography to inspect critical internal components for defects.

Within manufacturing, radioisotopes act as industrial tracers to monitor filtration and the flow of fluids, to locate leaks, to gauge wear and to monitor the corrosion of equipment.

In the oil and gas industry, radiotracers are used to determine the extent of oil fields, to log formation parameters, to determine injection profiles and to locate cracks caused by hydraulic fracturing.

Gamma radiography also been successfully put to use in inspecting the integrity of critical civil structures such as hospitals, schools, civic buildings etc in the aftermath of natural disasters such as the devastating earthquake in Nepal in 2015.

Nucleonic gauges are especially useful where the presence of corrosive substances, pressure or heat make it difficult, or impossible, to use direct contact gauges.

In addition, they also offer the key advantage of being employed without requiring any direct physical contact with the material or the product being examined.

Medical applications of industrial isotopes

The commercial availability of radioisotopes has spearheaded some of the most significant transformations in science and biomedicine, as well as playing a major role in the rise of molecular biology.

According to the World Nuclear Organisation, an estimated 10,000 hospitals worldwide use radioisotopes as part of their radiotherapy practices on a routine basis, with approximately 90% of procedures (representing some 40 million annually) being used solely for the purposes of medical diagnosis.

The applications for radioactive materials within the world of medicine are wide-ranging, with perhaps the most commonly known being the use of x-ray radiography in the conducting of medical examinations.

Under the broader banner of radiography there are also a wide variety of specialised areas that utilise radioactive sources - including computerized tomography (CT) scanning, cardiology, mammography and nuclear medicine therapies in which safe quantities of radioactive materials are injected into the body.

Radioisotopes have a multitude of practical and life-saving uses in our modern world. However, their potentially hazardous properties also dictate that their use be closely regulated.

Inevitably, there will be instances where accidents occur - and in such situations it is vital that those tasked with responding to the scene are able to recognise, and safely manage, the hazard that they encounter.

For anyone working within the field of HazMat, CBRNe or radiation protection, having an understanding of the applications of radioisotopes, and the wide variety of environments in which they may be present, will be a vital factor in maintaining safety.

Lessons Learnt from Fukushima Soil Decontamination

Source: http://www.homelandsecuritynewswire.com/dr20191213-lessons-learnt-from-fukushima-soil-decontamination

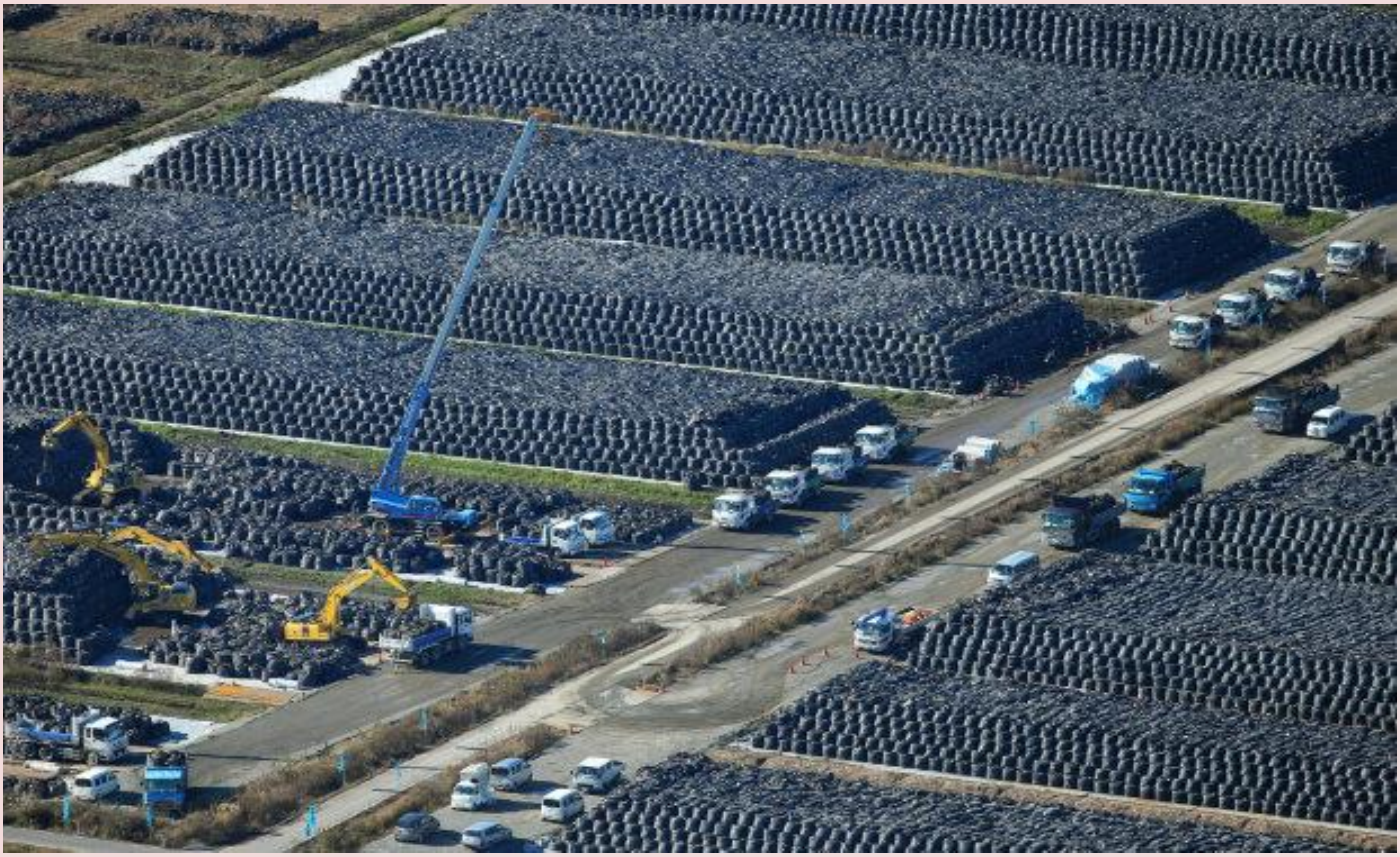
Dec 13 – Following the accident at the Fukushima nuclear power plant in March 2011, the Japanese authorities decided to carry out **major decontamination works in the affected area, which covers more than 9,000 km².** On 12 December 2019, with most of this work having been completed, the scientific journal *Soil* of the European Geosciences Union (EGU) is publishing a synthesis of approximately sixty scientific publications that together provide an overview of the decontamination strategies used and their effectiveness, with a focus on radiocesium. This work is the result of an international collaboration led by Olivier Evrard, researcher at the Laboratoire des Sciences du Climat et de l'Environnement [Laboratory of Climate and Environmental Sciences] (LSCE – CEA/CNRS/UVSQ, Université Paris Saclay).

The EGU says that soil decontamination, which began in 2013 following the accident at the Fukushima Dai-ichi nuclear power plant, has now been nearly completed in the priority areas identified[1]. Indeed, areas that are difficult to access have not yet been decontaminated, such as the municipalities located in the immediate vicinity of the nuclear power plant. Olivier Evrard, a researcher at the Laboratory of Climate and Environmental Sciences and coordinator of the study (CEA/CNRS/UVSQ), in collaboration with Patrick Laceby of Alberta Environment and Parks (Canada) and Atsushi Nakao of Kyoto Prefecture University (Japan), compiled the results of approximately sixty scientific studies published on the topic.

This synthesis focuses mainly on the fate of radioactive cesium in the environment because this radioisotope was emitted in large quantities during the accident, contaminating an area of more than 9,000 km². In addition, since one of the cesium isotopes (^{137}Cs) has a half-life of thirty years, it constitutes the highest risk to the local population in the medium and long term, as it can be estimated that in the absence of decontamination it will remain in the environment for around three centuries. "The feedback on decontamination processes following the Fukushima nuclear accident is unprecedented," according to Olivier Evrard, "because it is the first time that such a major clean-up effort has been made following a nuclear accident. The Fukushima accident gives us valuable insights into the effectiveness of decontamination techniques, particularly for removing cesium from the environment."

This analysis provides new scientific lessons on decontamination strategies and techniques implemented in the municipalities affected by the radioactive fallout from the Fukushima

accident. This synthesis indicates that **removing the surface layer of the soil to a thickness of 5 cm, the main method used by the Japanese authorities to clean up cultivated land, has reduced cesium concentrations by about 80 percent in treated areas.** Nevertheless, the removal of the uppermost part of the topsoil, which has proved effective in treating cultivated land, has cost the Japanese state **about €24 billion.** This technique generates a significant amount of waste, which is difficult to treat, to transport and to store for several decades in the vicinity of the power plant, a step that is necessary before it is shipped to final disposal sites located outside Fukushima prefecture by 2050. By early 2019, Fukushima's decontamination efforts had generated about 20 million cubic metres of waste.



Decontamination activities have mainly targeted agricultural landscapes and residential areas. The review points out that the forests have not been cleaned up – because of the difficulty and very high costs that these operations[2] would represent – as they cover 75 percent of the surface area located within the radioactive fallout zone. These forests constitute a potential long-term reservoir of radiocesium, which can be redistributed across landscapes as a result of soil erosion, landslides and floods, particularly during typhoons that can affect the region between July and October. Atsushi Nakao, co-author of the publication, stresses the importance of continuing to monitor the transfer of radioactive contamination at the scale of coastal watersheds that drain the most contaminated part of the radioactive fallout zone. This monitoring will help scientists understand the fate of residual radiocesium in the environment in order to detect possible recontamination of the remediated areas due to flooding or intense erosion events in the forests.

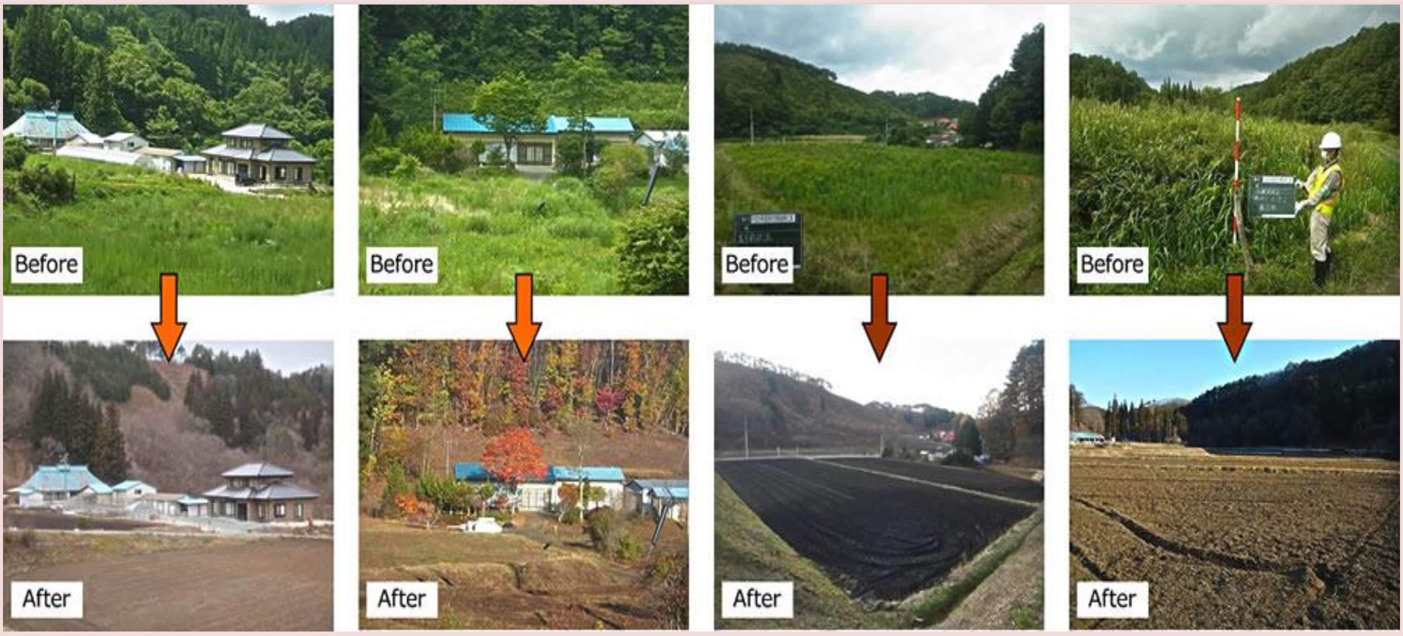
The analysis recommends further research on:

- the issues associated with the recultivation of decontaminated agricultural land[3],
- the monitoring of the contribution of radioactive contamination from forests to the rivers that flow across the region,
- and the return of inhabitants and their reappropriation of the territory after evacuation and decontamination.

This research will be the subject of a Franco-Japanese and multidisciplinary international research project, MITATE (Irradiation Measurement Human Tolerance viA Environmental Tolerance), led by the CNRS in collaboration with various French (including the CEA) and Japanese organizations, which will start on 1 January 2020 for an initial period of five years.

Complementary Approaches

This research is complementary to the project to develop bio- and eco-technological methods for the rational remediation of effluents and soils, in support of a post-accident agricultural rehabilitation strategy (DEMETERRES), led by the CEA, and conducted in partnership with INRA and CIRAD Montpellier.



Decontamination techniques

- ❖ In cultivated areas within the special decontamination zone, the surface layer of the soil was removed to a depth of 5 cm and replaced with a new "soil" made of crushed granite available locally. In areas further from the plant, substances known to fix or substitute for radiocesium (potassium fertilizers, zeolite powders) have been applied to the soil.
- ❖ As far as woodland areas are concerned, only those that were within 20 metres of the houses were treated (cutting branches and collecting litter).
- ❖ Residential areas were also cleaned (ditch cleaning, roof and gutter cleaning, etc.), and (vegetable) gardens were treated as cultivated areas.

[1] In Fukushima prefecture and the surrounding prefectures, the decision to decontaminate the landscapes affected by the radioactive fallout was made in November 2011 for 11 districts that were evacuated after the accident (special decontamination zone – SDZ – 1,117 km^2) and for 40 districts affected by lower, but still significant levels of radioactivity and that had not been evacuated in 2011 (areas of intensive monitoring of the contamination – ICA, 7836 km^2).
[2] 128 billion euros according to one of the studies appearing in the review to be published on 12 December 2019 in SOIL.
[3] Relating to soil fertility and the transfer of radiocesium from the soil to plants, for example.

Lethal flu strains, dirty radiation bombs — can humans survive?

By Lisa M. Krieger

Source: https://www.mercurynews.com/2019/12/21/lethal-flu-strains-dirty-radiation-bombs-can-humans-survive/

Dec 21 – Inspired by recent breakthroughs in genetics, Bay Area scientists are dialing up our inner strength to survive a bioterrorism attack.

Two Defense Department-funded projects strive to give us a new kind of DNA superpower if a rogue actor unleashed a lethal flu virus or a radiation-laced "dirty bomb."

Our existing tools — vaccines, medicines, even bone marrow transplants — aren't fast or furious enough to defend us.

So, the Bay Area teams — at Stanford, UC San Francisco, UC Berkeley and the San Francisco biotech firm DNARx – are using a modified form of CRISPR gene editing to boost our body's ability to briefly and reversibly protect us from these threats. The concept: In a crisis, we'd get a quick "puff" of gene-altered medicine to the lungs, like asthma treatment.

If successful, the therapies could be given before or after exposure to reduce illness and death.

"Researchers seek to improve rates of survival and recovery in catastrophic scenarios for which reliable countermeasures don't currently exist," said Renee Wegrzyn, program manager for the military's PREPARE (Preemptive Expression of Protective Alleles and Response Elements) initiative.

The science behind the projects could have powerful peacetime application, as well – helping us fend off ordinary dangers such as aggressive strains of seasonal flu and high-dose radiation cancer treatment.

The initiative is funded by the military's "mad science" venture capital program, called DARPA, which pioneered technologies ranging from the Internet and personal computer to the laser and disaster relief robots. DNARx and the Stanford scientists were awarded up to $10.7 million. UCSF and UC Berkeley, through their collaboration called Innovative Genomics Initiative, received $10 million, with another $10 million awarded in two years.

It's a biological version of the nation's ballistic missile defense program, our network of interceptors, radars, sensors and weapons designed to track and destroy an incoming attack.

Experts say that if a terrorist designed and released a deadly flu virus, it would overwhelm our healthcare system. Three times in the last century — the 1918 global outbreak also known as the Spanish flu, the 1957 Asian flu and the 1968 Hong Kong flu — virulent strains of the virus killed millions.

A radioactive bomb would also quickly strain our resources. Now we treat victims of radiation illness with transfusions and medications. But very large doses of nuclear fallout are lethal. Additionally, resilience to radiation would also help the thousands of cancer patients in the U.S. who get therapy to shrink their tumors – but must reduce exposure due to illness, which gives cancers a chance to regrow.

Despite the advantages, some critics fear that developing enhanced bio-defenses could trigger a biological arms race with other nations.

They worry that the U.S. could leverage this biotech advantage, using it to protect soldiers in an offensive, not defensive, strategy. Or it could be used to reduce the enemy population's immune defenses.

"Inadvertently, the project may contribute to rising international tensions in the biological field," said Filippa Lentzos, a senior research fellow in the Departments of War Studies and of Global Health and Social Medicine at England's King's College London.

"Prepare is a defensive program, but what if intentions change? What if all of a sudden there is a military advantage to using the technology offensively? How can other countries be certain the United States will not leverage that technological advantage?" she said. The second concern, she added, is that "capacity build-ups in the United States will likely be echoed in other countries in a sort of biological arms race. This increases overall risks of the technology being misused and causing considerable damage."

In an article in the Bulletin of Atomic Scientists — entitled "Preparing for What?" — she instead urged other biodefensive measures, such as better protective masks and clothing, air and water filtration systems, detection and identification devices, and decontamination systems.

But given the ubiquity of biotechnology, DARPA says it is important to plan for weaponized pathogens.

It sounds like sci-fi. But these tools simply harness the power of our own innate defenses, written in our DNA, say scientists.

Every day, our body fends off the natural radiation of the sun. And our immune system mounts a defense when we get the flu. But these responses aren't enough to defend us from a catastrophic onslaught.

"The human body is amazingly resilient. Every one of our cells already contains genes that encode for some level of resistance to specific health threats, but those built-in defenses can't always express quickly or robustly enough to be effective," said Wegrzyn, in a statement.

The project was conceived as a result of breakthroughs in the field of genetic editing, launched by discovery of the tool CRISPR-Cas9. This revolutionary technology is less than a decade old, but its use has already exploded in medical and agricultural research and is anticipated to grow into a $10 billion market in 2025.

But unlike CRISPR-Cas9, the goal isn't to permanently edit our underlying genetic code. Instead, it uses a modified form of the technique to control genes' function, changing the behavior of cells.

Rather than cutting DNA, it binds to it — and can swap in different molecular tools to dial up or down gene expression. Repressor molecules work like red lights, telling gene activity to stop. Activator molecules are like green lights, telling it to go. This influences the production of protective proteins.

The gene changes are transient, so they'd only last for a couple of weeks or months. They're not passed on to future generations.

"Deliver the message," said professor Jonathan Weissman of the Department of Cellular and Molecular Pharmacology at UCSF, who is working with IGI's Fyodor Urnov to combat radiation. "And once the messenger is gone, you're back to normal."

The specific strategies differ for flu and radiation exposure.

To combat flu, Stanford teams led by the San Francisco biotech company DNARx, under investigator Dr. Robert Debs, aim to develop a gene therapy that prevents infection by boosting the natural immune response and other protective functions of our nasal passages and lungs.

They're also developing a gene therapy that could kill the virus in infected cells, so it doesn't multiply and cause an epidemic.

"Hopefully, you can protect the cell from being infected – but if it is, you want to stop the virus from taking over the cells," said Debs. He is working with Stanford's pediatric immunologist David Lewis, bioengineer Stanley Qi and research scientist Marie LaRussa.

This new approach, which could be administered as a nebulizer or inhaler, could provide near instantaneous immunity from all types of influenza viruses – and prevent epidemics.

If successful, it could also be used against the fast-changing strains of flu that race around the globe every year — and other deadly viruses in the future.

Invincibility against nuclear fallout means finding a different target. A team led by Weissman is finding genes — especially in the rapidly dividing blood and gut cells — that when turned on or off can protect against acute radiation sickness.

"We are not just keeping these cells alive," said Weissman. "We're keeping them alive in a way that they still have the ability to replenish."

The researchers strive to create treatments that could be given either before or after exposure, and persist for several weeks.

It could also help astronauts survive radiation while traveling in space.

Before being tested in humans, both approaches need to be tested extensively in animals. Three other research universities, in addition to Stanford and IGI, have been awarded contracts. By the end of the project, DARPA wants the teams to submit at least one product for Food and Drug Administration approval.

It's a futuristic bet, the scientists agree.

"But there is nothing inherent about life," Weissman said, "that it can't survive."

***Lisa M. Krieger** is a science writer at The Mercury News, covering research, scientific policy and environmental news from Stanford University, the University of California, NASA-Ames, U.S. Geological Survey and other Bay Area-based research facilities. Lisa also contributes to the Videography team. She graduated from Duke University with a degree in biology. Outside of work, she enjoys photography, backpacking, swimming and bird-watching.*

International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C²BRNE DIARY

EXPLOSIVE NEWS

To counter IED threats, Army to use artificial intelligence e-tool

Source: https://www.tribuneindia.com/news/nation/to-counter-ied-threats-army-to-use-artificial-intelligence-e-tool/866054.html

Nov 25 – As the threat from improvised explosive devices (IEDs) in the country continues unabated, the Army is developing an artificial intelligence-based e-tool for analysing past incidents and developing customised decision support models.

Called **IED Database Management and Analytical Platform (IDMAP),** the project is being executed by engineering training institutions and technical establishments under the aegis of the Army Training Command, sources said.

IEDs are defined as "homemade" bombs of varying shape and size, generally fabricated by terrorists or criminal elements from explosives and other openly available materials. These can be disguised as items of common use or be placed in bags and vehicles. IEDs can be quite effective against security forces as well as the public.

The terror attack in Pulwama earlier this year that killed 40 CRPF personnel is a recent example of an IED attack.

According to official reports, IEDs have killed over 260 security personnel in the past three years in India. Only today, the Delhi Police claimed to have averted a terror attack by arresting three persons and recovering an IED.

The IEDs have been extensively used in India by terrorists in Jammu and Kashmir and the northeast and by naxals in the red corridor as well as in other conflict-infected places such as Pakistan, Afghanistan, Ireland, Beirut, Syria, Lebanon and Iraq. There have also been isolated instances of IEDs being used in other places. In Boston, a pressure cooker was used to construct an IED.

"IDMAP is being designed to compile a comprehensive database of IED-related incidents worldwide, analyse the type of the IED used, the manner of its deployment, the perpetuators of the incident and the political and security background in the affected area, and use artificial intelligence to throw up actionable solutions that can be applied in specific situations," an officer said.

A key element of the system would be the domain knowledge base comprising standard operating procedures, training syllabus, available equipment and technical support, human resources and research literature on the subject, which can be integrated and collated. A user would be able to define his operational requirement and extract pertinent information.

An added feature of IDMAP would be a geographic information database containing digital maps, emergency centres such as police stations and hospitals, populated areas and important landmarks that could be used for situational awareness and decision support, sources added.

Conan, dog injured in al Baghdadi raid, honored by President Trump at White House

Source: https://www.foxnews.com/politics/conan-dog-injured-in-al-baghdadi-raid-honored-by-president-trump-at-white-house

Nov 26 – The dog injured during the mission that killed ISIS leader Abu Bakr al-Baghdadi was honored Monday afternoon during a surprise ceremony at the White House, with President Trump, Vice President Pence and First Lady Melania in attendance.

Conan, a Belgian Malinois who was named after talk show host Conan O'Brien, was hailed by Trump as a "special" animal who helped execute a "flawless attack" on the ISIS leader.

"Conan came over from the Middle East -- just arrived with some of the great people from the special forces that did the -- it was a flawless attack," the president said. "And al-Baghdadi is gone. That was a flawless attack and I just met quite a few of them. And we just gave Conan a medal and a plaque.

As the president spoke, Conan stood next to Vice President Mike Pence, who petted his head.

"And I actually think Conan knew exactly what was going on," Trump continued. "The dog is incredible... We spent some good time with it. And so brilliant -- so smart.

"The way it was with the special forces people that have worked with him, for obvious reasons they can't be out in front of the media," he added. "But they did a fantastic job. Conan did a fantastic job. We're very honored to have Conan here."

Conan has since recovered from his injuries and returned to active duty.

At one point while the first lady and Conan were walking back toward the White House, a reporter asked if she had any interest in adopting Conan as a pet for her son Baron, and she laughed before replying, "no."

U.S. forces killed six ISIS members – four women and another man aside from Baghdadi – in the October raid. Baghdadi detonated an explosive vest as U.S. forced closed in, also killing two children he had brought with him into a tunnel.

The death of Baghdadi was a milestone in the fight against ISIS, which brutalized swaths of Syria and Iraq and sought to direct a global campaign from a self-declared “caliphate.” A yearslong campaign by American and allied forces led to the recapture of the group's territorial holding, but its violent ideology has continued to inspire attacks.

Baghdadi's identity was confirmed by a DNA test conducted onsite, Trump said. The ISIS leader was later buried at sea.

Some have called for the heroic canine to receive a Purple Heart. Earlier this month, Lt. Col Daniel Gade directly addressed the president and offered up his own Purple Heart to Conan as a symbol of the canine's accomplishments.

“Look, these dogs are heroic. The president’s instincts are right and right on the Purple Heart medal, it says, ‘The President of the United States,’” Gade explained on "Fox & Friends," rejecting the Pentagon's policy on the matter.

3D-printed training ‘bombs’ drastically cut costs for US Air Force in England

Source: https://www.stripes.com/news/3d-printed-training-bombs-drastically-cut-costs-for-us-air-force-in-england-1.608622

Nov 25 – A 3D printer has slashed the time and cost required to get explosive training devices to the experts at RAF Lakenheath who need them as they prepare for deployments.

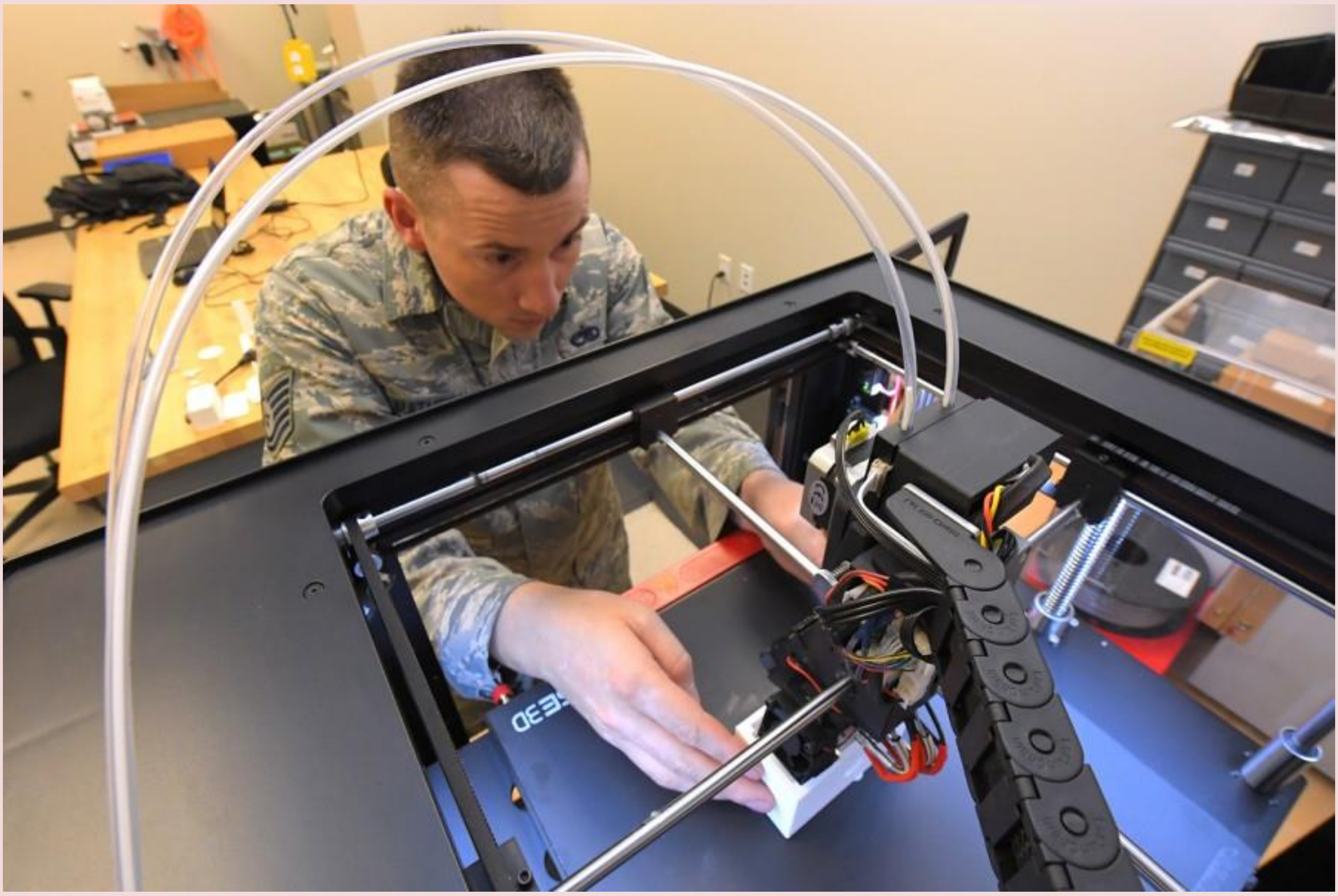
Staff Sgt. William Riddle has been using a 3D printer to produce dummy improvised explosive devices, rocket-propelled grenades and mortars that are used to train the explosive ordnance disposal airmen with the Air Force's 48th Fighter Wing at Lakenheath, cutting the cost and time of having the training devices shipped from the U.S.

“A decent year’s worth of ordnance training for a flight of 25 airmen costs about $60,000” when the dummy weapons are made and shipped from the U.S., Riddle said.

But using a 3D printer, the cost of producing the “weapons” falls by 96%, the 48th Fighter Wing said in a statement.

Printing the training aids at Lakenheath also saves time, said wing spokeswoman Capt. Miranda Simmons.

“Using traditional purchasing methods, it takes approximately 30 days for procurement, but with this innovative process, it now takes between 24 and 48 hours,” Simmons said in an email.



The new system also promotes safety by cutting down “the time it takes for our EOD technicians in a deployed location to work on a possibly live munition,” Riddle said. “This … means less time being deployed, resulting in less time in danger. They can do their job and come back home safely.”

The printing system is easy to learn, too, said Riddle. “I can take anyone who hasn’t done any 3D printing and give them a five-minute tutorial and have them printing with ease,” he said.

Riddle is set to brief the Innovation and Transformation Board at U.S. Air Forces in Europe — Air Forces Africa on his idea, for which he recently received an award from the 48th Continuous Process Improvement Office.

If the board approves the idea, it could be offered to EOD units across the theater, said USAFE spokesman Capt. Christopher Bowyer-Meeder.

EOD Marines receive new IED wire detector

Source: https://www.dvidshub.net/news/351900/eod-marines-receive-new-ied-wire-detector

Nov 15.— Explosive Ordnance Disposal Marines recently received new handheld detectors to locate command detonation wires on improvised explosive devices.

The **Buried Command Wire Detector** is a portable device that can identify command wires of various types and diameters. Fielded to EOD Marines in the fourth quarter of 2019, the wire detector includes a one-piece foldable design that is lighter and more time-efficient than the previous systems.
The device reached Full Operational Capability for EOD Marines in September 2019.
"Instead of carrying multiple tools, Marines have one device to use for detection purposes," said Master Sgt. Joseph Kenyon, project officer for Bridging, M9 Armored Combat Earthmover and Family of Engineer Construction Tool Kit at Marine Corps Systems Command.
Physically similar to a compact metal detector, the system is an easy-to-use device that does not require manual calibration. It is operational in a short amount of time and includes a long-lasting battery, said Kenyon.
Kenyon emphasized the importance of locating IED command wires in completing missions and protecting Marines. He noted how the BCWD supports EOD teams when disarming and destroying anti-personnel explosive devices.
In the past, these teams identified IEDs visually or by tracking components after explosion. The newer system enables Marines to accurately pinpoint command wires prior to detonation, which saves time and lives.
"The Buried Command Wire Detector allows Marines the ability to have a multi-tool detector, enhancing lethality through increased detection and identification in a hazardous environment," said Michael Poe, team lead for MCSC's Mobility/Counter Mobility program.
For years, Marines employed handheld metal and carbon rod detectors to ascertain remote threats. However, the BCWD has several advantages over the existing system, said Kenyon.
"The Buried Command Wire Detector has more sensors than the previous system," said Kenyon. "The new device can detect wire and conductive material better."
EOD Marines are the only group to have received the system. However, MCSC plans to field the BCWD to combat engineers, infantrymen, military police, artillery Marines and Light Anti-aircraft Defense teams later in fiscal year 2020.

Smart vehicle-camera system designed to spot IEDs

Source: https://newatlas.com/military/smart-camera-system-spots-ieds/

US Army vehicles make their way around blast holes caused by Improvised Explosive Devices, in Southern Afghanistan (SrA Kenny Holston/US Air Force)

Dec 10 – Improvised Explosive Devices (IEDs) can be very difficult for soldiers to detect, as they're made in a wide variety of shapes and sizes, and are typically buried in the road. A new vehicle-mounted system, however, is designed to "spot the signs" of IEDs.
The technology is being developed by a team led by electrical engineer Dennis van de Wouw, of the Netherlands' Eindhoven University of Technology. Hardware-wise, it incorporates a stereoscopic video camera, a GPS positioning system, and an image-analyzing computer/interface – all of these components would be installed in existing military vehicles.
When such a vehicle was out and about, its camera would be trained on the road ahead.
Utilizing the GPS and the image-analysis platform – along with artificial intelligence-based algorithms – real-time images of that road would be compared to previously-recorded images of the same location. If "warning signals" were detected, such as evidence of recent soil

disturbances or above-ground triggering devices, the vehicles' occupants would be alerted to their location through the interactive interface.

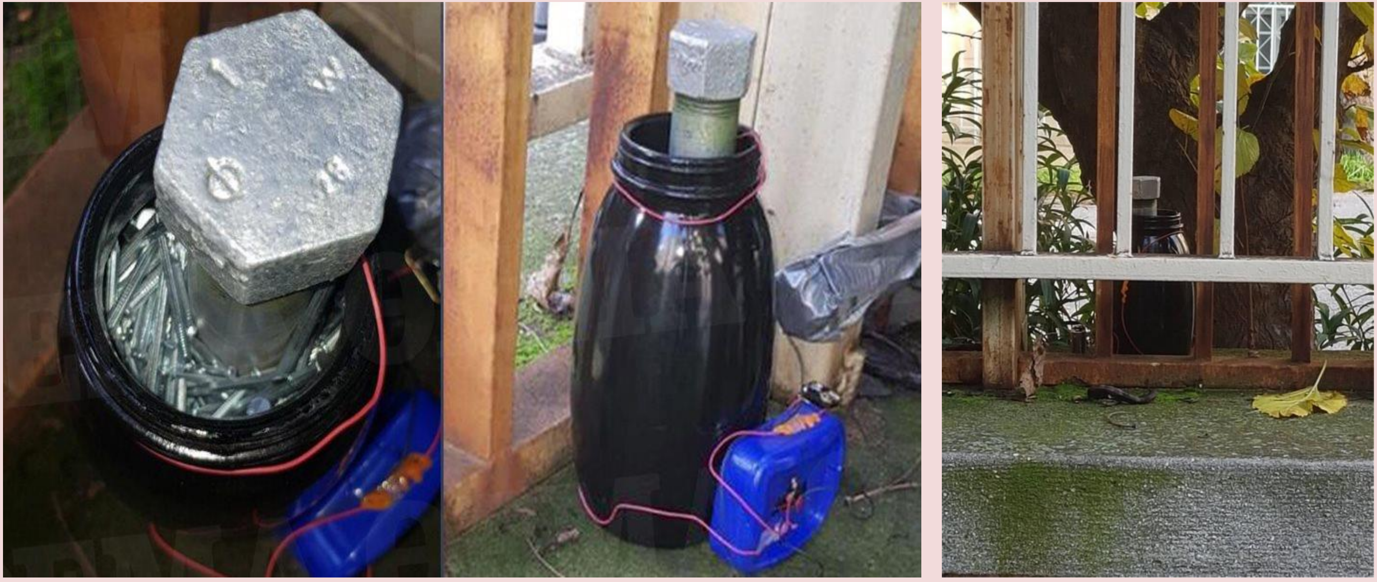
A test vehicle equipped with the new system (Eindhoven University of Technology)

Even if the real-time video and the reference video are recorded under different lighting or weather conditions (or from slightly different angles), recent field tests of the technology have shown that it's able to compensate for such variables, effectively spotting test objects that were placed along a stretch of road.
Van de Wouw is now working with Eindhoven University spinoff company ViNotion, and with the Dutch Ministry of Defense, to further develop the technology.

Greece: Urban terrorist (pipe) IED

Deactivated on-time

December 2019, Athens



Second brother guilty of plane bomb plot

Source: https://www.theflindersnews.com.au/story/6396230/second-brother-guilty-of-plane-bomb-plot/

Sept 2019 – Two Sydney brothers have now been found guilty of plotting to blow up an Etihad plane with a bomb hidden in a meat grinder and to carry out a lethal poisonous gas attack.
The siblings plotted with their older brother, Tarek Khayat, who was involved with Islamic State in Syria, and "the controller", an unidentified person connected with the older brother, according to the prosecutor Lincoln Crowley QC.
Khaled Khayat, 51, was found guilty in May of conspiring, between mid-January and late-July 2017, to prepare or plan a terrorist act, but the NSW Supreme Court jury failed to agree on a verdict for his brother.
Mahmoud Khayat, 34, faced a retrial and another jury found him guilty of the same charge on Thursday afternoon.
Their motivation was said to have included supporting violent jihad and they were accused of doing many preparatory acts during the seven-month conspiracy.

The plane plot involved a bomb in a meat grinder being put into the luggage of a fourth brother, Amer Khayat, who was flying out of Sydney on an Etihad flight, Mr Crowley told the first trial.

But the plan was abandoned because the baggage was found to be overweight at the airport.

Khaled Khayat then proposed that he himself would arrange to take the bomb, Mr Crowley said.

"The controller told him not to do that because he had to stay for the continuation of the work here and had to find someone else," he said.

The second plot involved poisonous gas which the older brother was going to make at his home following instructions given by the controller.

When Khaled Khayat was arrested police found a piece of paper in his wallet that had Arabic words, numbers and symbols written on it.

The paper was examined by a forensic chemist and Arabic interpreters, who determined that one side of the paper included the correct chemical equation for poisonous gas, while the other side had further details relating to the gas.

In his three-day police interview, Khaled Khayat spoke of walking into the airport with the concealed bomb.

He said when he saw children at the airport he thought "Don't do it, don't be stupid, don't do it" and removed the bomb from the baggage.

But his barrister, Richard Pontella, told the jury that contrary to what his client told police, he never took the bomb to the airport and was actually trying to prevent a terrorist attack.

Mahmoud Khayat's barrister, Bruce Warmsley QC, said Khaled Khayat had admitted to police taking the bomb to the airport to put in Amer's luggage.

But his client told police he went to the airport with his two siblings to see one of them off.

"He was not aware one of his brothers was intending to murder the other brother by putting a bomb in his hand luggage," Mr Warmsley said.

Justice Christine Adamson will hear sentencing submissions on a later date.

A few hours before his brother was found guilty in Sydney, Amer Khayat was acquitted by Lebanon's military court, Reuters reports.

It reported Lebanon's state news agency NNA said Amer Khayat would leave Roumieh prison, where he has spent two years and two months, on Thursday night.

The military court also sentenced the three other Khayat brothers - Khaled, Mahmoud and Tareq - in absentia to hard labour for life, NNA said.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C^{2}BRNE DIARY

CYBER NEWS

The Biggest Cyber Attacks of 2019 and What's Ahead for 2020

Source: https://www.globalsign.com/en/blog/2020-predictions/

Nov 18 – This has been another busy year for hackers. In 2019 they successfully attacked major cities, governments, businesses, hospitals, and schools around the world. In the past few weeks alone, the city of Johannesburg, Africa was mulling over whether or not to pay $30,000 in Bitcoin – four coins – to hackers. In the end, the city did not pay, despite the hackers' threat to release citizens' private data.

Let's take a look back at some other big security events this year:

An attack in January was detected which involved two different types of malware – Vidar and Grandcrab – in conjunction with an information-stealing trojan. In this scenario the attacker is usually able to reap some cash, unfortunately.

Then in March, a new strain of ransomware, LockerGoga, infected one of the world's largest aluminum producers, Norsk Hydro. The impact was severe, effectively shutting automation down for days and forcing them to go on manual operation. This led the company to buy hundreds of new computers. In April, the company said it would cost at least $52 million to pay for the damage caused by the attack.

In May, the city of Baltimore was attacked by hackers who froze thousands of city computers and demanded $76,000 in bitcoin as ransom. The city did not pay the ransom. The attack cost the city $18 million and impacted many of their critical systems, including disrupting employees' email service, halting water billing, and even suspending real estate transactions. In addition, in early October, the city signed up for a $20M cyber insurance policy.

During the summer, the state of Texas was significantly impacted by a wave of ransomware attacks that targeted 23 local government entities. The state refused to pay attackers for the August attack, but the entire event still ended up costing at least $12 million.

In early October, it was revealed that numerous hospitals across the state of Arkansas were hit by a massive attack. The attack encrypted files and restricted access to computer systems at DCH Health Systems Regional Medical Center, Northport Medical Center, and Fayette Medical Center. Medical staff was forced to shift to manual mode and rely on paper copies instead of digital records while the IT system was being repaired.

As a result of all this activity and more, the U.S. Department of Defense recently released a highly-anticipated new draft of cybersecurity standards, which tightens the rules that government contractors must abide by for fending off hacks. The DOD is expected to issue its final framework for cybersecurity standards in January, according to FedScoop.

As for what we can expect in 2020, only time will tell. In the meantime, we've asked some of GlobalSign's brightest minds to share their thoughts below.

Lila Kee, GlobalSign General Manager, Americas

#Prediction2020: Increase in private PKI communities of trust

While enterprises and closed communities of interest increase their reliance on PKI for strong authentication of users and devices, expect to see an increase in privately hosted PKIs. Browsers and public root store programs will continue to serve as the foundation for public trust for external facing eCommerce sites (SSL/TLS), executables associated with external applications (code signing), and secure email (S/MIME), where identities are validated through popular email clients, browsers, and operating systems. There will, however, be a swelling requirement for private trust to support traditional and emerging uses around:

- Remote access user authentication
- Device (IoT, mobile, machine) authentication
- DevOps – both SSL and code signing
- Digital signatures associated with consortiums, industries, and governments

The trend toward cloud everything will drive these private PKIs to be hosted by cloud CA providers to provide the security expertise, certificate agility, low investment barrier, and performance needs of these organizations and private communities.

Lancen LaChance, Vice President, IoT Solutions

#Prediction2020: The quantum computing threat is not yet a real risk, so ignore the hype
Companies are increasingly talking about quantum computing, including Google. But the reality is this, while quantum is going to have an impact on our industry, it certainly won't be in 2020, nor will it be for at least a decade. There are still many questions to be answered, such as: What is the best algorithm for quantum resistance? Nobody has that answer and until there is an industry consensus, you're not going to see any quantum solutions in place.
This doesn't mean we're not thinking about quantum computing and what it could mean down the road –we certainly are. But in the meantime, crypto-agility is what we'll be focused on, as it is a much more likely issue in the security industry.

Ted Hebert, Vice President, Marketing

#Prediction2020: A global smart device hack is imminent
There are nearly 30 billion active IoT devices in the world. That's 127 new devices being brought online every second. Expand that to the 2025 prediction of 75 billion active IoT devices, and the question is not *CAN* they be hacked but *WHEN.* That's just too much temptation for the dark lords of the dark web to resist.
Want to hear something else scary? In 2019 Amazon reported 100 million Alexa smart devices had been sold. Just about the same as Google Home. What – not scary enough? Check out these fast facts: It took 13 years for televisions to reach the 50 million mark in the U.S. alone, versus two for smart speakers. It took four years for internet access to reach 50 million, and two years for Facebook.
The numbers bare it out: The world is moving on quickly. Smart devices and social media are intertwined, leaving users, homes, healthcare, financial, manufacturing and other industries vulnerable, hackable and ripe to be taken down and/or held for ransom. While I wish it were not so, the numbers are getting too large to ignore, and the steps manufacturers, companies, and consumers are taking to secure us all are too slow and too few.
Many of these companies are themselves suffering from cybersecurity budget cuts along with cybersecurity staff shortages. GlobalSign has begun working one-on-one with customers to develop not only a PKI plan but IoT plans as well, to help shore up these deficiencies – including an IoT Developer Portal that encourages experimentation, development, and collaboration between developers/DevOps and crypto experts to bring to market the next generation of more secure smart devices, cobots (collaborative robots), and the like.

Nisarg Desai, Director, IoT Solutions

#Prediction2020: IoT is gaining success, but lack of security continues to be problematic
IoT is successful, but quite a few deployments are delayed due to lack of security. In 2020, cloud service providers will be providing or partnering with security companies to provide secure device provisioning and management, as well as a general secure IoT ecosystem, for their customers.
I am also expecting that regulatory frameworks for IoT manufacturing and deployments will continue to be primarily led by the EU, though we will see an increase here in the U.S. as well. In addition, IoT attacks, compromises, and hacks will continue, unfortunately. Add to that, security standards will not be met, nor will we even be close to a higher percentage of devices being secure. Why? Original equipment manufacturers (OEMs) are still not willing to either pay the costs involved or pass them on to consumers, for fear of losing out on sales.
#Prediction2020: Better web applications will lead to higher adoption of DevOps tools
As more capable web applications give rise to more complex service infrastructure, we will see the overall adoption of DevOps tools and practices rise at a strong pace in 2020. This will also open up more threat vectors and we will see more high-profile hacks, vulnerabilities, and compromises in 2020. Security will become an increasing concern for enterprises and some of these will start investing more heavily in a holistic security approach including, but

not limited to, the encryption of all internal and external data in motion and at rest. Data security, compliance, and governance will be big themes, and solution adoption in this space will increase.

Diane Vautier, IoT Marketing Manager

#Prediction2020: Healthcare will continue to be a prime target for cyberattacks

The introduction of IoT connected healthcare devices, and the high value of private electronic medical record (EMR) information, creates a unique and attractive attack surface which makes it absolutely irresistible to hackers. Namely, it's growing and it's lucrative. Researchers and forecasters agree that the healthcare-related IoT will continue to experience rapid growth.

But more devices may lead way to more attacks. According to Health IT Security magazine, "The majority of healthcare organizations, IoT manufacturers, and other organizations that leverage IoT devices have faced a cyberattack focused on IoT within the last 12 months." That includes businesses in Germany, the UK, the U.S., Japan, and China.

These attacks and their costs have everyone on high alert. Medical device manufacturers and health delivery organizations (HDOs) will be looking for ways to reduce the attack surface. They will find relief through traditional PKI-based identity platforms which provide unique device identities to authenticate users, devices, networks, and gateways. By building a network of identity and trust, manufacturers can then enable secure and connected communication.

Patrick Nohe, Senior Product Marketing Manager

#Prediction2020: The internet-wide deprecation of TLS 1.0 and TLS 1.1 will not go as smoothly as hoped

Hopefully this prediction ends up being more along the lines of sounding the alarm bell than a prescient look into the future, but last Spring in a rather unprecedented joint announcement, some of the largest companies leading the internet – Google, Mozilla, Microsoft and Apple – announced they would deprecate support for the now outmoded TLS protocol versions 1.0 and 1.1. Unfortunately, SSL news doesn't really stay around in the headlines long, and there hasn't been a great deal of conversation around the upcoming deprecation since then.

As of the beginning of 2019, around one quarter of the Alexa Top 100,000 didn't support TLS 1.2 yet. But it's a lot bigger than that – web and mobile applications also use SSL/TLS. So, when the deprecation date arrives it's a not a huge leap to assume there will be thousands of broken websites and apps on both desktops and phones. The decision to deprecate older protocol versions is a good one. But as an industry, there seems to be a consistent lack of discussion around upcoming technology shifts and how to make these types of transitions in a smooth and user-friendly way. Hopefully this won't be yet another example of that.

#Prediction2020: More attacks and RSA exploits will be discovered and presented

At this point, the only good argument for continuing to use RSA key exchange with SSL/TLS is interoperability. The ubiquity of the RSA cryptosystem makes it difficult to deprecate. But from a purely best practice standpoint we should all be using an elliptic curve-based approach, meaning ECDHE and ECDSA. The most recent TLS version, TLS 1.3, took the decision out of our hands by eliminating RSA key exchange all together. That's for good reason, too. The cryptosystem is on its last legs. Last year several new attacks against RSA were presented at various security conferences. That comes on top of a fairly extensive list of previous exploits that have already been addressed but may still be exploitable with a little finesse.

On top of that, RSA key sizes make computation expensive and as they scale upwards in size, the increase in security isn't commensurate to the increase in resources used to encrypt and decrypt with them. And perhaps no cryptosystem is more threatened by the (eventual) arrival of quantum computing down the road. If you want to have a discussion about crypto-agility, save the quantum-cryptography stuff for after you've moved away from RSA.

Lea Toms, Marketing Manager, EMEA'

#Prediction2020: Expect to see more biometric data hacks

While hacks involving unencrypted passwords and personal data are devastating news for the people involved, they are fixable, to an extent. In the future, we will hear more news about exposed biometric data and the consequences it has for businesses and people. Once biometric data has been

exposed, there is no way to change it. You can update your password, but not your fingerprint. You can replace your email address, but not your iris. Businesses will have to get ahead of the game and do more to protect the most valuable and personal information there is – biometrics! I expect to see huge record fines for businesses that suffer data exposure of biometric information, and more and more horror stories of people affected by such hacks. It will be increasingly important to protect data with a combination of two or more types of information; with a changeable password or pin in addition to forever biometric information.
As you can see, our predictions span a wide range of topics within cybersecurity, but now we'd love to hear from you. What's on the top of your mind as we enter 2020? Did we miss any major vulnerabilities or risks?

Spookier Than Ghosts: 5 of the Biggest Cyberattacks We Saw in 2019

Source: https://www.vxchnge.com/blog/biggest-cyberattacks-2019

Oct 31 – The days are shorter, and it's impossible to ignore how cold it's getting. Fall is definitely here, and that means it's the spookiest time of year — Halloween.
There's something more frightening than ghosts and ghouls, though — it's the way 2019's cyberattacks showed how easy it is for our data to fall into the wrong hands.

1. The Facebook User Data Leaks

In April, about 540 million records about Facebook users were exposed. They were published on Amazon's cloud computing service by two third-party app developers.
The leak came almost exactly one year after the Cambridge Analytica scandal. It was revealed that the political consulting firm had harvested user data from millions of Facebook profiles without user consent for the purposes of political advertising.
Later in April, Facebook admitted there had been another leak. In this case, however, no hackers were involved. Instead, Facebook had unintentionally made public more than a million user emails.
These two leaks show the scale of information that large corporations like Facebook are working with — and how easy it can be for a simple mistake in data management to turn into a huge privacy issue for millions of people.

2. The Capital One Breach

In March, a hacker — working alone — gained access to Capital One's secure network and more than 100 million customer accounts and credit card applications.
The hacker also accessed more than 100,000 Social Security numbers, 80,000 bank accounts and several addresses, credit scores and balances that Capital One declined to disclose. The infiltrator was considering distributing the Social Security numbers publicly, according to the FBI agent who investigated her.
The hacker was discovered when she posted the stolen information on the software development platform GitHub, along with her full first, middle and last name.
Capital One did note that 99% of Social Security numbers were not compromised. This probably wasn't much comfort to those whose information was accessed by the hacker — especially if they know how easily exposed information and cyberattacks can cause problems with identity theft and other forms of fraud.

3. The Canva Hack

The information of more than 139 million users was exposed in May when a hacker broke into the servers of the graphic design website Canva.
Usernames, passwords and other information — which was encrypted — were accessed by the hacker. Credit card numbers and user designs were not exposed, according to Canva.

4. The Quest Diagnostics Breach

2019 was a record-setting year for health care data breaches. One of the largest was the Quest Diagnostics attack, which saw the information of more than 12 million patients exposed to a user who had unauthorized network access.
The user gained access through the network of a third-party vendor in August of last year, and had maintained access until this March.

According to Quest Diagnostics, the user had access to patients' medical information, certain financial data and some Social Security numbers.

5. The DoorDash Hack

In May, DoorDash confirmed that an unauthorized third party had gained access to data from more than 4.9 million users. Information that was accessed included profile names, email addresses, delivery addresses, order history and phone numbers. Encrypted passwords were also obtained, but wouldn't be decipherable by the third party.

DoorDash also confirmed that the last four digits of some users' credit card numbers were exposed, but that no CVVs or full card numbers were compromised.

It took DoorDash five months to learn about and report the unauthorized access.

The Biggest Cyberattacks of 2019

2019 mostly demonstrated how easy it is for data to become compromised. When companies rely on third parties, they need to make sure their own massive systems are secure while also making sure the businesses they work with are also implementing good security practices.

The different kinds of companies that suffered data breaches also showed the variety of information that can end up in the wrong hands — anything from diagnoses to financial information can be at risk.

Right now, there isn't a great deal consumers' can do except continue to practice good cybersecurity in their own lives, pay attention to the latest news and pressure companies to adopt policies that better defend their data.

START

NATIONAL CONSORTIUM FOR THE STUDY OF TERRORISM AND RESPONSES TO TERRORISM

RESEARCH BRIEF

Significant Multi-Domain Incidents against Critical Infrastructure (SMICI) Dataset

Source: file:///C:/Users/I.Galatas/Desktop/START_UWT_SignificantMultiDomainIncidentsAgainstCriticalInfrastructure_Dec2019.pdf

HI - I NEED YOUR HELP, QUICK. I AM AT THE AIRPORT AND MY PHONE'S BATTERY IS JUST ABOUT TO GO FLAT...
I NEED YOU TO GIVE ME THE EMAIL ADDRESS FOR...
SLANE co.nz

It's ok to hang up on social engineers.

ICI International CBRNE INSTITUTE

CBRNE-Terrorism Newsletter

C2BRNE DIARY

DRONE NEWS

What Can Drones Do to Protect Civilians in Armed Conflict?

Source: http://www.homelandsecuritynewswire.com/dr20191211-what-can-drones-do-to-protect-civilians-in-armed-conflict

Dec 11 – Drones are usually in the news for bad reasons, like controversial killings of suspected terrorists in the Middle East, bombings of Saudi oil facilities or an assassination attempt on Venezuelan President Nicolas Maduro.
Michael Yekple writes in *The Conversation* that what many people may not know is that United Nations peacekeepers use drones to protect civilians from violence. These drones are different: They don't carry weapons.
He writes:

> *I have followed the U.N.'s use of drones since its beginning in 2013 and have spoken with peacekeepers and U.N. officers who are familiar with their use. I believe drones have the potential to save lives.*
> *But that doesn't mean they necessarily will.*

There are many problems associated with using drones in peace-keeping missions, but Yekple writes:

> *All these problems don't mean drones are useless at protecting civilians. For instance, U.N. drones discovered armed groups smuggling gold believed to be providing funding for the armed groups and their activities. That was news to the U.N., and authorities stopped the smuggling. Drones also helped save 14 people in Democratic Republic of Congo after their boat capsized.*
> *I believe these efforts and others aimed at preventing violence could be more effective with more support from U.N. member nations. In recent years, though, wealthy countries have slashed their contributions to the U.N. peacekeeping budget and reduced the number of soldiers they'll send on missions. That has left peacekeeping missions to do their work with ill-equipped, poorly trained soldiers from poor nations.*

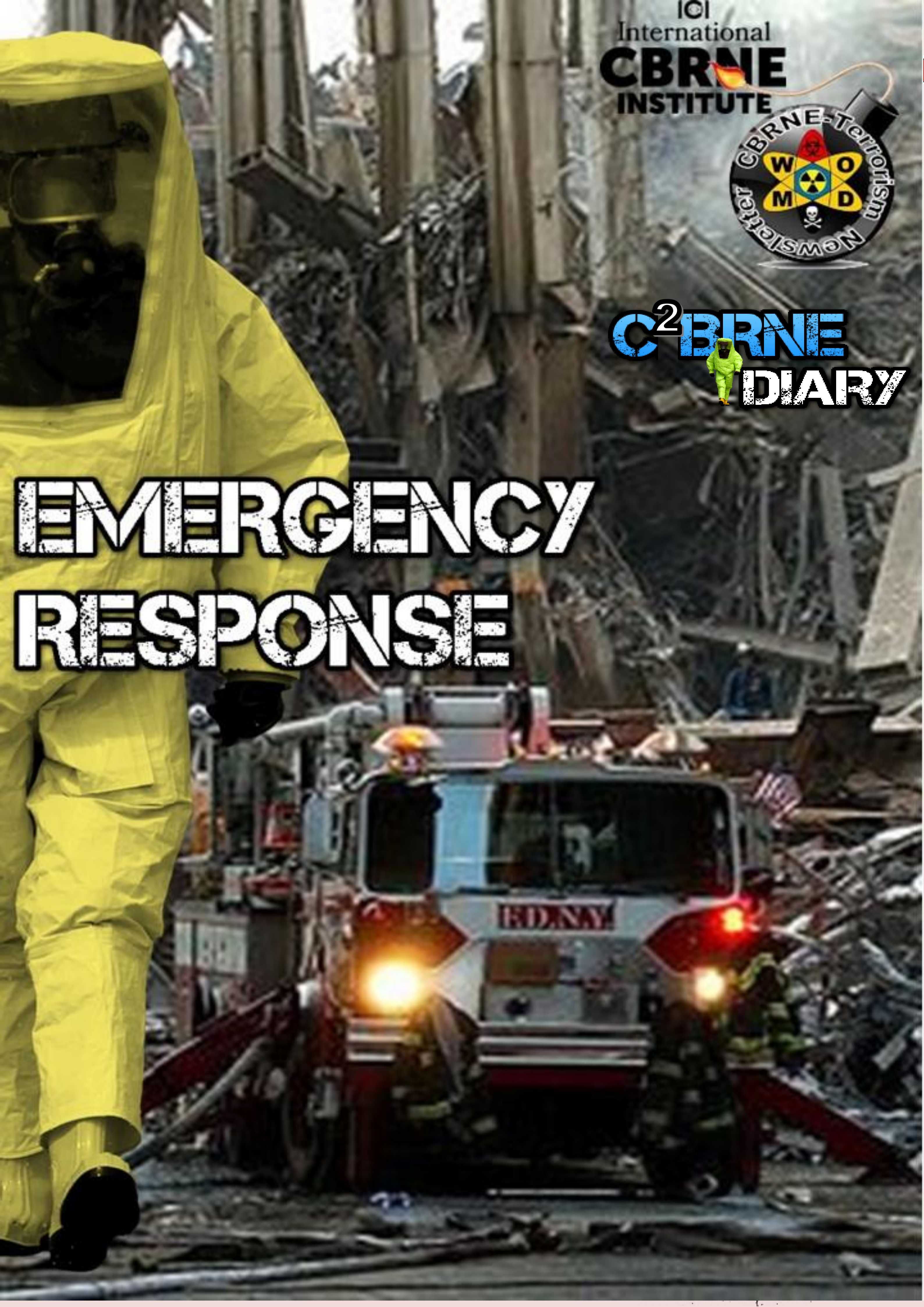
China flight systems jammed by pig farm's African swine fever defences

Source: https://www.scmp.com/news/china/society/article/3042991/china-flight-systems-jammed-pig-farms-african-swine-fever

Dec 21 – **A Chinese pig farm's attempt to ward off drones – said to be spreading African swine fever – jammed the navigation systems of a number of planes flying overhead.**
The farm, in northeastern China, was ordered last month to turn in an unauthorised anti-drone device installed to prevent criminal gangs dropping items infected with the disease, according to online news portal Thepaper.cn.
The device came to light after a series of flights to and from Harbin airport complained about losing GPS signals while flying over Zhaozhou county in Heilongjiang in late October. In some cases, the ADS-B tracking technology – which determines an aircraft's position via satellite navigation – failed.
A check on radio blockers in the area identified the farm and its owner, Heilongjiang Dabeinong Agriculture & Pastoral Foods, was ordered to turn in the equipment. No further punishment was imposed, Thepaper.cn reported. The company declined a request for comment.

⚠ **Chinese state media reported last week that gangs were exploiting the African swine fever crisis by deliberately spreading the disease by using drones to drop infected items on to pig farms.** The farmers are then forced to sell meat cheaply to the gangs, who then sell it on as healthy stock, according to *China Comment* magazine, which is affiliated to state news agency Xinhua.

In more common cases, according to the magazine, the criminals spread rumours about the presence of the virus to achieve a cheap purchase price.
Pork prices have more than doubled in China as millions of pigs have been slaughtered since the first case of African swine fever was identified in Shenyang in August last year. The disease is fatal to pigs but does not pose a threat to humans.



EMERGENCY RESPONSE

2019 National Preparedness Report

December 09, 2019

The National Preparedness Report evaluates annual preparedness progress and challenges facing the whole community. The 2019 National Preparedness Report highlights the diverse range of preparedness challenges the Nation faces—from terrorism and active shooter incidents, to cyberattacks, to natural disasters, as well as how stakeholders across the nation are using preparedness grant funding to invest in preparedness improvements.

View Full Report

A Guide to Critical Infrastructure Security and Resilience

December 05, 2019

The U.S. Department of State and the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) developed this guide to serve as an overview of the U.S. all-hazards approach to critical infrastructure security and resilience. It is intended for both domestic and international partners.

View Full Report

Preparing Children with Special Healthcare Needs for an Emergency

By Holly Gay

Source: https://www.domesticpreparedness.com/updates/preparing-children-with-special-healthcare-needs-for-an-emergency/

Dec 08 – In my home both of my children have special health care needs. My daughter Charlotte is 4 years-old, and my son, Zachary, is 2 years-old. Both were diagnosed with asthma at an early age. Having children with special health care needs means that my husband and I must think ahead, plan ahead, and prepare our children for an emergency where we may not be with them, or where we may not have access to the comforts of home and the routine we are used to. Below are tips on preparing your family for an emergency, and how that emergency may impact transportation and reunification.

Preparation

First and foremost, establish a personal support network or self-help team that is familiar with your child's special healthcare needs, and available to help before, during, and after an emergency. Work with your team to identify the 7 key areas of support:

1. Make arrangements prior to an emergency for your team to immediately check-in with you when disaster strikes.
2. Exchange important keys or codes, such as, house keys, car keys, and garage door codes.
3. Show them where you keep emergency supplies.
4. Share copies of your emergency documents, evacuation plans and emergency health information card.
5. Review and practice ways for contacting each other in an emergency.
6. Notify your team when you have plans to travel, and make sure they know when you will return.
7. Learn about each other's needs and how you can help before, during and after an emergency.

In order to prepare your family and your team ahead of time, make sure you create an emergency care plan that considers the special needs of your child. For example, if your child has specific dietary needs or mobility limitations, make sure that your emergency plan has information on the kinds of food to avoid or a list of items that your child may need for his or her assistant devices (ex. Spare battery for an electric chair). It might also be helpful to create a kit or go-bag that has necessary back-up battery supplies, special non-perishable foods and special medicines. For example, if your child has asthma, make sure you have an adequate supply of asthma medications such as albuterol. You may also need to consider having spare albuterol inhalers at school and at home in case there's an emergency.

Work with your healthcare provider and your child's school to make sure they are aware of your child's needs and have plans in place to accommodate those needs in case of an emergency. The American College of Emergency Physicians and the American Academy of Pediatrics developed an Emergency Information Form to help emergency care professionals and healthcare providers give appropriate care for children with special healthcare needs during an emergency.

Transportation

Each emergency is different and may require different actions to keep your family safe. Depending on the emergency, authorities may ask you to stay where you are by sheltering in place, or they may recommend that you evacuate.

The American Academy of Pediatrics advises that children with special health care needs need to have access to safe transportation, specifically family vehicles and school buses that are specific to their needs.

In order to do this, families, healthcare professionals, and school administrators need to be aware of the current guidelines for properly securing and transporting children of different ages, and with different physical and mental abilities.

Families and caretakers of children with special health care needs need to avoid using makeshift restraint systems or products that are not suitable to the child being transported.

When transporting a child with special healthcare needs, please consider the following:

1. Place the child in the back seat of a motor vehicle.
2. For a child who requires observation during travel, and for whom an adult is not available to ride in the back seat with, an air bag on/off switch may be considered for the vehicle.
3. Follow all instructions by the manufacturer of the vehicle, and safety seat.
4. Children with a medical problem should have a special care plan that details how to transport them during an emergency.
5. Families of children with special healthcare needs need to properly install appropriate restraint systems in family vehicles and know how to use them.
6. Parents, healthcare professionals, and educators should consider a child's transportation needs and incorporate those needs into the child's Individual Education Plan (IEP).

Reunification

Each day, 69 million children in the United States attend childcare or school. As a caregiver you can protect your children by knowing their school or childcare center's emergency plan.

If an emergency occurs during the school day, school authorities will activate their emergency action plan, which may include evacuating the children off site to a safer place or emergency shelter.

In situations such as this, wait until emergency or school authorities say it is safe for you to pick up your child. Do not go to your child's childcare center or school during an emergency, doing so can put you and your child at greater risk. Instead, take steps now to help with reunification:

- On an annual basis, make sure that your child's school has up-to-date emergency contact information for your child. Be sure to notify the school every time your address or phone number changes.
- Get a copy of your child's school or child care center emergency plan. These will explain their evacuation plans, how the facility will contact you, and how you will be reunited with your child during or after an emergency.
- Send your child to school with an updated backpack emergency card. It's an easy way to share emergency contact information and can help when there is a communication barrier. Also, if your child is able, teach them how to call 9-1-1 and memorize important phone numbers.
- Create reunification and communication plans that cater to your child's special and specific needs. This may involve establishing non-verbal cues that will allow a child to communicate their needs to a trusted adult or peer.
- Reviewing and practicing your plan with your team and family before an emergency will also help you recognize what might be missing from your plan.

The U.S. Department of Education's Office of Safe and Supportive Schools (OSSS) and its Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center offers a variety of resources on the topics of reunification, access, and functional needs via web pages hosted on their website. Each page offers resources from the REMS TA Center and other national and Federal partners, including CDC that can support planning around these topics before, during, and after emergencies.

Crisis Architecture: Building to Defend against Active Aggressors

Source: http://www.homelandsecuritynewswire.com/dr20191203-crisis-architecture-building-to-defend-against-active-aggressors

Dec 03 - A study of mass shootings in the United States shows that a consistent feature of these attacks is that they are over quickly. Daveed Gartenstein-Ross and Tadd Lahnert write in *War on the Rocks* that at Sandy Hook a single shooter killed 26 children and adults in ten minutes. In the 2016 terrorist attack at the Pulse nightclub in Orlando, Florida, a gunman killed 49 people in nine minutes. Not counting the 2017 Las Vegas shooting because it occurred outdoors, the U.S. remaining five deadliest active aggressor events (that is, incidents in which an individual is actively trying to kill people in a confined or populated area) left 154 people dead in a 49-minute span. "The average time between an attacker entering a structure and the end of the shooting was a mere 9 minutes and 48 seconds," they write, adding:

> *When so much blood is spilled so quickly, every tool should be brought to bear. Communities should look beyond rapid police response or individual heroics to maximize survivability; their efforts should include the design of the structure where an attack may occur. This article introduces an architectural paradigm we call crisis architecture, which one of this article's authors has been developing over the past four years. It incorporates integrated tactical, psychological, and technological security measures, while preserving the function and aesthetics of buildings to which these measures are applied. The focus of this paradigm is designing the built environment in a way that increases the likelihood that individuals will survive an active aggressor incident.*

They conclude:

> *There is a long history of using design to address social problems, and today's challenges require this practice to evolve yet again. The crisis architecture paradigm can mitigate the effects of active aggressor attacks that result in mass casualties…. While crisis architecture is not a panacea for casualties in active aggressor attacks, we believe that it is an unfortunately necessary measure at a time when a lack of comprehensive solutions ensure that these attacks will continue.*

LET'S SEE... AH! HERE IT IS: "YOUR POLICY DOES NOT COVER FLOODS, EARTHQUAKES OR AXE OF GOD." SORRY ABOUT THAT, MR. FINKLEMAN.
SCOTT HILBURN 10/4
CARTOONSTOCK .com
Search ID: shl111004
© Scott Hillburn /Distributed by Universal Uclick via CartoonStock.com

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

Climate Change Is Altering Migration Patterns Regionally and Globally

By Jayla Lundstrom

Source: https://www.americanprogress.org/issues/immigration/news/2019/12/03/478014/climate-change-altering-migration-patterns-regionally-globally/

Dec 03 - At least 2014, a growing number of asylum-seekers from Central America have arrived at the U.S.-Mexico border. While the response from the Obama administration raised genuine protection concerns, the Trump administration has taken the draconian and unwelcoming approach of dismantling the U.S. asylum system by restricting grounds for asylum, separating families, and illegally blocking access to ports of entry. The current administration has also adopted the "Remain in Mexico" policy and so-called safe third country agreements, which forces asylum-seekers to remain in dangerous situations.

Many individuals coming to the United States from Central America are fleeing violence, poverty, and corruption. But climate change is emerging as both a direct and an indirect driver of migration that complicates existing vulnerabilities. Persistent drought, fluctuating temperatures, and unpredictable rainfall have reduced crop yields throughout the Northern Triangle—a region that comprises El Salvador, Honduras, and Guatemala—challenging livelihoods and access to food in agriculturally dependent communities. By denying the reality of climate change and taking a hard-line approach to migration, the Trump administration has shown its unwillingness to address the root causes of migration in the Americas.

A lack of a legal framework for environment and climate-induced migration

There is currently no international legal framework to address environmental disasters and climate change as drivers of migration. There is also no consensus on what terminology should be used to describe individuals moving due to environmental factors. The 1951 Refugee Convention and 1967 Refugee Protocol, multilateral agreements that define "refugee" and set states' obligations for protection, were not crafted with the environment, climate change, or environmental disasters in mind—and therefore do not mention them as grounds for refugee protection. U.S. refugee policy, codified in the Refugee Act of 1980, is largely based on the framework outlined in these agreements and thus excludes these terms.

The current multilateral agreements and definition of a refugee have provided crucial protections for individuals fleeing life-threatening situations. However, it has been nearly 40 years since these definitions have been updated, and circumstances globally have since changed. Notably, climate change and increased environmental disasters are now influencing migration.

The International Organization for Migration, along with the U.N. High Commissioner for Refugees and the World Bank, advocate the explicit use of "climate migrant"—instead of "climate or environmental refugee"—when referring to this migration, as designating someone as a "refugee" has legal ramifications. The use of "migrant" avoids the tricky issues that would arise if the United Nations were to reopen the technical definition of a "refugee," as set out by the 1951 and 1967 agreements. In today's climate, such an effort could result in a watered-down definition of what it means to be a refugee rather than a more robust definition appropriate to the global challenges of today and of the years ahead.

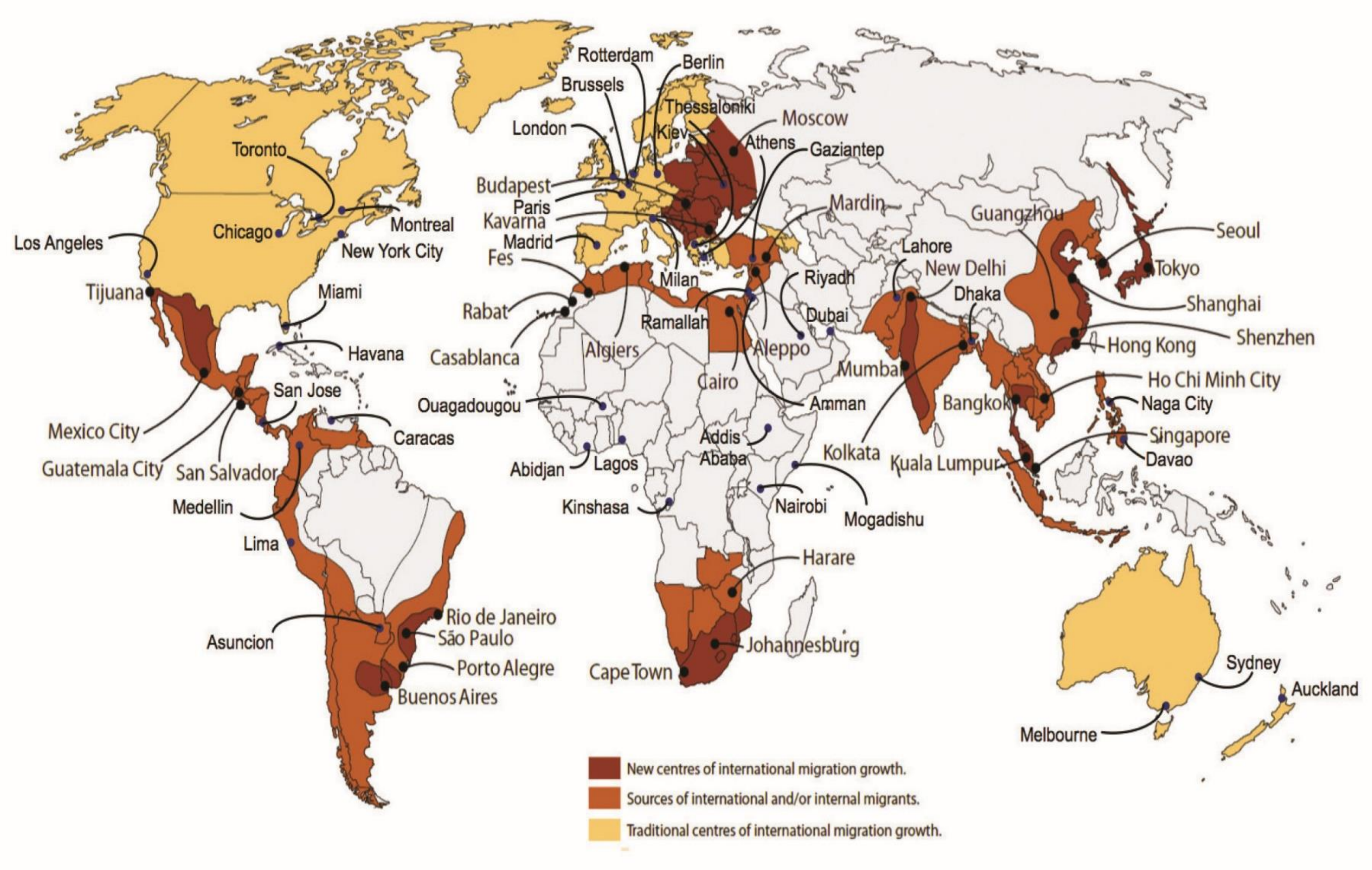
Additionally, migration is multicausal, and it is likely that the most vulnerable people would not be able to prove climate and environmental factors as the sole reason migration is necessary—something that could be required if climate change and environmental disasters are incorporated into existing agreements. Climate change outcomes are more abstract than poverty and malnutrition, for example, and economic insecurity is not considered a valid reason to grant someone asylum and refugee protections under current legal frameworks. But the need to protect individuals facing these circumstances is urgent.

The different types of climate-related migration

Different environmental events prompt different migration trends. Migration driven by sudden-onset disasters, such as typhoons, hurricanes, wildfires, and landslides, is often an immediate survival response. In most cases, those fleeing remain within the borders of a nation, and international refugee law does not consider internally displaced people as refugees. However, as climate change continues, these disasters will become more frequent and intense—forcing greater numbers of individuals to flee both internally and across borders.

Climate change is also increasing the likelihood and impacts of slow-onset disasters and environmental degradation, such as droughts, desertification, sea level rise, and rain pattern shifts. With more drawn-out consequences, these events can result in long-term, mass migration over international borders. Decisions to migrate due to slow-onset disasters are influenced by preexisting socio-economic, demographic, and political factors. People who are wealthy, educated, or otherwise privileged are more likely to have the resources required to either adapt to the changing environment or leave. Meanwhile, marginalized communities who are most vulnerable are likely to remain trapped.

Although a universal agreement on terminology is important to give recognition to climate-related migration and work toward some legal framework, getting lost in the legality and semantics of the situation quickly removes the humanity from the issue. What is evident is that the global community is ill-prepared to deal with environment and climate-induced migration in a compassionate and just manner.



Climate-change induced migration in the Northern Triangle

This link between climate change and migration is apparent at the U.S.-Mexico border, where individuals arriving from the Northern Triangle are naming crop failure and food insecurity as a growing driver of migration. Fluctuating temperatures and unpredictable rainfall throughout the Northern Triangle have destroyed crops and livelihoods, making food insecurity increasingly acute and driving migration. Climate change disproportionally affects indigenous communities who engage in traditional agricultural activities and who have long faced persecution and discrimination. This is the case in the Western Highlands of Guatemala, where years of climate-related drought have threatened the income and food security of subsistence farmers, contributing to increased poverty and chronic malnutrition rates—as high as 79 percent and 58 percent, respectively—for indigenous peoples. Vacant homes and dried-up crops are scattered throughout the region, providing physical proof of how climate change complicates social and economic conditions and triggers the need to move.

In addition to causing the failure of basic grains, warming temperatures and fluctuating rainfall patterns are also a culprit of coffee rust—a fungus that has wiped out coffee crops throughout the Northern Triangle. The crop is extremely sensitive to temperature variations, and, as drastic shifts in temperature become more frequent, coffee farmers who once had stable incomes are being forced across borders.

An internal U.S. Customs and Border Protection report found that crop shortages, poverty, and food insecurity were among the conditions pushing people to leave the region. However, for several months, the Trump administration froze U.S. aid that was directed at mitigating the effects of climate change in the Northern Triangle, once again working against any efforts to understand and manage migration responsibly and effectively.

Recognizing climate-related migration

First and foremost, the federal government needs to recognize that climate change is happening and that it affects vulnerable communities, requiring ambitious and comprehensive climate solutions. Migration must also be accepted as an understandable and viable adaptation strategy to environmental and climate change that can empower and protect individuals and communities as well as reduce stress on fragile environments. Overall, resources and pathways need to be in place on regional and international levels to support individuals' right to choose to remain in their community or to move if it becomes necessary.

Legislation has been introduced in the U.S. House and Senate that would create a humanitarian program to provide protections to migrants fleeing environmental and climate disasters. The proposed bills would require the White House to collect data on individuals displaced by climate change and report findings to Congress and the secretary of state, in coordination with the U.S. Agency for International Development, to create a "Global Climate Resilience Strategy." The bills are a significant step in bringing domestic awareness to the issue, and although they are unlikely to pass under the current administration, they set a needed precedent for future actions.

More so, the United States must return to climate leadership at home, regionally, and globally. Policymakers should consider increasing aid directed at mitigating the severe impacts of climate change on the livelihoods of individuals throughout the Northern Triangle.

As climate change continues to increase the likelihood and intensity of environmental disasters and degradation, more and more people will be forced to leave their homes. The factors that drive migration are inextricably linked, and environmental phenomena will only exacerbate economic and social instability. Greater recognition and acceptance of the issue on a domestic and global scale is only the beginning. Policies need to work to address climate change, mitigate its impacts, and provide protections to those affected.

***Jayla Lundstrom** is an intern with the Immigration Policy team at the Center for American Progress.*